AGGRESSION IN CYBERSPACE AND SELF-DEFENCE

Qaisar NASRAT*

Abstract

Cyber attack is a new phenomenon that can change the classical warfare techniques carried out by state and non-state actors. The unique nature of this extremely destructive threat and attacks through cyberspace have the power to damage, kill and physically destroy. Traditional definitions of the use of force have therefore changed. The real question is whether a cyber attack is the use of force equal to an armed attack in terms of international law, or is it basically a prohibition of interference in the internal affairs of countries. In other words, based on Article 2(4) of the United Nations Convention, an answer is sought to the question of whether cyber attack can be considered as the use of armed force.

On the other hand, in the case of a large-scale cyber-attack that causes human casualties or property damage or to basic infrastructure comparable to an armed attack with only conventional weapons, does the victim state have the right to defend itself against the cyber-attack? It also gives the armed forces the right to respond with conventional weapons.

This study details the question of when a cyberattack constitutes an armed attack according to Article 51 of the UN Charter and allows a state to take kinetic measures alongside active cyber defense measures. Then, the rules prohibiting the use of force in international law will be discussed and whether there is a right of self-defense against cyber attacks will be examined within the framework of current international law, and suggestions will be made regarding cyber attack and kinetic defense policy options for states.

Keywords: Self defense, cyber attack, cyberwar, cyber space, international law

* Assistant Prof. Dr., University of Ibn Haldun Faculty of Law, E-mail:qaisar.nasrat@ihu.edu.tr, Orcid No: 0000-0003-4676-8122.

SİBER UZAYDA YAPILAN SALDIRILAR VE MEŞRU MÜDAFAA

Özet

Siber saldırı, devlet ve devlet dışı aktörler tarafından yürütülen klasik savaş tekniklerini değiştirebilecek yeni bir olgudur. Son derece yıkıcı özelliğe sahip olan bu tehdidin kendine özgü doğası ve siber uzay yoluyla gerçekleştirilen siber saldırıların zarar verme, öldürme ve fiziksel olarak yok etme gücüne sahiptir. Dolayısıyla güç kullanımının geleneksel tanımları değişmiştir. Asıl soru, uluslararası hukuk bakımından siber saldırının silahlı saldırıyla eşit ölçüde güç kullanımı mı yoksa temelde ülkelerin iç işlerine müdahale yasağı şeklinde mi olduğudur. Başka bir deyişle, öncelikle Birleşmiş Milletler Sözleşmesi'nin 2(4) maddesine dayanarak, siber saldırı silahlı kuvvet kullanımı olarak kabul edilebilir mi sorusuna cevap aranmaktadır. Öte yandan, yalnızca konvansiyonel silahlarla yapılan silahlı bir saldırıyla karşılaştırılabilir insan kaybına yol açan veya maddi hasar ya da temel alt yapıya yönelik büyük ölçekli bir siber saldırı durumunda, mağdur olan devlet siber saldırıya karşı kendini savunma hakkına sahip midir? Ayrıca silahlı kuvvetlere konvansiyonel silahlar yoluyla karşılık verme hakkı tanır mı?

Bu çalışma, bir siber saldırının BM Sözleşmesinin 51. maddesine göre ne zaman silahlı bir saldırı oluşturduğu ve bir devletin aktif siber savunma önlemlerinin yanı sıra kinetik önlemler almasına izin verdiği sorusunu detaylandırmaktadır. Ayrıca, uluslararası hukukta kuvvet kullanmayı yasaklayan kurallar tartışılmış olup siber eylemlere karşı meşru müdafaa hakkının olup olmadığı mevcut uluslararası hukuk çerçevesinde incelenecek ve devletler için siber saldırı ve kinetik savunma politikası seçeneklerine ilişkin önerilerde bulunulmaktır.

