European Proceedings of
Social and Behavioural Sciences
EpSBS

www.europeanproceedings.com
e-ISSN: 2357-1330

DOI: 10.15405/epsbs.2022.06.70

AMURCON 2021
AmurCon 2021: International Scientific Conference

CYBERATTACKS AS A CRIME OF AGGRESSION AND INTERNATIONAL TERRORISM: LEGAL QUALIFICATION PROBLEMS

Dmitriy V. Lobach (a)*, Sergey S. Shestopal (b)
*Corresponding author

(a) Far Eastern Law Institute (branch) of the University of the Prosecutor's Office of the Russian Federation, Vladivostok, Russia, dimaved85@mail.ru
(b) Yaroslav Mudryi National Law University, 77 Pushkinskaya St., Kharkov, Ukraine, ss.shestopal@ya.ru

Abstract

The paper considers the political and legal aspects of the possible qualification of cyberattacks as acts of aggression and international terrorism. It is stated that cyber threats, which in the modern conditions of the development of the information and digital environment are considered in many national security doctrines as new challenges that threaten not only national interests but also international law and order. The digital transformation of social relations and the widespread of cyberattacks around the world, leading to material, organizational and reputational losses, as well as the change in military doctrines and national security strategies, considering modern trends in the development of international relations, taking into account the current state of scientific and technological progress, demonstrate the possibility of qualifying cyber-attacks as acts constituting a crime of aggression or international terrorism. It is concluded that modern trends in the development of international relations, taking into account the current state of scientific and technological progress, demonstrate the possibility of qualifying cyberattacks as acts constituting a crime of aggression or international terrorism.

Keywords: Cyber terrorism, cyber threats, ınternational terrorism, ınternational peace, ınternational security

https://doi.org/10.15405/epsbs.2022.06.70
Corresponding Author: Dmitriy V. Lobach
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

1. Introduction

Modern socio-economic, geopolitical, cultural and information technology processes predetermine new emerging risks and threats to stability, law and order, sovereignty, territorial integrity and independence of individual states, that, ultimately, foreground the need for a conceptual and legal comprehension of the status of security in the focus of those destructive manifestations of international relations that impinge on or create a threat to international peace and the security of all mankind. Today, security at the national level and in the practice of international relations is defined as a complex interdisciplinary phenomenon of social reality, characterized by a condition of sustainability and stability in the development of social systems, which is expressed through the sufficiency and adequacy of measures to prevent threats and overcome dangers. In this aspect, cyber threats are of particular interest, which in the modern status of the development of the information and digital environment are considered in many national security doctrines as new challenges that threaten not only national interests but also international law and order (Blanck, 2013).

Many states are pursuing active domestic cyber security policies, thus giving a new vector to their national security strategy. For example, the 2011 US International Cyberspace Strategy determined that modern threats to cyber security can endanger international peace and security more likely than traditional forms of international conflicts since political and military confrontation is transferred to cyberspace. At the same time, the document notes that cyber threats by their nature are cross-border, and as a result, resisting these threats can be effective only with active cooperation and interaction with other states, military and civil structures in the direction of raising awareness and to organize work to prevent cyber threats in the format of the development of means and methods of collective self-defence in cyberspace (International strategy for cyberspace, 2011).

The Japan Information Security Strategy submits the real danger of large-scale cyber-attacks for Japan in the light of foreign incidents (the United States and South Korea) and the functional connection between many aspects of economic activity and social life, on the one hand, and information and communication technologies - from the other (Information Security Strategy for Protecting the Nation, 2010). The strategy also fixes special measures to counter large-scale cyber-attacks, manifested in strengthening control over cybercrime, international interaction in the field of ensuring national interests in cyberspace, as well as active cooperation between the state and the private sector.

