June 2022 (№22)
Volume 8; Issue 2; Page No. 17-23
ISSN: 2346-7916 (Print)
ISSN: 2587-5043 (Online)

INTERNATIONAL JOURNAL OF LAW: "LAW AND WORLD" www.lawandworld.ge

https://doi.org/10.36475/8.2.2


# International Legal Basis for the Right to Defense in the Cyber Era

Khatuna Burkadze
*Professor, Business and Technology University*

ARTICLE INFO

*Article History:*

Received 10.06.2022
Accepted 17.06.2022
Published 30.06.2022

*Keywords:*

Cyberattack,
Defense,
State and Non-state Actors

ABSTRACT

Against the background of the growing development of information and communication technologies and the digital transformation of various fields, it has become possible to produce war using digital tools. Today a cyberattack can cause similar or more damage than a conventional operation. This, in turn, changes the traditional perception of armed attack and creates the possibility to say that cyberattacks may significantly harm the country's defense capabilities, and security, and impede the development of the society and state. Illegal access to computer networks could cause substantial damage to the functions of the critical information system, the protection of which is directly related to the vital interests of the state. This fact leads to a new understanding of the international legal basis of the right to defense. In particular, the purpose of the article is to analyze whether a cyberattack is the international legal basis that enables a state to exercise the right of defense and protect its sovereign interests.

## INTRODUCTION

The current international legal norms do not correspond to the reality created by the digital world, because the basic documents of modern international law were adopted in the last century. Consequently, the non-digital age could not foresee the needs of the digital age. Before international actors can agree on the need to develop an international digital regime at the global level, it is necessary to analyze issues related to the response of the state to cyberattacks based on the interpretation of existing international norms.

Unfortunately, states become targets of cyberattacks regularly, and due to the nature of cyberspace, it is difficult to promptly identify an adversary, making it difficult to protect the country's interests in a timely and effective manner. Furthermore, one state can hire a group of hackers against another state and cause significant damage without crossing the border and carrying out a conventional operation.

Even though there is no international legally binding document to define and regulate cyberattacks at both global and regional levels, Tallinn Manuals were published in 2013 and 2017 with the support of NATO, which provide a reinterpretation of existing binding international norms regarding cyber issues. 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*".[1] Consequently, this means that a cyberattack can reach the threshold of an armed attack and this increases the likelihood that such an act could become the basis for a state to exercise its right of defense, which is governed by Article 51 of the Charter of the United Nations. Thus, the analysis of the international legal basis of the right to defense in the digital age requires both a reinterpretation of Article 51 and a clarification of the factual circumstances and criteria by which a cyberattack represents a legal basis to exercise the right of defense.

## THE REINTERPRETATION OF ARTICLE 51 OF THE CHARTER OF THE UNITED NATIONS IN THE CYBER ERA

Article 51 of the Charter of the United Nations defines the basis for exercising the right of self-defense. According to the article, a state has 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 measures to maintain international peace.[2] Therefore, an armed attack represents a legal basis for using the right of self-defense. However, Article 51 does not determine the concept of an attack. It is necessary to define the term an armed attack.

In this regard, an armed attack should be understood as including not merely action by regular armed forces across an international border, 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 an actual armed attack conducted by regular forces.[3] The majority of scholars agree that an armed attack is an active attack that has already taken place, rather than the threat of such an attack.[4]

In the digital era information and communication technologies have changed the traditional understanding of warfare. In the light of the above, it is essential to explore when a cyberattack reaches the level of an armed attack and under which circumstances states can have the right to use individual or collective defense against a cyberattack as an armed attack.

In determining if a cyberattack has risen to the level of an armed attack, the instrument-based approach, the target-based approach, and the effects-based approach have emerged in this context.[5] The self-defense component of Article 51 of

1 Tallinn Manual 1.0 on the International Law Applicable to Cyber Warfare, (Michael N. Schmitt, ed.), Cambridge University Press, (2013), 106.

2 Charter of the United Nations, <http://www.update.un.org/en/documents/charter/intro.shtml> [Last seen: June 12, 2022].

3 Nicaragua v. the United States of America, (1986). Case Concerning Military and Paramilitary Activities in and against Nicaragua, p. 93.