Anahtar kelimeler: Meşru müdafaa, siber saldırı, siber savaş, siber uzay, uluslararası hukuk

INTRODUCTION

The world was faced with a new technology revolution at the end of the twentieth century. The name of this new era is the “information age”. Computer technologies, the internet and other new information and communication technologies have been among the most important and influential inventions of human life. Computer and technology in the past; While it is used as a selective tool for certain purposes, today all social, political, health and military infrastructures of societies, including information technology, banking system, energy and public transportation, have become dependent on computers. While these technological addictions create opportunities, they also create many threats. These threats include cyber-attacks and attacks against countrie's infrastructures. These cyber actions constitute the most serious threats to the national security of states. These attacks can create the most danger to other countries, economically and easily with the least risk.

In addition, the enormous expansion in information and information technologies has caused a fully interconnected society (both in the field of civilian structures and in the structures of the armed forces) to become even more dependent on them. Thus, the security of cyberspace has become a major concern of the international community, as the more digitized a State becomes, the greater its vulnerability.[1]

In this way, the issue of cybersecurity is of fundamental importance for States because it is closely linked to the protection of their national interests. This implies that States will gradually assign greater value to access and the ability to exploit cyberspace and, as a consequence, they will have more interest in protecting the infrastructures and cybernetic activities on which they depend.[2]

In this area, one of the aspects that has attracted the attention of jurists is the applicability of ius ad bellum, that is the set of rules that regulate the use of force in the context of international relations. Particularly, because as Schmitt[3] and Roscini[4] point out, cyberattacks can be conceived as an end in themselves or can be part of a larger-scale military maneuver within an armed conflict. It should be noted that far from reducing these operations cybernetics have been increasing year by year.[5]

The most important of these cyber attacks so far; Attacks on Iranian nuclear facilities in 2010 and attacks on Estonian critical infrastructures in 2007. Of course, the origin of these attacks remains unclear. In some cases, the source may be obvious. Therefore, if the source is known, it is possible to use the right of self-defense by characterizing the cyber attack as an armed attack.

The aim of this study is to answer the following questions; Can cyber attacks qualify as armed attacks? Do cyber attacks constitute an attack under the UN Charter? Can cyber attacks be attributed to a state? If attributable, under what conditions does the right of self-defense arise?

I. CYBER OPERATIONS IN INTERNATIONAL LAW

In todays world, dependence of States on computers, the possibility of using computer tools as defense and attack mechanisms in interstate relations has become one of the most viable alternatives available to States. This is due, in part, to the fact that cybernetic operations are relatively accessible to any

1 María Pilar Llorens, 'Los Desafíos del Uso de la Fuerza en el Ciberespacio', (2017) XVII Anuario Mexicano de Derecho Internacional 785, 816.

2 Michael N. Schmitt, 'The Law of Cyber Warfare: *Quo vadis*?', (2014) 25, 2 Standford Law & Policy Review 269, 300.

3 ibid 269.

4 Marco Roscini, 'World Wide Warfare - Jus ad bellum and the Use of Cyber Force', (2010) 14 Max Planck Yearbook of United Nations Law 85, 130.

5 Llorens (n 1) 785-816.

State, regardless of their degree of development, since they do not require large infrastructures to be carried out.[6]

In addition to their relative low cost, there are two other characteristics that make them attractive for military strategy and, therefore, increase the frequency with which they are used: anonymity and versatility. The first supposes, in practical terms, the existence of a real difficulty in reliably tracing the source where the cyber operation originated. Meanwhile, the second allows the use of cybernetic operations in a great variety of situations, whether they involve civil or military objectives; This is because, on the one hand, the possibility of causing collateral damage is reduced[7] and, on the other, they have the ability to have potentially devastating effects, especially on critical structures of the States.[8]

Both offensive or defensive cybernetic operations could be carried out through two mechanisms: the first is physical components, which allow a cyberoperation to be carried out, such as computers, modems or cables and the second, which Raboin identifies as the cybernetic component such as computer programs or viruses, that is, those mechanisms that only work in cyberspace.[9]

Therefore, the rise in the use of cybernetic operations has certain particularities since it is necessary to determine if the international legal system has the capacity to regulate the use of this new technologies, especially when they are used as attack. In addition, defense mechanisms within the framework of interstate relations. Thus, the state and academic debates have focused their attention on the fact of specifying whether the appearance of these new technologies justifies a differentiated regulatory treatment that implies the elaboration of a set of particular regulations and that is motivated by the differences with the pre-existing technologies. However, the truth is that cyberspace, due to its very characteristics, requires the establishment of clear regulatory guidelines that allow solving the problems that arise. Particularly, taking into account that the use of cybernetic tools to carry out military operations will become more common every day.[10]

II. CYBER ATTACKS AND USE OF FORCE

When a cybernetic operation violates the prohibition on the use of force in Article 2. Paragraph 4 of the United Nations Charter is a question of interpretation. This is due to the fact that, firstly, it is necessary to determine the scope of the term force in order to identify which force is prohibited and,

6 ibid, 785-816.

