Revista de **Relaciones Internacionales, Estrategia y Seguridad**

2023
Vol. 18(2)

Editorial Neogranadina

julio-diciembre ■ ISSN: 1909-3063 · ISSN-e: 1909-7743 ■ **pp. 61–72**

DOI: https://doi.org/10.18359/ries.6639

Self-Defense Strategies Against Cyber-Attacks by Non-State Actors*

Tomás Urbina Escobar[a]

Abstract: This article aims to analyze and provide a state-of-the-art conceptualization of the notion of self-defense within international law and the cyber realm. In the first section, the paper explores the concepts of self-defense, attack, and the use of force in international law, followed by their application in the cyberspace. The subsequent section, specifically applies the concept of self-defense in the event of a cyber-attack perpetrated by a non-state actors. The conclusion highlights that the cyber realm context introduces the possibility that aggressions from non-state actors can yield consequences even more severe than traditional kinetic attacks. This article serves as a foundation for future discussions in the defense sector and international law.

Keywords: International Law; Use of Force; Cyber-Attacks; Non-State Actors; Self-Defense

Recibido: 26/01/2023 **Aceptado:** 05/10/2023 **Disponible en línea:** 29/12/2023

Cómo citar: Urbina Escobar, T.(2023). Self-Defense Strategies Against Cyber- Attacks by Non-State Actors; Revista De Relaciones Internacionales, Estrategia Y Seguridad, 18(2), 61–72. https://doi.org/10.18359/ries.6639

* Reflection article.

a Master in Public Administration, Syracuse University (Syracuse, United States), Lawyer, EAFIT University (Medellín, Colombia). Email: turbina@eafit.edu.co ORCID: https://orcid.org/0000-0002-8051-9499

Estrategias de autodefensa contra ciberataques de actores no estatales

Resumen: Este artículo tiene como objetivo analizar y proporcionar una conceptualización de vanguardia de la noción de autodefensa dentro del derecho internacional y el ámbito cibernético. En la primera sección, el documento explora los conceptos de autodefensa, ataque y el uso de la fuerza en el derecho internacional, seguido de su aplicación en el ciberespacio. La siguiente sección aplica específicamente el concepto de autodefensa en caso de un ciberataque perpetrado por actores no estatales. La conclusión destaca que el contexto del ámbito cibernético introduce la posibilidad de que las agresiones de actores no estatales puedan tener consecuencias incluso más graves que los ataques cinéticos tradicionales. Este artículo sirve como base para futuras discusiones en el sector de la defensa y el derecho internacional.

Palabras clave: derecho internacional; uso de la fuerza; ciberataques; actores no estatales; autodefensa

Estratégias de autodefesa contra ciberataques de atores não-estatais

Resumo: Este artigo tem como objetivo analisar e fornecer uma conceitualização vanguardista da noção de autodefesa no âmbito do direito internacional e cibernético. Na primeira seção, o documento explora os conceitos de autodefesa, ataque e uso da força no direito internacional, seguido de sua aplicação no ciberespaço. A próxima seção aplica especificamente o conceito de autodefesa em caso de um ciberataque perpetrado por atores não-estatais. A conclusão destaca que o contexto do âmbito cibernético introduz a possibilidade de que as agressões de atores não-estatais possam ter consequências ainda mais graves do que os ataques cinéticos tradicionais. Este artigo serve como base para futuras discussões no setor de defesa e direito internacional.

Palavras-chave: direito internacional; uso da força; ciberataques; atores não-estatais; autodefesa

New era

The massive expansion of information and communications technology has led to an ever-growing dependency on them in a modern society that is fully connected both in civilian and military terms. As a result of this considerable dependence, actions and security in cyberspace have become critical concerns for the international community, particularly for the most developed and digitalized states, given their significant dependence and thus greater vulnerability.

Cybersecurity is of vital importance for states because it is closely linked to the protection of their national interests. Professor Michael Schmitt posits that this dependency means states will progressively assign greater value to access and the ability to exploit cyberspace. Consequently, states have undoubtedly tended to employ their full cyber capabilities to defend their cybernetical infrastructure and the cyber activities they depend on (Schmitt Michael, 2014, p. 273-274).

The world has entered a period where cyber warfare is replacing conventional warfare. Hence, a fundamental issue is how states respond to increased cyber threats. As argued by Finlay and Payne (2019), the law has not kept pace with this reality. Cyberattacks have reached the same level of threat as kinetic attacks. However, sometimes the law, especially international law, has not explicitly addressed and regulated the situation due to its novelty and complexity (p. 202-206).