4 Dinstein, Y., (2005). "War, Aggression and Self-Defence", Fourth Edition, *Cambridge University Press*, pp. 165-169.

5 Moore, S., (2013). Cyber Attacks and the Beginnings of an International Cyber Treaty, 39 *The North Carolina Journal of International Law and Commercial Regulation*, p. 247.

the Charter of the United Nations was drafted with an instrument-based approach.[6] Professor Michael Schmitt argues this choice by the drafters of the Charter of the United Nations to use an instrument-based approach is inappropriate for addressing self-defense claims against cyberattacks. Because armed attacks inherently include kinetic military force, and cyberattacks often utilize non-kinetic approaches, the instrument-based approach fails to encapsulate cyberattacks that do not look like armed attacks but have the same ultimate effect.[7] Instead, he argues an effects-based approach, though not the current norm of international law, would better address cyberattacks because it allows broader latitude for a state to respond in self-defense.[8]

Particularly, Professor Michael Schmitt argues that a cyberattack's effects should be measured by reference to six factors: (1) Severity: the type and scale of the harm; (2) Immediacy: how quickly the harm materializes after the attack; (3) Directness: the length of the causal chain between the attack and the harm; (4) Invasiveness: the degree to which the attack penetrates the victim state's territory; (5) Measurability: the degree to which the harm can be quantified; and (6) Presumptive legitimacy: the weight given to the fact that, in the field of cyber-activities as a whole, cyberattacks constituting an armed attack are the exception rather than the rule.[9]

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).[10]

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".[11]

The harm caused by a cyber operation should be similar to the 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 Article 51 of the Charter of the United Nations.[12]

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 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.[13]

In view of the above, it is important to clarify some parameters of reinterpretation of Article 51 of the Charter of the United Nations. First, this article defines that an armed attack represents a legal ground for the victim state to use individual or collective defense mechanisms. Second, because of the destructive nature of cyberattacks, the interpretation of Article 51 of the Charter of the United Nations has been expanded to include cyberattacks as armed attacks. Particularly, the International Group of Experts agreed that "scale and effects" are qualitative and quantitative factors that would apply when determining if a cyber operation qualifies as the gravest form of use of force (armed attack).[14] According to Tallinn Manual 1.0 cyberattacks rise to the level of an armed attack if they cause injury or death to persons or damage or destruction to objects.[15] Third, due to

6 Id., at 248.
7 Id.
8 Id.
9 Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The Law of Cyber-Attack. *California Law Review*, 100(4), p. 847.
10 Pipyros, K., Thraskias, Ch., Mitrou, L., Gritzalis, D., & Apostolopoulos, T., (2018). "A new strategy for improving cyber-attacks evaluation in the context of Tallinn Manual", 74 *Computers and Security*, p. 375.
11 Id.
12 Chayes, A., (2015). "Rethinking Warfare: The Ambiguity of Cyber Attacks", 6 Harvard National Security Journal, p. 482.
13 Michael N. Schmitt, (Spring, 2014). "The Law of Cyber Warfare: Quo Vadis?", 25 Stanford Law & Policy Review p. 287.
14 Voitasec, D., (2015). Applying International Humanitarian Law to Cyber-Attacks, *22 Lex ET Scientia International Journal*, p. 126.
15 See supra note 1.

the reinterpretation of the term an armed attack, the notion of a cyberattack should not be limited by the state actor. Particularly, such destructive actions can be carried out by both state and non-state actors.

## CRITERIA FOR EXERCISING THE RIGHT OF DEFENSE

According to the International Customary Law, defense measures should be proportional to the armed attack and necessary to respond to it.[16] The International Court of Justice reaffirmed the need to abide by criteria of proportionality and necessity while responding to an armed attack in its decision in 2003, in a case concerning Oil Platforms.[17] Therefore, this means that there are defined principles that should be protected by states in cases of exercising the right of defense. In view of the above, it is important to understand how these criteria can be used by states to respond to cyberattacks.

In addition to this, it should be mentioned that the third criterion is imminency. The third requirement *"appears to impose a restrictive test in which the defensive force can only be used just as the attack is about to be launched"*.[18]

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 the cyberattack. However, the state was unable to achieve this goal. It had to use force against cyberattack because all non-forceful options were exhausted.

