Criminal Justice Issues
Journal of Criminal Justice and Security
Year XIV, Issue 5-6, 2016. p. 61-76
ISSN 1512-5505

INTERNATIONAL LAW AND CYBER SECURITY

Review Paper

Sakib SOFTIĆ

Abstract

Cyber attacks constitute a new security threat that appeard in the twenty-first century. This security threat put new known and unknown challenges to the international community and single State. The security threat may come from other states or from non-state actors. In this article the author deals with issues related to the application of the rules of international law and the right of armed conflict to counteract cyber threats. The Author first endeavor to explain and define the concept of international cyber security law, then analyzes the question of the state's relationship to cyber-attacks and the right of the state to use force to counter cyber-attacks, and finally analyzes whether cyber-attack can be considered as an act that entitles rights to individual and collective self-defense within the meaning of the UN Charter. And under what conditions.The right to self-defense is not just a passive right of the state to wait for to be attacted. And that the damage be done. The state has the right to active self-defense, which also manifests itself as the right to anticipatory self-defense. The state is also entitled to proportional countermeasures. The right to self-defense also exists in the case of attacks committed by non-state actors. This article is divoted to complex international legal issues related to this security threat, and certainly contributes to a better understanding of this issue and represents a contribution to the development of international law in this matter.

Keywords

security threat, cyber security, cyber atacks, the law of the armed conflict, the right to self-defense

1. Introduction

Cyber attacks constitute a new security threat that states face in the begining of twenty-first centuries. Cyber attacks may, in their severity, be equivalent to conventional attacks. They can produce the same or even more detrimental effects on the state and its inhabitants than conventional attacks. Therefore, the question arises of the applicability of the law of armed conflict and international humanitarian law, to situations caused by Cyber attacks.

Since this is a new phenomenon, it is necessary to establish a new one or to confirm the application of existing rules of international law to cyber attacks. There is still no full agreement on these issues among states and legal writers. As it is known, international law is the product of interstate relations and is created through international treaties and international customs.

Here is the problem that not exist international treaties that directly deal with cyber attacks.[1] Nor is customary international law sufficiently developed in this matter. Because cyber attack is a new phenomenon.

The question of the existence of international law norms applicable to cyber attacks has been raised especially after the hacker attacks in the first decade of this century (Estonia, Georgia, Ukraine, Iran, US). Which has brought this kind of attack into the focalpoint of modern states and the international community as a whole.

Some States, such as Canada, the United Kingdom, and the United States, have adopted certain documents in response to this type of threat.[2]

This issue was also on the agenda of the United Nations, which confirmed that international law, and in particular the part contained in the UN Charter, was applicable to Cyber attacks. [3]

Some international organizations have tend to establish rules of international law applicable to armed conflicts. [4]

Most legal writers are the view that international law also applies to Cyber space. [5] Although

---

1 The 2001 Council of Europe Convention was enacted to prevent acts that violate the confidentiality, integrity and availability of computer systems, networks and data, as well as prevent the misuse of those systems, networks and data, ensuring the adoption of powers sufficient to enable the effective fight against these criminal offenses. acts, facilitating their detection, investigation and prosecution, both domestically and internationally, and by providing substantive provisions for faster and more confidential international cooperation. See introduction: Convention on Cybercrime 185 CETS (opened for signature 23 November 2001, entered into force 1 July 2004).

2 In 2011, the US Department of Defense issued a Strategy for Action in Cyberspace, marking cyber attacks as a security threat. The Strategy has been revised several times.

3 See: U.N. Secretary-General, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, ¶ 19, U.N. GAOR, 68th Sess., U.N. Doc. A/68/150 (June 24, 2013).

4 NATO suradnički centar za izvrsnost u Cyber odbrani sa sjedištem u Talinu, izdao je 2013. godine ''Tallinn manual o međunarodnom pravu koje se primjenjuje na cyber ratovanje. Priručnik (manuel) je dopunjen 2017. godine i predstavlja najpotpuniju kompilaciju međunarodnog prava primjenjivog na ovu oblast. Sačinjen je od strane istaknutih neovisnih međunarodnih pravnika iz dvadeset pet zemalja. U daljem tekstu: Tallinn manual. Vidi: https://ccdcoe.org/research/tallinn-manual/.