The increasing and constant peril of cyber-operations as a weapon has made it vital in the international law for a consistent and reasonable legal framework under *jus ad bellum* to be developed for this type of attack.

The final point, as elucidated by Carr (2012), extensively details the modern usage and perception of *jus ad bellu,* asserting its origin from the United Nations Charter (UN Charter) and the corresponding customary international law (p. 49). Consequently, these foundations of international law serve as the initial driving force for future state practices in the cyber realm. A consensus exists regarding the fully applicability of existing international law to cyberspace, with the applicable laws stemming from 'the interpretation of longstanding rules of international law, primarily by states' (Schmitt, 2022, p. 16).

This paper will be limited in scope to the right of self-defense under the *jus ad bellum* regime, especially for concerning cyber-attacks that could be considered armed attacks under the international law of self-defense. Towards the end of the paper, the focus will shift to the involvement of non-state actors' attacks in the cyber-realm and how and when offended states can respond.

Concept of self-defense

According to the *jus ad bellum* framework, the lawfulness and legitimacy of defensive use of force are determined by the law of self-defense. As general rule, the use of force is prohibited by Article 2(4) of the UN Charter in. The law of self-defense is established as an exception to the prohibition of Article 2, as outlined in Article 51. This article acknowledges that nothing shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a member of the United Nations.

In addition to Article 51, the UN Charter establishes another exception to Article 2(4). This exception is outlined in Articles 39-42 of the Charter. It includes scenario where the United Nations Security Council could authorize the use of force if any threat to peace or breach of the peace is determined.

Prohibition of use of force

Understanding the concept of the prohibition of the use of force is crucial in grasping how of self-defense unfolds. This prohibition stands as a central element in the UN Charter framework and customary international law, recognized as *jus cogens* (Roscini, 2014, p. 43).

There is no formal description of what constitutes the use of force under international law, and states differ in their agreement on a clear definition. However, the scale and the effect of an act are generally the criteria to be considered when assessing the threshold of the use of force (Gray, 2018, pp. 601-618).

Regarding the Cyber-Realm, the Tallinn Manual 2.0 on International Law Applicable to Cyber Warfare (Tallinn Manual 2.0) asserts the same prohibition in its Rule 68: ''Cyber operations that are considered as 'threat or use of force against the territorial integrity or political independence of any State, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful."

The significance of this article is that it extends to all cyber operations, even if they do not violate the territorial integrity or political independence of a state. The importance lies in the fact that any type of cyber operation is prohibited if inconsistent with the framework provided in the UN Charter.

Use of force in the cyber-context

In the advisory opinion on Legality of the Use by a State of Nuclear Weapons in Armed Conflict of 1996, the International Court of Justice indicated that the understanding of UN Charter Article 51 and Article 2(4) could apply to self-defense and the use of force, respectively, regardless of the weapons employed in the attack (International Court of Justice, 1996, p. 39).

In cyber operations, as affirmed by the Tallinn Manual 2.0, it is not the technique or process employed that defines whether the "use of force" threshold has been breached.

Rather, as described in Rule 69 of the Manual, the effects of the operation and its specific considerations would aid in this assessment. The Manual asserts that the use of force in cyber-operations falls within the scope of application of Article 2(4) of the UN Charter, and that the amount of force in cyber operations could be equivalent in effect and scale to kinetic operations. However, as stated by the Group of Experts, "the fact that a cyber operation fails to rise to the level of a use of force does not necessarily render it lawful under international law" (Schmitt, 2017, p. 330-333).

One of the most important comments on Rule 69 is the one made by the Experts regarding the nature of the targeted cyber-infrastructure being definitive in the analysis of whether the cyber-operation qualifies as a "use of force." This is a significant understanding because it signifies it is noteworthy that almost all the targets in cyber-infrastructure could potentially meet the threshold established in Rule 69. The Tallinn Manual 2.0 (2017) Experts provide a non-exhaustive list of factors that should be considered in determining if an operation is considered "use of force":