The cyber security strategy of Canada from 2010 (Canada's Cyber Security Strategy, 2010) describes the public danger of modern cyber-attacks, which consists in the onset of serious consequences for private and public interests (in particular, the undermining of electrical networks, disruption of the operation of water treatment plants, malfunctions of telecommunication networks, increased production costs, violation of confidentiality, loss of intellectual property, etc.). It should be noted, not without interest, that the strategy proposes to differentiate all cyberattacks according to four types: cyber espionage, sponsored by the state; military operations, where cyberattacks are the central element of military strategy; cyber terrorism; cybercrime. At the same time, depending on the ratio of the funds spent, the qualifications of the hackers and the result achieved, taking into account the goal set, it is proposed to subdivide all cyberattacks into four types: low-cost cyberattacks (hacking tools can be

https://doi.org/10.15405/epsbs.2022.06.70
Corresponding Author: Dmitriy V. Lobach
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

purchased at an affordable price or downloaded from the Internet), easy cyberattacks (attackers have only basic skills and can carry out attacks that cause or may cause significant damage), effective cyberattacks (insignificant in terms of organizing and carrying out attacks against computer systems can cause widespread consequences), low-risk cyberattacks (sophisticated attacks that minimize the likelihood of intruders being identified by implementing sophisticated cover-up schemes and exploiting gaps in national legislation and the international legal regime) (Canada's Cyber Security Strategy, 2010; Dinstein, 2011; Shull & Wark, 2021).

2. Problem Statement

In the context of the complication of international relations, the dynamics of globalization processes and trends in scientific and technological progress, the need to rethink the traditional threats that encroach on the international world, acting as an element of the international legal order, is actualizing. Modern legal science and political thought emphasize the crime of aggression and international terrorism among the traditional threats to international peace (Sayapin, 2016; Suvorov, 2019). Each of the presented forms of aggressive policy is committed against the sovereignty, territorial integrity, and political independence of another state, which leads or may lead (create a threat) to various manifestations of complications in international relations, up to open armed confrontation.

Let us consider each of the presented threats that encroach on or pose a threat to international peace and security and are committed using computer network attacks from the standpoint of the international legal regulation of relations related to the prohibition of armed aggression and acts of international terrorism.

3. Research Questions

In a historical retrospect, in international public law, these forms of aggressive policy are subject to legal prohibition and (or) politico-declarative condemnation. For example, the war of aggression has a long history of political and legal prohibition, including its criminalization. Back in 1928, the Briand-Kellogg Pact was adopted, providing for the refusal of war as a means of national policy (Dinstein, 2011). Subsequently, aggression - the illicit use of armed forces against another state - was criminalized as an international crime as a result of the work of the Nuremberg and Tokyo Tribunals (ad hoc tribunals that took place as a result of the end of the Second World War). In 1974, the UN General Assembly adopted a special resolution defining aggression as an illegal phenomenon of foreign policy. Further on, aggression was criminalized at the international level as a result of the adoption in 1998 of the Rome Statute of the International Criminal Court. In 2010, a resolution was adopted (resolution RC / Res.6) defining a normative definition of the crime of aggression (Dinstein, 2011). By this statement, the crime of aggression means the planning, preparation, initiation or implementation of an act of aggression by a person who is actually in a position to exercise governance or control over the political or military actions of a state, which, by its nature, gravity and scale, is a gross violation of the Charter of the United Nations. In this case, an act of aggression means the use of armed force by a state against the sovereignty, territorial inviolability or political independence of another state or in any other way incompatible with

https://doi.org/10.15405/epsbs.2022.06.70
Corresponding Author: Dmitriy V. Lobach
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

the Charter of the United Nations. The resolution regulates that any of the actions reflected in resolution 3314 (XXIX) of the UN General Assembly of December 14, 1974, will be qualified as an act of aggression (Dinstein, 2011).

From the standpoint of modern international criminal law, aggression is considered as an international crime, that is, as an act, whose criminalization is carried out at the national level, and not international, that causes the spread of the regime of international jurisdiction about individuals responsible for acts that constitute the objective side of the crime of aggression (Brilliantova, 2016).

The resolution of the UN General Assembly "Definition of aggression" of 1974 provides a legal definition of aggression (Article 1), as well as a non-exhaustive list of acts of aggression (Article 3) (Dinstein, 2011). At first glance, the literal interpretation of these acts does not allow us to conclude about the possible consideration of a cyberattack as an act of aggression, since we are talking about the traditional use of armed force. However, it is necessary to understand the fact that this list is not comprehensive, and the UN Security Council may determine that other acts constitute aggression by the provisions of the UN Charter (Article 4) (Dinstein, 2011). At the international level, there is a tendency to recognize the use of computer network attacks as an act of aggression. For example, the “Tallinn Guidelines on the Application of Legal Norms of International Law to Military Operations in Cyberspace” was recently adopted, which states that the use of force can cover acts committed in cyberspace and lead to consequences comparable to those of traditional use of armed forces (Tallinn manual on the international law applicable to cyber warfare, 2013).