7 Duncan B. Hollis,'Why States Need an International Law for Information Operations', (2007) 11, 4 Lewis & Clark Law Review 1023, 1061, 1032.

8 Llorens (n 1) 785-816.

9 ibid, 785-816.

10 ibid, 791.

secondly, to specify when a cybernetic operation reaches the standards set by international law to configure a violation of this type.[11]

This means that, the use of force is not explained in the relevant article of the Charter and is left entirely to the discretion of the commentators.

The majority doctrine understands that the use of force that is prohibited is that of armed force.[12] In support of this interpretation, it is pointed out that in the first place, the other provisions of the Charter use the expression "armed force", as well as the Preamble, Article 41 and Article 46 do so. Secondly, the preparatory work for the Charter, since a proposal by the delegation of Brazil[13] to include a reference to economic pressures was left aside; and thirdly, various provisions of resolution 2625 (XXV) refer to the use of armed force.[14] Consequently, this interpretation determines that any type of political or economic coercion will be excluded from the prohibition on the use of armed force. Although they may be covered by the principle of non-intervention.[15]

However, it is worth asking if cybernetic operations can be considered as armed force, and if so, if they are included in the prohibition of article 2 (4) of the Charter. For these purposes, it is necessary to point out that the International Court of Justice in the Advisory Opinion on Nuclear Weapons pointed out that none of the provisions of the United Nations Charter refers to a specific type of weapon and consequently they apply to any use of force regardless of the weapon used.[16] This implies that any cybernetic operation that is considered a use of armed force will be subject to the prohibition of article 2 (4) of the Charter.[17] In addition to this, the Tallinn Manual specifies: *"A cybernetic operation that constitutes a threat or use of force against the territorial integrity or political independence of any State, or is in any other way incompatible with the Purposes of the United Nations is illegal."*

It should be remembered that Article 2(4) of the UN Charter prohibits not only the use of force but also the threat of use of force. As Roscini points out, a threat to use of force can be understood as an action or statement that carries an implicit or explicit promise of a future and illegal use of armed force against one or more States, the performance of which depends entirely from the will of the issuer.[18]

---

11 ibid, 785-816.

12 René Värk, 'The Legal Framework of the Use of Armed Force Revisited', (2013) 15, 1 Baltic Security & Defence Review 61, 62; Yoram Dinstein, *War, Agression and Self Defence*, Fifth edn (Cambridge University Press 2011).

13 Ian Brownlie, *International Law and the Use of Force by States* (Oxford University Press 2002).

14 Värk (n 12) 61; Roscini (n 4) 6.

15 Roscini (n 4) 106; Marco Benatar, 'The Use of Cyber Force: Need for Legal Justification?' (2009) 1, 3 Goettingen Journal of International Law 375, 396.

16 Advisory Opinion on Nuclear Weapons, paragraph 39, 244.

17 Roscini (no 4) 106.

18 ibid, 104.

In the field of cybernetic operations, there are two cases related to the threat of the use of force: on the one hand, when a cybernetic operation is used to communicate a threat of use of force, whether kinetic or cybernetic, and on the other hand, when a threat is made by any means to carry out a cybernetic operation that qualifies as a use of force. However, to establish whether it is a threat contrary to article 2 (4), it will be necessary to determine whether the threatened use of force is illegal or not. That is, the threat will be legal if the threatened action is itself legal.[19]