a. *Severity*: Considered the most important factor in the entire analysis. The duration, scope, and intensity are important in evaluating this factor. The consequences must affect critical national interests, going beyond mere irritation or inconvenience.
b. *Immediacy*: Especially related to how the consequences of the attack manifest; states would likely consider a "use of force" if the consequences are immediate. It focuses on the temporal aspect.
c. *Directness*: Considers the causation of actions and the consequences of the acts. In the cyber realm, operations that cause and effect are undoubtedly connected could be easily characterized as "use of force."
d. *Invasiveness*: Indicates the degree to which cyber operations interfere or damage the attacked state, especially its cyber systems.
e. *Measurability of effects*: If the consequences of the cyber operation are more recognizable and quantifiable than others, it will be easier to be classified as a "use of force."
f. *Military Character*: If there is a nexus between the cyber operation and some specific military operation.
g. *State Involvement*: Determine if there is a clear connection between the cyber-attack and the author. It will be easier to be classified as a "use of force" if the author is a state.
h. *Presumptive Legality*: if the international law does not prohibit the cyber operation.

Armed attack

One of the key concepts is what constitutes an attack. A general definition that can be used is the one offered by international humanitarian law, which is primarily significant in the context of

armed conflict. In *jus in Bello*, the concept of attack signifies a specific military operation within the particular conflict. Additionally, the 1977 Additional Protocol I to the Geneva Conventions, in the Article 49(1), describes an attack as "acts of violence against the adversary, whether in offense or defense."

Article 51 of the UN Charter does not provide a specific meaning for "armed attack," rendering its interpretation ambiguous. There are measures taken by states that are not considered attacks but may still be deemed as a "use of force." Therefore, there is a constant debate over the level of destruction necessary to categorize the effects of "use of force" as an armed attack.

The International Court of Justice (1986) delves further into this issue in the *Nicaragua v. United States of America* case. Nicaragua claimed a violation of the prohibition on the use of force and the principle of non-intervention by the United States against the Nicaraguan state due to the support provided to the armed opposition of the left-wing government (the *contras*) and the military activities performed by the US armed forces.

The Court ruled that not every violation of the prohibition on the use of force could be considered an armed attack in the interpretation of Article 51 of the UN Charter. The Court (1986) specified that for an event to be classified as an attack, it must have certain "scale and effects" mentioning that, as in the events of the specific case, a "mere frontier incident" is insufficiently grave and "it will be necessary to distinguish the most grave forms of the use of force (those constituting an armed attack) from other less grave forms."

Similarly, the ICJ (2003) in the *Islamic Republic of Iran v. United States of America* case, where Iran argued that the US performed a "fundamental breach" of provisions of the Treaty of Amity, Economic Relations and Consular Rights between the United States and Iran of 1955 and violated international law by the destruction of three offshore oil production complexes, owned and operated for commercial purposes by the National Iranian Oil Company in retaliation for the damage one US warship suffered from striking a mine in international waters near Bahrain.

Nicaragua's understanding of an armed attack was reaffirmed in the judgment regarding the gravity requirement. The Court (2003) affirmed that in order to justify the attacks on the oil platforms, the US should have demonstrated that the attacks on the US warships were considered armed attacks under Article 51 of the UN Charter and customary law. This also necessitates the distinction between of the gravest forms of the use of force and other less severe forms, with the former considered armed attacks.

This definition presents a dilemma for cyber operations and cyber-attacks, as it is challenging to determine when these operations can be deemed "attacks". Some cyber operation actions may not generate the same consequences as a kinetic attack, raising questions about where the threshold is drawn to classify cyber-attacks as an armed attack.

An interesting situation that would spark considerable debate is whether cyber intelligence gathering and theft or cyber operations involving a brief interruption of non-essential cyber services would constitute an armed attack. One significant solution to this debate is provided by the Tallinn Manual 2.0 (2017), which explicitly states that neither of these situations mentioned above could be considered an armed attack. This position, as assumed in the Tallinn Manual 2.0, would exclude many of the daily cyber operations from the armed attack spectrum.

However, is important to highlight in contrast that other notable scholars position themselves with the idea that "no tangible criteria have been defined for that purpose in international law" (Oorsprong *et al.,* 2023, p. 220).

Overall, cyber-attacks pose a significant challenge due to their diverse forms and varied nature and scope, necessitating a comprehensive examination of the fulfillment of the *jus ad bellum* analysis.

