

Issues of Establishing of the International Legal Regulation System to Combat Cybercrimes

Viktor Shestak¹^a and Artur Adigamov¹^b

¹*Moscow State University of International Relations (MGIMO University), Moscow, Russia*

Keywords: Criminal law, cybercrimes, cyber threats, international regulation, Internet.


Abstract: Relevance of studying issues of establishing of the international legal regulation system in the digital space is related to the division of the world into different socio-political systems, unions of states, controversies between world powers. In this regard in the article is analyzed present international legal basis of combating cybercrimes and regulation of cyberspace. The main aim of the study is the evaluation of the level of legal regulation adequacy at the level of international organizations, unions of states, issues, which are caused by proliferation of cybercrimes in the world, new challenges, which are connected with the use of cyberweapons in international conflicts between states, evaluation of the role of the UN in searching of main directions of cybersphere regulation. Objects of the research are analysis from the historical perspective of the actions of the UN in the sphere of cyberspace regulation, ccoordination of cybercrimes control at the level of UN decisions, identification of the most effective forms of international legal regulation of cybercrimes control at the level of unions of states. The conducted research on the basis of dialectical methods of learning of social processes, which are related to the use of the cyberspace in the modern world, allowed to determine main directions for the UN actions from the point of finding of compromise solutions, which can create unified international mechanism of legal regulation of processes in the digital sphere. Experience of the EU is a successful example of legal regulation at the level of unions of states on the basis of harmonization of international law in the sphere of cybercrimes combating. Studying of experience of other unions in this sphere allowed to draw conclusions of inefficiency of legal regulation at the level of certain unions, which don't have such a high level of integration as EU has. Significance of the objectives in the research is determined by the fact that in the article issues of international legal regulation of cybercrimes control are firstly studied at the level of certain states and at the level of harmonization of criminal law for the purpose of international unions and unions of certain groups of states.


1 INTRODUCTION

Scale of computer technologies implementation almost in all spheres of human life are so huge that without them it is impossible to imagine functioning of the modern world. Possibilities, which emerge in the use of digital technologies make them at the same time quite attractive to the criminal world and persons, who prone to commit crimes. Countermeasures against use of digital technologies for criminal purposes are related to legal countermeasures, which are aimed against imperfection of law in this sphere at the international and national level. The main issues of legal regulation of cybercrimes control is its transborder nature, easy

and fast commission of such crimes in contrast to traditional crimes.

Crimes, which are committed in cyberspace are defined different by the researchers (Nomokonov V., 2012): cybercrimes; computer crimes; crimes in the sphere of digital data; digital crimes; crimes in the digital space, which are modulated by computers. (Fedorov F., 2006); crimes differing by their character (Baturin Yu., 1991). Modern Russian criminal law uses term «crimes in the sphere of computer data», which according to our point of view restricts opportunities of the enforcers in the sphere of qualification of socially dangerous, guilty, illegal acts, which are committed in the cyberspace by the persons, who have attained age of criminal liability.

^a <https://orcid.org/0000-0003-0903-8577>

^b <https://orcid.org/0000-0002-1087-7274>

The situation is also complicated by terminological controversy, which emerges due to lack of accounting of new phenomena related to computer technologies. Generally accepted and new technological terms as site, hosting, provider of hosting, search engine etc. are being legally implemented and without them criminal qualification of committed crimes is impossible. (Federal Law No. 149-FZ, 2006).

We consider cybercrime as set of crimes, which are committed in the cybersphere by or with computer systems and nets and also against computer systems, computer nets and digital data (Tropina T., 2005; Chekunov I., 2013). Also we should take into account that cybercrimes –is the consequence of globalization of telecommunication technologies and emergence of international communication nets.

In this study is examined legal practice of the UN, which has been trying to coordinate efforts of certain states as the USA and the Russian Federation for a long time, in the sphere of creation of general, uniform regulation of digital space. As a successful means of legal regulation at the level of unions of states on the basis of harmonization of national law against cybercrimes is studied experience of the EU, CIS and also it this paper are analyzed directions of actions in the sphere of cybercrimes countering.

2 METHODS AND MATERIALS

Methodological basis of the research of international legal experience of cybercrime control is dialectical method of social processes and phenomena examining, which are connected with the emergence, proliferation and turning into global problem international crime, which is related to computerization of economy, social life, emergence of internet and social nets. This helped to receive and summarize objective information about proliferation of cybercrimes, which are of transborder nature in modern circumstances, to determine legal methods and tools, which are related to criminalization of acts committed in the cyberspace, to recognize patterns of international cooperation as the main condition of effectiveness of penal legal countermeasures against cybercrimes. Received information was construed taking into account aims and objectives of the research, requirements of validity and credibility. System analysis was used in the studying of certain international legal acts, which were adopted at the level of the UN, Council of Europe Conventions, Agreements of CIS and other regional legal acts. The use of theoretical provisions of criminalistic, criminology, penal and penal procedure law

predetermined scientific validity, representativeness of digital data in the basis of conclusions.