Considering the digital transformation of social relations and the widespread of cyberattacks around the world, leading to material, organizational and reputational losses, as well as the change in military doctrines and national security strategies, considering cyberspace as a promising theatre of military-technological countermeasures in the face of increasing geopolitical confrontation, in the theory of international criminal law, computer network attacks (cyber-attacks) are proposed to be considered as acts of possible aggression.

4. Purpose of the Study

The study aims to analyze the conceptual political and legal positions regarding the nature and possibilities of the legal qualification of cyberattacks as a crime of aggression and international terrorism within the context of the current development of the theory of international criminal law with the subsequent substantiation of the conceptual definition of the phenomenon under consideration.

First, we should conduct a descriptive analysis of current approaches regarding the nature of the phenomenon under consideration, revealing the relevant characteristics of the phenomenon. Based on the intermediate results obtained, it is necessary to carry out a comparative legal analysis of the conceptual and legal definitions of the declared subject, which will make it possible to formulate an inductive definition (inductive inference) of an international crime.

https://doi.org/10.15405/epsbs.2022.06.70
Corresponding Author: Dmitriy V. Lobach
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

5. Research Methods

The paper uses such methods as analysis, synthesis (the method is reflected in the generation of a general definition of cyberattack crime), and a formal legal method, which allowed analyzing international documents regulating relations in the field of combating international crimes. The use of the method of continuous analysis allows for an overview comparison of theoretical positions regarding the concept of "international crime", "acts of aggression" and "acts of international terrorism".

6. Findings

The possibility of qualifying cyberattacks as an act of aggression.

In the theory of international criminal law, there have been several approaches in the field of international legal regulation of responsibility for the crime of aggression.

Thus, some representatives of the science of international criminal law emphasize that the nature of armed attacks undergoes natural changes in connection with the active use of information technology tools against objects of the information-critical infrastructure of other states. The theory of international criminal law argues that cyberattacks can be classified as a type of armed attack, provided that such attacks lead to consequences characteristic of the traditional use of force. It is proposed to include among those the shutdown of computers that control hydraulic structures and dams, which leads to flooding of settlements, destruction of information security, disorganizing military infrastructure and disruption of the economic system no less than the direct use of the armed forces (Brownlie & Crawford, 2019).

On the other hand, positions are also expressed to qualify cyberattacks as unarmed forms of aggression. So, Timoshkov (2017) notes that the modern concept of aggression can and should cover cyberattacks, which is due to the complication of interstate relations in the context of globalization and the development of scientific and technological progress. Interference in the inner affairs of a state or disruption of state sovereignty at the present stage can be carried out with the help of a cyber-attack, which, under certain conditions, can be qualified as an act of aggression that has an unarmed character. At the same time, the damage from a cyber-attack should be commensurate with an armed attack and can also be expressed in the distortion of the infrastructure of an entire state, including the country's missile defence system. Thus, the author proposes a new approach to understanding aggression through its unarmed character. Despite the relevance of this approach, due to the modern realities of complications of international relations as a result of incidents in cyberspace, at the same time, this vision of an act of aggression (an act of unarmed aggression) seems relevant and contradicting the very essence of aggression as a form of political violence of an armed nature. Meanwhile, the author can be supported in the sense that modern armed conflicts are hybrid, expressed in the use of various forms and means of warfare, while cyber weapons are given key importance in the context of implementing the concept and strategy of network-centric warfare. Despite the academic temptation to recognize cyber-attacks as a possible act of aggression, at the same time it is necessary to understand that the legal essence of aggression as a crime against international peace is expressed not so much in the objective aspect (the use of armed force by one state against another), but rather in the contextual element acting as a special feature of an international crime (in addition to the features of corpus delicti). The contextual element of

https://doi.org/10.15405/epsbs.2022.06.70
Corresponding Author: Dmitriy V. Lobach
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