This has been stated in the Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons of the International Court of Justice: *'...If the intended use of force is itself unlawful, a statement of willingness to use it would be a prohibited threat under Article 2(4)...The concepts of "threat" and "use" of force under Article 2, paragraph 4, of the Charter are linked in the sense that, if the very use of force in certain cases is unlawful, for whatever reason, the threat to resort to that force shall be equally unlawful. In short, to be considered legitimate, the announcement by a State that it is willing to resort to force must refer to a use of force that is in accordance with the Charter...'.*[20]

In this sense, the Tallinn Manual (rule 12) provides that a threat to use of force unlawfully will be considered when the threatened action (a cybernetic operation or the threat of a cybernetic operation), if carried out, would be a use of force unlawfully.[21]

In addition, the criteria for using force in the Charter are not listed. In this case, if the cyber attack leads to death and destruction, it is debatable whether it is covered or not.

For these purposes, the doctrine has developed various criteria with which to assess whether a cybernetic operation meets the standards to be considered a use of force. Among them, the following stand out: a) the instrumental approach (instrumentality approach); b) the criterion based on the objective (target-based approach); c) the criterion of consequences (consequentiality approach). The first criterion —instrumental— will take into account the means used in the act (armed, economic or political) more than its harmful consequences; in this way a cyber operation will not normally be considered as an armed force due to its lack the typical characteristics of military coercion and the physical or kinetic effects. For its part, the criterion based on the objective (target-based approach) will consider that a cybernetic operation constitutes a use of force as long as it affects a critical infrastructure of a State, even when there is no destruction or significant injuries. Finally, the consequence criterion (consequentiality approach) will analyze the effects of a cybernetic operation and understand that it has reached the parameters to be

19 (no 16) 246.

20 (n 16) 246.

21 Schmitt (n 2) 52.

considered a use of force whenever its consequences are equivalent to those of a traditional military operation. In other words, whenever property destruction and deaths are caused, there will be a use of force contrary to the prohibition of article 2 (4) of the UN Charter.[22]

Among these criteria, the most important and the subject of concern is the result-oriented criterion. This means that cyber attacks have the potential to cause massive destruction.

III. SELF DEFENSE AGAINST CYBER ATTACKS

The right to self-defense is enshrined as a fundamental principle in both UN Charter Article 51 and customary law. Today, however, Article 51 comes to the fore. Therefore, the evaluations in this work are made in this context. Self-defense against attacks can be individual or collective.

In this sense, the Court has established that States cannot exercise the right to self-defense solely on the basis of their own analysis of the situation. It is necessary for the State that has been the victim of an armed attack to declare that it has been attacked, and consequently request the assistance of the other State(s).[23]

In short, in order for a state to use its right of self-defense against a cyber attack, the following conditions are required: *"(1) cyber attack(s) meets the standards of an armed attack, (2) cyber-attack is attributable to the state where the self-defense is being carried out and (3) the use of force carried in self-defense is necessary and proportional".*[24]

A. CYBER ATTACKS AS AN ARMED ATTACK?

To distinguish the serious forms of the less serious forms of the use of force, the Court uses the criterion of "scale and effects". Roscini, points out that the doctrine has tried to define this criterion in the following terms: *"An armed attack is, "an act or the beginning of a series of acts of armed force of considerable magnitude and intensity (scale) that have as a consequence (effects) the production of substantial destruction on important elements of the attacked State, such as the population, economic and security infrastructures, destruction*

---

22 Llorens (n 1) 785-816.

23 Militarv and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Merits, Judgment. I.C.J. Reports 1986, pp. 104-105.

24 Metodi Hadji-Janev, 'Use of Force in Self-Defense Against Cyber-Attacks and the Shockwaves in the Legal Community: One more Reason for Holistic Legal Approach to Cyberspace' (November 2013) Vol. 4 Mediterranean Journal of Social Sciences editerranean Journal of Social Sciences 115-124, https://www.researchgate.net/publication/259335648_Use_of_Force_in_Self-Defense_Against_Cyber-Attacks_and_the_Shockwaves_in_the_Legal_Community_One_more_Reason_for_Holistic_Legal_Approach_to_Cyberspace?enrichId=rgreq-4e15131cf80a3f9acf4f5335c5314332-XXX&enrichSource=Y292ZXJQYWdlOzI1OTMzNTY0ODtBUzo5OTM0Njk5NzU3OTc4M0AxNDAwNjk3NTc4NTY4&el=1_x_2&_esc=publicationCoverPdf > accessed 08 January 2023.

