Olha Grytsun
Taras Shevchenko National University of Kyiv

MILITARY AND POLITICAL ASPECTS OF INTERNATIONAL CYBER SECURITY: ISSUES OF INTERNATIONAL LEGAL REGULATION

This article examines the problem of legal regulation of political and military aspects of international cyber security and provides the qualification of its basic definitions, such as "cyber war" and "cyber weapons" in the existing juridical documents of international organizations, dedicated to the problems of international cyber security. The article comprises an analysis of the relevant provisions of the conventions, conducted within the Shanghai Cooperation Organization, the Council of Europe, the Commonwealth of Independent States, as well as the existing concepts of international documents, expert views of the North Atlantic Treaty Organization and a brief overview of the United Nations Group of Governmental Experts on issues, related to the international cyber security. The detailed analysis of juridical documents and theoretical concepts gives better understanding of the doctrinal approaches to military and political aspects of international cyber security.

Key words: international cyber security, cyberspace, international law, cyber-attacks, information and communication technologies, cyber war, cyber weapons.

A Problem Statement. The rapid development of scientific progress, as well as the information and communication technologies, contributed to the emergence of constantly-growing interconnection of all critical significant infrastructures of states, including defense systems with the cyber infrastructure, which eventually led to their vulnerability to external and internal factors. While in the early 90th the international community, considering the problem of international cyber security, was discussing only the issue of protection of personal data, connected with the active cooperation between states in the political, social, economic, scientific and technical fields, nowadays it is safe to state that there is a threat of military operations to be undertaken in cyber space. It should be noted that almost all the countries in the world are doing researches and developments in the field of cyber weapons usage.

States used to direct their efforts towards the development of defensive strategies, but nowadays we can discuss the development of offensive strategies within the cyberwar as well. Undoubtedly, this issue is a serious concern of the international community and demands the urgent need for regulation at the international level.

Research and Publications Analysis. Certain issues of military and political aspects of international cyber security were previously examined in the works of T. Morth, G. Kenneth, A. Krutskyh, R. Deibert, R. Clarke, T. Maurer, A. Fedorov, A. Smirnov and others. In their research papers the above-mentioned authors concentrated mainly on the subject, connected with the prohibition to use weapons in cyberspace, or to use cyberspace for military purposes.

However, the subject of comprehensive analysis of the main regulatory documents, related to this issue, remains unexplored. The analysis will make it possible to identify the main approaches to the regulation of the research issue at the international level and in terms of certain regional organizations.

The aim of the research is to explore the development of conceptual approaches to the regulation of military and political aspects of international cyber security and to define its place in the overall understanding of the concept of international cyber security.

The Objectives of the Article: analysis of the main regulatory documents of international organizations, dedicated to the management of the issue, connected with the military and political aspects of the international cyber security and the research of the conceptual framework of legal regulation of this issue.

Basic material. The problem of use the information and communication technologies (ICT) for purposes, incompatible with the maintenance of international peace and security, recently has become the main subject of scientific researches and political negotiations between countries at the international and regional levels.

In the course of sixty-five session of the United Nations General Assembly, the Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security was heard. The above-mentioned report stated that the existing and potential threats to cyber security are the most serious problems of the XXI century. These threats are caused by a wide range of different sources and they are manifested in subversive activities directed against the individuals and entities, as well as against the national infrastructure and governments[1]. The Group of Governmental Experts emphasized that inherently the cyber security threats are not exclusively civil or military technologies, they have a dual nature of the action.

It should be noted that the Group of Governmental Experts has recognized the fact that more and more countries develop ICTs as tools of warfare and for some political purposes as a separate threat to international peace and security. As an example, we shall note that according to various estimates, more than 120 countries are doing researches in the field of warfare in the cyberspace. Security problems in cyberspace have been a part of the national defense strategies of many countries and organizations for a long time. Thus, the "International Strategy for Cyberspace" has been approved of in the United States, in the UK and Germany these documents are known as "Cyber Security Strategy", in India – "National Cyber Security Strategy", in Finland – "Finland's Cyber Security Strategy", within the North Atlantic Treaty Organization the "NATO's Cyber Defense Concept and Action Plan" and the Plan of Action have been adopted, within the International Telecommunication Union – "Global Cybersecurity Agenda", within the European Union – "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace". Apart from that, states are creating specialized governmental agencies on cyber security and even some military units, whose main task is to prevent cyberthreats and conduct defensive and offensive operations in cyberspace.