an international crime is a certain condition that must accompany the commission of the act itself and this predetermines its highest social (international) danger. Concerning the crime of aggression, the contextual element covers the direction of the use of armed force against the sovereignty, territorial integrity, and political independence of another state, as evidenced by the likely qualification of such use of armed forces as an act that encroaches on international peace, that is, as a war of aggression. For this reason, from a de-jure standpoint, ordinary, simple, or systematic cyberattacks that do not infringe or are not capable of infringing on the national interests of another state, expressed in its sovereignty, political independence, and preservation of territorial integrity should be qualified only as an unfriendly act. Moreover, we should note that on the one hand, these approaches intersect with each other. On the other hand, they coincide in some moments. For example, understanding an international crime through a violation of obligations arising from the operation of jus cogens norms overlaps with the definition of international crimes as crimes against the peace and security of humanity since the violation of such norms may threaten international legal order. Not only do acts violate jus cogens norms endanger international peace and the security of humankind (for instance, acts of aggression that are not sufficiently serious or sporadic (isolated) war crimes). A similar situation manifests itself with a functional relationship with the government, acting as a subject of criminal politics.

The ability to qualify cyberattacks as terrorism.

International terrorism is a collective term that encompasses various terrorist crimes that are criminalized at the international level. The Convention Mechanism for Countering Terrorism represents many international treaties of a universal and regional character. Currently, 40 "anti-terrorist" international treaties have been adopted, including 18 treaties signed within the framework of lawmaking work under the auspices of the United Nations, and 22 regional documents. Many questions regarding interstate cooperation and the development of national measures in the fight against terrorism are covered in special declarations and UN resolutions. For this reason, from a de-jure standpoint, ordinary, simple, or systematic cyberattacks that do not infringe or are not capable of infringing on the national interests of another state, expressed in its sovereignty, political independence, and preservation of territorial integrity should be qualified only as an unfriendly act.

In terms of ensuring international peace and security of mankind, the 1994 Declaration on Measures to Eliminate International Terrorism (1994) is of particular importance. The document reflects that suppression of acts of international terrorism, committed both directly and indirectly by states, is one of the most important elements for maintaining international peace and security. In essence, this declaration, without giving a legal definition of international terrorism, demonstrates a general danger to the international legal order. From the standpoint of modern criminal law, criminal acts of a terrorist nature belong to the category of conventional crimes, which should be understood as acts expressing an international danger (capable of causing harm to relations protected by international law) and prohibited by special international legal acts. The criminalization of such acts at the conventional level at the same time predetermines the emergence of international obligations about the state related to the need to counteract such acts through the implementation of regulations in national legislation (Vučić, 2020; Weisbord, 2019).

https://doi.org/10.15405/epsbs.2022.06.70
Corresponding Author: Dmitriy V. Lobach
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

Despite the wide coverage of the problems of the spread of cyber terrorism in the low efficiency of national law enforcement systems in countering this phenomenon, a single concept of this phenomenon has not yet been developed. The wide range of concepts of cyber terrorism presented in the academic field evidence the complexity associated with the legal certainty of this phenomenon and expresses the different essence of this phenomenon. However, the generalization of various approaches to understanding the political and legal essence of this phenomenon and its conceptual and legal definitions allows us to state that terrorism manifested in the information space through the intensive use of information and communication technologies is often determined differently depending on the chosen paradigm of thinking and instrumental- functional approach. In this aspect, this object begins to be considered from the standpoint of general ideas or particular concepts prevailing in the academic sphere, that predetermines terminological confusion in terms of convergence with concepts such as cyber intervention, cyber-attack, cyberwar, cyber incident, cyber aggression (Kapustin, 2017; Kerschischnig, 2012).

These concepts reflect the real phenomena of social reality manifested in the information and communication space, which in modern conditions of the development of scientific and technological progress, acts as an independent sphere of political and legal interaction among the subjects of international relations. Thus, cybercrime is a generic concept of cyberterrorism.

