Harmonizing international cybercrime laws and procedures

Xo`jametova Gulhayo Muxtor qizi
Tashkent State University of Law
gulhayotsul@gmail.com

Abstract

Nowadays harmonizing international cybercrime laws could become an important global legal framework for international cooperation on preventing and investigating cybercrime, and prosecuting cybercriminals. Cybercrime, including massive and coordinated cyber attacks against countries' critical information infrastructure, and terrorist misuse of the Internet, are global crimes. Cyberspace has made a new environment for criminal offenses. Through international organizations, efforts must be taken to ensure the similarity of provisions in the individual countries. This harmonization may be achieved by means of conventions, recommendations or guidelines. This article analyzes approaches to the harmonization of legislation in this area, as well as the features of the use of an international instrument regulating measures to combat cybercrime, which have been adopted by most states of the world.

Key words: cybercrime, cyberspace, cybercrime law, harmonization of laws, international human rigts, international cooperation.

I.Introduction. Every state is constantly balancing between the principles of human rights and freedoms, integration into the international community, the need to ensure economic growth and national security, including restrictions on the rights and freedoms of citizens, development of forms for regulating restrictions on business activity, protection of honest interests in the international arena. The choice is made by both the population and public authorities, but in a number of areas no internal reasons should outweigh the need for international cooperation in the fight against crime, which should be built on the principles of openness, mutual

assistance, and activity in developing new forms of interaction. It appears that international cooperation in cybercrime must be carried out on the basis of the participation of all countries, which is predetermined both by the property of the information itself as an object of attack, and by the nature of the crimes committed. As noted by international expert on harmonization of legislation in the field of cybercrime Stein Stein Schjolberg, “cyberspace, as the fifth common space, after land, sea, air and space, requires coordination, cooperation and special legal measures at the international level". So this article analyze The harmonization of procedural provisions of cybercrime laws facilitates, among other things, global evidence collection and sharing through international cooperation.

II.Methodology. The research methodology for harmonizing international cybercrime laws and procedures adopted a kind of methods approach. This approach combines both quantative and qualitative data collection techniques to provide a comprehensive understanding of the research topic.The research paper involves various sources, such as academic journals, legal documents, scientific articles to illustrate cruial aspects of topic.

III.Results. The harmonization of procedural provisions of cybercrime laws facilitates, among other things, global evidence collection and sharing through international cooperation. Harmonization of criminal and criminal procedural legislation, as well as the creation of an effective system of mutual legal assistance through the adoption of a universal an agreement governing the fight against cybercrime at the global level is now becoming increasingly difficult. One of the obstacles is the already existing regional and international mechanisms for harmonizing legislation in the field of combating cybercrime, or more precisely, their fragmentation and “competition” between already existing regional approaches and attempts to develop tools that will go beyond regional scope.

IV.Discussion. The “mosaic” nature of the development of international instruments in this area is especially noticeable now, ten years after the adoption of the first agreement designed to establish global standards in the fight against crime

in the information space - the Council of Europe Convention on Cybercrime, signed in Budapest on November 23, 2001. Unfortunately, the document that was intended become a standard for national legislators and reach the global level, since it was the first international document in this area, coped only to a certain extent with the first of the tasks, but at the same time not only did not become a universal solution to the problem of joining forces in the fight against cybercrime due to a number of shortcomings, but also led to fragmented approaches to the harmonization of legislation.

It should be noted that the importance of the Council of Europe Convention in the fight against crime in cyberspace cannot be overestimated - it was this document that laid the foundations. However, the Council of Europe Convention suffers from serious shortcomings that make it impossible to use this instrument to harmonize cybercrime legislation at the global level. In particular, the problems of the Convention are as follows:

- lack of an effective implementation mechanism and lack of implementation monitoring.

The Convention provides for the need to implement its provisions at the national level. It would be logical to assume that the more than 30 countries that have ratified the Convention should have comparable rules governing liability for cybercrimes, as well as procedural mechanisms to investigate this type of crime. However, an analysis of the legislation of the parties to the Convention shows that this has not yet happened. Moreover, The Council of Europe has never carried out a full assessment of the implementation of the provisions of the document in the national legislation of countries and its compliance of legal norms with obligations under the convention.

The main problem in harmonizing cybercrime legislation at the international level at present is not the lack of models for developing legislation, but the fact that the ever-increasing number of these models in no way leads to breadth of coverage

and cooperation at the global level. Instruments developed by the European Union, Council of Europe, Commonwealth of Nations, Caribbean countries region led to the criminalization of electronic attacks in the national legislation of countries and the harmonization of the general part of criminal legislation at the level of regions of the world. However, in the field of procedural cooperation, mutual legal assistance, as well as in matters of jurisdiction, these instruments have not yet been able to create a legal basis for effective cooperation at the operational level. Even with all the fragmentation of the implementation of international standards in national legal systems, the legislation of most countries of the world already has rules providing for liability for cybercrimes. However, the question of the correspondence of these norms to each other and the problem of procedural interaction between law enforcement agencies in the investigation of cybercrime remain relevant. At first glance, the efforts of various international organizations in the field of harmonization of legislation to combat cybercrime seem to be complementary. However, cooperation between these organizations is currently either ineffective or virtually non-existent. Thus, the main problem of effective cooperation is that there is no single approach to international standards and to the question of who should develop them and regulate the process of their implementation.

Despite the disparate and fragmented approaches to combating cybercrime, new proposals have recently emerged to create global instruments that require a much higher level of international cooperation than the harmonization of legislation.

Conclusion

At the same time, information security is already considered by states as one of the priority tasks in the field of national security and international politics. Computer attacks on companies and even states, such as the Stuxnet virus, show that even if information weapons do not become a real threat in the near future, they can in any case cause serious problems to the economy and military security

of states. Probably discussions about the creation of an international tribunal for cybercrime needs to start now. However, for the creation and effective functioning of this institution, a solid legal basis is needed, which is currently missing.

-internationally harmonized criminal law, a set of minimum standards that will be implemented in all member states of the agreement on the international tribunal;

-development at the international level and implementation into national legislation of procedural standards that make it possible to effectively investigate crimes in global information networks, obtain, investigate and present evidence taking into account the international component of the problem of cybercrime;

-effective mechanisms of mutual legal assistance in the field of investigation of cybercrimes, well-functioning cooperation of law enforcement agencies at the operational level;

– mechanism for resolving jurisdictional issues in cyberspace

International cooperation is key to curbing the complex phenomenon of cybercrime. development of new control and management mechanisms -the only path to information security, which currently seems to be an elusive goal, but at the same time is an urgent need.

References

1.Farwell J.P., Rohozinski R. Stuxnet and the Future of Cyber War // Survival. 2011.

2.Gercke M., Tropina T. From Telecommunication Standardization to Cybercrime Harmonization // Computer Law Review International. 2009.

3.Goodman M. International Dimensions of Cybercrime // Ed. by S.Ghosh and E. Turrini. Cybercrimes: A Multidisciplinary Analysis. Berlin, Heidelberg, 2010.

4.Explanatory Report to the Convention on Cybercrime
https://rm.coe.int/16800cce5b

5.Harmonization of legislation on Cybercrime and Electronic Evidence with rule of law and human rights safeguards // https://rm.coe.int/16800cce5b.

.