INTERNATIONAL LEGAL DEFINITION OF A CYBERATTACK

Khatuna Burkadze
Business and Technology University,
Doctor of Law, Professor

Abstract. In the era of information and communication technologies, computer networks can be used to carry out modern forms of warfare. In light of technological advances, cyberattacks are becoming more sophisticated and control over IT infrastructure is being lost. States can use digital tools or enlist hacker groups to launch cyberattacks against other states. Such destructive actions damage the defence capacity, security, stability, and economic sustainability of a country, and hinder the activities of public and private organisations alike. The situation is further complicated due to the lack of a common understanding of the definition of the term „cyberattack" among international actors. Furthermore, the existing international legal framework does not regulate the issue of cyberattacks. The Charter of the United Nations was adopted in the 20th century when the process of creating cyberspace could not have been foreseen. Therefore, this article aims to explore the legal definition of a cyberattack based on the reinterpretation of existing international norms. It is important to examine the possibilities of the development and adoption of new norms in cyberspace and clarify the responsible cyber behaviour of states.

Keywords: cyberattack, the use of force, armed attack

INTRODUCTION

Cyberattacks as a new category of attacks are different from traditional hostilities. Unlike the latter, cyberattacks can also be carried out during peacetime. Furthermore, instead of kinetic force, an attacker uses computer networks to gain unauthorised access to information systems to disrupt or manipulate data. Also, cyber threat is not constrained by political and geographical boundaries[1]. This allows the parties who initiate and carry out cyberattacks to remain anonymous. The difficulty of identifying the enemy leaves room for the aggressor state to take more destructive actions against the victim, making it difficult to identify the aggressor promptly and respond appropriately.

The cyberattacks against Estonia in 2007 and against Georgia in 2008 highlighted the need

1. Michael Schmitt, „Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework", 37 Columbia Journal of Transnational Law, (1998-1999), 888.

to develop cyber defence capabilities. Unlike the Estonian case, in August of 2008, the Russian Federation launched cyberattacks against Georgia alongside conventional military actions. Georgia still faces cyber challenges. For example, on 28 October 2019, the Russian Federation carried out large-scale cyberattacks to damage Georgia's critical infrastructure again. Overall, the Kremlin conducted these cyberattacks in an attempt to undermine Georgia's national security, sow discord and disrupt the lives of the population of Georgia by hindering the operation of various organisations, including the state authorities.

In the digital era, the national security policies of states focus on the protection of their interests in cyberspace. Since cyberspace is not limited by boundaries, it amplifies the scale of the accompanying challenges. The nature of cyberattacks requires analysis of the current international legal framework and subsequent identification of the trends, by which states will be able to respond effectively to these attacks and protect their interests. The urgency of the issue is highlighted by the absence of international agreements that would directly regulate the international legal issues related to cyberattacks and cyberwarfare. The only existing international legal document is the Convention on Cybercrime, which was adopted by the Council of Europe[2]. However, it deals with cybercrime and does not address cyberattacks as a form of warfare.

DEFINITION OF THE USE OF FORCE IN INTERNATIONAL LAW IN THE CONTEXT OF CYBERATTACKS

To explore, in the digital era, how a cyberattack can cross the threshold of the use of force, it is important to define the core elements of the concept of the use of force. To maintain international peace and security, the states agreed to derail from monopolising the use of force and permit the use of force only in exceptional cases defined under international law.

The contemporary international legal definition of the use of force is based on the Charter of the United Nations. The authors of the Charter wished to ban any use of force but at the same time envisaged a few exclusions.

One of the reasons for establishing the United Nations was to modernise international law in the 20th century. Leaders decided to establish a system that would be based on respect for the obligations arising from treaties and other sources of international law[3]. From their perspective, it was necessary to protect future generations from another world war.