To date, there is no general international convention governing relations in resisting cybercrimes. However, the political and legal counteraction to specific acts committed in the information space and qualified as cybercrimes is reflected in five regional conventions in combating computer crimes (Council of Europe Convention on Cybercrime (ETS N 185) of November 23, 2001 (the Council of Europe Convention, 2001), African Union Convention "On Cybersecurity and Personal Data Protection" dated June 27, 2014 (2014), Agreement on Cooperation of the Member States of the Commonwealth of Independent States in Combating Crimes in Computer Information dated June 1, 2001 (The Agreement.., 2001), the 2010 League of Arab States Convention "On Combating Crimes in Information Technology" (Arab States Convention, 2010) and the Agreement between Governments of the Shanghai Cooperation Organization member states on cooperation in international information security of 2009 (The Agreement.., 2012).

A comparative legal analysis of the above regional conventions allows us to conclude about different approaches to the legal regulation of acts as cybercrimes (Lilienthal & Nehaluddin, 2015).

On the one hand, there are general aspects of the political and legal definition of acts as computer crimes. Here it is necessary to note a unified approach (but with the differentiation of the constitutive features of specific offences) in identifying three groups of cybercrimes: acts against confidentiality, integrity and availability of computer data and systems; actions performed through the use of computers for personal or financial gain, as well as causing harm; acts related to computer content.

On the other hand, different approaches are seen in the definition of crimes related to computer content (affiliated with other crimes). For example, in Art. 3 of the African Union Convention, such crimes include incitement to hatred using computer technology, as well as the production, distribution or possession of child pornography. The Council of Europe Convention refers to only offences related to child pornography (Art. 9). On the contrary, the agreement on cooperation of the member states of the

https://doi.org/10.15405/epsbs.2022.06.70
Corresponding Author: Dmitriy V. Lobach
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

Commonwealth of Independent States in the fight against crimes in computer information does not contain such a group of crimes.

Attention is drawn to the regional experience of countering computer crimes related to terrorist activities. So, Art. 15 of the Arab League Convention discloses the legal content of terrorism-related crimes committed through information technology. Such crimes include dissemination and propaganda of ideas and principles of terrorist groups; financing and preparation of terrorist operations, as well as providing communication between terrorist organizations; the proliferation of methods for manufacturing explosives for terrorist operations; the spread of religious fanaticism, discord, and religious enmity. An obligatory contextual feature is a condition for the commission of these acts, which is expressed in using information technologies. In part 1 of Art. 2, this document gives a legal definition of information technology, which means any material or virtual means, as well as a group of interrelated means that are used to store, sort, organize, retrieve, process, transform and exchange information under the commands and instructions in force in this respect. The African Union Convention also contains a special rule regulating the adaptive connection between computer crimes and certain terrorist crimes. An illustrative example is the norm of paragraph "b" of Part 1 of Art. 30 of this document, which stipulates that the participating States must take the necessary regulatory and legal measures making it an aggravating circumstance to use information and communication technologies to commit theft, fraud, concealment of stolen property, breach of trust, extortion, money laundering and terrorism.

Of particular interest is the 2009 Agreement between the Governments of the Shanghai Cooperation Organization member states on cooperation in ensuring international information security. Unlike the above conventions, this document provides a working definition of information terrorism, which is understood as the use of information resources and (or) impact on them in the information space for terrorist purposes (The agreement.., 2012). By the second paragraph of Appendix No. 2 "List of the main types of threats in international information security, their sources and signs" (The agreement.., 2012) of this agreement, the signs of the threat under consideration are the use of information networks by terrorist organizations to carry out terrorist activities and attract new supporters; destructive impact on information resources, leading to disruption of public order; control or blocking of media transmission channels; using the Internet or other information networks to promote terrorism, create an atmosphere of fear and panic in society, as well as other negative effects on information resources. This agreement is fundamentally different from other regional conventions also in the sense that it differentiates information terrorism from related threats in international information security. In particular, information terrorism within the meaning of this agreement should be distinguished from information warfare, information crime, the use of a dominant position in the information space to the detriment of the interests and security of other countries, the dissemination of information harmful to socio-political and socio-economic systems, spiritual, moral and the cultural environment of other states, as well as from the threat to the safe, stable functioning of global and national information infrastructures of a natural and (or) man-made nature.