As materials of the research have been used papers of Russian and foreign researchers, who specialize in scientific directions related to international legal regulation of the digital space and computer crimes control, criminal legal regulation of acts committed in the cyberspace at the level of national law. Documents devoted to different aspects of digital space regulation, countermeasures against cybercrimes adopted under UN auspices, international regional legal acts and statistics (Series of university modules, 2020).

3 DISCUSSION AND RESULTS

Creation and production of electronic computers marked new a new stage of development of international economy – transition from mechanical to computer processing of data.

The use of computers, which allowed to process large amounts of economic data also increased the risk of manipulation of such databases for criminal purposes – by falsification, theft of computer data, which contains trade secrets. The lack of defense of digital data processing programs allowed dishonest users use flows of social-economic information for the commission of crimes. (Liu, Z. et al, 2020).

However prior to the emergence of computer nets, which had globally formed by telecommunication technologies the world net – Internet, crimes with the use of electronic computers had been committed at the local level – in certain companies, states, this means they had not been of transborder nature and had not been so proliferated in the economic life and in the criminal world. (Gura D. Et al, 2020).

In the age of internet digital computer technologies even in the early 21st century have started to turn into global system of communication of the human society. Its' feature is the idea of free transmission of data between receiving, broadcasting and transmitting persons through arbitrary ways by specially created joints on the basis of self-regulation and decentralization model (Stepenko V., 2021).

In the ensuring of internet functioning the main role plays security of its use and countermeasures against the use of the Internet for illegal purposes. This is related to the fact that with the development of new communication technologies have emerged new threats of global, regional and national nature. With the use of cybertechnologies emerges intergovernmental confrontation in the cybersphere – cyberwars, emerge new terroristic unions, which use

internet for cyberattacks, international and national criminal groups and individuals, who use computer technologies more often for the commission of crimes. Particular concern of the international community causes the use of cyber technologies and devices for the destabilization of international relationships, undermining security of certain states. At the end of the 20th century and in the early 21st century were realized a number of initiatives aimed at the creation of international legal security mechanism against the threat of misuse of cyber technologies in the digital space. The proponent of the use of UN authority for the digital security problem solving in the circumstances of comprehensive development of new digital technologies was the Russian Federation. In 1998 the Russian Federation prepared and submitted to the UN General Assembly draft resolution, which raised the problem of security of states related to possible misuse of achievements in the sphere of digitalization and telecommunication.

This document, which was adopted as UN resolution on 4th December 1998 included recommendations about creation at the level of international community general principles to combat new threats and challenges in the digital sphere. Further development of this direction of international security regulation in the sphere of digital technologies became resolution A/RES/54/49 1999, which admitted reality of possible use of new digital technologies for causing damage to states in civil and military areas (Broadhurst, 2006).

The next stage of the development of international efforts to create comprehensive international system of digital security should be considered the year 2009. In 2009 was created the new group of governmental experts of the UN about issues of studying new threats in the information and communication technologies sphere, which managed to submit the final report to the General Secretary of the UN on the basis of compromises on controversial issues.

In 2013 was prepared the new report of the group of governmental experts, whose main objective was to determine directions of states cooperation in order to create and to strengthen safe digital space. Taking into account recommendations of the group of governmental experts in December 2013 was adopted new UN Resolution A/RES/68/243, which created the new group of governmental experts in the number of 20 representatives of states. In the developed report of this group were underlined studying of issues of possibility of the use of international legal provisions for such sphere as information and communication technologies.

In 2015 during the 70th session of the UN General Assembly on the initiative of 84 UN member-states was created a new group of 25 governmental experts. The main aim of this groups as believed Secretary of the Security Council of the Russian Federation N.P. Patrushev, was to elaborate «universal provisions of responsible behavior of states in the digital sphere and adoption of such provisions under UN auspices, (Patrushev, 2020).

In all reports of the group of governmental experts, which were supported by the majority of states, are underlined base principles of organization of safe, peaceful, free from threats digital space. To the are related firstly such principles as the use of information and communication technologies only for peaceful purposes, purposes of prevention of conflicts in the digital sphere with the use of information and communication technologies. In 2018 UN General Assembly adopted proposed by the Russian Federation draft resolution «Developments in the field of information and telecommunications in the context of international security». This resolution was supported by 119 states.

