Application of international humanitarian law to armed conflicts in cyberspace

© A. A. Streltsov*

Abstract: This article considers the issues of application of international humanitarian law to armed conflicts in cyberspace. The term "cyberspace" is interpreted as well as the concept of state sovereignty in cyberspace and challenges to its implementation. In addition, challenges to the application of international humanitarian law to armed conflicts in cyberspace are analysed and proposals are made on the areas of adaptation and progressive development of international humanitarian law with regard to carrying out humanitarian tasks in armed conflicts in cyberspace.

Keywords: international humanitarian law, armed conflicts, cyberspace, information and communications technologies, state sovereignty, borders, methods and means of warfare, combatants, legal protection, adaptation of international humanitarian law.

1. Relevance of the matter. While many states have been increasingly developing methods and ways of using information and communications technologies (ICTs) in military and political matters, studying the application of international humanitarian law (IHL) to armed conflicts in cyberspace is becoming more and more relevant. As pointed out by the Group of UN Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2014-2015), common understanding of the applicability of international law to the use of ICTs by states is essential to "promoting an open, secure, stable, accessible and peaceful ICT environment".[1]

When determining the areas of implementation of the public policy of the Russian Federation in the field of creating an international information security system, President of the Russian Federation V.V. Putin set the following objective: "to facilitate the preparation and adoption by the UN member states of international instruments regulating the application of the principles and rules of international humanitarian law in the use of ICTs".[2]

As experts point out,[3] application of IHL principles and rules (the law of the Hague and the law of Geneva) to armed conflicts in cyberspace is related to certain difficulties in interpreting these principles and rules. These difficulties are caused, on the one hand, by the novelty of cyberspace as a field of IHL application, and, on the other hand, by the lack of universal international treaties regulating relations in the field of using ICTs as a means of armed violence.

***Anatoly A. Streltsov,** Doctor of Engineering, Doctor of Law, Professor, Deputy Director of the Information Security Institute of Lomonosov Moscow State University.

[1] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Presented by the UN Secretary General at the 70th session of the UN General Assembly, 22 July 2015, A/70/174.

[2] Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года. 2013 г. // www.scrf.gov.ru/documents/6/114.html.

[3] Proceedings of the International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law. 17-19 November 2004. Stockholm, Sweden // https://www.icrc.org/eng/resources/documents/misc/68lg92.htm.

By way of a possible approach to overcoming the said difficulties, some experts suggest using international custom.[4] At that, the challenge of overcoming the difficulties in the interpretation of international custom applicable to armed conflicts in cyberspace essentially rests with parties to the conflict. It appears that the absence of general practice in the application of international custom to the relations under review paves the way for a state or a group of states to arrogate the right to adopt, in response to the malicious use of ICTs, certain countermeasures[5] not authorised by the UN Security Council as well as to abuse the inherent right of individual or collective self-defence provided for in Article 51 of the UN Charter.

The present article, in elaboration of joint work by A.V. Krutskikh and the author,[6] examines the characteristic features of cyberspace as a field of implementation of state sovereignty; main challenges to IHL application to armed conflicts in cyberspace; and possible areas of adaptation and progressive development of IHL with regard to furthering humanitarian goals in armed conflicts in cyberspace.

2. Cyberspace. At present, there is no universal rule or definition setting forth the term "cyberspace". International treaties of the Shanghai Cooperation Organisation and some bilateral treaties of the Russian Federation use the concept of "information space" as a field of expertise related to formation, creation, transformation, transfer, use and storage of information and affecting, inter alia, individual and public conscience, information infrastructure and information proper.[7] This concept is interpreted with regard to the field of innovative activities in the intergovernmental Agreement of the Commonwealth of Independent States.[8] The Agreement defines "information space" as "a complex of information resources, information systems and technologies, information and communications infrastructure ensuring information interaction of organisations and individuals as well as satisfying their information needs". "Information infrastructure of

---

[4] Russian-Swedish Seminar on International Information Security. 2 April 2013. Stockholm, Sweden; Eighth International Forum "State, Civil Society and Business Partnership on International Information Security", 21-24 April 2014, Garmisch-Partenkirchen, Germany; International Engagement on Cyber: Developing International Norms for a Safe, Stable and Predictable Cyber Environment. 2013 // *Georgetown Journal of International Affairs*. 10 April 2013; US-Russia Workshop on Internet Governance & Cyber Conflicts: Models, Regulations and Confidence Building Measures, 31 October - 1 November 2013, New York (USA); Manual on the International Law Applicable to Cyber Warfare (Tallinn Manual) / Ed.by M.Schmitt et al., Cambridge University Press, 2013; Peacetime Regime for State Activities in Cyberspace // International Law, International Relations and Diplomacy. Tallinn: NATO CCDCOE Publication. 2013.

