Institución Universitaria
SALAZAR Y HERRERA

QUID 2018, pp. 125-128, Special Issue N°2, ISSN: 1692-343X, Medellín-Colombia

INTERNATIONAL TERRORISM AND INTERNATIONAL CYBERTERRORISM

TERRORISMO INTERNACIONAL Y CIBERTERRORISMO INTERNACIONAL

(Recibido el 26-05-2018. Aprobado el 19-07-2018)

PhD. Kseniya E. Kovalenko
Altai State University,
Associate professor, PhD in Law,
Department of Labor, Environmental
Law and Civil Procedure, Law Institute
Barnaul, Russian Federation.
kovalenko1288@mail.ru

PhD. Anna I. Rozentsvaig
Samara National Research
University,
Associate professor, PhD in Law,
Vice-dean of the Faculty of
Law,Department of Theory and
History of State and Law and
International Law, Samara,
Russian Federation
lawyeranna@mail.ru

PhD. Anna V. Gubareva
Ural State Law University,
Associate professor, PhD in Law,
Department of Business Law,
Ekaterinburg, Russian
Federationashipova@mail.ru

Abstract. This article deals with the problem of international terrorism. It arises the complexity of determining the composition of the crime. A special feature is that international terrorism is considered to be one of the most complex and most dangerous crimes with an international nature. It includes diverse compositions: piracy, hostage-taking, etc. The concept of "cyberterrorism" and its features are also discussed. It is emphasized that the existing universal and regional international anti-terrorism agreements are not adapted for effective counteraction to all possible modern variants of manifestation of terrorist behavior. Cyberterrorism can be singled out among the most urgent threats that are not covered by international law.

Keywords. International terrorism, international cyberterrorism, crime.

Citar, estilo APA: Kovalenko, K., Rozentsvaig, A. & Gubareva, A. (2018). International terrorism and international cyberterrorism. *Revista QUID (Special Issue)*, 125-128.

1. INTRODUCTION

From the beginning of the 21st century, the international community has seen a real threat of increasing risks of terrorist acts by terrorist organizations. The waves of terrorism have overwhelmed Western countries. Many conventions and resolutions have been adopted to prevent them. They mainly reflect methods and plans to combat the phenomenon of international terrorism. The universal level is occupied by the following international legal instruments: the Vienna Convention on combating illicit traffic of narcotic drugs and psychotropic substances (1988), the Rome Convention for the suppression of unlawful acts against the safety of Maritime navigation (1988), the international Convention for the suppression of terrorist bombings (1997), the world Convention for the suppression of the financing of terrorism (1999); the United Nations Convention against transnational organized crime (2000).

The regional level is supported by the following documents: The code of the Islamic conference organization on combating international terrorism (1994), the Treaty on cooperation of the CIS member States in combating terrorism (1999), the Shanghai Convention on combating terrorism, separatism and extremism (2001), the European Convention on laundering, detection, seizure and confiscation of the proceeds from crime (1990) and many others.

International legal doctrine distinguishes several criteria that can help to define crimes at the international level and an international crime with terrorism nature. These include the degree of public danger to the citizens of the state, the importance and significance of acts with an international legal nature that have been violated, the reasons for the emergence of international crimes of a terrorism nature, and the gravity of the crime of an international terrorism nature. All the above mentioned refers to the force of gravity, as defined by the plan: the enormity, barbarism, cruelty, fanaticism, etc., or resulting from the scale committed illegal acts.

In recent years, new non-traditional forms of terrorism attacks, made on knowledge-based technologies and not falling under the category of "weapons": electromagnetic, information and computer attacks, have been actively spreading. Currently, the relevance of this problem is due to the growing activity of international terrorism, which is gradually integrated into the Internet environment and becomes a high-tech way to achieve the goals. The radical part of our society is increasingly resorting to the use of electronic and computer technology, computer cryptographic encryption, mobile communications, technically sophisticated equipment. Even in the organization of rallies and demonstrations against the government, opposition forces use a modern approach: social networks (Vkontakte, Odnoklassniki, Facebook), microblogs for instant messaging (Twitter) and IP-telephony (Skype) are actively involved (Uslynskiy, 2014).

2. DISCUSSION

The corpus delicti of international terrorism and national terrorism can be attributed to the corpus of real danger, not excluding some of the signs, which are: qualifying features (group by prior agreement, with the use of firearms); especially qualifying features (organized group, if it caused the death of a person or other serious consequences, which can include serious harm to the health of two or more persons, the failure of life support facilities, disruption of transport, material damage, if they involved an attack on the objects of nuclear energy or the use of nuclear materials, radioactive substances or sources of radiation.)

The threat of a terrorist act is in the nature of information expression, information sign. It turns out the act of terrorizing-an intermediate crime, a kind of advance of the public, wearing the intimidation of the population. Usually it is brought to power authorities, that does not reach the masses of the population in open form (Sedyh, 2012).

The nature of cyberterrorism is qualitatively different from the generally accepted concept of terrorism, retaining only the core of this phenomenon, but signs similar goals. A cyberterrorist can do more harm by using an inexpensive smartphone than an explosive device in a criminal arsenal. Cyberterrorism is an action that is expressed in a deliberate, politically motivated attack on information processed by a computer and computer systems, creating a danger to life or health of people or the occurrence of other serious consequences, if such actions were committed with the aim of violating public security, intimidating the population, provoking a military conflict.