Unfortunately, at present there is no unified conceptual apparatus for the definitions of "cyber war" and "cyber weapons", thus we will try to analyze the scientific approaches to the definition of these concepts and their ability in terms of the existing juridical documents on international cyber security.

Nowadays there are only three international legal agreements regulating the international cyber security. They include: Convention on Cybercrime of the Council of Europe, dated 23 November, 2001; Agreement among the Governments of the Shanghai Cooperation Organisation Member States on Cooperation in the Field of Ensuring International Information Security, dated 16 June, 2009 with corresponding appendices and The Commonwealth of Independent States Agreement on Cooperation in Combating Offences Related to Computer Information, dated 01 June, 2001.

Two of the above-mentioned documents, in particular, the Convention on Cybercrime of the Council of Europe and The Commonwealth of Independent States Agreement on Cooperation in Combating Offences Related to Computer Information do not include within the scope of their regulatory any issue of military and political aspects of cyber security, and limit their authority only to the criminal aspect.

Therefore, it is reasonable to analyze the principles of the Agreement among the Governments of the Shanghai Cooperation Organisation Member States on Cooperation in the Field of Ensuring International Information Security and the two of its appendices. Appendix 1 contains definitions of the notions, including the notion of "cyber war", defined as "the confrontation between two or more states in cyber space for the purpose of causing damage to cyber systems, processes and resources, critical and other infrastructures, undermining the political, economic and social systems and causing massive psychological impact on the population in order to destabilize the society and the state, in general, and to force the state to make decisions to the advantage of its enemy"[2] and "cyber weapons" which, according to the establishers of the Convention, means "cyber technologies, tools and methods, used for the purpose of leading to a cyber war"[3].

[1] *Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности*, ГА ООН Документ A/65/201 (08 декабря 2010 года). <http://www.un.org/disarmament/HomePage/ODAPublications/DisarmamentStudySeries/PDF> (2015, January, 15).

[2] *Угода між урядами держав-членів ШОС про співробітництво в області забезпечення міжнародної інформаційної безпеки* (прийнята 16 червня 2009 року, вступила в силу 02 червня 2011року). <http://base.spinform.ru/show_doc.fwx?rgn=28340> (2015, January, 20).

[3] *Угода між урядами держав-членів ШОС про співробітництво в області забезпечення міжнародної інформаційної безпеки* (прийнята 16 червня 2009 року, вступила в силу 02 червня 2011року).

Convention of the Shanghai Cooperation Organisation Member States has identified a non-exhaustive list of cooperation areas, which are subdivided on the basis of the threats in the sphere of international cyber security. All in all, there are six threats of this kind, defined at the Convention, but only four of them are related to the subject of our research. They include:

1. "Development and usage of cyber weapons, preparation for and conduction of cyber war;
2. The usage of a dominant position in the cyber space for the purpose of causing damage to the interests and security of other states;
3. Endangerment of safe functioning of global and national cyber infrastructures of man-caused or natural type;
4. Spread of information, which may harm the socio-political, socio-economic, spiritual, moral and cultural systems of other states"[1].

Appendix 2 provides a brief description of each type of threat, specifying them in terms of the sources of their origin and their basic features. Thus, production and development of cyber weapons is recognized as the first source of threat, and its main features include the usage of these weapons for the purpose of cyber war, destructive impact on critical infrastructures of another state, and the impact on any other system of its defense facilities. The authors of the document define the increase of digital inequality and the uneven development of cyber-communication technologies in different countries as the second thread. Thus, its main features include monopolization of software development by some states, the ability to build in hardware and software facilities some hidden functions in order to establish control over the cyber resources of another country and to restrict the participation of other states in cyber-technological cooperation. In accordance with Appendix 2, natural and man-caused disasters that may have been induced by quite different factors are also recognized as the source of threats to the stable functioning of national and global cyber structures, and their main feature is the violation of the cyber infrastructure functioning of a state. Finally, the source of the 4th threat include states, organizations or individuals that spread the information, harmful to the socio-political, socio-economic, spiritual, moral and cultural systems of other countries through the usage of cyber infrastructure. Its features may include a spread via media or Internet resources of the information that distorts the image of the political regime, political system, foreign and domestic policy of a state or the spiritual and moral principles of its population.