Separately, it should be said about the existing international convention mechanism for countering terrorism. In most cases, international conventions are focused on the detection, prevention, suppression, investigation, and disclosure of terrorist crimes. However, in certain cases, acts of cyber terrorism are also

https://doi.org/10.15405/epsbs.2022.06.70
Corresponding Author: Dmitriy V. Lobach
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

subject to the regulatory effect of some conventions. For example, cyberattacks on IT systems or databases can have a negative impact on objects in the real world, which is explained by the functional connection between the IT system and the management infrastructure itself. For this reason, attacks on aircraft or airport IT systems fall under the definition of terrorism under the 1971 Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971). Cyberattacks on the nuclear power plant management system and against the safety of maritime navigation can also be classified as terrorist acts under the International Convention for the Suppression of Acts of Nuclear Terrorism of 2005 (Kapustin, 2017) and the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation of 1988 (1988). The legal norm, paragraph "b" of Part 1 of Art. 2 of the International Convention for the Suppression of Acts of Nuclear Terrorism of 2005 defines that any illegal and deliberate use of radioactive material or devices that leads or may lead to the release of radioactive material should be qualified as a crime under this Convention (Kapustin, 2017). The expanded interpretation of this norm in modern conditions makes it possible to qualify as a terrorist crime the use of information and communication technologies to take over the entire electronic control system of a nuclear facility to use or damage it to release or create a danger of releasing radioactive material. The same can be said about the possibility of a regulatory expansion of the 1988 Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (1988). Here, attention is drawn to the norm of clause "e" of Part 1 of Art. 3 of this document, which determines that actions related to the destruction of maritime navigational equipment, as well as causing serious damage to it or interfering with its operation, should be considered a criminal act if any such action could threaten the safe navigation of the vessel (Convention for the suppression of unlawful acts against the safety of maritime navigation, 1988). The convention does not say about the nature of such an action; therefore, it is possible to assume that not only physical actions are performed, but also remote acts of electronic interference in navigation control systems.

However, if we proceed from a broader definition of cyberterrorism, which covers not only computer network attacks on social infrastructure facilities but also actions related to the spread of propaganda of ideas of terrorism, recruitment, financing, training of potential terrorists and incitement to commit terrorist acts, then within this standpoint, it is natural to assume about the possibility of expanded regulatory action of several conventions. In this aspect, the 1999 Convention for the Suppression of the Financing of Terrorism should be noted (Kapustin, 2017), which regulates the criminalization of any actions related to the collection and provision of funds for the commission of terrorist crimes. This document does not indicate the use of the Internet space to raise funds for terrorists, but this possibility cannot be ruled out, since modern terrorist organizations are increasingly moving into the shadow segment of the Internet, where they create various kinds of resources aimed at financing terrorism. A similar situation is observed with the 2005 Council of Europe Convention on the Prevention of Terrorism regulating measures to combat the recruitment and training of terrorists, as well as incitement to commit a terrorist offence. Based on the literal interpretation of the regulations of articles 5-7 of this document, a logical assumption should be made about the possibility of recruiting, training and abetting through the use of information and communication technologies, including information networks. In a special report of the UN Office on Drugs and Crime from 2013 (The use of the Internet for terrorist purposes, 2013), it

is noted that terrorists use different versions of the methods by which they mobilize and collect funds and resources. These methods include, inter alia, direct requests for donations, e-commerce, the use of online payment instruments, and the mediation of charitable organizations.

7. Conclusion

In conclusion, it should be noted that these acts, encroaching on national security and international peace, are historically associated with traditional forms of manifestation of unlawful behaviour, which can be expressed in the conduct of strategic operations, battles, hostilities (about the crime of aggression) and the commission of explosions, arson and other actions that frighten the population and create the danger of human death, causing significant property damage or other grave consequences (about terrorism). However, modern trends in the development of international relations, taking into account the current state of scientific and technological progress, demonstrate the possibility of qualifying cyberattacks as acts constituting a crime of aggression or international terrorism (Yakoviyk et al., 2018). To date, there are no special conventions in the system of public international law regulating countering cyber terrorism. Nevertheless, given the ambivalence of this act (which is expressed, on the one hand, because signs of terrorism are seen in the phenomenon as a whole, and on the other hand, unlawful acts are committed through the use of information and communication technologies on the Internet), the international legal regulation of counteracting this it becomes appropriate to consider this phenomenon within the framework of the conventional mechanism for combating various types of terrorism.