of aspects of governmental authority, that is, its political independence, as well as damage to or deprivation of its physical element, also called its territory".[25]

As a result of this, and as stated in the Tallinn Manual (rule 13),[26] any cyber operation that involves an armed attack will give rise to the exercise of the right of legitimate defense. The use of this criterion makes it possible to equate the effects of a cybernetic operation with those of a kinetic operation. In this way, any cyber operation that produces a significant destruction of elements of transcendence of the attacked State can give rise to the exercise of the right of legitimate defense.[27]

If a conventional military operation (bombardments, armed naval or air attacks) results in the destruction of property or loss of life, then it is classified as an armed attack. In the same sense, any cybernetic operation that causes injury or death to a person/s or that causes damage to or destruction of property will satisfy the scale and effects requirement and will therefore be considered an armed attack.[28]

In the context of the exercise of the right of legitimate defense in relation to cybernetic operations, there are a series of controversial issues. Firstly, the determination of whether an attack on civilian infrastructures can be considered as an armed attack that gives rise to the exercise of the right of legitimate defense; In this case, the doctrine argues that if the infrastructure affected by a cybernetic operation is a critical infrastructure for the State, then that operation, as long as it meets the standards of scale and effects, will be considered an armed attack and will therefore give rise to the exercise of the right of legitimate defense.[29] Secondly, the determination of whether those operations that do not cause physical damage but do generate severe non-destructive or harmful consequences can be considered an armed attack; In this case, there is a consensus that cybernetic operations that do not cause damage cannot be considered as armed attacks and consequently in these cases the right to legitimate defense cannot be exercised.[30] Finally, if the cyberoperations carried out by actors non-state may give rise to the exercise of the right of legitimate defense; this issue is currently governed by the rules of State responsibility. Consequently, only those cases in which the activities of non-state actors can be attributed to a particular State will be possible to exercise legitimate defense.[31]

---

25 Avra Constantinou, *The Right of Self-Defence under Customary International Law and Article 51 of the UN Charter* (Ant. N. Sakkoulas 2000).

26 Schmitt (n 2) 54.

27 Michael Gervais, 'Cyber Attacks and the Laws of War' (2012) 30, 2 Berkeley Journal of International Law 543.

28 ibid, 288.

29 Roscini (no 4) 116-118.

30 Schmitt (n 2) 282-283.

31 Llorens (n 1) 785-816.

B. THE CHALENGE OF ATTRIBUTION

One of the central elements of this requirement is the attribution of the attack. Dinstein[32] points out that the State seeking to invoke the right of self defense must unequivocally determine that an armed attack was launched by a particular State and not by another. However, as noted above, the identification of the attacker in the cyber context is not easy.

So attributability or finding the responsible is the hardest part of cyber attacks. If this principle is not fulfilled, it is not possible to talk about self-defense.

Raboin states that: *"The possibility of masking the origin of a cyber operation generates a problem of special importance since this technical difficulty of determining who are the authors of a cyber operation affects the attribution of responsibility of the State. The determination of what facts can be attributed to a State is relevant in two aspects: first, because it allows an adequate response from the State that has been the victim of a cyber attack against the person responsible for the attack, and second, because the right of legitimate defense depends that the attacker can be effectively identified"*.[33]

The principles of reference to the purposes of state responsibility are codified in Part I of the Articles on the *International Liability of States for Wrongful Acts* adopted by the *International Law Commission (ILC)* and are also contained in many decisions of the International Law Commission.[34] Also, the drafters of the Tallinn Manual have based their sixth rule on the Articles on State Responsibility, this rule states that:

"A State bears international Legal Responsibility for a cyber operation attributable to it and which constitutes a breach of an international obligation."[35]

According State Responsibility Articles, a state bear responsibility for an act when the act:

(a) is attributable to the State under international law; and

(b) constitutes a breach of an international obligation of the State.[36]

According to the Roscini there are three levels of evidence that are needed to attribute a cyber attack to a specific state:

"First, the computer(s), or server(s) from which the operations originate must be located; secondly, it is the individual that is behind the operation that

---

32 Dinstein (n 12) 231-232.

33 Bradley Raboin, 'Corresponding Evolution: International Law and the Emergence of Cyber Warfare' (2011), 31, 2 Journal of the National Association of Administrative Law Judiciary 640-641.