Thus, we conclude that the Governments of the Shanghai Cooperation Organisation Member States pursue the position of three-element structure of international cyber security – in particular, the presence of military and political, criminal and terrorist elements in it.

According to the SCO Member States, the vast majority of threats, emerging in cyberspace are mostly of a military and political character. Given to this fact, the directions of international legal cooperation in this area have been suggested. They include the following ones, in particular: "the arrangement of common activities for the development of international law in the field of limiting the spread and usage of cyber weapons, which pose a threat to defensive capacity, national and public security; promotion of sustainable functioning and internationalization of the Internet management; the establishment of common monitoring and responding to threats in the cyber environment; deepening of mutual trust-building measures that contribute to the international cyber security; the exchange of information on the legal framework in this area; the improvement of the international legal framework and practical mechanisms of cooperation among states; the cooperation within international organizations and forums; the experience exchange and special training in the field of international cyber security", etc.[2].

The issue of military and political aspects of international cyber security has been repeatedly raised within the United Nations Organization. During the 55th session of the United Nations General Assembly the work on the resolution entitled "Developments in the field of information and telecommunications in the context of international security" had been renewed. In response to a note verbale of the UN Secretary-General, the Russian Federation offered the draft entitled "Principles, related to the international cyber security". Under the provisions of this document, "cyber security" refers to "the protection of the basic

<http://base.spinform.ru/show_doc.fwx?rgn=28340> (2015, January, 20).

[1] *Угода між урядами держав-членів ШОС про співробітництво в області забезпечення міжнародної інформаційної безпеки* (прийнята 16 червня 2009 року, вступила в силу 02 червня 2011року). <http://base.spinform.ru/show_doc.fwx?rgn=28340> (2015, January, 20).

[2] *Угода між урядами держав-членів ШОС про співробітництво в області забезпечення міжнародної інформаційної безпеки* (прийнята 16 червня 2009 року, вступила в силу 02 червня 2011року). <http://base.spinform.ru/show_doc.fwx?rgn=28340> (2015, January, 20).

interests of an individual, the society and the state in cyberspace, including information and telecommunications infrastructure and information itself in terms of its characteristics such as integrity, objectivity, confidentiality and availability"[1]. The document defines a typology of international cyber security terms and its five basic principles. These principles establish that the activities of each state and other subjects of international law in international cyber space should contribute to the overall social and economic development and they have to be carried out in the way to correspond to the tasks of sustainable peace and security. The principles also presuppose that states and other subjects of international law must bear international responsibility for the cyberspace activities, carried out by themselves, under their jurisdiction or within international organizations that they belong to[2].

Besides, during the 66th session of the UN General Assembly the document entitled "Rules of conduct in the area of international cyber security" was discussed. The above-mentioned document was suggested in the letter addressed to the Secretary-General by the representatives of China, Russia, Tajikistan and Uzbekistan. The main purpose of this document was to define the rights and obligations of states in cyber space, to stimulate their responsible behavior and strengthen the cooperation.

According to the above-mentioned document, each state, that voluntarily agrees to implement these rules, obliges: to comply with the UN Charter and generally accepted norms of international law; not to use the information and communication technologies, including networks, to carry out hostilities, acts of aggression, threats to international peace and security; not to spread cyber weapons and corresponding technologies; to promote the development of multilateral and democratic international Internet governance mechanisms; to assist developing countries in the advancement of their capabilities in the field of cyber security and the elimination of the digital divide; to promote peaceful resolution of disputes, refraining from the usage of military force or threat of force[3].

These rules were also secured in the Concept of the Convention on International Information Security, which was presented at the London Conference on Cyberspace in 2011.