[5] Draft Convention on the Responsibility of States for internationally wrongful acts // UN General Assembly Resolution 56/83 of 12 December 2001.

[6] **Крутских А.В., Стрельцов А.А.** Проблемы применения международного права к злонамеренному использованию ИКТ // Международная жизнь. 2014. № 11.

[7] Agreement among the Governments of the Shanghai Cooperation Organisation Member States on Cooperation in the Field of Ensuring International Information Security. 16 June 2009; Соглашение между Правительством Российской Федерации и Правительством Республики Беларусь о сотрудничестве в области обеспечения международной информационной безопасности, 25 декабря 2013 г. // Официальный интернет-портал правовой информации www.pravo.gov.ru, 27.02.2015, N 0001201502270007; Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности, 8 мая 2015 г.

[8] Соглашение о создании инфраструктуры инновационной деятельности государств - участников СНГ в форме распределенной информационной системы и портала СНГ «Информация для инновационной деятельности государств – участников СНГ», Минск, 19 мая 2011 г. ст. 1// Бюллетень международных договоров. 2013. № 2.

innovative activities" is regarded as "a multitude of legal entities, resources, means and other elements related and connected to each other, forming a whole designed to ensure information support of innovative activities".

In view of the above, to attain the set objective, one can agree with the opinion of the group of Russian and American experts who studied the foundations of critical terminology in the field of cybersecurity.[9] According to these experts, "cyberspace" is a part of information space and constitutes "an electronic medium through which information is created, transmitted, received, stored, processed and deleted".

As it is known, an electronic medium is formed by hardware systems ensuring the propagation of electromagnetic waves through wire and wireless communication channels for the purposes of transmitting information (communication equipment), as well as hardware systems ensuring the execution of information processing algorithms (electronic computing machines), i.e. "hardware and systems for creating, transforming, transmitting, using and storing information", which form the "information infrastructure" of the society.[10]

The Russian legislation most often unites the processes and methods of searching for, collecting, storing, processing, providing and propagating information as well as ways of implementing these processes and methods in an electronic medium in the term "information and communications technologies".[11] In Anglophone literature, this term is interpreted more generally as a concept integrating all the telecommunications, computers as well as, if need be, special and general software, storage and audio-visual systems employed by users to store, transmit and process information.[12]

Three main areas of state rule are identified in cyberspace:

− an electronic medium for collecting, transmitting, storing and processing information, formed by a complex of computer networks, telecommunication networks and information storage networks situated in the national territory;

− ICTs defining the methods and ways of use of an electronic medium to satisfy the needs of a specific actor in cyberspace (an individual, organisation, public authority as well as parties to armed conflicts and members of criminal, including terrorist, organisations), related to collecting, transmitting, storing, receiving or disseminating information;

− local and distributed information systems, systems of computer-aided production and personnel management.

---

[9] Russia – US Bilateral on Cybersecurity. Critical Terminology Foundations. EastWest Institute Worldwide Cybersecurity Initiative. Information Security Institute of Moscow State University. November 2013.

[10] Agreement among the Governments of the Shanghai Cooperation Organisation Member States on Cooperation in the Field of Ensuring International Information Security. 16 June 2009; Соглашение между Правительством Российской Федерации и Правительством Республики Беларусь о сотрудничестве в области обеспечения международной информационной безопасности, 25 декабря 2013 г.; Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности, 8 мая 2015 г.

[11] Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г.№149-ФЗ // Собрание законодательства РФ. Вып. № 31, 2006. Ст. 3448.

[12] See https://en.wikipedia.org/wiki/Information_and_communications_technology.