Right self-defense

The exception of self-defense allows a state, subject to an armed attack, to respond with the use of force. However, for such a response to be lawful, self-defense must meet the conditions imposed by

international law, especially UN law, particularly Article 51. As outlined in the Nicaragua Case by the International Court of Justice (1986), the "inherent right" is recognized by the UN Charter Article 51 as a pre-existing customary law right (p. 14).

Moreover, the right of self-defense extends beyond Article 51. As Professor Yoram Dinstein correctly described (2011), the International Court of Justice acknowledged in the Nicaragua Case that the drafters of the Charter must have intended to declare the right even outside the Charter. They aimed to uphold it equally for both Member and non-Members, creating the obligation for both types of actors to refrain from using force and recognizing the self-defense right they possess (p. 181-182).

In addition, the self-defense action must be necessary and proportionate. These principles of the concept are currently part of customary international law.

Self-defense against armed attack in the cyber context

Under the aforementioned conditions, there is no doubt that a state facing under a cyber threat or an attack by non-state actors can respond with the understanding that the response is lawful within the *jus ad bellum*.

The Tallinn Manual 2.0 (2017) in Rule 71 embraces the "scale and effects" argument to determine if the cyber operation qualifies as an armed attack. Thus, if an armed attack is committed, the affected state has the right to self-defense. (p. 339) As stated by the Group of Experts, the "scale and effects" argument is borrowed from the Nicaragua judgment. Regarding non-state actors, the Group of Experts has commented on Rule 71 that "State practice has established a right of self-defense in the face of cyber operations at the armed attack level by non-state actors acting without the involvement of a State, such as terrorist or rebel groups" (p. 345).

Anticipatory self-defense

As mentioned above, states have a clear and undoubted right of self-defense. However, there have been developments in the concept for situations that could lead to anticipatory defense from states, even before an armed attack occurs in their territory. Scholars have theorized about the different types of self-defense, usually contemplated under the generic term of anticipatory self-defense. This term includes several other theories: interceptive self-defense, preventive self-defense, precautionary self-defense, and preemptive self-defense.

The first is **interceptive self-defense**, defined by Professor Dinstein (2011), as the reaction from a state to an event that is already taking place, even if its consequences are not fully developed. This includes attacks that have been initiated but have not reached their first target. Dinstein clarifies how the determination of the beginning of an armed attack can be resolved, suggesting that one solution is when an actor has "committed itself to an armed attack in an ostensibly irrevocable way" (p. 205). Dinstein (2011) also theorizes that a state's response in these situations could be legal under Article 51 of the UN Charter (p. 204). He provides a detailed example in his book *War, Aggression and Self-Defense*: "if the radar of a Carpathian military aircraft locks on to – or illuminates (*i.e.* aims laser beams at) – an Apollonian target, although no missile has been fired (and no bomb has been dropped), an armed attack may be deemed to be in progress, and a timely response by Apollonia would constitute interceptive self-defense"(p. 203).

The concept of **preventive self-defense** can be understood as the use of force in response to non-imminent and not yet materialized attacks, as stated in the "Report of the Secretary-General's High-level Panel on Threats, Challenges and Change" of the United Nations (2004). This type of self-defense is invoked in The National Security Strategy of the United States of America of 2002 to legitimize the use of force. This is done to establish the right to counter threats before they evolve into concrete actions, as in the context of the Bush doctrine, the potential use of Weapons of Mass Destruction (WMD) against America or any of its allies.

Another self-defense classification is **precautionary self-defense**; according to Byers (2003), it is the allegedly reasonable legitimate use of force that responds to a possible armed attack while there is no further evidence of the attack (p. 181).

Finally, the last concept of self-defense is **preemptive self-defense**, as described in the aforementioned UN report of the Secretary-General. It is the presumably legitimate use of force in response to a real and imminent attack on a state that has not been launched yet, and the usage of armed force is pursued to prevent the attack from becoming a real one.

Preemptive self-defense is the only type that considers the real and objective imminence of an attack. In the Interceptive type, the threat of an attack has already begun, whereas at the opposite end of the spectrum, in the preventive type, the use of force anticipates a simply distant threat. To underscore the importance of the self-defense concept, it is essential to illustrate the requirements and principles of self-defense.

Requirements of self-defense

Necessity and proportionality

Self-defense must be undertaken exclusively in the context of an armed attack that is in progress or an imminent threat against a state, and there is no other reasonable and viable alternative reaction, making it necessary. In addition to the necessity principle, the ICJ (1986) has established that self-defense and the use of force in response must be proportional and solely aimed at deterring the specific attack and prevent additional future attacks from the same specific actor (p. 176).