Modern legal regulation of the use of force and conflict begins with the Charter of the United Nations, and specifically with Article 2(4) thereof, which mandates[4] that „all Members shall

2. „Convention on Cybercrime", Budapest, 23.XI.2001, Council of Europe, https://rm.coe.int/1680081561 (Accessed April 23, 2022).
3. Charter of the United Nations, http://www.update.un.org/en/documents/charter/intro.shtml (Accessed April 23, 2022).
4. Matthew C. Waxman, „Cyber Attacks as Force under UN Charter Article 2(4)", 87 International Law Studies Series, US Naval War College, 44 (2011).

refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or any other manner inconsistent with the purposes of the United Nations"[5].

The wording of Article 2(4) of the Charter of the United Nations illustrates that the authors of the document chose to use the broader term „use of force" instead of „war". The latter refers to a specific set of circumstances that usually begins with the declaration of war and ends with the conclusion of a peace treaty. Such prohibition led to countries using other terms such as „military operation" to create a perception that they were not violating the norms prohibiting war. Therefore, taking into consideration the international practice, it became necessary to develop a broader concept. Thus, the term „use of force" covers all forms of hostilities, both nominal wars and incidents falling short of an official state of war, which ranges from minor border clashes to extensive military operations. Thus, the prohibition of the use of force is not dependent on how the involved states prefer to define their military conflict[6]. Furthermore, in its argument on a case concerning Nicaragua, the International Court of Justice has rejected a narrow interpretation of „use of force". The Court held that a state's arming and training of guerrilla forces engaged in hostilities against another state qualified as a use of force[7].

However, every unfriendly act does not cross the use of force threshold. In the case of Nicaragua, the Court held that financing guerrillas, albeit an unlawful „intervention", did not rise to that level[8]. It is also noteworthy that the authors of the Charter of the United Nations did not include measures of economic coercion in the notion of the use of force. It may be concluded that cyber operations intended to economically coerce another state to engage in, or desist from, a particular course of action would not amount to a use of force; nor would financing a rebel group's cyber operations[9].

In assessing whether an event constituted a use of force in or through cyberspace, it is essential to evaluate the following factors: the context of the event, the actor perpetrating the action, the target and location, effects, and intent[10]. Under these factual circumstances, whether a cyberattack reaches an appropriate level of an act of violence that is equivalent to the use of force, it may be concluded that Article 2(4) of the Charter of the United Nations applies to cyberspace. Furthermore, the document does not provide an exact definition of the use of force. The analysis of the international practice shows that the use of force is not limited only to one type of coercive method, but rather combines kinetic, non-kinetic, regular, and irregular means. Thus, the legality of the use of cyberweapon depends on the interpretation of the existing international norms that determine the scope of the exceptional cases of the use of force.

5. See supra note 3.
6. René Värk, „The Use of Force in the Modern World: Recent Developments and Legal Regulation of the Use of Force", 2 Baltic Defence Review, 29-30 (2003).
7. Michael N. Schmitt, „The Law of Cyber Warfare: Quo Vadis?", 25 Stanford Law & Policy Review, (Spring, 2014), 279, 280.
8. Id., 280.
9. Id.
10. Antonia Chayes, „Rethinking Warfare: The Ambiguity of Cyber Attacks", 6 Harvard National Security Journal, (2015), 507.

INTERNATIONAL LEGAL REGULATION OF THE USE OF FORCE IN ACCORDANCE WITH THE CHARTER OF THE UNITED NATIONS AND THE NORTH ATLANTIC TREATY

The Charter of the United Nations, which determines fundamental rules of relations among the states, and the North Atlantic Treaty, the founding treaty of NATO, were adopted in 1945 and 1949, respectively. At that time, the issues of cyberspace could not have been taken into consideration by the global and regional systems, as it was a matter of the future. Nevertheless, in the face of growing cyberattacks, the need to clarify the existing international legal norms to allow countries to properly adapt to digital reality has come to the fore. In this regard, in 2013, the Group of Governmental Experts of the United Nations (UN GGEs) published its third report, according to which the Charter of the United Nations applies to digital space[11].