This document significantly expanded the range of military and political threats in cyberspace, defined the basic principles of international cyber security, as well as, in separate chapters, regulated countermeasures of cyber space usage for military and political, terrorist and criminal purposes. The main means of military conflicts resistance in cyber space is the obligation of states to cooperate in the field of international cyber security, to take all necessary measures to prevent the destructive impact of information from its territory and to cooperate with the aim to detect the source of cyber-attacks and to eliminate their consequences, to refrain from the development of schemes and doctrines that can provoke threats in cyber space or the emergence of cyber war, to refrain from the actions that could affect the integrity of cyber space of another state, to not use the information and communication technologies with the aim to interfere with the internal affairs of other states, to refrain from the threat or use of force against cyber space of another state, to refrain from hostile propaganda and slander with the aim to interfere with the internal affairs of another state, to refrain from spread of false information and to take action against the proliferation of cyber weapons[4]. Moreover, the concept defines the measures of trust between states within the military growth of cyber space. They include the exchange of national cyber security concepts, rapid exchange of information on critical events or threats, as well as the measures that have to be taken in order to regulate and neutralize them and guidance on cyber space activities.

It should be noted, that the definition of "cyber war" and "cyber weapons" in the above-mentioned Concept of the Convention coincides with the definitions, suggested at the SCO Member States Convention. Therefore, it can be stated that the suggested concept fully reflects the approach to the

[1] Крутских, А.В. (2004). *Технологический прогресс и современные международные отношения.* Москва: Просвещение.

[2] Крутских, А.В. (2004). *Технологический прогресс и современные международные отношения.* Москва: Просвещение.

[3] *Письмо Постоянных представителей Китая, Российской Федерации, Таджикистана и Узбекистана при Организации Объединённых Наций от 12 сентября 2011 года на имя Генерального секретаря ООН*, ГА ООН Документ A/66/359 (14 сентября 2011 года). <http://rus.rusemb.org.uk/data/doc/internationalcoderus.pdf> (2015, January, 23).

[4] *Конвенция об обеспечении международной информационной безопасности (концепция)* (представлена 23 сентября 2011 года). <http://www.mid.ru/bdomp/nsosndoc.nsf/e2f289bea6297f9c325787a0034c255/542df9e13d28e06ec3257925003542c4!OpenDocument> (2015, January, 22).

understanding of international cyber security, depicted at the SCO Member States Convention, and, additionally, significantly expands and details its position. Despite the fact that the document has been extensively discussed by the international community, currently we are unable to reach a consensus on it and it is still being just a concept.

Within the study of military and political aspects of international cyber security it is relevant to state yet another conceptual approach to the understanding of it. In 2013 in Tallinn, the experts of Cooperative Cyber Defence Centre of Excellence (CCDCOE) manifested the document entitled "The Tallinn Manual on the International Law Applicable to Cyber Warfare". This document is not official, and only reflects the views of individual NATO experts. But, despite this, it is extremely interesting in terms of the interpretation of existing international law and its possible application in warfare within cyber space.

Tallinn Manual regulates an extremely wide range of issues, including: international law of cyber security, issues of sovereignty, jurisdiction and state responsibility in the cyber space, issues of use of force and right to self-defense, international organizations activity. A separate part regulates the issues, concerning the law applicable to armed conflicts in cyber space. They include: general issues, conduct of hostilities, participation in armed conflict, definition of cyber attacks, cyber attacks against persons and objects, means and methods of war, perfidy, improper use of emblems and indicators of international organizations, cyber espionage, blockade and legal regimes of special zones, issues concerning the activity of certain persons and objects, among them are the following: medical and religious personal, United Nations personnel, children, journalists, detained persons, objects containing dangerous forces, objects indispensable to the survival of the civilian population, cultural property, issues concerning the protection of the natural environment, protection of diplomatic archives and communications, humanitarian assistance, occupation and neutrality[1].

Thus, Tallinn Manual includes the aspects of jus ad bellum, i.e. the provisions of international law that regulate the issue of the use of force by states as an instrument of national policy and the aspects of jus in bello, i.e. the provisions of international law that regulate the conduct of states in the course of an armed conflict – the provisions of international humanitarian law. The paper comprises the analysis of the four Geneva Conventions provisions: Convention Relative to the Protection of Civilian Persons in Time of War; Convention Relative to the Treatment of Prisoners of War; Convention for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of Armed Forces at Sea; Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field and protocols relevant to them; provisions of Hague Conventions, namely Convention Respecting the Laws and Customs of War on Land; Convention Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land; Convention Concerning the Rights and Duties of Neutral Powers and Persons in Naval War, provisions of the Vienna Convention on Diplomatic Relations, Convention on the Safety of United Nations and Associated Personnel, Hague Convention for the Protection of Cultural Property in the Event of Armed Conflict, Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques, Convention of the Rights of the Child, Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, Convention on Jurisdictional Immunities of States and their Property, provisions of the Rome Statute of the International Criminal Court, Constitution of the International Telecommunications Union and also Statutes of the International Criminal Tribunal for the Former Yugoslavia and Rwanda.