Regarding the cyber context, the Tallinn Manual 2.0 (2017) states in its Rule 72 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" (p. 384).

Cyber-attacks and other cyber-operations generate additional circumstances to be evaluated and considered. When a state faces an attack of this type, its response may take the form of a kinetic, cyber, or a combination of both to counter the attack. Additionally, it is imperative that the response does not surpass the magnitude of the initial attack or unnecessarily escalate the conflict.

Professors Dapo Akande and Professor Thomas Lieflaender (2013) present one of the most critical points in the discussion of necessity and proportionality when non-state actors are the authors of the attack. They argue that target states (in the self-defense response) must be involved with the non-state actors that cause the original attack on the affected state. This involvement is crucial for the analyzing the necessity dimension of self-defense. This specific issue extends even further concerning the actions the potential targeted states of the self-defense (the host of the non-state actors). For instance, if the state is capable and willing to control the non-state actor, then the use of force would not be necessary. Conversely, if the host state of the non-state actors is reluctant or unable to deal with the aggressor actors, then the necessity condition would be met, and the attacked state could lawfully resort to self-defense against the non-state actors, even if it is in the host state's territory (p. 563).

Imminence

Dinstein explains that this principle indicates that the attacked state's self-defense measures should be performed without any delay. Dinstein (2002) continues indicating that self-defense does not have to commence immediately from the initial attack, and states must have a reasonable response period (p. 110).

Regarding the Cyber-context, Roscini (2014) asserts that immediacy does not mean "instantaneous" and allows some room for flexibility for states. In this sense, a cyber-attack on a state's military cyber-infrastructure could lead to temporary complete incapacitation of the state infrastructure, making the responsive self-defense attack potentially delayed, whether it is cyber or kinetic. Furthermore, the immediacy of the self-defense can be affected in the cyber-context since assembling adequate and sufficient evidence to attribute the attack could be a monumental and time-consuming task (p. 91).

One interesting debate regarding anticipatory self-defense and the concept of imminence is raised in Tallinn Manual 2.0 (2017) Rule 73 comments. There is a controversy regarding the temporal threshold for self-defense, centering the discussion on whether anticipatory self-defense is

lawful or not. The Group of Experts considers that "a state may act in anticipatory self-defense against an armed attack, whether cyber or kinetic, when the attacker is clearly committed to launching an armed attack, and the victim state will lose its opportunity to effectively defend itself unless it acts. In other words, it may only act during the last window of opportunity to defend itself against an armed attack that is forthcoming. This window may present itself immediately before the attack in question, or, in some cases, long before it occurs" (p. 351).

For instance, imagine that state X has received irrefutable information that state Y is preparing a cyber-attack that will destroy the electrical grid of one of the most populated cities in the country, causing damage similar to what kinetic weapons can achieve. State X only knows that the attack would be performed within a specific timeframe and from a specific location in state Y but, it cannot effectively mount an effective defense of the electrical grid. X state could be justified in assuming that an armed attack is imminent. and the use of force to defend its territory is necessary under Rule 72 of the Tallin Manual 2.0; therefore, an attack against state Y to prevent the attack would be lawful under the argument of proportionate anticipatory self-defense.

Attribution

Attribution is one of the most critical points in the concept of self-defense. The discussion encompasses who is responsible for the attack and, if the responsible party is a state or a non-state actor, who is the prospective target of the self-defense.

There are three primary interpretations to determine attribution and its requirements. The first one is the interpretation of the "effective control test" developed in the ICJ Nicaragua case (1986). This theory asserts that the state targeted by the self-defense response must have been in "effective control" of the individuals who carried out the initial attacks (p. 114).

The second theory is that although attribution is required, a lower threshold than "effective control" is needed to establish attribution. Therefore, the test is replaced by a threshold of support where harboring or acquiescence is enough (Proulx, 2005, p. 615).

The final theory explores the possibility that attribution requirement is not necessary, and states can invoke self-defense against any attacking state within its territory, regardless of whether the state is in any way accountable for the attacks, thus providing almost ungovernable self-defense.

Most international lawyers concur with the ICJ's effective control theory, viewed as the correct approach. In this sense, the ICJ (1986) argues that self-defense attacks are only permissible when an armed attack by a non-state group is attributed to a state (p. 194-196).