As for NATO's official position on the interconnection between the existing international legal regulations and cyberspace, the Wales Summit Declaration issued on 4-5 September 2014 states that NATO member countries agreed that international law, including international humanitarian law and the Charter of the United Nations, applies in cyberspace. They believe that cyberattacks can reach a threshold that threatens national and Euro-Atlantic security. Their impact could be as harmful to modern societies as a conventional attack. Therefore, NATO leaders affirm that cyber defence is part of NATO's core task of collective defence[12]. Furthermore, before the adoption of the Wales Summit Declaration, the NATO Cooperative Cyber Defence Centre of Excellence launched an international research project in Estonia in 2009. The Tallinn Manuals[13], published in 2013 and 2017, provide the International Experts' analysis of how existing international law applies to cyber warfare and cyber operations.

According to the Charter of the United Nations, the Security Council is responsible for maintaining international peace and security. This mandate gives the Security Council the discretion to determine what types of actions threaten international peace. In the cases of any threat to the peace, or breach of the peace, the Security Council decides on the measures necessary to maintain international peace. Such measures may include complete or partial interruption of economic relations, rail, sea, air, postal, and other means of communication, and the severance of diplomatic relations, with an aggressor state[14]. Whether the Security Council considers that the aforementioned measures are inadequate for maintaining peace, under Article 42 of the Charter of the United Nations,

11. Back to Square One? The NATO Cooperative Cyber Defence Centre of Excellence, https://ccdcoe.org/back-square-one-fifth-un-gge-fails-submit-conclusive-report-un-general-assembly.html (Accessed April 26, 2022).
12. The Wales Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, September 4-5, 2014, https://www.nato.int/cps/ic/natohq/official_texts_112964.htm (Accessed April 26, 2022).
13. The Tallinn Manual, The NATO Cooperative Cyber Defence Centre of Excellence, https://ccdcoe.org/research/tallinn-manual/(Accessed April 26, 2022).
14. See supra note 3, 5.

it may take action by air, sea, or land forces[15]. Simultaneously, the International Group of Experts agreed that any action undertaken based on this rule may be implemented by, or against, cyber capabilities[16]. All or some members of the United Nations may become involved in a collective security operation according to the decision taken by the Security Council. Thus, threats to international peace, breach of the peace, or act of aggression thereof constitute the exceptional cases in which countries may use force to ensure peace and security based on the permission of the Security Council.

Another exception to the general prohibition of the use of force is defined by Article 51 of the Charter of the United Nations, according to which each member of the United Nations has the inherent right of individual or collective self-defence if an armed attack occurs against it until the Security Council has taken measures necessary to maintain international peace and security[17]. According to the International Customary Law, a response to an armed attack should be proportional and necessary[18]. In addition to this, it should be mentioned that the criteria of proportionality and necessity are supplemented by the third criteria of need for the imminence of response[19]. The principle of proportionality limits any defensive action to that necessary to defeat an ongoing attack or to deter or pre-empt a future attack[20]. As for the principle of necessity, to meet this criterion, the state should demonstrate that it used all peaceful means including diplomatic, economic, judicial, or other measures for deterring an armed attack including a cyberattack. However, the state was unable to achieve this goal. It had to use force against an attack because all non-forceful options were exhausted.

As for the collective defence, Article 5 of the North Atlantic Treaty is noteworthy in this regard. Under Article 5 of the North Atlantic Treaty, NATO member countries agree that an armed attack against one or more of them shall be considered an attack against them all[21]. According to the Wales Summit Declaration: „a decision as to when a cyberattack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis“[22]. This means that, on the one hand, international legal norms related to the exceptional cases of the use of force apply to cyberattacks. On the other hand, it is not determined in which cases Article 5 should be invoked for deterring cyberattacks, and it depends on a set of factual circumstances that would convince the leaders of the need for a collective defence operation. In addition, the scope provided by Article 51 of the

15. Id.

16. Tallinn Manual 1.0 on the International Law Applicable to Cyber Warfare, (Michael N. Schmitt, ed.), Cambridge University Press, (2013), 71.

17. See supra note 3, 5, 14.

18. Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. the United States of America), 1986, http://www.icj-cij.org/docket/ index.php (Accessed April 28, 2022).

19. Michael N. Schmitt, Preemptive Strategies in International Law, Michigan Journal of International Law, (2003), 55.

20. Id.

21. Founding Treaty – the North Atlantic Treaty, April 4, 1949, https://www.nato.int/cps/en/natohq/topics_67656.htm (Accessed Last seen: April 29, 2022).

22. See supra note 12.

Charter of the United Nations and the International Customary Law should be taken into consideration in the case of using force.

Analysis of the international legal regulation of the use of force would suggest that the use of cyber force is illegal if it does not comply with the exceptional cases and criteria established by the existing international law. Cyber operations should be carried out within the scope of individual and collective self-defence and based on a decision made by the Security Council in the cases of threat to the peace, breach of the peace, or act of aggression while implementing collective security measures.

DEFINITION OF A CYBERATTACK AS A NEW FORM OF ATTACK

The analysis of the international legal framework for the exceptional cases of the use of force suggests that an armed attack represents the international legal basis for exercising the right to individual or collective self-defence. In addition to this, scholars agree that an armed attack is an active attack that has already taken place, rather than the threat of such an attack[23].

Although Article 51 of the Charter of the United Nations determines the basis for exercising the right of self-defence, it does not define an armed attack. The document does not determine the criteria, based on which an action rises to the level of an attack. In this regard, Rule 13 of the Tallinn Manual entitled „Self-Defense against Armed Attacks“ states that „a state that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defense. Whether a cyber operation constitutes an armed attack depends on its scale and effects“ (Tallinn Manual, 2013)[24].

The Nicaragua case is significant in the context of the „scale and effects“ model assessment. In the Nicaragua Judgment, the International Court of Justice initially identified the „scale and effects“ criteria as those qualitative and quantitative elements that help differentiate an „armed attack“ from „a mere frontier incident“[25].

Given the consequences of an armed attack, the definition of a cyberattack developed by the authors of the Tallinn Manual is significant. According to Rule 30 of the document, „A cyberattack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects”[26]. This definition indicates that the harm caused by a cyber operation should be similar to the

23. Yoram Dinstein, War, Aggression and Self-Defence, Fourth Edition, Cambridge University Press, (2005), 165-169.

24. Kosmas Pipyros, Christos Thraskias, Lilian Mitrou, Dimitris Gritzalis, Theodoros Apostolopoulos, “A new strategy for improving cyber-attacks evaluation in the context of Tallinn Manual”, 74 Computers and Security, (2018), 375.

25. Id., at 376.

26. See supra note 16, 106.

harm caused by conventional sea, land, or air forces. A cyberattack that does not result in serious casualties might not be qualified as a new form of attack that provides grounds for the application of either Article 51 of the Charter of the United Nations or Article 5 of the North Atlantic Treaty[27].

Operating cyberspace without borders increases the number of actors carrying out cyberattacks. From the international legal point of view, Article 51 of the Charter of the United Nations does not specify who can carry out an armed attack against a state. This does not exclude the possibility of an attack against a state by a non-state actor from the territory of another state. In this context, Professor Michael Schmitt highlights that future cyber operations will weaken the ICJ's narrow interpretation of actors of armed attacks. For non-state actors, cyberspace is a domain where it is easier to acquire appropriate means for carrying out offensive operations[28].

A cyberattack can be defined as an attack that uses the capabilities of computer networks to unlawfully gain access to critical information systems, disrupt or manipulate data to undermine the country's defence, and security, impede the development of a state and cause harm to the society with the scales and effects of the damage equivalent to a conventional operation. Furthermore, the nature of cyberspace allows a state to remain anonymous while attacking another state, and cause harm by enlisting a group of hackers, without conducting conventional military actions against the country.

CONCLUSION

Information and communication technologies have transformed the forms of warfare and facilitated the reinterpretation of an armed attack. The existing international legal norms, including the Charter of the United Nations and the North Atlantic Treaty, apply to cyberattacks because the latter can threaten the national security of states and cause as much harm to countries and their societies as conventional attacks.

Given the above, it is important to clarify some parameters of the international legal definition of a cyberattack based on Article 51 of the Charter of the United Nations and Article 5 of the North Atlantic Treaty. First, according to those articles, an armed attack represents a legal ground for a victim state to use individual or collective defence mechanisms. Second, because of the destructive nature of a cyberattack, such action can reach a threshold of an armed attack. In this context, based on the interpretation of the Tallinn Manual, it is noteworthy that if a cyberattack causes serious injury or death to persons or damage or destruction to objects which hinders the ordinary functioning of a state, it is an armed attack, i.e., equivalent to the most severe form of the use of force. Third, the notion of a cyberattack

27. See supra note 10, 482.

28. See supra note 7, 287.

should not be limited by a state actor. Such destructive actions can be carried out by both state and non-state actors. Furthermore, Article 51 of the Charter of the United Nations does not provide for a limitation that an attack is carried out only by one state against another. The advances in digital technologies allow non-state actors to develop offensive cyber tools. In particular, if a non-state actor carries out a cyber-attack through the sponsorship and within the territory of a sponsor state against the other state, such a cyberattack may trigger an invocation of the right to defense.

It is noteworthy that the Tallinn Manuals are not binding documents. They only provide the reinterpretation of the existing international legal framework. Therefore, it is necessary to hold active discussions among states in both global and regional formats to eliminate ambiguity in international legal aspects of cyberspace. From a realistic point of view, ambiguity may be strategically advantageous for certain states to launch new offensive operations and remain anonymous in a new operational domain of the digital world. However, new technological advances with their opportunities and challenges will facilitate a dialogue among actors of the international community to think about a new international regime – an international cyber regime. The international cyber regime will define the rules for responsible behaviour of states in cyberspace, and establish the relevant forms of international legal accountability for those who will violate the new norms. This process will help ensure cyber security and protect the critical information systems of states.

REFERENCES

1. Antonia Chayes. „Rethinking Warfare: The Ambiguity of Cyber Attacks“. Harvard National Security Journal, (2015).
2. Back to Square One? The NATO Cooperative Cyber Defence Centre of Excellence, https://ccdcoe.org/back-square-one-fifth-un-gge-fails-submit-conclusivereport-un-general-assembly.html.
3. Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. the United States of America), 1986, http://www.icjcij.org/docket/ index.php.
4. Charter of the United Nations, http://wwwupdate.un.org/en/documents/charter/intro.shtml.
5. Founding Treaty – the North Atlantic Treaty, April 4, 1949, https://www.nato.int/cps/en/natohq/topics_67656.htm.
6. Kosmas Pipyros. Christos Thraskias. Lilian Mitrou. Dimitris Gritzalis. Theodoros Apostolopoulos. „A New Strategy for Improving Cyber Attacks Evaluation in the Context of Tallinn Manual“. 74 Computers and Security, (2018).
7. Matthew C. Waxman. „Cyber Attacks as Force under the U.N. Charter Article 2(4)“. 87 International Law Studies Series, the U.S. Naval War College, (2011).
8. Michael Schmitt. „Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework“. Columbia Journal of Transnational Law, Volume 37, (1998-1999).
9. Michael N. Schmitt. „Preemptive Strategies in International Law“. Michigan Journal of

International Law, (2003).

10. Michael N. Schmitt. „The Law of Cyber Warfare: Quo Vadis?“ 25 Stanford Law & Policy Review, (Spring, 2014).
11. René Värk. „The Use of Force in the Modern World: Recent Developments and Legal Regulation of the Use of Force“. Baltic Defence Review No. 10, Volume 2, (2003).
12. Tallinn Manual 1.0 on the International Law Applicable to Cyber Warfare, (Michael N. Schmitt, ed.), Cambridge University Press, (2013).
13. The Wales Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, September 4-5, 2014, https://www.nato.int/cps/ic/natohq/official_texts_112964.htm.
14. Yoram Dinstein. War, Aggression, and Self-Defence. The Fourth Edition, Cambridge University Press, (2005).