An important feature of cyberspace is its global nature that ensures the possibility of information interaction between people and objects situated in the territory of different states. The global nature of cyberspace is attained through combining national electronic media into a single electronic medium for collecting, transmitting, storing and processing information, based on unified digital address system of actors and objects in cyberspace.

In the absence of universal international treaties, international legal regulation of relations in the digital address system is conducted based on international custom as evidence of a general practice accepted as law.

An example of such custom is the activities carried out by the Internet Corporation for Assigned Names and Numbers (ICAAN), an American non-governmental organisation, to support and develop the system of distribution and use of digital address space (domain name system). This system ensures creation and keeping up-to-date the global space of digital addresses (domain names) of actors and objects in global cyberspace. This lays the groundwork for the use of the resources of national cyberspaces for the purposes of implementing ICTs of various actors in the life of society and state.

An important consequence of the application of the international custom under consideration to regulation of international relations is the absence in cyberspace, contrary to other "traditional" spatial dimensions, of state sovereignty of national borders or international agreements concerning the allocation of address space between states and, accordingly, their connection to objects of information infrastructure situated in the national territories. This is largely due to the fact that the ICANN is not an international intergovernmental organisation and, therefore, is not a subject of international law. Consequently, it has neither international legal capacity, nor international capacity to act or passive dispositive capacity.

As it is known, maintenance of the digital address space system (domain names system) and ensuring the continuity of the process *de jure* do not fall within the scope of the US state sovereignty and their international legal personality in the field of cyberspace. Hence, it can be stated that there is no actor in the system of international relations that would bear international responsibility for ensuring the stability of global cyberspace against political risks, which have significantly increased in the contemporary system of international relations.

There is another important consequence of the application of the international custom under consideration to regulation of relations in the field of maintaining a unified system of digital addresses (domain names) in a unified electronic medium. It consists in the fact that the USA have *de facto* extended their state sovereignty to the regulation of matters related to ensuring the unity of the global electronic medium, the stability of connection of national electronic media as well as information interaction between nationals of different states, the use of resources of national information infrastructures for the implementation of ICTs in the interests of actors in various spheres of the life of society. At the same time, other states of the world are unable to ensure complete state rule in national cyberspace. Moreover, there is ambiguity as to the state jurisdiction in matters of control over the national electronic medium.

This problem cannot be solved by putting in place a mechanism for defining state borders in cyberspace through connecting objects of information infrastructure to the national

territory, as suggested by some experts,[13] as it will not remove the cause of the problem under consideration.

Hence, it can be pointed out that in order to build international relations in global cyberspace based on the principle of equal sovereignty, which is one of the most important principles of international law, it appears expedient to codify the rules regulating international relations in global cyberspace.

3. Armed conflict in cyberspace and IHL application. International armed conflict and armed conflict of a non-international nature (hereinafter – armed conflict) are, primarily, a confrontation of large social groups of population taking place in the territory of several states or one state and involving armed forces and, possibly, militias or volunteer units meeting certain requirements.[14]

As it is known, IHL is a system of international legal principles and rules regulating relations between subjects of international law for the purposes of carrying out humanitarian tasks necessitated by the armed conflicts.[15] Several important aspects of IHL application to armed conflicts in cyberspace can be singled out:

– the territory, in which armed confrontation is taking place;
– methods and means employed in armed confrontation;
– international legal status of parties to an armed conflict;
– legal protection of persons and objects during an armed conflict;
– responsibility for violations of IHL.

Let us consider the above aspects of IHL application to armed conflicts in cyberspace.

Territory of an armed conflict is limited to the territory of the state (states) involved in the conflict.[16] This territory is separated from the territories of non-belligerent states based on international treaties on state borders concluded with neighbouring states according to the results of border delineation. For that matter, the existence of state borders makes it possible to take measures to localise a conflict within the borders of opposing states.

Armed confrontation in cyberspace and, most notably, in the global electronic medium makes it possible to "affect by means of a weapon" any object whose digital address is included in the unified space of digital addresses (domain names) regardless of its "connection" to objects of information infrastructures situated in the territory of national states. The absence of a "mapped connection" between objects of the national information infrastructure and objects of community infrastructure makes it considerably challenging for belligerent parties to observe such principles of IHL as distinguishing between civilians and military personnel; prohibition of attacks against persons taking no part in the hostilities; prohibition of causing unnecessary suffering; principle of proportionality; principle of necessity; principle of humanity. For the same reason, considerable difficulties are encountered by belligerent states in fulfilling their

[13] Manual on the International Law Applicable to Cyber Warfare (Tallinn Manual) / Ed. by M. Schmitt et al. New York: Cambridge University Press, 2013.