34 Jens David Ohlin, Kevin Govern and Claire Finkelstein, 'Cyberwar: Law and Ethics for Virtual Conflicts' (2015), Oxford University Press 220.

35 The Tallinn Manual 29.

36 The Draft Articles on Responsibility of States for Internationally Wrongful Acts, The International Law Commission, UN Doc A/56/10. Arts, 1-2.

need to be identified; and thirdly, what needs to be proved is that the individual acted on the behalf of a state so that his or her conduct is attributable to it".

As seen in Denmark and Indonesia examples, the attribution process even more is the use of foreign servers are method that complicates to launch the attack.[37] If an attack is initiated this way, the victim state can only attribute the attack to the state in which the server is located and has to rely on that state to find the source of the attack.[38] But, states may be ignore necessary cooperation and provide the information requested by the victim state. For such cases, the Tallinn Manual has stated that the fact that *"a cyber operation has been routed via the cyber infrastructure of another state is not sufficient evidence for attributing the operation to that state".*[39] In this context, The Tallin Manual establishes a standard for behavior for states: *"states shall not knowingly allow the cyber infrastructure on its territory or under governmental control to be used for acts that unlawfully or adversely affect other states".*[40]

C. REQUIREMENTS FOR THE EXERCISE OF THE USE OF FORCE

These conditions found their place primarily in common law. Today, they are becoming the basic concepts of international law. These principles should also be applied to cyber attacks. However The Tallinn Manual reflects these requirements in the following terms:

A use of force that implies cyber attacks carried out by a State in the exercise of the right of legitimate defense must be necessary and proportionate.[41]

This criterias does not mentioned in Article 51, but the 1996 Advisory Opinion on Nuclear Weapons stated that:

"The submission of the exercise of the right to self-defense to the conditions of necessity and proportionality is a rule of customary international law, but "this dual condition applies equally to Article 51 of the Charter, whatever the means of force employed.[42]

In the cyber space field, the United States has reaffirmed that a use of force in self-defense against a cyber attack *"must be limited to what is necessary to address an imminent or actual armed attack and must be proportionate to the threat that is faced."*[43]

---

37 Kim Zetter, 'How Digital Detectives Deciphered Stuxnet, The Most Menacing Malware in History' (2011) Wired Magazine. http://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/ accessed 21 January 2023.

38 Heintschel von Heinegg, 'Territorial Sovereignty and Neutrality in Cyberspace' (2012), 4th International Conference on Cyber Conflict C. Czosseck, R. Ottis, K. Ziolkowski (Eds.) NATO CCD COE Publications 18.

39 (n 35) 36.

40 ibid 26.

41 Schmitt (n 2) 61.

42 Advisory Opinion, para. 41.

43 UN Doc A/66/152, 15 July 2011, p. 19.

1. Necessity Against Cyber-attacks

The principle of necessity is whether self-defense is necessary against the use of a force, including cyberattacks. In addition, it is possible to respond in conventional ways if it meets the requirement against cyber attacks.

In addition, necessity principle mentioned as *"non-forcible remedies must either prove futile in limine or have in fact been exhausted in an unsatisfactory manner."* The meaning is that the final result is that there is no effective substitute for the use of force against self-defense.[44]

According to The Tallinn Manual, the important issue to the necessity principle in the cyber space is the existence or lack of alternative courses of action that do not rise to the level of use of force.[45] Also Roscini mentioned that *"even a cyber attack that is severely disrupting the critical infrastructure of a state, does not automatically entitle the attacked state to use forcible measures in self-defense in all cases, as the use has to be proportional and necessary".*[46]