However, this theory has a significant flaw in practice. Some attacking states could use non-state individuals to perform the attack and excuse themselves with the argument of not having "effective control" over the individuals responsible for the attacks, even though they offer them some beneficial conditions such as sheltering and support.

In addition, the Tallinn Manual 2.0 (2017) presents an interesting scenario regarding attribution. The Manual offers two possible conditions to determine whether states are responsible for cyber operations performed by non-state actors (Rule 17): the first one is that the conduct is "engaged in pursuant to its instructions or under its direction or control", or when "the state acknowledges and adopts the operations as its own" (p. 94).

This idea continues to be very critical and controversial. The legitimacy and ability of an offended state to attribute the responsibility to non-state actors and the subsequent self-defense has been and continues to be controversial under international law due to the state of international law regarding this matter.

This point about attribution is extremely important. Suppose the ICJ "effective control" is applied, and the attacked state fails to determine the effective control. In that case, this could essentially preclude the right of lawful self-defense against cyber-armed attacks by non-state actors of offended states.

In short, as mentioned throughout this section, due to the legal and technical complexity of the

definition of armed attacks in the cyber-realm, it is rare that one attack of this type could meet all the required conditions referred in Article 51 of the UN Charter (Pangrazzi, 2021, pp. 18-19).

Non-state actors

Definition

One of the most critical points of the non-State actors is determining who they are. Philip Alston (2005) offers a solution to this question; he affirms that there is no uniformly accepted definition of non-state actors in international law. In the broadest sense, the term can be used to designate any actors that are not States (p. 14).

Moreover, The International Law Commission (ILC) offers a narrower definition. It is defined as "legally recognized, and organized entities that are not comprised of nor governed or controlled by states nor groups of states, and that actually perform functions in the international arena that have real or potential effects on international law" (pp. 4-6).

In the Cyber context, the best definition could be a middle ground between both definitions because the former is too broad, but the latter requires to be broader. For instance, the "legally recognized" requirement in the ILC definition should eliminate in the cyber context because some cyber actors are not legally recognized or are even secret; examples of these groups will be provided later in the paper.

Classification of non-state actors in the cyber context

As mentioned earlier in the paper, the technical complexity of the cyber-realm makes the attribution element definition extremely problematic to the degree that even trying to identify the ultimate location of the parties involved in the attack may be extraordinarily challenging.

The cyber context introduces various types of actors who can pose significant threats to states through a cyber-attack. However, as mentioned in the sections before, even if there is no evidence or association between the non-state actors and the state where they operate, it is clear that an attack on them would fall under the classification of self-defense.

The current development of the cyber realm offers the possibility that a full range of actors participate within it. Professor Johan Sigholm (2016) presents a descriptive chart of the principal non-state actors within the cybersphere. He includes their motivations and methods in the field, along with the targets when an attack is conducted.

Table 1. Non-State Actors in Cyberspace

Actor	Motivation	Target	Method
Ordinary Citizens	None (or weak)	Any	Indirect
Script Kiddies	Curiosity, thrills, ego	Individuals companies, governments	Previously written scripts and tools
Hacktivist	Political and Social Change	Decisionmakers or innocent victims	Protests via web page defacements or Distributed Denial of Service (DDOS) attacks
Black-hat hackers	Ego, personal animosity, economic gain	Any	Malware, viruses, vulnerability exploits
White-hat hackers	Idealism, creativity, respect for the law	Any	Penetration testing, patching
Grey-hat hackers	Ambiguous	Any	Varying
Patriot hackers	Patriotism	Adversaries of own nation-state	DDOS attacks, defacements

Cyber insiders	Financial gain, revenge, grievance	Employer	Social engineering, backdoors, manipulation
Cyber terrorist	Political or social change	Innocent victims	Computer-based violence or destruction
Malware authors	Economic gain, ego, personal animosity	Any	Vulnerability exploits
Cyber scammers	Financial gain	Individuals, small companies	Social engineering
Organized cyber criminals	Financial gain	Individuals, companies	Malware for fraud, identity theft, DDOS for blackmail
Corporations	Financial gain	ICT- based systems and infrastructures (public and private)	Range of techniques for attack or influence operations
Cyber espionage agents	Financial gain and political gain	Individuals, companies, governments	Range of techniques to obtain information
Cyber militias	Patriotism, professional development	Adversaries of own nation-state	Based on the group capabilities

Source: Own elaboration.