[14] Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field. Geneva, 12 August 1949. Art. 14.

[15] **Бекяшев К.А.** Международное гуманитарное право // Международное право. Учебник. М.: Проспект, 2015. С. 305.

[16] Convention respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. The Hague, 18 October 1907. Section III.

international obligations with regard to neutral states as well as by neutral states in fulfilling their obligations with regard to states involved in an armed conflict.

It is important to note that the existing system of supporting the digital address space (domain names system) gives the USA quite an abundant scope for manipulating the digital address space (domain names) of national electronic media of states involved in an armed conflict.

An important element of international legal regulation of relations in an armed conflict is the restriction of **methods and means of armed confrontation,** i.e. the restriction of the choice of weapons, other technical means of destroying the enemy as well as methods of using weapons and other technical means in hostilities.

As it is known, the term "weapon" in its conventional sense denotes "any means suited or technically usable for attack or defence as well as the totality of such means."[17] Experts are virtually unanimous in the opinion that, from a legal point of view, ICTs are neither weapons nor a technical means altogether. Russian specialized literature often considers the term "ICTs" as a synonym of the concept of "information technologies". As pointed out above, the Russian legislation understands "information technologies" as "the processes and methods of searching for, collecting, storing, processing, providing and propagating information as well as ways of implementing these processes and methods." In Anglophone specialized literature this term is interpreted more generally as a concept integrating all the telecommunications, computers and, if need be, special and general software, storage and audio-visual systems employed by users to store, transmit and manipulate information.[18] From this point of view, ICTs cannot be classified as "weapons", i.e. means (devices) designed to cause damage to life and health or to serve as a means of attacking or defending human beings.

Nevertheless, regional and bilateral international treaties of the Russian Federation have already set forth a number of concepts, which reflect states' concerns as to the possible hostile use of ICTs to seriously harm their national interests. Thus, Russia's Agreements with the Republic of Belarus and the People's Republic of China on cooperation in the field of international information security introduce the concept of "information weapons", which is defined as "information technologies, means and methods used for the purposes of information warfare." The term "information warfare", in its turn, is defined as "a confrontation between two or more states in information space, aimed at damaging information systems, processes and resources, critically important and other structures, undermining political, economic and social systems, massively brainwashing the population to destabilize society and government as well as compelling the state to take decisions in the interests of the opposing party."

The 2015 international treaty between the RF Government and the Government of the People's Republic of China sets forth the concept of "computer attack", defined as "a deliberate interference, using software (software and hardware) tools, with information systems, information and telecommunications networks, electronic communication networks and automated process control systems, conducted for the purposes of disrupting (putting a stop to) their functioning and/or jeopardizing the safety and security of the processed information."

---

[17] Ожегов С.И. Словарь русского языка. М.: Русский язык, 1986. С. 394. (Ozhegov's *Russian Language Dictionary*).

[18] See https://en.wikipedia.org/wiki/Information_and_communications_technology.

According to many experts, malicious use of ICTs can cause harm sometimes comparable to the effects of traditional weapons and in a number of cases to those of weapons of mass destruction,[19] and from this point of view, such use of ICTs constitutes a serious threat to international peace and security and should activate states' inherent right of self-defence in the meaning of Art. 51 of the UN Charter.

It appears that ICTs can cause such harm only if they are used to disrupt processes and methods of controlling high-risk facilities as well as hazardous production facilities and other units and installations containing dangerous forces, which, should the operating protocols be violated, may cause danger of severe losses among the civilian population, real danger to life and health or to the environment.