In 2019 the Russian Federation submitted to the UN General Assembly resolution about the necessity of elaboration of the new Convention about cybercrimes control. As mention special representative of the President of the Russian Federation Andrey Krutskih, the idea of the resolution «is to fight this evil together, which causes huge, trillion damage to the world economy and individuals (UN General Assembly, 2020).

The problems of cybercrimes at the level of UN have been also discussed at the level of UN congresses. So, at the X UN Congress in 2000 in Vienna was adopted resolution «Vienna Declaration on Crime and Justice: Meeting the Challenges of the 21st Century». In this declaration was stated the taking the decision on elaboration of recommendations about crimes prevention, related to the use of computers and combating such acts, «and strengthening of opportunities about prevention, investigation and prosecution of crimes with the use of high technologies and computers».

At the 12th Congress of the UN was created special intergovernmental group of experts, and their main objective were defined as research of cybercrimes problems and elaboration of countermeasures at the level of states against crimes in this sphere.

At the 13th UN Congress in Doha 2015 in the paragraph b pf the Declaration was paid special attention to the role of the UN in the creation of

sustainable and secure cyberspace, prevention of crimes with the use of Internet (Tarasov, 2019).

Analysis of documents adopted at the level of the General Assembly of the United Nations at the congresses shows that issues of cybersecurity at the international arena became one of aspects of political struggle of the USA and the Russian Federation.

We consider that the main condition of effective countering of cybercrimes at the international level is development at the UN level of international Convention on struggle against cybercrimes on the basis of the adopted Resolution of the UN General Assembly proposed by the Russian Federation on 28 December 2019.

When considering problems of creation of the international legal security system, it turns out that on the European Continent haven been conducted first efforts of international legal regulation of countering cybercrimes.

So, the OECD in 80s has started to create legal mechanism of countering the use of electronic computers for criminal purposes.

In the Council of Europe issues of cybercrimes have been firstly considered in 1983. Such document became Recommendation № R89 of the Council of ministers, member-states of the Council of Europe.

The first union of states, which implemented into its program documents issues of computer security of member-states was the European Union. The main international legal act regulating at the supranational level of countering cybercrimes in the EU became European Convention on cybercrimes adopted in Budapest in 2001. 47 states signed it – all members of the European Union, certain states of the Council of Europe, Japan, Canada, South Africa, USA.

Convention determines provisions about liability for cybercrimes, which shall be implemented into the national law of member-states.

Further harmonization of criminal law of EU member-states was conducted on the basis of the Lisbon Treaty.

Over the past years after the adoption of the Convention, the European Union could create harmonized legal basis, establishing at the national level liability for crimes in the cybersphere, creating for this system of generally accepted principles of countering cybercrimes, which can regulate criminal law and also criminal procedure. [9].

This historical experience is an example for the creation of legal system of regional cybersecurity for the other states (MacDonald, 2014).

Issues of legal regulation of countering cybercrimes are thoroughly considered at the level of the CIS. In 1999 was adopted model law on

information exchange, which reveals main terms related to information and communication technologies and digital security.

One of the most crucial documents of the CIS in this sphere is the agreement of member-states on cooperation in the sphere of realization and creation of information resources and systems, adopted in 1999. In 2001 Agreement was devoted to the cybercrimes countering (Menthe, 2020).

Another union of states is Shanghai Cooperation Organization in 2006 made a statement expressing concern of member-states about possible use of cybertechnologies for criminal purposes.

Created by the SCO group of intergovernmental experts prepared adopted in 2009 Agreement between SCO member-states on international data security. This agreement is one of the first agreement in the international practice, which providing terminological, conceptual framework for such terms as information weapons, information war, information terrorism, reveals terms related to cyber threats, determines main directions, principles of cooperation in the area of digital security (MacLean, 2004; Major, 2015).

In 2015 the SCO submitted as an official document to the UN «Rules of behavior in the international data security».

Another important international document in the sphere of prevention and countering of cybercrimes is the Convention of the League of Arab States on the countering of crimes in the sphere of information technologies 2010. The main aim of this Convention is coordination of cooperation between member-states in the sphere of cybercrimes countering. (Hakmeh, 2018).

4 CONCLUSIONS

The analysis of the historical aspect of the creation of the legal system of countering cybercrimes shows that solving of problems in the sphere of harmonization of national law about countering cybercrimes is depends on international and regional acts against cybercrimes. In the XXI century work on elaboration and adoption of international legal acts has intensified (Kshetri, 2019).