Acknowledgments

This work was financially supported by the Grant of the President of the Russian Federation No. NSh-2668-2020.6 "National-cultural and digital trends in the socio-economic and political-legal development of the Russian Federation in the XXI century.

References

African Union Convention on cybersecurity and personal data protection. (2014). University of Oxford. https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

Arab Convention on Combating Information Technology Offences. (2010). https://www.asianlaws.org/gcld/cyberlawdb/GCC/Arab%20Convention%20on%20Combating%20Information%20Technology%20Offences.pdf

Blanck, L. R. (2013). International Law and Cyber Threats from non-states Actors. *International Law Studies, 89*(406), 406-409.

Brilliantova, A. V. (2016). *International criminal law.* Moscow: Yurayt Publishing House.

Brownlie, I., & Crawford, J. (2019). *Brownlie's principles of public international law*. Oxford University Press, USA.

Canada's Cyber Security Strategy. For a stronger and more prosperous Canada. (2010). https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/canadaNCSS.pdf

Convention for the suppression of unlawful acts against the safety of civil aviation (1971). http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=INT&n=15384#005911886845499725

Convention for the suppression of unlawful acts against the safety of maritime navigation (1988). http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=INT&n=15694#022063366524796812

Declaration on Measures to Eliminate International Terrorism (1994). *Official website of the United Nations.* https://www.un.org/ru/documents/decl_conv/declarations/terrdec1.shtml

Dinstein, Y. (2011). *War, Aggression and Self-Defence. Fifth Edition*. Cambridge University Press.

Information Security Strategy for Protecting the Nation. (2010). https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/New_Strategy_English_Japan.pdf

International strategy for cyberspace. Prosperity, Security, and Openness in a Networked World. (2011). https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

Kapustin, A. Ya. (2017). On the question of the international legal concept of threats to international information security. *Journal of foreign legislation and comparative jurisprudence*, (6), 44-51.

Kerschischnig, G. (2012). *Cyberthreats and International Law*. Eleven International Publishing.

Lilienthal, G., & Nehaluddin, A. (2015). Cyber-attack as Inevitable Kinetic War. *Computer Law & Security Review, 31*(3), 390-400.

Sayapin, S. (2016). *Crime of Aggression in International Criminal Law: Historical Development, Comparative Analysis and Present State*. Springer International Publishing. - Scopus

Shull, A., & Wark, W. (2021). Reimagining a Canadian National Security Strategy. *CIGI Special Report*. https://www.cigionline.org/static/documents/NSS_Special-Report_web_eX1LDtj.pdf

Suvorov, V. A. (2019). *Ugolovnaya otvetstvennost' za akt mezhdunardonodnogo terrirozma [Criminal responsibility for an act of international terrorism]*. Krasnodar: North-Caucasus federal university.

Tallinn manual on the international law applicable to cyber warfare (2013). http://csef.ru/media/articles/3990/3990.pdf

The agreement between the governments of state members of the Shanghai Cooperation Organization on cooperation in the field of ensuring the international information security. (2012). *Bulletin of international treaties*, (1), 13-21.

The agreement on cooperation of the State Parties of the Commonwealth of Independent States in fight against crimes in the field of computer information. (2001). https://base.garant.ru/12123778/

The use of the Internet for terrorist purposes. (2013). *United Nations Office on Drugs and Crime*. https://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Terrorist_Purposes/Use_of_the_internet_for_terrorist_purposes_Russian.pdf

Timoshkov, S. G. (2017). *Agressiya kak mezhdunarodnoye prestupleniye [Aggression as an international crime]*. The Institute of Legislation and Comparative Law under the Government of the Russian Federation.

Vučić, M. (2020). Cyberattack as the Act of International Crime. *International public and criminal law in the XXI century, Belgrade*, 285-301.

Weisbord, N. (2019). *Cyberattacks, Insurgents, and Autocrats*. Princeton University Press.

Yakoviyk, I. V., Baranov, P. P., Shestopal, S. S., & Pokhodzilo, Y. N. (2018). The legal-theoretical issues of the state sovereignty in the globalization. *Opción*, *34*(87-2), 369.