The possibility of weaponizing regular (non-specialized) technical means through their improper use was employed by terrorists when carrying out the attacks of 11 September 2011 in the USA. This occasion enabled the US government, with the support of the international community,[20] to declare its right of individual and collective self-defence and to commence armed actions against Afghanistan accused of supporting the terrorists. Thus, the terrorist attack of 11 September 2001, using the airplanes hijacked by terrorists, was *de facto* equated to "an armed attack" in the meaning of Article 51 of the UN Charter. Obviously, this decision somewhat expands the interpretation of the term "arms" or "weapon", which has come to include devices that, in certain circumstances, take on the properties of "weapons". This type of weapons may be designated as "virtual weapons".[21]

Conditions, in which malicious use of ICTs turns a certain object or device into a "virtual weapon", may include:

– ability to damage (destroy) personnel and materiel in case their normal (proper) functioning is disrupted;

– presence in a device or object of information or communications systems capable of implementing an act of ICT malicious use causing damage to personnel and materiel;

– availability of an ICT designed to turn a non-military device or object into a weapon.

At present, there are no IHL rules restricting the use of ICTs in an armed conflict, despite the fact that their hostile use can cause superfluous injury or have indiscriminate effect.

It appears that introduction, as suggested by some experts, of the legal term "cyber operation", defined as "the employment of cyber capabilities with the primary purpose of achieving objectives", plays no significant role in filling this gap.[22] This definition essentially refers to the use of an electronic medium to implement ICTs capable of causing intentional damage to personnel and materiel. It is implied, at that, that ICTs exist, which are designed to achieve the intended goal.

---

[19] **Hoizington M**. Cyberwarfare and the use of Force Giving Rise to the Right of self-Defense // 32 B.C. Int'l &Comp.L. Rev. 432 (2009). V. 32. Article 16.

[20] Provisional record of 4370th meeting of the UN Security Council of 12 September 2001; Provisional record of 4375th meeting of the UN Security Council of 18 September 2001; Resolution 1368 of the UN Security Council of 12 September 2001; Resolution 1373 of the UN Security Council of 28 September 2001, etc.

[21] **Стрельцов А.А.** Основные направления развития международного права вооруженных конфликтов применительно к киберпространству // Право и государство. 2014. №3.

[22] Manual on the International Law Applicable to Cyber Warfare (Tallinn Manual).

An important aspect of IHL is determining **the international legal status of participants in an armed conflict**. In this area, relations are regulated, which are related to the international legal status of members of the armed forces and groups representing parties to a conflict that are actors responsible for the use of weapons and other technical means as a means of armed violence.

Under the rules of international law, these actors should meet, at least, the following requirements:[23]

– being commanded by a person responsible for his subordinates;
– carrying arms openly;
– conducting their operations in accordance with the laws and customs of war.

These requirements determine the legal characteristics of combatants entitled, under certain circumstances, to the legal protection under the rules of IHL.

Application of these IHL rules to participants in an armed conflict in cyberspace makes it apparent that the requirement that combatants carry openly the weapons used for armed violence cannot be met. Furthermore, the "virtual" nature of ICTs as a means of armed confrontation enables states to incite participation therein of any individuals with the necessary skill set and access to the global electronic medium and objects of global information infrastructure.

Thus, the international legal status of participants in an armed conflict in cyberspace so far remains indeterminate.

Another aspect of IHL application to armed conflicts in cyberspace is **legal protection of persons and objects during an armed conflict**. This legal protection through guaranteed conferment of a certain amount of rights is provided to all the persons who do not take or no longer take a direct part in the hostilities and find themselves in the power of an adverse party or in the territory of an armed conflict. Persons who enjoy this legal protection include the wounded, sick and shipwrecked; prisoners of war; women; children; journalists; civilians.

General legal protection is also provided by IHL to civilian objects, including critically important objects of infrastructure and cultural property.

Observance by parties to an armed conflict in cyberspace of the rights of persons listed above and ensuring the legal protection of relevant objects is largely limited by the impossibility of their identification in an electronic medium. This is attributable to the lack of international legal confirmation of characteristics of objects of the electronic medium and other objects of the information infrastructure of opposing states, which are related to the enjoyment of rights guaranteed by IHL or to the conferment of the appropriate legal protection.

---

[23] Convention respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. The Hague, 18 October 1907. Art. 1; Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field. Geneva, 12 August 1949. Art. 13; Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977. Art. 44.