Currently the main subject at the level of the UN nations in the sphere of creation of international legal mechanism of combating crimes in the digital sphere is the Russian Federation, which has been proposing for 20 years initiatives on coordination of efforts of all states of the world in the aspect of countering the

use of developments in the sphere of informatization and telecommunication for criminal purposes.

Regularly adopted Resolutions of the UN General Assembly about issues of the use of international law in the sphere of cybercrimes, including the use of cybertechnologies in military areas are supported by the majority of the UN member-states. At the same time there is a group of states including the UN states, which don't support Russian initiatives in this sphere. It is generally explained reluctance of the United States to transfer to the international responsibility coordination of the Internet, including creation at the international level of the Internet security system.

The non-regulation at the international level of the issues of cyberattacks and cyberwars between states is the matter of concern. The lack of criteria of evaluation of work of international authorities in the cybersphere allows on the one hand to conduct unpunished, non-condemned at the level of international documents cyberattacks in the digital sphere, and on the other hand such actions without possibility of international legal regulation at the UN level lead to escalation of intergovernmental conflicts.

REFERENCES

- Federal law, 2006. 149. On information, information technologies and data security. <http://www.consultant.ru>.
- University modules on cybercrimes. <https://www.unodc.org>.
- Secretary of the Security Council of the Russian Federation N.P. Patrushev. VII Meeting of high representatives dealing with issues of security. <http://www.scrf.gov.ru>.
- General Assembly of the UN adopted the resolution of the Russian Federation on the development of the Convention to combat cybercrimes. <https://tass.ru>.
- Liu, Z., et al, 2020. Issues of crowdsourcing and mobile app development through the intellectual property protection of third parties. *In Peer-to-Peer Netw. Appl.*
- Gura, D., Khudyakova, N., et al, 2020. Chatbot design issues: building intelligence with the Cartesian paradigm. *In Evol. Intel.*
- Stepenko, V., Dreval, L., et al, 2021. EU Personal Data Protection Standards and Regulatory Framework. *In Journal of Applied Security Research.*
- Broadhurst, R., 2006. Developments in the global law enforcement of cyber-crime. *In Policing An International Journal of Police Strategies and Management.* p. 29.
- Tarasov, A., 2019. The Okinawa Charter and the Congress of the United Nations: cybercrime countering issues. *In Information Technology Security.* 26. pp. 120-131.
- Moroz, N. O., 2018. Features of international legal cooperation in the fight against cybercrime within the EU. *In Bulletin of the Mari State University. Series "Historical Sciences. Legal Sciences".* 4(16). pp. 87-94.
- MacDonald, Stuart K., 2015. Cyberterrorism and Enemy Criminal Law (March 30, 2014). *In Cyber War: Law and Ethics for Virtual Conflicts.* p. 20.
- Menthe, D. Jurisdiction in Cyberspace: A Theory of International Spaces. *In Michmann Telecommunication Technical Revue.* p. 69. <http://www.law.umich.edu>.
- MacLean, D., 2004. Herding Cats: Some Conceptual Tools for Thinking about Internet Governance. *In Internet Governance: a Grand Collaboration: an Edited Collection of Papers.* N.Y.: UN ICT TASK FORCE. pp. 73-100.
- Major, P., Internet Governance: Trends and realities. Part 2. *In Business Informatics.* 4(34). pp. 7-14.
- Mathiason, J., 2004. *Internet Governance: The State of Play: Report Commissioned by the UN ICT Task Force.* <http://dcc.syr.edu>.
- Hakmeh, J., 2018. *Cybercrime Legislation in the GCC Countries Fit for Purpose?*
- Kshetri, 2010. The Global Cybercrime Industry. ISBN-13: 978-3642115219. ISBN-10: 3642115217.
- Nomokonov, V. A., Tropina, T. L., 2012. Cybercrime as a new criminal threat. *In Criminology: yesterday, today, tomorrow.* 24. p. 4.
- Fedorov, F. V., 2006. *Information security in the global political process.* M.: MGIMO-UNIVERSITY. p. 10.
- Baturin, Yu. M., Zhodzishsky, A. M., 1991. Computer crime and computer security. M.: JURID. LIT. pp. 32-35.
- Tropina, T.L., 2005. *Cybercrime: concept, state, criminal-legal measures of struggle.* VLADIVOSTOK. p. 234.
- Chekunov, I. G., 2013. *Criminological and criminal law support for the prevention of cybercrime.* p. 8.