UDC: 341.1 / 8

*M. Y. Yatsyshyn*

*(National Aviation University, Ukraine)*

**International legal opposition to cyberwars**

*The international legal opposition to the cyberwar at present is under formation. The article substantiates the need to adopt a universal international legal agreement which would contain the prohibition of the cyberwarfare.*

Implementation of the priority objective of modern international law - being the maintenance and protection of peace in the world - is not possible without the ban and exclusion of war as a means of national policy.

Based on the basic principles of international law, in particular the peaceful settlement of disputes and non-use of force and threat of force, as well as the goals of the UN Charter, the international community must take collective means for the prevention and removal of threats to peace and suppress acts of aggression or other breaches of peace.

With the development of social relations should note the transformation of international disputes are now resolved not typical methods and means. As noted, M. Tukhachevsky in "The contemporary strategies' (1926):" It is impossible to answer the question - what will be the nature of all future war - it changes its form and its character as it develops and it is impossible to predict these in advance " [1]. Under such conditions, the international rule-making should react to the challenges of our time, including the origin of the emergence of new trends to asymmetric power sources, including cyber capabilities to influence .

One of the features of modern wars is the use of new technologies in the confrontation between states. As stated by the Finnish scientist Erik Castren "technical development that began in the last century and continues at an accelerated pace in the present, creating new opportunities for such weapons as submarines, aircraft, nuclear weapons. This development increases the role and value of rules governing the conduct of hostilities on land and sea "[2]. However, modern technological advances are changing not only the means of armed struggle known to mankind, but also tactical strategy of modern warfare. At the same time there are new threats, which primarily include - cyberwar.

The term "cyberwar" is not new, but its generic definition is missing. In the doctrine and practice of international law simultaneously used terms such as «cyberwar», «cyber warfare», «cyber attack», and a number of similarities to them, the content of which means confrontation and warfare in «cyberspace».

J. Andres and C. Vinterfild state it is difficult to determine what cyberwar is. In fact, the two definitions – «cyber» and «war» - are a subject of debate [2, 2]. A.A. Merezhko notes that in international law there are no clear criteria on which to separate the ordinary acts of computer hooliganism from such attacks, which due to its seriousness have the character of an armed attack on the state, or the beginning of armed aggression against a state [3, 150].

Although the international community has repeatedly expressed concern that the latest technology can potentially be used for purposes incompatible with the objectives to ensure international stability and security and is able to affect the integrity of the infrastructure of states to the detriment of the safety of both the civil and military sectors (Tunis Agenda for the information society, Code for the protection of user rights in cyberspace UNESCO Resolution UNGA a / HRC / 20 / L.13 on 29.06.2012; UNGA Resolution a / HRC / 17/27 dated 16.05.2011 etc.) as of today, there is no international legal instrument that would contain a definition of "cyberwar" and forbade it.

Cybernetic war - a systematic struggle in cyberspace between states (groups of states), political groups, extremist and terrorist et al. groups, which is held in the form of attacking and defensive actions. The main objectives of both attack and defense in cyberwar are information resources properties are in terms of security (integrity, availability and confidentiality) may be affected [4, 90]. Considering this systemic struggle means that the actions of the parties have a certain integrity, consistency, unity, subordination to the given purpose, combined with other actions.

In his book "Theory of international public and private law" A.A. Merezhko offers draft Convention on the prohibition of cyberwar in the global information network of information and computing resources [5, 152]. In Art. 1 of the draft provided a definition of "cyberwar - use of the Internet and related technology and information means one state to harm the military, technological, economic, political and information security and sovereignty." The project by offering the Internet to recognize common heritage of mankind, to be used exclusively for peaceful purposes.

We consider being slightly inaccurate narrowing cyberwar only to Internet use. We believe that cyber war is happening in cyberspace, which is one of the essential features of this phenomenon. Despite the rather controversial interpretation of the term cyberspace, which was first used by the science fiction writers: V. Gibson, B. Sterling, John. Barlow, today it is often used in international legal treaties and acts of international organizations (UN, ITU, UNESCO, NATO, etc.).