5 See: Gary D. Brown: International law Apllies to Cyber Warfare! Now What. 355 BROWN (DO NOT DELETE) 4/11/2017 7:52 PM. https://www.swlaw.edu/sites/default/files/2017-08/355%20International%20Law%20Applies%20to%20Cyber%20Warfare-Brown.pdf 20.09.2019.; MIRANDA GRANGE: CYBER WARFARE AND THE LAW OF ARMED CONFLICT LAWS 533: LAW OF ARMED CONFLICT, RESEARCH PAPER. Faculty of Law Wictoria 2014. https://core.ac.uk/download/pdf/41339676.pdf 20.09.2019. 20.09.2019

some believe that the application of international law to Cyber security is in crisis. [6]

In order to raise the issue of the applicability of international law to cyber attacks, it is necessary that attacks have some weight. In the opinion of the International Court of Justice, the law of armed conflicts applies to "any use of force, regardless of the weapon used." [7] But 'used force' must produce consequences relevant to international law.

International law contains two sets of provisions applicable to these situations. The first concerns *jus ad bellum*, that is, the right to resort to the use of force. The second *jus in bello* group applies when the war has already begun and concerns the application of the rules of law of war, the law of armed conflicts and international humanitarian law to a specific situation.[8]

The particular problem of applying rules of international law to cyber attacks is caused by the nature of an "computer network" that makes it difficult to detect and identify an attacker. It is indisputable that states tend to cover up the fact that they are the perpetrators of a cyber attack. They often engage anonymous individuals and groups to commit cyber attacks instead. After that, any traces that might bind the attacker's country to the attack are removed.

Since the question of the applicability of international law to cyber attacks is a new topic, very little has been said about it especially in our language. Therefore the author's intention is to contribute to the development of this section of international law and to explore and analyze the applicability of some of the existing institutions of international law to cyber attacks.

2. The concept of International law of cyber security

International cyber security law is a new term in international law. It serves to identify those parts of international law that deals with hostile use of Cyber space. And if international cyber security law is a new term in international law, it does not mean creating a new branch of international law.[9] No new institutes of international law are being created. This is more about the specifics of applying existing institutes to a new situation.

International law establishes the responsibility of states for international wrongful acts committed by their national authorities, as well as for certain non-state actors whose acts are

---

6 See: Kubo Mačák: Is the International Law of Cyber Security in Crisis? 2016 8th International Conference on Cyber Conflict. 127-139.

7 INTERNATIONAL COURT OF JUSTICE REPORTS OF JUDGMENTS, ADVISORY OPINIONS AND ORDERS LEGALITY OF THE THREAT OR USE OF NUCLEAR WEAPONS ADVISORY OPINION OF 8 JULY 1996. U daljem tekstu: Nuclear Weapons Advisory Opinions, para. 39.

8 See: Michael N Smitt, ''Attack'' as a Term of Art in International law: The Cyber Operations Context. 2012 4thInternational Conferenc on Cyber Conflict. (283-293).

9 Ovaj pojam je više deskriptivan i obuhvata pojmove suverenosti, jurisdikcije i odgovornosti država ukoliko se ovi bave međunarodnim pravom rata i međunarodnim pravom u ratu. Vidi: Tallinn manual o međunarodnom pravu koje se primjenjuje na cyber ratovanje. General editor Michael N Schmitt. Cambridge University Press 2017. str. 24

attributable to the state under certain circumstances.[10] States can be held responsible for the cyber operations of their respective state authorities and non-state actors that are attributable to it.

These are hostile cyber attacks of such gravity that activate the application of rules of international law that prohibit the use of force against other independent states. Or, they are attacks of such intensity that initiate the application of Chapter VII of the UN Charter, which provides for the right of states to individual or collective self-defense and the use of force by the UN Security Council to counter cyber attacks.

The UN Charter prohibits the unlawful use of force in relations between states, using two terms relevant to our subject.

The first is the *use of force* against another state.

The general prohibition of war is based on the provision of Article 2, paragraph 4 of the UN Charter: ''…All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.''

Prohibition on the use of force has been accepted as customary international law and even as the *ius cogens* norm, as confirmed in the judgment of The Hague Tribunal in Nicaragua v. The United States. [11]

Another used term is *aggression*. Article 39 of the UN Charter empowers the Security Council to assess whether it is a threat to peace, a breach of peace or an act of aggression. In its 3314 (XXIX), of 1974 Resolution, the United Nations defined aggression as: ''...the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations…''.

The UN Charter does not define attack. But it does the another generally accepted international law document 1977 Additional Protocol I to the 1949 Geneva Conventions. Article 49 of Protocol I defines an attack. „'Attacks' means acts of violence against the adversary, whether in offence or in defence.''

Protocol I shall apply to all attacks, irrespective of the territory in which they are undertaken, including the national territory belonging to the conflicting party but controlled by the opposing party. Also, Protocol I applies to land, air or naval warfare that may affect civilians, individual civilians or civilian objects on land.[12]

---

[10] United Nations A/RES/56/83 from 28 January 2002. Responsibility of States for internationally wrongful acts. http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf. 16.09.2019.

[11] Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgement, ICT Reports 1986, p 14, para 190.

[12] See Michael N Smitt, ''Attack'' as a Term of Art in International law: The Cyber Operations Context. 2012 4thInternational Conferenc on Cyber Conflict. (283-293).

Cyber attacks to constitute attacks within the meaning of Article 49 of Additional Protocol I, must cause physical destruction or injurious harm as well as other weapons: conventional, nuclear, chemical and biological.[13] Several approaches have been noticed in analyzing whether a cyber attack constitutes an attack within the meaning of international law.

The first approach is *performance* based. To be an attack, a cyber attack requires the same consequences as other types of attack. The second approach is *target* based. If the attack is directed against anything called critical infrastructure then the attack meets the criteria set by international law. An approach involving the means used in attack was dismissed as inapplicable.[14]

Law of armed conflict applies to cyber operations as well as to other operations undertaken during an armed conflict. Thus, according to Tallinn's manual, "Cyber operations executed in the context of an armed conflict are subject to the law of armed conflict." [15] The law of armed conflict applies to cyber operations, whether international or internal armed conflict[16].

On the other hand, the law of armed conflict does not apply to the activities of private corporations unrelated to armed conflict.[17] The key issues for cyber armed conflict are the location from which the cyber operations were launched, the location of the cyber operations devices, and the location where the cyber operations are directed. Also, these issues are related to neutrality rules that may be notintentionaly violated by this type of operation.

> ''International armed conflict exists whenever there are hostilities, which may include or be limited to cyber operations, occurring between two or more states.''[18] ''While ''A Non - International armed conflict exists whenever there is protracted armed violence, which may include or be limited to cyber operations, occurring between government armed forces and the forces of one or more armed groups, or between such groups. The confrontation must reach a minimum level of intensity and parties involved in the conflict must show a minimum degree of organization''.[19]

The law of cyber armed conflicts applies not only to the issues of its application *jus ad bellum* but also to *jus in bello*. Tallinn's Manual regulates the issue of the criminal responsibility of commanders and superiors for war crimes resulting from orders to carry out cyber operations that constitute war crimes. Also, the commander and superior are responsible for not taking measures to prevent such crimes or to punish the perpetrators.[20]

---

13 See: Mateusz Piatkowski, The Definition of the Armed Conflict in the Condition of Cyber Warfera, Polish politikal Science Yearbook vol. 46 (2017) pp. 271 – 280.

14 See: Mateusz Piatkowski, The Definition of the Armed Conflict in the Condition of Cyber Warfera, Polish politikal Science Yearbook vol. 46 (2017) pp 275.

15 Article 20 Tallinn manuala.

16 See articlies 22 i 23 Tallinn manual.

17 See. Tallinn manual 2017. p. 69.

18 Article 22 Tallinn manual.

19 Article 23 Tallinn manual.

20 Article 24 Tallinn manual.

3. States and cyber attacks

The basic rule is that, on the basis of their sovereignty, the state can exercise control over cyber infrastructure and activities within its territory. [21]

This right derives from the concept of sovereignty as defined by international law. Sovereignty implies the exercise of effective authority over territory and population. ''The state need not need have any particular form of government, but there must be some authority exercising government functions and able to represent the entity in international relations.''[22]

In the case of the *Aaland Islands*, an International Committee of Lawyers was appointed to investigate the status of the island on the issue of the time of the establishment of the Finnish Republic. The question was raised to determine responsibility for the damage of riots that arose during the Russian Revolution and the gaining independence of Finland. The Committee drew up a report outlining the legal aspects of the Åland Islands issue. The Sovereignty Report states:

> ''[t]his certainly did not take place until a stable political organisation had been created, and until the public authorities had become strong enough to assert themselves throughout the territories of the state without the assistance of the foreign troops.''[23]

In the *Palmas Island case*, Max Huber emphasized:

> ''Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State. The development of the national organisation of States during the last few centuries and, as a corollary, the development of international law, have established this principle of the exclusive competence of the State in regard to its own territory in such a way as to make it the point of departure in settling most questions that concern international relations.'' [24]

A state suvereignty over cyber infrastructure within its territory has two consequences. First, that cyber infrastructure is subject of the legal and regulatory control of the State. Second, the State territorial soveregnty protects such infrastructure.[25] A cyber attack by one State directed against the cyber infrastructure of another State violates its sovereignty.[26]

Each state has the right to regulate its own legal order and therefore to regulate the rights and obligations of all legal entities located in its territory. At the same time, a state cannot execute

---

[21] Tallinn manual str. 25.

[22] Carter/Trimble/Bradley. (2003) International Law, forth edition. New York: Aspen Publisher. Str. 433.

[23] L.N.O.J., Special Supp. No. 3., p.3 (1920). Harris (2004) Cases and Materials on International Law, sixth edition. London: Thomson, Sweet§Maxwell. Str. 100-101; Shaw, N. M. (2008) International Law, sixth edition, Cambridge: Cambridge University Press. Str.200-201.

[24] Island of Palmas Case. RIAA II 829, at 838. Cit. Prema Malanczuk, P. (1997) Akehurst's modern introduction to International Law, seventh revised edition, London and New York: Routledge. Str. 109-10.

[25] Tallinn manual. p. 25.

[26] Tallinn manual. p. 25 -27.

any act of government in the territory belonging to another state. These rights arise from the rights of the jurisdiction. Jurisdiction is the right of the state to legislate, to adjudicate in disputes between legal entities, and to enforce its laws through judicial and extrajudicial means.

Jurisdiction is closely linked to sovereignty because it constitutes the exercise of state power by which the rights and obligations of legal entities arise, cease or change in areas where the state has territorial sovereignty.

Article 2 Tallinn Manual confirms the jurisdiction of states with regard to cyber infrastructure:

''Without prejudice to applicable international obligations, State my exercise its jurisdiction:

(a) Over persons engaged in cyber activities on its territory;
(b) Over cyber infrastructure located on its territory; and
(c) Extraterritorially, in accordance with international law.

To be held responsible for committing a cyber attack as an international wrongful act, conduct (attacks) must be attributable to that state. The general rule is that only the behavior of a state authority or its agents can be attributable to the state.[27]

Article 4 Rules of responsibility of States for internationally wrongful acts specifis the authorities of the State whose conduct entails responsibility for the State. [28]

> ''1.The conduct of any State organ shall be considered an act of that State under international law, whether the organ exercises legislative, executive, judicial or any other functions, whatever position it holds in the organization of the State, and whatever its character as an organ of the central government or of a territorial unit of the State.
> 2. An organ includes any person or entity which has that status in accordance with the internal law of the State.''

The state is also responsible for persons or entities that actually act as organs of the state, even if they are not so classified as such under national law. The acts of persons or entities which are not state organs but are empowered by internal law to exercise the elements of govornmental authority shall be regarded as acts of the State if, in the specific case, the person or entity acts in that capacity.[29]

The rules also cover relatively new phenomena such as parastatal bodies and privatized state corporations. Even private individuals and entities may be included if they are empowered under domestic law to perform state functions such as enforcing state regulations on the execution of imprisonment, as is the case in some states.

---

[27] Persons or entities acting on instructions or encouraged or controlled by the State or its authorities.

[28] United Nations A/RES/56/83 from 28 January 2002. Responsibility of States for internationally wrongful acts. http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf. Pristupio 16.09.2019.

[29] United Nations A/RES/56/83 from 28 January 2002. Responsibility of States for internationally wrongful acts. Articl 5.http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf. Pristupio 16.09.2019.

An international wrongful act exists when it is a conduct of the state, which may consisting of an action or omission: ''(a) Is attributable to the State under international law; and (b) Constitutes a breach of an international obligation of the State.''[30]

If an act is an wrongful act under international law, its unlawfulness cannot be ruled out by its characterization as a permissible act by the rules of domestic legal order. The characterization of an act of a state as wrongful under international law is done according to the criteria established in international law (Article 3 of the Rules).

4. The use of force by states to counter cyber attacks

As already stated in article 2, paragraph 4 of the Charter, it prohibits any use of force and provides that all UN members in their international relations will refrain from threatening force or from using force against the territorial integrity or political independence of any other state, or which on any other way was contrary to the objectives of the United Nations.

The Charter of United Nations has centralized control of the use of force at the hands of the UN Security Council. Only the Security Council has the right to determine "the existence of a threat to peace, breach of peace or aggression" (Article 39 of the UN Charter).

The term 'prohibition on the use of force' used in Article 2, paragraph 4 of the UN Charter is not defined. Also, the existence of a threat to peace, breach of peace and an act of aggression, the terms used in Article 39 of the UN Charter have no precise definition. This gives the Security Council wide discretion when deciding whether there is a situation under Article 39 of the Charter, or whether it is another situation. Article 51 of the UN Charter gives States the right to individual and collective self-defense in the event of an armed attack.

The International Court of Justice has stated in the Nikaraqua case that Article 2 paragraf 4 and Article 51 of the Charter apply to "any use of force, regardless of the weapons employed." [31]

According to Article 10 of Tallinn Manuel ''A Cyber operations that constitutes a threat or use of force against the territorial integrity or political independence of any state, or that is in any other manner incompatible with the purposes of the UN, is unloweful.''[32]

There is no one authoritative international document defining the threat of force and the use of force.

Article 11 Tallinn defines the use of force in cyber space by stating that: "A Cyber operation constitutes a use of force when its scale and effects are comparable to non-Cyber operations rising to the level of a use of force."

---

[30] United Nations A/RES/56/83 from 28 January 2002. Responsibility of States for internationally wrongful acts. Articl 2.http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf. Pristupio 16.09.2019.

[31] Nuclear Weapons Advisory Opinion, para. 39.

[32] Tallinn manual o međunarodnom pravu koje se primjenjuje na cyber ratovanje. General editor Michael N Schmitt. Cambridge University Press 2017. str. 45.

Here are emphasized the scope and consequences as a quantitative and qualitative factor for defining the use of force.

The International Court of Justice in the Nikaraqua case distinguishes the most serious forms of use of force that constitute armed assault and less serious forms.[33] This view of the Court implies that any unlawful use of force of a certain magnitude which has caused certain consequences may be qualified as an armed attack.

In assessing whether to qualify a situation as an armed attack, states take into account certain factors: seriousness, immediacy, directness, invasiveness, measurable consequences, military character, state involvement and presumed legality. [34]

Article 12 Tallinn Manuel defines a cyber threat as follows: '' A cyber operation, or threatend cyber operation, constitute an unlawful threat of force, when treatened action, if caried out, would constitute an unlawful use of force. ''

Article 13 confirms the right to self-defense against an armed attack. '' A State that is target of a cyber operation that rises to the level of an armed attack may exercise its own inherent right of self-defense. Whether a cyber operation constitutes an armed attack depends on its scale and effects.''

5. The right of states to selfdefence against armed attack

As we have seen in Article 13, Tallinn Manuel follows the rules of general international law regarding the right of states to self-defense against cyber attacks.

Article 51 of the Charter of the United Nations, which constitutes source of the right to self-defense, reads:

''Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of selfdefense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.''

In order to determine the exact meaning of this article, it must be considered in the context of the UN Charter as well as in relation to customary international law. In the context of the UN Charter, it must be viewed first and foremost in relation to Article 2 (4), which obliges all UN members to refrain in their relations from threats of force or use of force against the territorial integrity or political independence of any State, or which in any other way contrary to the objectives of the United Nations.

---

[33] Nuclear Weapons Advisory Opinion, para. 191.

[34] Vidi: Tallinn manual o međunarodnom pravu koje se primjenjuje na cyber ratovanje. General editor Michael N Schmitt. Cambridge University Press 2017. str. 49 – 52.

Armed attacks should be directed against territorial integrity or political independence. Such an armed attack allows for an exception to the general prohibition on the use of force under the Charter, and entitles every state to resort to self-defense.

There are some obvious situations that justify states' right to self-defense.

In the Nicaraqua case, the International Court of Justice used the definition of aggression (Article 3.g) to define the meaning of the term armed attack in international law.[35] An armed attack must be understood as including not merely action by regular armed forces, but also "the sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to '(inter alia) an actual armed attack conducted by regular forces,' or its substantial involvement therein".[36]

After the terrorist attack of September 11, 2001, by resolution 1368 of September 12. 2001, the terrorist attack was designated as a threat to international peace and security within the meaning of Chapter VII of the Charter UN.[37]

The right of the state to self-defense extends to the defense against cyber attacks. '' The international group of experts unanimously concluded that some cyber operations may be sufficientlyi grave to Warrant classifying them as an 'armed attack' within the meaning of the Charter. Which then gives the State the right to self-defense in accordence with the UN Charter.[38] This conclusion is in line with the opinion of the International Court of Justice in Case Law on the Legality of the Use of Nuclear Weapons, which states: ''These provisions do not refer to specific weapons. They apply to any use of force, regardless of the weapons employed.''[39]

The right to self-defense against cyber-attacks also involves the use of permissible countermeasures aimed to induce the State witch was responsible for an internationally wrongful act to cease breach of international legal obligations and to respect its international obligations.[40] The right to countermeasures lasts as long as there is unlawful conduct. With the cessation of violation of international obligations, the right to countermeasures ceases to exist. Countermeasures must be necessary and proportionate and time-limited.

Tallinn manual in Article 9 confirms the state's right to countermeasures:

---

[35] United Nations General Assembly Resolution 3314 (XXIX). Definition of Aggression. Available: http://jurist.law.pitt.edu/3314.htm, 2.10.2019.

[36] Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgement, ICT Reports 1986, p 14, para 195.

[37] Resolution S/RES/1368 (2001), Dostupno na: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N01/533/82/PDF/N0153382.pdf?OpenElement, 21.12.2010.

[38] Tallinn manual o međunarodnom pravu koje se primjenjuje na cyber ratovanje. General editor Michael N Schmitt. Cambridge University Press 2017. str. 54.

[39] Nuclear Weapons Advisory Opinion, para. 39. https://www.icj-cij.org/files/case-related/95/095-19960708-ADV-01-00-EN.pdf. 1.9.2019.

[40] See art. 49. Draft articlies. United Nations A/RES/56/83 from 28 January 2002. Responsibility of States for internationally wrongful acts. http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf. 16.09.2019.

''A state injured by an international wrongful act may, resort to proportionate countermeasures, including cyber countermeasures, against the responsible state. ''

6. Preconditions for the existence of the right to self-defense

It has been accepted in the legal literature almost unanimously that in order to exercise the right to self-defense, it is necessary to fulfill the conditions: necessity and proportionality.

Rules of necessity and proportionality are rules of customary international law and their content depends on the circumstances of each particular case. Have these conditions been met is estimated first, by a state that finds in a situation that requires recourse to self-defense, and then by the international community. Every nation is free at any times regardless of the provisions of the treaty to defend itself and is the only judge in what constitutes the right of self-defense, necessity and proportionality and what they encompass.[41]

A state of emergency exists when a state is forced to use its armed forces in response to an armed attack, since there are no other means to protect its rights.

The Internationl customery law of self-defense involves the assumption that the force used must be proportional to the threat. [42]

Proportionality must be appreciated with the necessary degree of flexibility, since there is no proportionality if a State respond to small violations with disproportionate means.

Tallinn Manuel in Article 14 stipulates that: ''A use of force involving cyber operations undertaken by a State in the exercise of its right of self-defense must be necessary and proportionate.''

The right to self-defense raises the question of whether it is possible even before the actual attack takes place. This issue is particularly important for countries possessing nuclear weapons, which could be the object of a strike, but also for others, since the outcome of the war may also depend on the first use of the weapon.

Article 51 of the Charter allows self-defense only in the case of an existing armed attack. With regard to the rights of preventive self-defense, opinions are divided. While some believe that there is no right to preventative war or anticipatory self-defense, most legal writers believe that customary international law allows for such self-defense.

In 1967, Israel launched a preventive attack on its Arab neighbors over the blockade of the port of Eliat and the conclusion of a military pact between Egypt and Jordan. Significantly, in the ensuing discussions, the United Nations did not condemn this Israeli attack and the means of exercising self-defense.

Tallinn Manuel in Article 15 provides: ''The right to use force in self-defense arises if a cyber armed attack occurs or is imminent .''

---

[41] See Brownlie, I. (1963). International law and the use of force by State, Oxford University Press, p. 237, nota 4.

[42] Ibid., str. 261.

Tallinn Manuel also prescribes that he right of self-defense maybe exercised collectively. Collective self-defense against cyber operations amounting to an armed attack may only be exercised at the request of the victim - State and within the scope of the request.[43]

7. Self-defense against terrorism

In response to the 9/11 terrorist attack, the United States launched a military campaign against Afghanistan known as Operation *Enduring Freedom* on October 7, 2001.[44] In informing the Security Council about the action taken, the US claimed to be acting in self-defense. The UK also called for individual and collective self-defense. Despite earlier dilemmas regarding the right to self-defense against past terrorist attacks, these actions have received general support. Security Council resolution 1368 of 12 September 2001 explicitly recognized the right to self-defense against terrorism. Later Resolution 1373 of 14 November 2001 also invoked the individual and collective right to self-defense.

This is obviously about extending the traditional model of the right of states to self-defense. But since it is a general support for the right to self-defense in the event of a terrorist attack, a reinterpretation of the Charter's provisions is in place by creating an instant international custom that allows it.

It is now clearly accepted that a terrorist attack on state territory by non-state perpetrators is an armed attack that justifies a response against a State that provides refuge to those responsible.[45] On the occasion of this attack, NATO invoked for the first time Article 5 of the founding treaty, which stipulates that an attack on one member State will be considered an attack on all of them.

The United States and the United Kingdom believe they have the right to both anticipatory and preventive self-defense against terrorism. This right is accepted by a large number of states but only in relation to the terrorist threat but not beyond. But in this respect, too, the condition is that the Security Council, by its resolution, determines the existence of a terrorist threat.

Tallinn Manuel in Article 36 provides: '' Cyber attacks or the threat of cyber attacks, the primary objective of which is civilian terror, are prohibited.'' In this way, Tallin manuel recognizes cyber attacks as a terrorist threat subject to the same rules as any other terrorist threat.

8. Conclusion

Cyber attacks are, by their content, types of armed conflict. The application of the right of armed conflict does not depend on the classification of the armed conflict. Or on the type of

---

[43] Tallinn Manuel, art. 16.

[44] Operation Enduring Freedom , Dostupno na: http://www.history.army.mil/brochures/Afghanistan/Operation%20Enduring%20Freedom.htm, 23.12.2010.

[45] Gray, C. The use of force and the international legal order. U Evans. M. D. (ed.). (2003). International Law. Oxford: University Press. str. 604.

military operations and the methods of war used. Therefore, cyber operations alone can mean, without the presence of other types of operations, both international and non-international armed conflict.

The law of armed conflict applies to all activities undertaken during the course of an armed conflict and to any consequences arising in the territory of a State involved in an armed conflict, not limited to the area where military operations are conducted.

For cyber attacks to represent attacks relevant to the law of armed conflict, they must be of such gravity and cause physical destruction or harmful injury as other weapons: conventional, nuclear, chemical and biological. That is, a cyber attack needs to have the same consequences as other types of attacks. Or the attack need to be directed against anything called critical infrastructure.

Cyber attacks are subject to the rules of *jus ad bellum* that relate to a state's right to use force to realize its national policy. They are also subject to the *jus in bello* rules governing the conduct of armed conflicts.

Not are necessary some new sources of law to apply the right of armed conflict to cyber warfare. Cyber attacks are governed by existing legal sources: international treaties, international customs and general principles of law.

All sovereign states are, on the basis of the right to jurisdiction, empowered to exercise control over cyber infrastructure and cyber activities within their territories.

The consequences of state sovereignty over cyber infrastructure are that cyber infrastructure is subject to the legal and regulatory control of the state concerned and that state sovereignty protects such infrastructure.

A cyber attack or a serious threat of a cyber attack by one country against the cyber infrastructure of another country violates its sovereignty, which implies a state responsibility for international wrongful acts. The general rule is that only the behavior of a state authority or its agents can be attributable to the state.

A country that is the target of a cyber attack has the right to self-defense under the UN Charter, with the obligation to respect the criteria of necessity and proportionality.

Opinions are divided regarding anticipatory self-defense. But it still prevails opinion on its justification and legality.**Conclusion**

Considering that terrorism is a very dynamic social phenomenon which can change its content and forms of action, it is possible to notice its relation to the genocide. It can be further concluded that terrorism precedes genocide.

The role of terrorism as a support instrument in carrying out genocide surfaces in form of spreading fear and forced movement or expulsion of the population from a certain territory.

It is important to underline that terrorism and genocide have a common denominator – force and violence.

Literature

a) Books and articles:

1. Akehurst's modern introduction to International Law, seventh revised edition, 1997. London and New York: Routledge.
2. Brownlie, J: International Law and the use Force by States, Oxford University Press 1963.
3. Bowett, D. W.: Self - Defence in International Law, Manchester University Press, 1958.
4. Carter/Trimble/Bradley. (2003) International Law, forth edition. New York: Aspen Publisher
5. Dinstein, Y.: War, Agression and Self -Defence, Cambridge University Press, 1994.
6. Harris (2004) Cases and Materials on International Law, sixth edition. London: Thomson, Sweet§Maxwell.
7. Mateusz Piatkowski, The Definition of the Armed Conflict in the Condition of Cyber Warfera, Polish politikal Science Yearbook vol. 46 (2017) pp. 271 – 280.
8. Michael N Smitt, ''Attack'' as a Term of Art in International law: The Cyber Operations Context. 2012 4thInternational Conferenc on Cyber Conflict. (283-293).
9. Softić, S. (2012). MEĐUNARODNO PRAVO. Sarajevo: DES doo - Sarajevo.
10. Shaw, N. M. (2008) International Law, sixth edition, Cambridge: Cambridge University Press.

b) Other sources:

1. Tallinn manual o međunarodnom pravu koje se primjenjuje na cyber ratovanje. General editor Michael N Schmitt. Cambridge University Press 2017.
2. International Court Of Justice Reports Of Judgments, Advisory Opinions And Orders Legality Of The Threat Or Use Of Nuclear Weapons Advisory Opinion Of 8 July 1996.
3. United Nations A/RES/56/83 from 28 January 2002. Responsibility of States for internationally wrongful acts. http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf.
4. Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgement, ICT Reports 1986.
5. Convention on Cybercrime 185 CETS (opened for signature 23 November 2001, entered into force 1 July 2004).

About the author

Sakib Softić, redovni profesor na Univerzitetu u Sarajevu, FKKSSS. Oblast: Međunarodno pravo. Predavao na Pravnom fakultetu Univerziteta u Tuzli i na AAB Univerzitetu u Prištini. Agent Bosne i Hercegovine u predmetu koji se odnosi na primjenu Konvencije o sprečavanju i kažnjavanju zločina genocida pred Međunarodnim Sudom Pravde u Hagu (BiH protiv Srbije i Crne Gore). Pravni savjetnik bošnjačkih članova Predsjedništva BiH u periodu od 2002. do 2009. godine. Sudija arbitražnog suda OSCE-a u Ženevi.