Proportionality is the fundamental component of the Law on the Use of Force.[19] Historically, it is part of the Just War Theory.[20] The proportionality limits any defensive action to that necessary to defeat an ongoing attack or to deter or preempt a future attack.[21]

Proportionality addresses the issue of how much force, including the use of cyber force, is permissible once force is deemed necessary. The criterion limits the scale, scope, duration, and intensity of the defensive response to that required to end the situation that has given rise to the right to act in self-defense.[22] It does not restrict the amount of force used to that employed in the armed attack since the level of force needed to successfully mount a defense is context-dependent; more force may be necessary, or less force may be sufficient, to repel the attack or defeat one that is imminent. In addition, there is no requirement that the defensive force is of the same nature as that constituting the armed attack. Therefore, a cyber use of force may be resorted to in response to a kinetic armed attack, and vice versa.[23]

The proportionality requirement should not be overstated. It may be that the originator of the cyber armed attack is relatively invulnerable to cyber operations. This would not preclude kinetic operations to compel the attacker to desist, although they must be scaled to that purpose.[24] Overall, the abidance of the criteria of self-defense can legitimize the use of cyber force if it is lawful under the exceptional cases of the use of force defined by the existing international legal norms.

16 See supra note 3, 84.

17 Case Concerning Oil Platforms (the Islamic Republic of Iran v. the United States of America), ICJ, (2003). <http://www.icj-cij.org/docket/fi les/90/9745.pdf> [Last seen: June 14, 2022].

18 Michael N. Schmitt, (2003). Preemptive Strategies in International Law, *Michigan Journal of International Law*, p. 533.

19 Gardam, J. G., (July 1, 1993). "Proportionality and Force in International Law", *American Journal of International Law*.

20 See James Turner Johnson, Ideology, Reason and the Limitation of War (1975); Frederick H. Russel, The Just War in the Middle Ages (1975).

21 See supra note 18, at 532.

22 See supra note 1, 15, at 62.

23 Id., at 62-63.

24 Id., at 63.

## THE PRINCIPLE OF COLLECTIVE SELF-DEFENSE UNDER ARTICLE 5 OF THE NORTH ATLANTIC TREATY

The right of collective defense authorizes state or multiple states to come to the assistance of another state that is the victim of an armed attack. This right, explicitly set forth in Article 51 of the Charter of the United Nations, reflects customary international law. When a state exercises collective self-defense on behalf of another state, it must do so within the scope of the other's request and consent. In other words, the right to engage in collective self-defense is subject to the conditions and limitations set by the victim state. That state may, for instance, limit the assistance to non-kinetic measures or to passive rather than active cyber defenses.[25]

An example of a collective defense treaty is the North Atlantic Treaty. Under Article 5 of this document, NATO member countries agree that an armed attack against one or more of them shall be considered an attack against them all.[26] 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"*.[27] 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 factual circumstances that would convince the leaders of the need for a collective defense operation. In addition, the scope provided by Article 51 of the Charter of the United Nations and the International Customary Law should be taken into consideration in the case of using force.

In this context, it is important to analyze NATO's other decision concerning cyberspace. At the Warsaw Summit the Allies: *"recognize cyberspace as a domain of operations, in which, NATO must defend itself as effectively as it does in the air, on land, and at sea"*.[28] Based on this clarification, it should be noted that: (1) NATO's historical understanding of the core elements of collective defense has been changed. Historically, NATO focused on land, air, and naval defense capabilities. Because of the cyber threats, the Alliance should defend itself in cyberspace as effectively as it does in the air, on land, and at sea. (2) By recognizing cyberspace as an operational domain, the cyber defense will continue to be integrated into the Alliance's operations and missions. NATO will focus on not only land, air, and naval defense capabilities, but also cyber defense capabilities. Currently, the Alliance has the best practice of how to improve cyber resilience through enhancing institutional cyber capacity and implementing multinational exercises, training, projects, and other activities.

## CONCLUSION

Based on the reinterpretation of Article 51 of the Charter of the United Nations in the digital age, it should be noted that a state has the right to carry out a defensive operation not only in the event of a conventional military operation but also in the case of a cyberattack, if the latter with the consideration of quantitative and qualitative elements reaches the threshold of the most extreme form of use of force – armed attack. In particular, the exercise of the right of defense depends on the scale and effects of the cyberattack. The substantial damage caused by a cyberattack to the state's defense capabilities, security, stability, economic development, and the normal functioning of society represents the legal basis for the country to use individual or collective defense mechanisms to defend its interests in a timely and effective manner.

In addition, the state must carry out a defensive operation against cyberattacks within the criteria developed by international customary law. In particular, the state must adhere to the principles of necessity, proportionality, and imminence.