In particular, Okinawan Charter of the information society provides: "The efforts of the international community aimed at the development of a global information society must be accompanied by concerted actions for making a safe and free from crime cyberspace" (p.8) [6]

Interesting in this context is the US Senate adopted in 2009, according to which cyberspace officially recognized the new environment (domain) combat actions and determined the feasibility of its association with the outer space within the framework of the new challenges, "geocentric theater of Action» (Spherical Area of ​​Operation).

To act in cyberspace are able not only to individuals, groups of individuals or organizations (including terrorism), but also the states or coalitions of states. Especially beneficial to "blur" the boundaries between war and peace. In fact committed "cyber attacks" may be alone or in combination with other attacks and threaten the sovereignty and security.

Despite the extraordinary activity of international political processes associated with the development of the global information society, international legal normalization of information sphere, including the determination of rules of conduct of related states and other actors is at the initial level. As a result, attacks committed in cyberspace can not be classified under international law. In such circumstances, the only way to counter is the qualification of these attacks just as certain cybercrimes, responsibility for which falls under national laws of countries and some regional international agreements.

In the absence of a unified international legal agreement on combating cyber-warfare particularly important doctrinal developments leading lawyers in international affairs. Tallinn guide the application of international law to cyberwarfare, published in 2013, prepared by experts in international law to order the Joint Center for NATO to exchange best practices in cyber defense (NATO Cooperative Cyber ​​Defence Centre of Excellence) [7] became extensive research in the specific field.

The manual specifies that cyberattacks using malware Stuxnet may be considered "armed attack." The victims of such attacks have the right to strike back in self-defense. Hackers involved in the conflict between states automatically acquire the status of combatants. The second edition of the manual should include provisions on human rights in cyberspace and will be published in 2016.

**Conclusions**

Thus, we conclude that the international legal opposition to the cyberwarfare at present is under formation. We consider the adoption of a universal international legal agreement, which would contain the prohibition of conduct of the cyberwarfare, where the definition of a key term would be: "cyberwar is a struggle between states (groups of states), implemented by means of systematic cyberattacks in cyberspace and threatening national sovereignty and security".

In addition, it is useful to recognize the universal level "cyberattacks" an act of aggression and attacks that are systematic - armed conflict of an international character.

We considers important extension of the principles of international humanitarian law with the "cybernetic" component. In particular, the principle of ratione loci should be extended to digital heritage sites and cultural heritage in cyberspace, and ratione conditiones - the "cyber weapons" that can cause excessive damage especially important or dangerous infrastructure (eg nuclear power plants).

**References**

1. Trebin M. P. "Hybrid" war as the new Ukrainian reality [electronic resource] / M. Trebin // Ukrainian society. - 2014 - Access to the property: http://www.ukr-socium.org.ua/Arhiv/Stati/US-3\_2014/113-127.pdf.

2. Antselevych G. A. Actual problems of International Law / GA Antselevych. - K .: Ukrainskaia academy External trade, 2006. - 282 p.

3. Andress J. Cyber ​​warfare: Techniques, tactics and tools for security practitioners / Andress J., Winterfeld S., Rogers R. - Amsterdam: Syngress / Elsevier, 2011. - 289 p.

4. Merezhko A. A. Theory of international public and private law / A. A. Merezhko. - K .: Yustinian, 2010. - 320 p.

5. Antonovich P. I. About the modern understanding of the term "cyberwar" / P. I. Antonovich // Bulletin of the Academy of Military Sciences. - 2011. - № 2 (35). - C. 89-96

6. Okinawan Charter of Global Information Society [electronic resource] - Access to the property: http://zakon5.rada.gov.ua/laws/show/998\_163.

7. The Tallinn Manual on the International Law Applicable to Cyber ​​Warfare [electronic resource] - Access to the property: http://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf.