Problems of Typology of Armed Conflicts in Cyberspace

Sergei Garkusha-Bozhko

Legal Adviser, Saint Petersburg School of Higher Sportmanship in Water Sports. Address: 10/1 Grebnoy Channel Embankment, Saint Petersburg 197110, Russian Federation. E-mail: garkusha-bozhko.sergej@yandex.ru

Abstract

The development of information technologies in the modern world affects all spheres of human activity, including the sphere of military activities of states. The current level of development of military information technologies allows us to talk about a new fifth possible theatre of military operations, namely, cyberspace. The Tallinn Manual on International Law Applicable to Cyber Operations, developed in 2013 and updated in 2017 by experts from the NATO States, also confirms the likelihood of armed conflict in cyberspace. It is indisputable fact that cyber operations committed in the context of an armed conflict will be subject to the same rules of International Humanitarian Law that apply to such armed conflict. However, many cyber operations that can be classified as military operations may be committed in peacetime and are common cybercrimes. In such circumstances, it is imperative to distinguish between such cybercrimes and situations of armed conflict in cyberspace. Due to the fact, that there are only two types of armed conflict — international and non-international, this problem of differentiation raises the question of the typology of armed conflicts in relation to cyberspace. The main questions within the typology of cyber armed conflicts are: whether an international armed conflict can start solely as a result of a cyber-attack in the absence of the use of traditional armed force; and how to distinguish between ordinary criminal behaviour of individuals in cyberspace and non-international armed conflict in cyberspace? The purpose of this article is to provide answers to these urgent questions. The author analyses the following criteria that play a role in solving the above problems: criteria for assigning a cyber attack to a state and equating such a cyber-attack with an act of using armed force in a cyber armed conflict of an international character; and criteria for the organization of parties and the intensity of military actions in a non-international cyber armed conflict. Based on the results of this analysis, the author gives relevant suggestions for solving the above issues.

Keywords

cyberspace; Tallinn Manual; International Humanitarian Law; armed conflict; cyber-operation; cyber-attack.

For citation: Garkusha-Bozhko S. Yu. (2021) Problems of Typology of Armed Conflicts in Cyberspace. *Legal Issues in the Digital Era*, no 2, pp. 82–103.

DOI: 10.17323/2713-2749.2021.2.82.103

Introduction

The development of information technologies affects all spheres of human activity and the military activity of states is not an exception. The current level of development of military technologies allows us to speak about possible spread of military operations to cyberspace. In other words, in the modern world, an armed conflict in cyberspace is no more an invention of science fiction writers and screenwriters of fantastic entertainment films — now it is a potential conflict that can begin due to the collision of interests of two or more states in the cybersphere. The likelihood of such a conflict is also recognized in the statement of Russian President Vladimir Putin, who noted that "one of the main strategic challenges of our time is the risk of a large-scale confrontation in the digital sphere."[1]

As noted in the doctrine [Melzer N., 2017: 51], cyberspace is now "the fifth domain of warfare" after land, sea, air and outer space. This statement cannot be challenged for the reason that, due to the level of development of modern technologies, cyberspace is, in fact, a potential theater of military operations. The high likelihood of such armed conflicts forced states to think about the legal regulation of such conflicts, and in 2013, thanks to the efforts of lawyers and military specialists from NATO countries, with the participation of specialists from the International Committee of the Red Cross (ICRC), the Tallinn Manual on the International Law Applicable to Cyber Warfare was adopted.

This Manual is an attempt to develop norms of international law applicable not only to this type of armed conflict, but also to cyberspace in general, both in wartime and in peacetime. The need for this kind of international law is very high, which led to the adoption of a new expanded version of this manual in 2017 (Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations).

The key point in the application of international humanitarian law to cyberspace is the fact that cyber operations are carried out in the context of an armed conflict or in connection with it. This conclusion is not contested in

[1] Vladimir Putin on the complex set of measures to restore Russian-American cooperation in the field of international information security. Available at: URL: http://kremlin.ru/events/president/news/64086 (accessed: 01.04.2021)

the doctrine [Droege C., 2014: 12]; [Streltsov A.A., 2014: 84]; [Schmitt M., 2002: 133]; [Schmitt M., 2019: 334]; [Schmitt M.. 2014: 191]; [Döge J., 2010: 491]. In other words, cyber operations carried out in the context of an armed conflict would be governed by the same rules of IHL as this conflict.

However, despite the obviousness of the above conclusion, many cyber operations that can be qualified as military operations in cyberspace can be carried out in the absence of any armed conflict. For example, we often see media reports of cyber attacks or acts of cyber terrorism that take place in times of peace[2]. In addition, various cyber operations can be trivial cyber crimes. As we know, there is already an international treaty addressing the cybercrime — the Convention on Cybercrime (Budapest, 2001).[3]

The above examples of hostile cyber operations emphasize the problem of their delimitation from armed conflicts in cyberspace. This problem can also be illustrated by an example where cyber operations are the only hostile actions carried out against a particular state.

We are talking here about such an example as the Stuxnet virus, which was aimed at disrupting the normal operation of a uranium enrichment plant in the Islamic Republic of Iran, the city of Netense. This case is one of the clearest examples of long-term hostile impact on state information systems. As it was later established, this virus was developed with the participation of experts from the security services of the United States and Israel, and its goal was the Iranian nuclear program.[4]

States, in particular Iran, did not qualify this situation related to the Stuxnet virus as an armed attack. However, the legal doctrine suggested that if a certain state was behind this virus, this situation can be qualified as an international armed conflict in cyberspace [Schmitt M., 2012: 252]. Thus, G. Brown explicitly states that the Stuxnet virus is a cyber attack, since it represents violation of the fundamental international legal principle of the non-use and threat of force, as well as in violation of *jus in bello* [Brown G., 2011: 71]. Based on such statements in the doctrine, the

[2] See, e.g. DDoS-attacks on the web-sites of the Ministry of Internal and KGB of the Republic of Belarus. Available at: https://iz.ru/1045947/2020-08-09/v-belorussii-soobshchili-o-ddos-atakakh-na-saity-kgb-i-mvd (accessed: 01.04.2021). Cyber-terrorists attacked the computers of Rosneft Oil Company. Available at: https://tvzvezda.ru/news/vstrane_i_mire/content/201706271530-owel.htm (accessed: 01.04.2021)

[3] Budapest Convention on Cybercrime, 2001. European Treaty Series. No. 185.

[4] Stuxnet was work of U.S. and Israeli experts, officials say. Available at: https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html (accessed: 01.04.2021)

thought may well arise about possible cyber attacks carried out by a non-governmental group against the government of a particular state, which will entail the question of the possible qualification of such a situation as a non-international armed conflict in cyberspace.

In such conditions, in order to solve this problem of delimiting situations of ordinary criminal cyber operations from situations of cyber armed conflicts, it is necessary to analyze the typology of such armed conflicts. As it is well known, there are only two types of armed conflict: international and non-international one. Their criteria are well enough studied and described in the doctrine, so we will not delve into the general typology of armed conflicts, but will limit ourselves to examining those aspects that poses problems to qualifying cyber operations in the context of armed conflicts. Let's start with an international cyber armed conflict.

1. International cyber armed conflict

Let's recall that, according to the Article 2 that is common for three Geneva Conventions of 1949, an international armed conflict means any case of "declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them. "[5] This provision is the only treaty definition of an international armed conflict. Paragraph 4 of Article 1 of Additional Protocol I supplemented this definition, referring to this type of armed conflict also situations of armed conflict "in which peoples are fighting against colonial domination and alien occupation and against racist régimes in the exercise of their right of self-determination, as enshrined in the Charter of the United Nations and the Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations".[6]

However, one must assume that the struggle against colonialism is already a thing of the past, and the exercise of the right to self-determination by peoples is unlikely to take place in cyberspace. Therefore, we will not take this addition into account and will consider an international armed conflict solely as a situation where armed forces are used between sovereign states, as clearly indicated by the International Tribunal for the former

[5] Geneva Convention for the amelioration of the condition of the wounded and sick in armed forces in the field. 1949. UNTS 970.

[6] Protocol additional to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of international armed conflicts (Protocol I). 1977. UNTS 17512.

Yugoslavia[7]. The authors of the Tallinn Manual proceeded from the same message, stating in Rule 82 that "[cyber] international armed conflict occurs whenever military action occurs between two or more states, which may include or be limited to cyber operations" [Tallinn Manual 2.0, 2017: 379]. As can be seen from the above, the issue of qualifying an armed conflict, including a cyber conflict, as an international one depends on the very fact of such a conflict, and not on the fact that the parties recognize the state of an armed conflict.

The key problem of the legal qualification of an international armed conflict in cyberspace is the question of whether such an armed conflict can start solely as a result of a cyber attack in the absence of the use of traditional armed force? The solution to this issue is influenced by two main criteria: 1) attribution of a cyber attack to the state and 2) equating such a cyber attack with the use of traditional armed force. In other words, these criteria require an answer to questions about whether such a cyber attack is attributed to a particular state; and whether it leads to the same consequences as the traditional use of military force.

1.1. Attribution of a cyber attack

Let's start with the first criterion. On the one hand, the attribution of a particular cyber attack or cyber operation to a particular state is an intractable problem due to the anonymity of users in cyberspace. But, on the other hand, until it is established that states are both the perpetrators of this cyber attack and the victims of it, there can be no question of qualifying the situation as an international armed conflict.

Of course, it should be kept in mind that this problem is more factual than legal in its nature, and it is indicated in the legal doctrine [Droege C., 2014: 14]; [Zhang L., 2012: 804]; [Tsagourias N., 2012: 233]; [Döge J., 2010: 500–501]; [Hathaway O., Crootof R. et al., 2012: 856]. One of the proposed ways to solve this problem is to use legal assumptions [Lin H., 2012: 521]. For example, it must be assumed that a cyber attack is attributed to a state if it originated from IT infrastructure owned by the government of that state.

However, such an approach based on legal assumptions is not consistent with the norms of international law for the following reasons. First, the Articles on Responsibility of States for Internationally Wrongful Acts

[7] *Prosecutor* v. *Dusko Tadić*. Case № IT-94-1-T. ICTY Appeals Chamber Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction of 2 October 1995. Para. 70.

(hereinafter — Articles on Responsibility of States) do not provide for the use of such assumptions for attribution of wrongful acts to a State[8]. In this regard, it is necessary to recall the decision of the International Court of Justice (ICJ) in the case «On oil platforms (Islamic Republic of Iran v. United States of America)», in which the Court established a sufficiently high threshold for attributing behavior to a state in the context of the right to self-defense. Specifically, the UN ICJ noted: «… the court must simply determine whether the United States has demonstrated that it was the victim of an" armed attack " by Iran in order to justify its use of armed force in self-defense; and the burden of proof of the existence of such an attack rests with the United States»[9].

Of course, this decision of the ICJ was made on the issue of the state's right to self-defense, i.e. in the context of *jus ad bellum*. However, we believe that this rule, derived by the International Court of Justice, is applicable to all questions of fact when attributing behaviour to a state, since attribution should be based on facts and not on assumptions. In addition, the attribution of a cyber attack to a state also raises questions, including in the context of the jus ad bellum, which once again proves the applicability of this ICS decision to cyberspace.

Second, the use of legal assumptions in relation to the attribution of cyber operations to a particular state is not possible due to the risks that exist in cyberspace. In particular, due to the risks of manipulation, the use of VPN technology and the possibility of remote control over the information system under a false name.

Of course, there is a point of view in the doctrine that the attribution of a cyber operation to a specific state is possible through the use of various intelligence data [Lin H., 2012: 522], however, it must be assumed that due to these risks, one cannot be completely sure of the reliability of such data.

Based on this, it is obvious that the burden of responsibility imposed on the state for all cyber operations carried out using the information infrastructure of such a state, in the absence of other evidence, would be excessive. This conclusion is also supported by the developers of the Tallinn Manual: in paragraph 13 of the commentary to Rule 15, which enshrined the regulation on the appropriation of cyber operations carried out by state

[8] Draft articles on. Responsibility of States for Internationally Wrongful Acts. Adopted by General Assembly Resolution No. 56/83 on 12.12.2001. Available at: https://undocs.org/pdf?symbol=ru/A/RES/56/83 (accessed: 01.04.2021)

[9] Oil Platforms (Islamic Republic of Iran v. United States of America). ICJ Judgment. 6 November 2003 // I. C. J. Reports. 2003. P. 161. Para 57.

bodies, the developers noted that «The mere fact that operations in cyberspace were launched or otherwise emanated from government infrastructure, or that malware used against a compromised information infrastructure is designed to "report" to another country's government infrastructure, is usually not sufficient evidence that that the operation should be assigned to the state. However, such use may serve as an indication that the State in question may be associated with the operation.» [Tallinn Manual 2.0, 2017: 91].

Another problem discussed in the doctrine [Droege C., 2014: 15]; [Backstrom A., Henderson I., 2012: 503, 505], arising in the framework of attribution of a cyber attack to the state, is the problem of appropriation of cyber attacks by the state, committed by private individuals, or as they are also called in the media — hackers or hacker groups. This problem is of particular importance in cyberspace due to the prevalence of user anonymity in it. Let us turn to the Articles on State Responsibility, Article 8 of which stipulates the following: «The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct».[10]

When analyzing this rule of the Articles on State Responsibility, the question arises: what does the wording «under instructions or under the direction or control» mean? In this regard, the International Court of Justice noted that in order for the conduct of an individual or an organized group to be attributed to the state, the state must exercise effective control over the operation during which the alleged offenses were committed, which must be demonstrated in relation to all unlawful acts committed by such individuals.[11] If such effective control is not exercised by the state over a specific operation, then such an operation cannot be attributed to such a state, even if this operation was carried out by a person (group of persons) whose degree of dependence on the authorities of such a state was very high.[12]

[10] *Draft articles* on. *Responsibility* of *States* for Internationally Wrongful Acts. Adopted by General Assembly Resolution No. 56/83 on 12.12.2001. Available at: https://undocs.org/pdf?symbol=ru/A/RES/56/83 (accessed: 01.04.2021)

[11] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Merits. ICJ Judgment of 27 June 1986 // I.C.J. Reports 1986. P. 14. Para 115–116; Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro). ICJ Judgment of 26 Feb. 2007 // I.C.J. Reports. 2007. P. 43. Para 400 — 406.

[12] Military and Paramilitary Activities in and against Nicaragua… Para. 115

The United Nations International Law Commission (UN ILC), in para 3 of its commentary on Article 8 of the Articles on State Responsibility, spoke in the same vein: the UN ILC points out that attributing conduct to a state in accordance with Article 8 requires that the state be in control of a particular operation and that the conduct in question must be an integral part of that operation.[13]

The International Criminal Tribunal for the former Yugoslavia has taken a completely different view on this issue. In particular, in the decision of his Appeals Chamber in the well-known Tadić case, he stated that if a group, such as a rebel armed group, has a degree of organization sufficient for a certain state to exercise so-called «general control» over such an organization with the necessary level of organization and hierarchical structure, then it is not necessary to establish the fact of effective control over specific operations — to attribute the behaviour of such a group to the state, general control is sufficient.[14] However, the ICTY also added to the above statement that if the state exercising control is not a territorial state, then more extensive and conclusive evidence is needed that the state does exercise control over individuals and groups, and this means that the participation of such a state in the leadership the operations of such individuals and groups will be difficult to demonstrate.[15]

In response to this statement by the ICTY, the International Law Commission, in para 5 of the commentary to Article 8 of the Articles on State Responsibility, noted that the question of the degree of control on the part of a particular state over certain behaviour, which is necessary for attributing such behaviour to a state, should be decided on the basis of actual circumstances of each individual case.[16]

Of course, the above discussion is not directly related to cyberspace. However, it must be assumed that this discussion sets out the basic principles that should be followed when deciding the question of attributing the behaviour of individuals to the state. In our opinion, there is no reason to deny their applicability to cyberspace, in particular, to the issue of

[13] ILC Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries. Adopted in 2001 // Yearbook of the International Law Commission. 2001. Vol. II. Part Two. P. 47.

[14] *Prosecutor* v. *Dusko Tadić*. Case № IT-94-1-A. ICTY Appeals Chamber Judgement of 15 July 1999. Para 120.

[15] Ibid. Para 138–140.

[16] ILC Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries. Adopted in 2001 // Yearbook of the International Law Commission. 2001. Vol. II. Part Two. P. 48.

appropriation of cyber operations. The problem here lies elsewhere — in the issue of identifying such individuals — due to the already mentioned problem of anonymity, it will be quite difficult to establish them for sure, and this difficulty, most likely, will lie in assessing the actual circumstances of the cyber operation.

Obviously, one of the solutions that can be proposed here is to involve technical specialists to solve the problem of anonymity. However, in our opinion, this will not be enough for the reason that there is still little interstate practice in this field, from which it would be possible to derive specific criteria for attribution of behavior in cyberspace. Therefore, in such a situation, states need to develop appropriate practice on this issue.

1.2. The use of armed force

Let's move on to the second criterion, which must be satisfied in order to establish the fact of the existence of an international armed conflict in cyberspace — to the criterion of the use of armed force between two or more states.

Before starting the study of this criterion, it is necessary to make the following remark. It is important to note that the classification of a conflict as an international armed conflict in accordance with *jus in bello* (international humanitarian law) must be separated from issues governed by *jus ad bellum*. Let us explain why it is important to make such a distinction.

It should be borne in mind that within in terms of application of *jus ad bellum* to cyberspace, the key issue is whether a cyber attack is an act of use of force in accordance with para 4 of Article 2 of the UN Charter, and if so, under what circumstances; and is it an act of armed attack (an act of aggression) in accordance with Article 51 of the UN Charter, and under what circumstances does it legitimize the right of the victim state to self-defense? These are the main problems discussed in the doctrine in relation to the application of jus ad bellum to cyberspace [Roscini M., 2010: 85–130]; [Schmitt M., 1998-1999: 885-937]; [Lin H., 2010: 63–86].

The developers of the Tallinn Manual proceeded from the same logic of differentiation between *jus ad bellum* and *jus in bello* — they dedicated a separate chapter to jus ad bellum: norms 68 to 75 [Tallinn Manual 2.0, 2017: 328–356]. In turn, we recall *that jus ad bellum* and *jus in bello* have different subjects of regulation: the subject of *jus ad bellum* is interstate relations with respect to the lawful use of force in relations between states; and the subject of *jus in bello* is interstate relations with respect to the conduct of

parties to an armed conflict and to the protection of victims of armed conflicts. Therefore, when qualifying an international armed conflict, an action is considered as an act of the use of armed force without prejudice to the question of whether such an action is an act of use of force in accordance with para 4 of Article 2 of the UN Charter (most often such acts are the use of force in accordance with this rule) or an act of aggression in accordance with Article 51 of the UN Charter. This distinction between *jus ad bellum* and *jus in bello* also applies to cyberspace.

Returning to international humanitarian law, we have to note that international treaties in this field do not enshrine the concept of "an act of the use of armed force". This issue, in fact, is attributed to the sphere of judicial practice — usually various international and national courts decide this issue. Let us try to deduce the doctrinal concept of the use of armed force in IHL.

The ancient Chinese philosopher Sun Tzu in his famous treatise «The Art of War» very accurately described the goal of military operations — «to defeat the enemy and increase strength» [Sun Tzu, 2016: 59]. Indeed, the goal of any armed conflict is victory over the enemy side, and to achieve this goal, the parties use weapons or means of military action, as it is called in international humanitarian law. In a classic armed conflict, the use of various traditional means and methods of military operations, in fact, is the use of armed force. However, as we know, cyber attacks are in no way connected with the use of such means and methods. Therefore, the question arises: what is considered to be the use of force in cyberspace in the context of an international armed conflict?

When thinking about this question, one of the first thoughts that arise is to compare the consequences of a cyber attack with the consequences of using «traditional» means of warfare. There is a unanimous opinion in the doctrine that if a cyber attack is assigned to a certain state and leads to the same consequences as the «classical» use of armed force, then such a situation must be qualified as an international armed conflict [Droge K., 2014: 18]; [Schmitt M., 2012: 251]; [Dinniss H., 2012: 131]; [Melzer N. 2011: 24]; [Backstrom A., Henderson I., 2012: 504]; [Hathaway O., Crootof R. et al., 2012: 848]. Niels Melzer also points out that "cyber operations sponsored by a state will lead to the outbreak of an international armed conflict if they are aimed at causing harm to another state, not only by directly causing death, injury or destruction, but also by a direct negative impact on its military operations or military potential "[Melzer N., 2011: 24].

In turn, let us express our agreement with this point of view, since it is quite logical to classify a situation as an international armed conflict when

a cyber attack leads to the infliction of death or injury to people, or to the infliction of harm or destruction of various physical objects. We also agree with the expanded point of view of N. Melzer, since based on the general goal of any armed conflict — to weaken and defeat the enemy, the impact on his military potential, including through cyber attacks, similarly plays an important role in the qualification of the situation, as an international armed conflict.

However, with all the effectiveness of this «consequences approach», it seems insufficient in terms of fixing the entire range of possible consequences of cyber operations and the harm they can cause. The point is that not all the consequences of cyber operations in the physical world will be similar to the consequences of the use of traditional weapons. It should be borne in mind here that sometimes cyber operations, including cyber attacks, are not aimed at physically destroying or damaging civilian or military infrastructure, but most often are aimed at disrupting its functioning. For example, cyber operations can be carried out with the aim of manipulating certain infrastructure. Moreover, a hacker carrying out such a cyber operation will try to do everything to ensure that this cyber operation goes unnoticed.

Examples of such cyber operations include cyber attacks aimed at manipulating the information systems of large banks in order to harm the financial system of a state or aimed at manipulating the energy sector in order to harm the energy system of such a state.[17]

At first glance, cyber attacks, even in the absence of the use of traditional weapons, inflict damage on the population of such a state comparable to the consequences of the use of armed force. However, in such situations, victim states often do not qualify such cyber operations as military aggression in order to avoid confrontation in the international arena (as well as, possibly, for other reasons). In fact, in cases of cyber attacks against them, states remain silent, and thus, do not form any practice. Based on this, the formulation of any legal position on this issue seems to be rather complicated. However, in the absence of state practice, the following options for possible solutions to this problem can be proposed.

The first option suggests considering any hostile cyber operation that negatively affects any infrastructure as an act of using military force. Such

[17] See e.g.: FSB reported cyber-attacks on Russian banks. Available at: URL: https://www.bfm.ru/news/340401 (accessed: 10.04.2021); Hackers attack Russian banks Available at: URL: https://www.gazeta.ru/tech/2020/02/18/12965743/bank_energy.shtml (accessed: 10.04.2021)

an approach will not contradict the norms of international humanitarian law due to the absence of a threshold of violence at which an international armed conflict takes place. Moreover, the well-founded desire to close the legal gap in the protection of the civilian population in the first place is also an argument in favour of this approach. In addition, based on the cyber security strategies of various countries, it can be concluded that states attach great importance to the protection of their main strategic infrastructures in cyberspace.[18] Therefore, it is entirely possible to assume that states could qualify a cyber attack aimed at disrupting the functioning of their strategic infrastructures as an armed attack. In this regard, N. Melzer proposes the concept of critical infrastructure in order to determine the "scale and impact" of a cyber attack on an information network, which will help in establishing the fact of an act of aggression in accordance with Article 51 of the UN Charter [Melzer N., 2011: 14].

The second option proposes not to focus solely on the consequences of a cyber operation, but to take into account a number of factors that determine whether it was an act of the use of armed force. These factors, in addition to the consequences of a cyber operation, must also include the technical means for the implementation of this cyber operation; the fact of participation in the implementation of this operation by a military department (in particular, cyber troops) or another body of the state; the duration of such an operation; and the nature of the target — whether it was a military or civilian target.

The above factors are not invented by chance — they also play a role in determining the fact of the use of armed force in its traditional sense. As

[18] See: Information Security Doctrine of Russian Federation. Adopted 5.12.2016. Available at: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html (accessed: 05.04.2021); Conception of Cybersecurity of Belarus. Adopted 18.03.2019. Available at: https://pravo.by/upload/docs/op/P219s0001_1553029200.pdf (accessed: 5.04.2021); Défense et sécurité des systèmes d'information. Stratégie de la France. Available at: https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf (accessed: 11.04.2021); GSchutz Kritischer Infrastrukturen durch IT-Sicherheitsgesetz und UP KRITIS. Available at: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Schutz-Kritischer-Infrastrukturen-ITSig-u-UP-KRITIS.pdf?__blob=publicationFile&v=7 (accessed: 10.05.2021); Canada: Stratégie nationale sur les infrastructures essentielles. Available at: https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-fr.aspx (accessed: 12.01.2021); The UK Cyber Security Strategy. Published on 25 November 2011. Available at: https://www.gov.uk/government/publications/cyber-security-strategy; National Cyber Strategy of the United States of America. Adopted in September 2018. Available at: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf. (accessed: 12.01.2021)

an example, let us give the following situation: if, suppose, the commander-in-chief of a state was killed as a result of an aerial bombardment by the air forces of another state, then this, of course, would be the use of armed force, and we can talk about the existence of an international armed conflict. But in the case of killing such a person by infecting him, for example, with anthrax, the spores of which were sent to him by a letter from another state, it is difficult to ascertain the existence of an armed conflict. Pointing out this most important factor of the difference between hostile acts committed by the armed forces, on the one hand, and hostile acts committed by other bodies of the state, on the other hand, it should be noted that in this regard M. Sassoli and A. Bouvier noted: "When the armed forces of two states are involved, one shot or one captured (according to government instructions) is enough for IHL to be applied, although in other cases (for example, an execution carried out by a secret agent sent by his government abroad), a higher threshold of violence is required "[Sassoli M., Bouvier A., 2008: 117].

Returning to cyberspace, it should be assumed that states will be more "sensitive" to cyber attacks directed against the information networks of their military and other state infrastructures than to cyber attacks against civilian networks. This conclusion finds its support in the doctrine [Droege C., 2014: 20]. Of course, this approach seems strange, but let's agree with it, because Governments will naturally focus primarily on the cybersecurity of their military and other public infrastructures. However, let us add to this conclusion: if a cyber attack directed against a civilian object results in civilian casualties or injury to civilians, states are likely to recognize the cyber attack as an act of military force as well. Therefore, this conclusion about the "sensitivity" of various information infrastructures for states should be taken conditionally.

Particular attention in the context of the use of force also needs to be paid to the nature and duration of a hostile cyber operation. Let's note that if a cyber attack is of a targeted nature and is not long-lasting, it will be possible to recognize it as an act of using armed force only if it has led to particularly destructive consequences. Returning in this regard, for example, to the Stuxnet virus, we have to note that it indicates that cyber attacks, sometimes, for a long time, are the only hostile actions against another state without the use of other traditional acts of the use of armed force, especially in situations of anonymous cyber attacks. Based on a comparison of the consequences, we can conclude that in the situation the Stuxnet virus was the use of armed force, because, as it was established, this virus led to the destruction of about a thousand IR-1 centrifuges at the uranium

enrichment plant in Netenze, Iran.[19] Based on this fact, many researchers came to the conclusion that this cyber attack can be considered an act of using armed force [Schmitt M., 2012: 252]; [Brown G., 2011: 71]. However, as you know, the Islamic Republic of Iran did not qualify these hostile acts in cyberspace as an act of using armed force. This position of Iran is quite understandable. It is one thing when a given plant could be destroyed as a result of an aerial bombardment by the air forces of another state, and this, unambiguously, would be the beginning of an international armed conflict; and it is quite another matter when the attack was cybernetic, there was no information about other cyber attacks, and the damage was limited only to the destruction of these centrifuges at nuclear installations — such a situation hardly meets the criterion of using armed force to reach the level of an international armed conflict. Therefore, Iran did not consider this situation as the use of armed force.

Of course, all of the above approaches are purely theoretical, and due to the lack of relevant state practice, it remains to be seen under what conditions states will qualify a cyber attack directed against them as an act of using armed force. It is clear that, for example, in the case of a cyber attack against the banking system of a state, even in a situation where such a cyber operation led to serious economic losses, such a cyber attack is outside the object and purpose of the use of armed force. But in the case of a cyber attack against electricity and water supply systems of the population and other vital infrastructures, which led to long-term hardships of the civilian population, it is quite possible to consider it as the use of armed force. Of course, in such a case, the impact of a cyber attack does not equate to the consequences of the traditional use of force, however, such a cyber attack leads to consequences from which the civilian population is guaranteed the protection afforded by the rules of international humanitarian law.

However, for all the importance of the position of states on the qualification of cyber attacks, it should be recalled that the rules of IHL apply regardless of whether states qualify a situation as an armed conflict or not — international humanitarian law applies in all cases of the actual existence of an armed conflict.

---

[19] Stuxnet was work of U.S. and Israeli experts..; Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? ISIS Report. 22 December 2010. Available at: https://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/ (accessed: 20.04.2021); Obama Order Sped Up Wave of Cyberattacks Against Iran. Available at: https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0 (accessed: 30.12.2020)

States simply cannot avoid applying such rules by declaring that there is no international armed conflict. Such "tricks" on the part of states, as you know, were suppressed even during the development of the Geneva Conventions of 1949, which was expressed in the content of common article 2: "... this Convention will apply to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, *even if the state of war is not recognized by one of them*"[20] (emphasis is mine. — S. G.-B.).

Let us also remind that in a commentary to this rule, ICRC lawyers noted the following: "... A state, committing a hostile act towards another state, can always pretend that it is not waging a war, but only carries out a police action or acts in the framework of lawful self-defense. The expression "armed conflict" complicates such disputes. Any disagreement arising between states and leading to the intervention of the armed forces is an armed conflict [...], even if one of the parties denies the existence of a state of war" [Pictet J., 1952: 32]. For all the importance of this comment, it is also important to take into account the presence of the *animus belligerendi*: some situations will not be considered an international armed conflict due to the fact that the necessary level of tension has not been reached in them, in particular, due to the absence of the *animus belligerendi*. This is noted in various national guidelines on the application of IHL. Therefore, random border clashes between the armed forces of different states will not be considered an international armed conflict.[21]

Obviously, in international humanitarian law, the existence of an international armed conflict does not depend on the qualifications of such situations by the parties to such a conflict. However, it must be assumed that in the case of international armed conflicts in cyberspace, due to the fact that cyberspace is a new theater of operations, many issues of qualifying such an armed conflict, in particular, issues of attribution of hostile behavior in cyberspace to a state and issues of the use of force, will depend on from the practice of states, which, unfortunately, has not yet been formed.

Let us now turn to consideration of the problematic of cyber non-international armed conflicts.

---

[20] Geneva Convention for the amelioration of the condition of the wounded and sick in armed forces in the field...

[21] See, e.g.: The UK Joint Service Manual of the Law of Armed Conflict. Joint Service Publication 383, 2004. Promulgated as directed by the Chiefs of Staff. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/27874/JSP3832004Edition.pdf. Para. 3.3.1 (accessed: 05.04.2021)

2. Cyber non-international armed conflict

The key rule for non-international cyber armed conflicts is rule 83 of the Tallinn Manual: "A non-international [cyber] armed conflict occurs whenever there is prolonged armed violence, which may include or be limited to cyber operations between government armed forces and organized armed groups or between such groups. The confrontation must reach a minimum level of intensity, and the parties involved in the conflict must have a minimum degree of organization" [Tallinn Manual 2.0, 2017: 385].

A key question in relation to this rule is how to distinguish between ordinary criminal conduct of individuals in cyberspace and non-international armed conflict in cyberspace? There are frequent reports in the media in which the actions of hackers and hacker groups, in particular such well-known ones as Wikileaks and Anonymous, are characterized as "cyber war".[22] Of course, such journalistic publications do not mean an armed conflict of a non-international character in the legal sense of the word. However, it is necessary to establish criteria for qualifying the situation as a non-international cyber armed conflict.

As is known, there is no definition of a non-international armed conflict in international treaty law. Therefore, this issue remained in the sphere of the doctrine and practice of states, on the basis of which the ICTY gave the following definition of an armed conflict of a non-international character: "An armed conflict [of a non-international character] occurs whenever ... there is a prolonged armed conflict between government forces and organized armed groups or between such groups within one state".[23]

The above norm of the Tallinn Guidelines is based on this definition proposed by the ICTY. Based on this, there are two criteria necessary to qualify a situation as a non-international armed conflict: the criterion for the intensity of violence and the criterion for the minimum level of organization of the parties. Let's start with the last criterion.

---

[22] WikiLeaks: Threat of cyberwar. Available at: http://rapsinews.ru/international_publication/20101130/251133841.html (accessed: 15.04.2021); Anonymous declared cyberwar to the Islamic State Available at: https://www.vesti.ru/hitech/article/625187 (accessed: 15.04.2021); WikiLeaks backlash: The first global cyber war has begun, claim hackers. 2010. December 11. Available at: https://www.theguardian.com/media/2010/dec/11/wikileaks-backlash-cyber-war (accessed: 15.04.2021); Anonymous: Protesters or Terrorists? Fog of cyberwar obscures truth. 2012. February 21. Availavle at: https://www.rt.com/usa/anonymous-freedom-cyber-wall-875/ (accessed: 15.04.2015)

[23] *Prosecutor* v. *Dusko Tadić*. Case № IT-94-1-T. ICTY Appeals Chamber Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction of 2 October 1995. Para 70.

2.1. Organization of the parties

For an armed group to be considered organized and to be qualified as a party to a non-international armed conflict, it is required that it has a level of organization that will enable it to engage in continuous hostilities and comply with international humanitarian law. The hallmarks of such a necessary organization are the existence of an organizational chart that defines the command structure and authority over the military operations in which the group participates; the ability to recruit and train new members; and the existence of internal discipline rules. These signs are confirmed by judicial practice.[24] It is important to note that such an armed group is not required to have the same level of organization as the government's armed forces. However, such a group must have a certain hierarchy, level of discipline and the ability to comply with IHL norms. This is also confirmed by the practice of the ICTY.[25]

When these criteria of organization are analyzed for their applicability to hacker groups, the question arises as to whether such groups, organized exclusively in cyberspace, can be organized armed groups in accordance with international humanitarian law? In connection with this issue, M. Schmitt pointed out that "members of virtual groups may have never met and do not even know each other's real names. However, such groups can act in a coordinated manner against the government (or an organized armed group), receive orders from the virtual leadership, and be highly organized. For example, one [member] of the group may be tasked with identifying the vulnerabilities of the target [information] system, the second may develop malicious software to target these vulnerabilities, the third may carry out [cyber] operations, and the fourth may provide cyber defense against oncoming [cyber -] attacks" [Schmitt M., 2012: 256].

However, M. Schmitt also adds to this passage that the requirement for an organized armed group to have some form of responsible command and the requirement for its ability to comply with international humanitarian law are likely to be an obstacle to qualifying hacker groups as organized armed groups in terms of IHL. In addition, M. Schmitt adds that

[24] Prosecutor v. Ljube Boškoski & Johan Tarčulovski. Case № IT-04-82-T. ICTY Trial Chamber Judgement of 10 July 2008. Para. 199–203; Prosecutor v. Fatmir Limaj et al. Case № IT-03-66-T. ICTY Trial Chamber Judgement of 30 November 2005. Para 94–134; Prosecutor v. Ramush Haradinaj et al. Case № IT-04-84-T. ICTY Trial Chamber Judgement of 3 April 2008. Para 60.

[25] Prosecutor v. Ljube Boškoski & Johan Tarčulovski. Case № IT-04-82-T. ICTY Trial Chamber Judgement of 10 July 2008. Para 202.

it is difficult to imagine a situation where an effective system of discipline will be created within a hacker group, including in order to ensure that such a group complies with the norms of international humanitarian law [Schmitt M., 2012: 257].

A similar point of view is supported by the head of the ICRC Legal Department, Cordula Droege [Droege C., 2014: 24]. A similar opinion is expressed by most of the developers of the Tallinn Manual. In particular, para 13–15 of the Commentary to Rule 83 indicate that it is unlikely that hacker groups and groups associated exclusively with virtual messages will have an appropriate degree of organization, a responsible command, an appropriate hierarchy and an effective discipline system in order to could be considered as a party to an non-international armed conflict [Tallinn Manual 2.0, 2017: 390–391].

Of course, the above point of view is quite reasonable, but let's not rush to agree with it. In our opinion, the rapid development of information technology makes it possible for hacker groups to meet the criterion of organization: it cannot be ruled out that a highly organized hacker group could be created with responsible command and an appropriate degree of hierarchy, as well as a clear disciplinary system. The problem lies not in this possibility, but in the fact that at the moment there have been no examples of such highly organized hacker groups, or rather, states have not yet encountered such hacker groups in practice.

Of course, one can speculate that well-known hacker groups such as Anonymous can satisfy the criterion of being organized. However, due to the lack of detailed information about the structure of such a group, which, in turn, is due to the anonymity that rules in cyberspace, such hasty conclusions cannot be drawn.

Summing up the reflections on the compliance of hacker groups with the criterion of organization, it can be noted that the key problem here is not the potential possibility or impossibility of such compliance, but in the very absence of relevant state practice. Let us now turn to the next criterion — the intensity of hostilities.

2.2. Intensity of hostilities

The key question in relation to the intensity criterion is whether the use of cyber-only means can achieve the level of intensity required to qualify such a situation as a non-international armed conflict?

When characterizing the criterion of intensity in relation to classical non-international armed conflicts, it should be noted that the ICTY point-

ed out a number of factors that must be taken into account when assessing a specific situation in terms of intensity.

In particular, this is the use of the armed forces, rather than the police and other law enforcement agencies; the collective nature of hostilities; the severity of the attacks; an increase in the number of armed clashes, their territorial coverage and duration; the number of civilians forced to leave the conflict zones; distribution of weapons between the parties to the conflict; the types of weapons used, in particular, the fact of the use of heavy weapons is important; and the degree of destruction and the number of casualties caused by such armed clashes.[26] The question arises about the applicability of these factors to cyber attacks.

Probably, the consequences approach should be applied in a similar way. At first glance, there is no reason to assert that cyber operations cannot lead to such consequences that would make it possible to speak of the necessary level of intensity to qualify the situation as a non-international cyber armed conflict.

However, as C. Droege notes, cyber operations by themselves do not lead to many of the consequences-indicators of the intensity of violence. In her opinion, cyber operations will most likely lead to consequences that are serious enough to reach the required level of intensity, such as large-scale destruction or catastrophic consequences for a large part of the population due to repeated attacks [Droge C., 2014: 25].

In turn, we note that it can be argued that in order to achieve the required level of intensity, it is necessary that the consequences of cyber operations be comparable to the consequences of classical military actions, but at the same time it is necessary to take into account the fact that a cyber attack still will not lead to the same consequences as the traditional use of armed force. It should also be borne in mind that this conclusion is again purely theoretical — due to the lack of relevant practice of states, we have yet to see exactly what circumstances will satisfy the required level of intensity to qualify the situation as a non-international cyber armed conflict.

Conclusion

Summing up, the following can be noted with regard to the problem of the typology of armed conflicts in cyberspace. Of course, in a situation

[26] Prosecutor v. Fatmir Limaj et al. Case № IT-03-66-T. ICTY Trial Chamber Judgement of 30 November 2005. Para 135–170; Prosecutor v. Ramush Haradinaj et al. Case № IT-04-84-T. ICTY Trial Chamber Judgement of 3 April 2008. Para. 49; Prosecutor v. Ljube Boškoski & Johan Tarčulovski. Case № IT-04-82-T. ICTY Trial Chamber Judgement of 10 July 2008. Para 177–178.

where cyber operations are carried out in the context of an armed conflict (international and non-international), the same rules of international humanitarian law will apply to them as to the desired armed conflict.

As for a purely cyber armed conflict, both international and non-international, without the use of any traditional armed forces, such a conflict is not excluded in theory, but in practice we still have to see what situations in cyberspace will be considered by states as such an armed conflict.

Touching upon the problem of state practice in relation to cyber armed conflicts, it is important to note that there are concerns in the doctrine about the trajectory of such practice development. In particular, C. Droege notes: "... it remains unclear in which direction the practice of states will develop. Given the reluctance of states to recognize situations of armed conflict, especially non-international armed conflict, it can be assumed that attempts will be made to evade discussion of the existence of an armed conflict. And this is not only due to the anonymity of many attacks on computer networks and practical problems with attribution, but also due to the fact that most of the situations may not represent extreme cases of physical destruction caused by attacks on computer networks, but rather, bloodless manipulation of infrastructure at a fairly low level. States can consider such situations from the point of view of law enforcement and criminal law, and not as situations regulated by the legal system applicable to armed conflicts" [Droge C., 2014: 25–26].

Let us express our solidarity with the above concerns. However, it must be considered that without the relevant practice of states, the above problems will remain unresolved. At the same time, waiting for the moment when states finally form the relevant practice also seems to be a rather short-sighted decision. Of course, one can expect when states will finally form a practice on this issue, but there are other ways to identify the prevailing attitude of states on the issue. In particular, it is necessary that the problems of the typology of armed conflicts in cyberspace be brought up for discussion in international organizations, best of all, in the agenda of their plenary bodies, in the activities of which the prevailing practice of states can be traced. The best place to discuss this issue is the United Nations General Assembly, since all states of the world are represented there. Therefore, it is necessary that the UN General Assembly pay attention to the problem of qualifying international armed conflicts, include it in the agenda, as a result of which a corresponding resolution would be adopted. Let's hope that the UN General Assembly will pay attention to this problem.

References

Backstrom A., Henderson I. (2012) New capabilities in warfare: an overview of contemporary technological developments and the associated legal and engineering issues in Article 36 weapons reviews. *International Review of the Red Cross*, vol. 94, no 886, pp. 483–514.

Brown G. (2011) Why Iran didn't admit Stuxnet was an attack. *Joint Force Quarterly*, issue 63, pp. 70–73.

Dinniss H. (2012) *Cyber Warfare and the Laws of War*. New York: Cambridge University Press. 331 p.

Döge J. (2010) Cyber Warfare. Challenges for the Applicability of the Traditional Laws of War Regime. *Archiv des Völkerrechts*, no 4, pp. 486–501.

Droege C. (2012) Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians. *International Review of the Red Cross*, no 886, pp. 533–578 (in Russian)

Hathaway O., Crootof R. et al. (2012) The Law of Cyber-Attack. *California Law Review*, no 4, pp. 817–885.

Lin H. (2012) Cyber conflict and international humanitarian law. *International Review of the Red Cross*, no 886, pp. 515–531.

Lin H. (2010) Offensive Cyber Operations and the Use of Force. *Journal of National Security Law and Policy*, vol. 4, pp. 63–86.

Melzer N. (2017) *International Humanitarian Law: A Comprehensive Introduction*. Moscow: ICRC. 420 p. (in Russian)

Melzer N. (2011) *Cyberwarfare and International Law*. UNIDIR Resources Paper. 38 p.

Pictet J. (ed.) (1952) *Geneva Convention (I) for the Amelioration of the Condition of the Wounded in Armies in the Field Commentary*. Geneva: ICRC. 466 p.

Roscini M. (2010) World Wide Warfare — *Jus ad bellum* and the Use of Cyber Force. *Max Planck Yearbook of United Nations Law*, vol. 14, pp. 85–130.

Sassòli M., Bouvier A. (2008) How does Law protect in War? Cases, Documents and Teaching Materials on Contemporary Practice in International Humanitarian Law. Vol. I. Outline of International Humanitarian Law. Moscow: ICRC. 672 p. (in Russian)

Schmitt M. (2019) Wired warfare 3.0: Protecting the civilian population during cyber operations. *International Review of the Red Cross*, no 1, pp. 333–355.

Schmitt M. (ed.) (2017) Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: University Press. 598 p.

Schmitt M. (2014) Rewired warfare: rethinking the law of cyber attack. *International Review of the Red Cross*, no 893, pp. 189–206.

Schmitt M. (2012) Classification of cyber conflict. *Journal of Conflict and Security Law*, no 2, pp. 245–260.

Schmitt M. (2002) Wired warfare: Computer network attack and jus in bello. *International Review of the Red Cross*, no 846, pp. 365–399 (in Russian)

Schmitt M. (1999) Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. *Columbia Journal of Transnational Law*, vol. 37, pp. 885–937.

Streltsov A. A. (2014) Main development directions of the international law of armed conflicts in relation to cyberspace. *Pravo i gosudarstvo: teoriya i praktika*, no 3, pp. 75–88 (in Russian)

Sun Tzu (2016) *The Art of War*. Moscow: AST, 220 p. (in Russian)

Tsagourias N. (2012) Cyber attacks, self-defence and the problem of attribution. *Journal of Conflict and Security Law*, no 2, pp. 229–244.

Zhang L. (2012) A Chinese perspective on cyber war. *International Review of the Red Cross*, no 886, pp. 801–807.