25 Id., at 67.

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

27 The Wales Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, (4-5 September 2014). <https://www.nato.int/cps/ic/natohq/official_texts_112964.htm> [Last seen: April 29, 2022].

28 The Warsaw Summit Communiqué issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw, (8-9 July, 2016). <https://www.nato.int/cps/en/natohq/official_texts_133169.htm> [Last seen: April 29, 2022].

In the context of collective defense, it should be noted that bilateral and especially multilateral agreements of mutual assistance help states overcome common challenges in cyberspace and strengthen cyber defense capabilities against offensive cyber operations carried out without crossing the border of the target state.

Not only state but also non-state actors have access to cyberspace. Furthermore, the latter can develop offensive means by using digital tools, making them easier to operate in cyberspace without crossing boundaries. Consequently, a cyber attack against a state may be carried out not only directly by another state, but also by a non-state actor. Such an explanation is consistent with Article 51 of the Charter of the United Nations, as it does not specify who may be the subject of an attack against a state. Therefore, it creates a legal ground for the broader interpretation of the actor of an armed attack. Particularly, states can carry out indirectly cyberattacks against other states by using special hackers' groups established and sponsored by themselves. In such cases it is necessary to take into consideration the following criteria: (1) Cyberattacks should be conducted by a non-state actor under the support and sponsor of another state; (2) Cyberattacks should be directed from the sponsor country against the other state; (3) Cyberattacks should reach the sufficient gravity of the armed attack. Therefore, if a cyberattack carried out by a non-state actor meets these requirements, it could serve as a basis for individual or collective defense.

Finally, it can be said that digital technologies have led to the development of new types of attacks that can replace conventional operations and with the scope of their impacts and results, reach the threshold of an armed attack. This digital reality expands the key fields of defense policies of states, as with the consideration of the naval, land, and air components it becomes necessary to develop cyber defense capabilities to protect the sovereign interests of countries in cyberspace.

BIBLIOGRAPHY:


1. Chayes, A., (2015). "Rethinking Warfare: The Ambiguity of Cyber Attacks", 6 *Harvard National Security Journal*;
2. Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. the United States of America), 1986;
3. Case Concerning Oil Platforms (the Islamic Republic of Iran v. the United States of America), ICJ, (2003). <http://www.icj-cij.org/docket/fi les/90/9745.pdf>
4. Charter of the United Nations, <http://www.update.un.org/en/documents/charter/intro.shtml>
5. Voitasec, D., (2015). Applying International Humanitarian Law to Cyber-Attacks, 22 *Lex ET Scientia International Journal*;
6. Founding Treaty – the North Atlantic Treaty, (April 4, 1949). <https://www.nato.int/cps/en/natohq/topics_67656.htm>
7. Frederick H. Russel, (1975). The Just War in the Middle Ages;
8. Johnson, J. Turner., (1975). Ideology, Reason and the Limitation of War;
9. Gardam, J. Gail., (July 1, 1993). "Proportionality and Force in International Law", *American Journal of International Law*;
10. Pipyros, K., Thraskias, Ch., Mitrou, L., Gritzalis, D., & Apostolopoulos, T., (2018). "A new strategy for improving cyber-attacks evaluation in the context of Tallinn Manual", 74 *Computers and Security*;
11. Michael N. Schmitt, (2003). "Preemptive Strategies in International Law", *Michigan Journal of International Law*;
12. Michael N. Schmitt, (Spring, 2014). "The Law of Cyber Warfare: Quo Vadis?", 25 *Stanford Law & Policy Review*;
13. Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). "The Law of Cyber-Attack". 100 *California Law Review*;

14. Moore, S., (2013). “Cyber Attacks and the Beginnings of an International Cyber Treaty”, 39 *The North Carolina Journal of International Law and Commercial Regulation*;
15. Tallinn Manual 1.0 on the International Law Applicable to Cyber Warfare, (Michael N. Schmitt, ed.), *Cambridge University Press*;
16. The Wales Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, (4-5 September 2014). <https://www.nato.int/cps/ic/natohq/official_texts_112964.htm>
17. The Warsaw Summit Communiqué issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw, (8-9 July 2016). <https://www.nato.int/cps/en/natohq/official_texts_133169.htm>
18. Dinstein, Y., (2005). “War, Aggression and Self-Defence”, Fourth Edition, *Cambridge University Press*.