Finally, an important aspect of international legal regulation of relations in the field of armed conflicts in cyberspace is **responsibility for violations of IHL.** In accordance with international treaties, a party to a conflict that violates the provisions of the 1949 Geneva Conventions or their Additional Protocols,[24], is liable to pay compensation, if the case demands. A state is responsible for violation of IHL rules both politically and financially, in the form of restitution and compensation.[25]

An International Fact-Finding Commission was established under Art. 90 of the Additional Protocol to the 1949 Geneva Conventions to enquire into any facts alleged to be a grave breach as defined in the Conventions and the Protocol or other serious violation of IHL.

Investigation of IHL violations in cyberspace is related to the necessity of performing the following activities:

– discovering signs of an IHL violation;

– identifying actors responsible for the hostile use of ICTs in the cyberspace of the opposing state (states), which has led to the violation of IHL;

– discovering, documenting and analysing electronic "traces" of the activities of participants in the armed conflict in cyberspace involved in the IHL violation as well as detecting the ICT, the use of which constitutes *actus reus* of the international offence;

– determining whether actors responsible for the hostile use of ICTs in cyberspace belong to the armed forces of states involved in the armed conflict or to opposition armed forces or other organised armed groups involved in the conflict;

– classifying the IHL violations and duly prosecuting the perpetrators.

The International Fact-Finding Commission would carry out the activities listed above based, primarily, on the interaction with actors ensuring the functioning of the national information infrastructure, analysis of information arrays containing information related to the activities of actors using information technologies.

National law enforcement mechanisms and agencies of many states of the world have already accumulated certain experience in carrying out relevant investigatory actions in national cyberspaces within the framework of national legislation and regional international legal acts in the field of combatting cybercrime. At the same time, the possibilities of utilizing this experience in the work of the International Fact-Finding Commission appear to be quite limited. This can be explained, first of all, by the disinterest of states involved in an armed conflict in conducting such investigations and the possibility of information containing "traces" of cyberspace activities being manipulated both by states parties to a conflict and by other states concerned.

4. Proposals. Several areas of adaptation and progressive development of IHL principles and rules with regard to cyberspace can be identified:

– formalizing in international treaties the content of state sovereignty in national cyberspace, including in the area of management of the address space of global cyberspace and its national segment;

– determining the procedure for delimiting of and delimiting the borders of national cyberspaces and formalizing the borders of these spaces in corresponding international treaties;

---

[24] Protocol I Additional to the Geneva Conventions of 12 August 1949, 8 June 1977. Art. 91.

[25] **Соколова Н.А.** Международное гуманитарное право // Международное право / Отв. ред. К.А. Бекяшев. М.: Проспект, 2015. С. 315.

– determining the objects, including critically important ones, of the public information infrastructure, which enjoy legal protection under IHL;

– drawing up and keeping up-to-date "maps" of connection of objects of national information infrastructure enjoying legal protection under IHL;

– specifying the conditions for conferring the international legal status of combatants on persons who carry out acts of hostile use of ICTs as a means of armed violence, being members of state armed forces or other armed groups involved in an armed conflict;

– specifying the signs of the hostile use of ICTs as a means of armed violence against the adversary, persons and objects protected by IHL;

– improving the procedure and conditions of the enquiry into the facts of IHL violations by the International Fact-Finding Commission;

– determining the expedience of establishing an international system for objectification of events related to the use of ICTs in armed conflicts in order to create conditions conducive to the accomplishment of tasks entrusted to the International Fact-Finding Commission.

Formalization of the corresponding legal innovations in each of the identified areas in universal international treaties will be conducive to ensuring the applicability of the rules of international law to the use of ICTs based on the principle of equal sovereignty, to strengthening common understanding for the purposes of increasing stability and security in global cyberspace, to developing consistent practice of IHL application to armed conflicts in cyberspace as well as methods of assessing the legality of the use of ICTs as a means of armed violence in the hostilities in the "traditional" spheres of the use of armed forces.

References

Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Presented by the UN Secretary General at the 70th session of the UN General Assembly, 22 July 2015, A/70/174.

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.

Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field. Geneva, 12 August 1949.

Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года. (Outlines of the Public Policy of the Russian Federation in the Field of International Information Security until 2020) 2013 г. // www.scrf.gov.ru/documents/6/114.html.

Convention respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. The Hague, 18 October 1907.

Provisional record of 4370th meeting of the UN Security Council of 12 September 2001.

Provisional record of 4375th meeting of the UN Security Council of 18 September 2001.

Draft Convention on the Responsibility of States for internationally wrongful acts // UN General Assembly Resolution 56/83 of 12 December 2001.

Resolution 1368 of the UN Security Council of 12 September 2001;

Resolution 1373 of the UN Security Council of 28 September 2001.

Agreement between the Governments of the Member States of the Shanghai Cooperation Organisation on Cooperation in the Field of International Information Security. 16 June 2009 (unofficial English translation can be found at: https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreement.pdf).

Соглашение между Правительством Российской Федерации и Правительством Республики Беларусь о сотрудничестве в области обеспечения международной информационной безопасности от 25 декабря 2013 г., Москва (Agreement between the Government of the Russian Federation and the Government of the Republic of Belarus on Cooperation in the Field of International Information Security, 25 December 2013. Moscow) // Официальный интернет-портал правовой информации www.pravo.gov.ru, 27.02.2015, N 0001201502270007.

Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности от 8 мая 2015 г., Москва. (Agreement between the Government of the Russian Federation and the Government of the People's Republic of China on Cooperation in the Field of International Information Security, 8 May 2015. Moscow)

Соглашение о создании инфраструктуры инновационной деятельности государств-участников СНГ в форме распределенной информационной системы и портала СНГ «Информация для инновационной деятельности государств - участников СНГ» от 19 мая 2011 г. (Agreement on the Establishment of Infrastructure for Innovative Activities of the CIS Member States in the Form of Distributed Information System and CIS Portal "Information for Innovative Activities of the CIS Member States" of 19 May 2011.) // Бюллетень международных договоров. 2013. № 2.

Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. №149-ФЗ (Federal Law No. 149-ФЗ of 27 July 2006 *On Information, Information Technologies and Protection of Information*) // Собрание законодательства РФ. Вып. № 31, 2006. Ст. 3448.

https://en.wikipedia.org/wiki/Information_and_communications_technology

Eighth International Forum "State, Civil Society and Business Partnership on International Information Security", 21-24 April 2014, Garmisch-Partenkirchen, Germany.

Бекяшев К.А. Международное гуманитарное право // Международное право. Учебник. (K.A. Bekyashev. International Humanitarian Law // *International Law. A Textbook*.) М.: Проспект, 2015.

Крутских А.В., Стрельцов А.А. Проблемы применения международного права к злонамеренному использованию ИКТ (A.V. Krutskikh, A.A. Streltsov. Challenges to the Application of International Law to Malicious Use of ICTs.) // Международная жизнь. 2014. № 11.

Ожегов С.И. Словарь русского языка. М.: Русский язык, 1986. С. 394. (Ozhegov's *Russian Language Dictionary*).

US-Russia Workshop on Internet Governance & Cyber Conflicts: Models, Regulations and Confidence Building Measures, 31 October - 1 November 2013, New York (USA)

Russian-Swedish Seminar on International Information Security. 2 April 2013. Stockholm, Sweden.

Соколова Н.А. Международное гуманитарное право (N.A. Sokolova. International Humanitarian Law.) // Международное право / Отв. ред. К.А. Бекяшев. М.: Проспект. 2015.

Стрельцов А.А. Основные направления развития международного права вооруженных конфликтов применительно к киберпространству (A.A. Streltsov. Main Areas of Development of International Law of Armed Conflicts in Connection with Cyberspace.) // Право и государство. 2014. № 3.

Hoizington M. Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense // 32 B.C. Int'l &Comp.L. Rev. 432 (2009). V. 32. Article 16.

International Engagement on Cyber: Developing International Norms for a Safe, Stable and Predictable Cyber Environment. 10 April 2013 // Georgetown Journal of International Affairs. 2013.

Manual on the International Law Applicable to Cyber Warfare (Tallinn Manual) / Ed. by M. Schmitt et al. Cambridge University Press, 2013.

Peacetime Regime for State Activities in Cyberspace // International Law, International Relations and Diplomacy. Tallinn: NATO CCDCOE Publication, 2013.

Proceedings of the International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law. 17-19 November 2004. Stockholm, Sweden.

Russia – US Bilateral on Cybersecurity. Critical Terminology Foundations. EastWest Institute Worldwide Cybersecurity Initiative, Information Security Institute of Moscow State University. November 2013.