It is worth mentioning that, analyzing the aspect of states' countermeasures, Tallinn Manual focuses on the regulation of the "cyber attacks in response to cyber attacks" of the other side issue. It can be depicted with the following examples: the cyber attacks against critical infrastructures of a state or causing some damage to the enemy's command systems. Thus, the Manual does not regulate the issues, connected, for example, with the air attacks on cyber centers of governance or the methods of electronic warfare, since these operations are implicitly covered by the law of armed conflict. In addition, Tallinn Manual applies to both: international and non-international armed conflicts. Relevant commentaries to every rule of the Manual indicate whether it applies to both types of conflict or is limited only to the international armed conflict regulation. It is necessary to point out that it is the international law, applicable to the international armed conflicts, that serves as a starting point for legal analysis[2].

[1] *The Tallinn Manual on the International Law Applicable to Cyber Warfare*, NATO Cooperative Cyber Defence Centre of Excellence (first published 2013). <https://ccdcoe.org/249.html> (2015, January, 20).

[2] *The Tallinn Manual on the International Law Applicable to Cyber Warfare*, NATO Cooperative Cyber

Conclusions. Thus, having analyzed the problem of legal regulation of the military and political aspects of international cyber security and qualifications of its basic concepts in existing legal documents, we conclude that currently there are two distinct points of view on the concept of regulation of international cyber security. Those, who support the first one, completely exclude the military and political aspects from the international cyber security matter and take the position of its exclusive criminal and terrorist aspects unification, reflected in the adopted international documents. The second approach supporters direct all their efforts towards the three-element structure formation of the international cyber security concept, including the military and political aspects, not only as one of the components, but also as the greatest threat to the international peace and security in cyber space. Although, this approach is relatively new and is only on the first stages of being discussed by the UN, NATO and other international organizations, it is clear that ignoring the military and political aspects of international cyber security in today's realities is absolutely impossible and demands an urgent need of regulation within the international community.

References

1. Doklad Gruppy pravitel'stvennykh ehkspertov po dostizhenijam v sfere informatizacii i telekommunikacij v kontekste mezhdunarodnoj bezopasnosti, *GA OON Dokument A/65/201* (08 dekabrja 2010 goda).
<http://www.un.org/disarmament/HomePage/ODAPublications/DisarmamentStudySeries/PDF> (2015, January, 15).
2. Konvencija ob obespechenii mezhdunarodnoj informacionnoj bezopasnosti (koncepcija) (predstavlena 23 sentjabrja 2011 goda).
<http://www.mid.ru/bdomp/nsosndoc.nsf/e2f289bea6297f9c325787a0034c255/542df9e13d28e06ec3257925003542c4!OpenDocument> (2015, January, 22).
3. Krutskikh, A.V. (2004). *Tekhnologicheskij progress i sovremennye mezhdunarodnye otnoshenija.* Moskva: Prosveshchenie.
4. Pis'mo Postojannykh predstavitelej Kitaja, Rossijskoj Federacii, Tadzhikistana i Uzbekistana pri Organizacii Ob'edinjonnykh Nacij ot 12 sentjabrja 2011 goda na imja General'nogo sekretarja OON, *GA OON Dokument A/66/359 (14 sentjabrja 2011 goda).*
<http://rus.rusemb.org.uk/data/doc/internationalcoderus.pdf> (2015, January, 23).
5. *The Tallinn Manual on the International Law Applicable to Cyber Warfare, NATO Cooperative Cyber Defence Centre of Excellence* (first published 2013). <https://ccdcoe.org/249.html> (2015, January, 20).
6. *Ugoda mizh urjadami derzhav-chleniv SHOS pro spivrobitnictvo v oblasti zabezpechennja mizhnarodnoi informacijnoi bezpeki* (prijnjata 16 chervnja 2009 roku, vstupila v silu 02 chervnja 2011roku). <http://base.spinform.ru/show_doc.fwx?rgn=28340> (2015, January, 20).

Defence Centre of Excellence (first published 2013). <https://ccdcoe.org/249.html> (2015, January, 20).