At the present stage of society development, cyberterrorism often acquires a political background, in fact, being a way of motivated attack on the existing information infrastructure, which consists of the direct management of society through preventive intimidation. This is manifested in the threat of violence, maintaining a state of constant fear in order to achieve political or other goals, coercion to certain actions, drawing attention to the identity of a cyberterrorist or terrorist organization that he represents. Threatening to do harm is a kind of warning about the possibility of causing more serious consequences if the conditions put forward are not met. On the other hand, cyberterrorism is a new weapon of terrorist groups, and it is impossible to cover all its features at this moment.

Since 2004 within the framework of the Council of Europe the only international legal document in this sphere is the Convention on crime in the field of computer information ETS № 185 (Budapest, November 23, 2001) (Convention, 2001). According to the reasoned opinion of a number of government officials, experts in the field of IT-technologies and international law, the analyzed document is imperfect, from a practical point of view, ineffective. The convention covers insufficient for today volume of computer crimes. Since this agreement appeared, new Internet services and new ways for criminals to participate in cyberspace have emerged. So outside the agreement was cyber-terrorism, which undoubtedly requires an adequate response from the world community.

An analysis of the legal technique of this provision of the Convention makes the following point. The drafters of this act are in the majority of the countries of traditional Europe, connected by close and strong political and legal ties, common destiny and history. Therefore, it seems natural for them to have a situation of free admission for their partners to the Holy of holies IT-content of national security. For other States, including Russia, which have competing political and economic interests on a regional and global scale, the provision of full transparency of their own information space may look critical and unacceptable.

In international law, the issues of countering cyberterrorism have a slightly different context than in national legislation. The main task of the document on combating cybercrime in General and the information version of terrorist crimes agreed between the States is to create a basis for harmonization of the legislation of the States parties to the treaty. It should cover the formation of rules of interaction between law enforcement bodies to prevent and suppress such acts, the development of universal jurisdictional approaches in the case of a transnational crime. In addition, the international document should consolidate the organizational structure of the global system of combating cybercrime. All these problems can be solved only by creating universal norms that establish uniform rules for the world wide web. Therefore, we should support the initiative of Russia, which proposed the Convention on international information security (concept) for discussion at the UN (Moskal'kova, 2007).

Article 5 of this document establishes the basic principles of information security. The fundamental premise of the fundamental part of the Convention, according to the draft, is that the information space is a common human asset. This statement is extremely important, emphasizing the modern importance of the global network and establishing a common vector of the IT-space development. Among the basic provisions of the document the ideas of indivisibility of security (the security of one state is inextricably linked with the security of all others), the preservation of state sovereignty over the national segments of the Internet, responsibility for their own information space, the inadmissibility of external interference should be noted.

The draft Convention calls upon States parties not to use IT technologies, including the Internet, to engage in aggressive activities and to pose threats to international peace and security. An important place in the document is designated to standards on combating criminal and terrorist activities and cooperation of States in combating them (articles 8 - 9).

These provisions are innovative, reflect the General position of the UN, has repeatedly expressed in the resolutions of the UN General Assembly, which calls for the development of international principles to improve the global information space and telecommunications, and helps to fight against information terrorism and criminality (Cyber-Rights and Cyber-Liberties Response to MEP, 2012).

The analysis of the draft Convention on international information security shows that it has a fundamentally different basis than the European Convention (2001). It can be a complicating factor for negotiating and developing a global position in the process of approving the final text and its adoption in the UN. Countries that have acceded to the European Convention (2001), due to the existing contradiction between the rules of the two documents, will not be able to be parties of both acts. They will insist on the European version of the agreement on information security.

3. CONCLUSION

Summing up, it should be said that international terrorism in the manifestation of its actions is characterized by signs of political and violent manifestation, and the qualification itself has the character of a foreign element, which is not difficult to guess from the very phrase "international terrorism".

This topic combines integrated approaches of scholars, a joint effort of studying a qualification of this crime, with all its aspect components, which are derived one from the other.

Due to the fact that cyberterrorism has extremely dangerous international potential, it is necessary to create international legal norms that ensure global protection of the Internet and other information networks from cybercrime in general and from cyberterrorism in particular.

An important argument in favour of international legal regulation of the global network is that in connection with the theoretical inconsistency of the nature of the offences in the sphere of IT-technologies we need a real evaluation and a practical response on the part of several States as to the option of fighting. This may lead to a military conflict that can involve states that are quite advanced from a technical point of view.

The fight against cyberterrorism in the international legal space requires addressing two important issues: the global regulation of the Internet and the creation of a legal framework to combat cyberterrorism.

REFERENCES

Criminal Code Of The Russian Federation. Part Two (1996). Legal reference system "Consultant Plus". Retrieved May 29, 2018, from URL: http://www.consultant.ru/document/cons_doc_law_10699/.

Batueva, E.V. (2015). Amerikanskaja koncepcija ugroz informacionnoj bezopasnosti i ee mezhdunarodno-politicheskaja sostavljajushhaja: Dis kandidata politicheskih nauk: 23.00.04 [The American concept of information security threats and its international political component]. Moscow.

Moskal'kova, T.N. (2007). Mezhdunarodno-pravovoe regulirovanie bor'by s terrorizmom v Rossijskoj Federacii [International legal regulation of the fight against terrorism in Russian Federation]. Rossijskij sud'ja. N 4.

Cyber-Rights and Cyber-Liberties Response to MEP Elena Paciotti. URL: http://gilc.org/cyber_response_52902.html (17.04.2012).

16. Convention on Cybercrime (2001). European Treaty Series - N 185 Council of Europe. URL: http://conventions.coe.int/Treaty

Sedyh, N. S. (2012) Terrorist threats and global risks of our time: psychological and political analysis. NB: International relations. 1.

Ulinski, F. A. (2014). Cyber-terrorism in Russia: its properties and characteristics. Law and cybersecurity. 1. society. Universidad y Sociedad. 10(3).