2. Proportionality Against Cyber-attacks

Proportionality seeks to determine how much force is necessary in order to respond to an armed attack. As Dinstein points out, it is a standard of reasonableness in responding to a use of force by means of force. The proportionality requirement limits the scale, scope, duration and intensity of the response necessary to put an end to an act that gave rise to the exercise of self-defense. It should be noted that the force used in the defense need not be of the same nature as that used in the armed attack. This implies that in the event of a cybernetic armed attack, a response can be made with both cybernetic operations and kinetic or conventional operations.[47]

The principle of proportionality also does not mentioned in UN Charter but The International Court of Justice has repeatedly stated that *"proportional to the armed attack and necessary to respond to it, a rule well established in international customary law".*[48]

As a result, proportionality in cyberspace has been privatised. Self-defense cyber-responses are possible if software is written with this purpose in mind and requires a high degree of information about the targeted systems that can be gathered through traditional cyber-exploit intelligence.[49]

---

44 Dinstein (n 12) 109.

45 The Tallinn Manual 62.

46 Roscini (n 4) 75.

47 Llorens (n 1) 785-816.

48 7 Nicaragua, paras. 176 and 194, Advisory Opinion, para. 41, Oil Platforms Case, para. 74, Armed Activities Case, para. 147.

49 Roscini (n 4) 91.

3. Immediacy Against Cyber-attacks

Another controversial issue is immediacy principle. This principle means that, action should immediately follow the onset of an attack. As Dinstein explains *"the isolated armed attack may not be the reason for starting a war for self-defence"*. At the same time he agrees that *"the principle of immediacy cannot be explained directly, because of different bureaucratic procedures the state faces with the beginning of hostilities by the adversary – the certain period of time passes after the state officials make a decision to act in response and give the instruction to the armed forces. Therefore if the interval between an armed attack and a war of self-defence is long, a war may still be lawful if the delay is objectively justified"*.[50] Some scholars argues that: *"link the criterion of immediacy with the criteria of necessity and also deny that the beginning of an armed attack must be sufficiently close to the action for self-defence. Again the interpretation of closeness in time between these two actions is dependent on the context of each situation"*.[51]

The requirement of immediacy makes it possible to distinguish between acts of defense and reprisals; This makes it clear that the objective of legitimate defense is to repel the armed attack and not punish the person responsible for it. Immediacy means that there should not be an excessive time lapse between the armed attack and the exercise of legitimate defense. This requirement must be interpreted reasonably, since among other elements must be considered: the temporal proximity between the attack and the response, the period necessary to identify the attacker and the time necessary to prepare the response.[52]

Flexibility in the interpretation of this requirement in the framework of cybernetic operations is essential since it can often happen that the existence of an armed attack is not apparent for a while; or it may happen that a cyberattack is made up of numerous waves of cybernetic operations and that the victim State considers that it is a "cybernetic campaign" and that consequently the exercise of legitimate defense does not end with the completion of each wave. It can also happen that the identification of the attacker is delayed due to the possibility of masking the IP addresses.[53]

FINAL CONSIDERATIONS

Cyberspace constitutes a new field in which States are entering and exploring at great speed through technological progress. The pace at which information technologies change is causing constant challenges that must be

---

50 Dinstein (n 12) 242–243.

51 Rīga Stradiņš University, 'Conditions for the lawful exercise of the right of self-defence in international law' (Int. Conf. Socıety. Health. Welfare 2016) https://doi.org/10.1051/shsconf/20184001008 > accessed 28 December 2022.

52 Llorens (n 1) 785-816.

53 ibid.

resolved by the international community to find the best way to regulate this space.

No explanation or determination has been made by the international community that one of the international cyber attacks carried out so far has reached the threshold of an armed attack. In light of the physical damage to the centrifuges as a result of cyber attacks with the Stuxnet virus on Iran's uranium enrichment facility in 2009, there is a widespread opinion among security experts that cyber attacks have reached the threshold of armed attack.

To clarify the legal principles and rules discussed in this article, I think we should witness a devastating cyber attack before the legal environment improves. But once a full-scale attack occurs, it will become clear whether the current legal paradigm can handle it.

The application of the principle of prohibiting the use and threat of force through cyberspace entails legal, political and technical problems, the solution of which is not only necessary, but absolutely inevitable.

If it is believed that the cyber attack meets the criteria of an armed attack defined in Article 51 of the United Nations Charter, the attacked state has the right to self-defense. In order for the right of self-defense to be exercised, the danger must have arisen at that moment, be sudden, irresistible, and must be such that it does not allow any other means of protection. However, the exercise of the right of self-defense is also subject to the conditions of necessity, proportionality, proximity and urgency.

However, due to the difficulty of attribution, the current international system limits the options available to states and makes it difficult to respond effectively without violating international law. Restricting a state's right to respond in self-defense will encourage states, terrorist organizations, and individuals to engage in cyber attacks that are both more violent and more frequent.

BIBLIOGRAPHY

Benatar M, 'The Use of Cyber Force: Need for Legal Justification?' (2009) 1, 3 Goettingen Journal of International Law 375, 396.

Brownlie I, *International Law and the Use of Force by States* (Oxford University Press 2002).

Constantinou A, *The Right of Self-Defence under Customary International Law and Article 51 of the UN Charter* (Ant. N. Sakkoulas 2000).

Gervais M, 'Cyber Attacks and the Laws of War' (2012) 30, 2 Berkeley Journal of International Law 543.

Hadji-Janev M, 'Use of Force in Self-Defense Against Cyber-Attacks and the Shockwaves in the Legal Community: One more Reason for Holistic Legal Approach to Cyberspace' (November 2013) Vol. 4 Mediterranean Journal of Social Sciences editerranean Journal of Social Sciences 115-124, https://www.researchgate. net/publication/259335648_ Use_of_Force_in_Self-Defense_Against_Cyber-Attacks_ and_the_Shockwaves_in_the_Legal_ Community_One_more_Reason_for_Holistic_Legal_Approach_to_Cyberspace?enrichId=rg reg-4e15131cf80a3f9acf4f5335c5314332-XXX&enrichSource=Y292ZXJQYWdlOz I1OTMzNTY0ODtBUzo5OTM0Njk5NzU3OTc4M0AxNDAwNjk3NTc4NTY4&el=1_x_2&_e sc=publicationCoverPdf > accessed 08 January 2023.

Heintschel von Heinegg, 'Territorial Sovereignty and Neutrality in Cyberspace' (2012), 4th International Conference on Cyber Conflict C. Czosseck, R. Ottis, K. Ziolkowski (Eds.) NATO CCD COE Publications 18.

Hollis DB,'Why States Need an International Law for Information Operations', (2007) 11, 4 Lewis & Clark Law Review 1023, 1061, 1032.

Llorens MP, 'Los Desafíos del Uso de la Fuerza en el Ciberespacio', (2017) XVII Anuario Mexicano de Derecho Internacional 785, 816.

Militarv and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Merits, Judgment. I.C.J. Reports 1986, pp. 104-105.

Ohlin JD, Govern K and Finkelstein C, 'Cyberwar: Law and Ethics for Virtual Conflicts' (2015), Oxford University Press 220.

Raboin B, 'Corresponding Evolution: International Law and the Emergence of Cyber Warfare' (2011), 31, 2 Journal of the National Association of Administrative Law Judiciary 640-641.

Rīga Stradiņš University, 'Conditions for the lawful exercise of the right of self-defence in international law' (Int. Conf. Socıety. Health. Welfare 2016) https://doi.org/10.1051/shsconf/20184001008 > accessed 28 December 2022.

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

Schmitt MN, 'The Law of Cyber Warfare: *Quo vadis*?', (2014) 25, 2 Standford Law & Policy Review 269, 300.

The Draft Articles on Responsibility of States for Internationally Wrongful Acts, The International Law Commission, UN Doc A/56/10. Arts, 1-2.

Värk R, 'The Legal Framework of the Use of Armed Force Revisited', (2013) 15, 1 Baltic Security & Defence Review 61, 62; Yoram Dinstein, *War, Agression and Self Defence*, Fifth edn (Cambridge University Press 2011).

Zetter K, 'How Digital Detectives Deciphered Stuxnet, The Most Menacing Malware in

History' (2011) Wired Magazine. http://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/ accessed 21 January 2023.