These classifications are extensively explained by the authors Jason Andress and Steve Winterfeld (2011). In this section, we will analyze some of the important players concerning cyber-attacks: hacktivists, black-hat hackers, cyber-terrorists, and organized cyber- criminals (p. 193-206).

Firstly, there are hacktivists**,** defined by Andress and Winterfeld (2011) as hackers who utilize their skills to support a particular point of view. Their motivations are usually politically oriented, aiming to influence opinions or decisions on a specific issue. For instance, in February of 2010, a group known as Anonymous attacked the web pages of the Australian Parliament House to halt the approval of a law that introduced filtering to the internet service in the country (p. 196).

Next, we have black-hat hackers -groups with higher levels of expertise than hacktivist. They aim to exploit weakness in the system and perform attacks on critical networks or systems with no respect for the law or the potential effects of the attack (p. 197).

Organized cyber-criminals are groups within organized crime that use cybernetic tactics, such as cyberwarfare, to achieve financial goals and generate power. These groups are, as described by the authors as the most dangerous due to the potential effect their activities can have on various state areas, especially population stability (p. 201).

Finally, cyber-terrorists can be explained similarly to traditional terrorist group. These groups or individuals are mostly associated with selecting targets with highly disruptive significance and enormous publicity. As mentioned by Andress and Winterfeld (2011), one of the most common supposed targets for cyber terrorism is large-scale electrical grids or water systems in various countries (p. 198-199).

Consequently, cyber-terrorism can be defined as "a range of very different actions, from the simple spread of publicity online, to the alteration or destruction of in-formation, and even to the planning and carrying out of terrorist attacks via the use of computer networks" (Mayer, 2018).

These are just some actors that could intervene in the cyber context and that are capable of performing an attack on state infrastructure or valuable resources from the countries, potentially triggering anticipatory self-defense.

Conclusions

The advancements in technology have brough diverse new risks to the sovereignty and national

security of the states in the cyber realm. This poses a challenge for the law on several levels, both domestic and the international. For instance, the international law has historically focused on covering kinetic operations rather than the challenges the cyber realm presents. How the current international legal system addresses this new environment is an enormous challenge that is evolving day by day.

The prognostication that cyber-attacks may reach the level of armed attacks is no longer unrealistic, and there is no doubt that self-defense could apply to cyber-realm. However, there is still uncertainty about applying the law in cyber operations, creating new legal challenges to be tackled.

As stated in Rule 72 (2017) of the Tallinn Manual 2.0, in the context of cyber operations, states are not bound to wait passively until an armed attack occurs. The cyber context offers speed as one of its advantages. Therefore, it is logical to assume that potential victims of cyber-attacks can use anticipatory but proportional forces to prevent any imminent and otherwise avoidable attack (p. 42).

Cyber uses of force and self-defense in the face of an armed attack must further meet the related requirements of attribution, necessity, proportionality, and imminency. Elements that would always limit the responses in anticipation of an attack or even sequent to an attack.

The lawfulness of self-defense against non-state attacks continues to be very problematic and mostly depends on the fulfillment of the attribution element. The attribution requirement is specifically challenging due to the prominent role of non-state actors in cyberspace conflicts and the complexities of attributing cyber-attacks to them because of the secrecy, boundlessness, and speed of cyber operations.

The cyber realm context offers the possibility that aggressions from non-state actors can generate consequences even deadlier than a kinetic attack. It is necessary for states to have the possibility and opportunity to exercise the right of self-defense and hold accountable a non-state actor that is attacking them, even within the territory of another state. However, to do so, the attribution factor must be, to some extent, fulfilled to avoid indiscriminate attacks.

References

Alston, P. (2005). The "Not-a-Cat" Syndrome: Can the International Human Rights Regime Accommodate Non-State Actors? In Philip Alston (Eds.), Non-State Actors and Human Rights (p. 14). Oxford University Press.

Andress, J., & Winterfeld, S. (2011) Non-State Actors in Computer Network Operations. In Cyber Warfare Techniques, Tactics and Tools for Security Practitioners Syngress (pp. 193-206), (p. 196), (p.197), (p. 201), (pp. 198-199)... https://doi.org/10.1016/b978-1-59749-637-7.00011-3.

Akande, D., & Liefländer, T. (2013). Clarifying Necessity, Imminence, and Proportionality in The Law of Self-Defense. In American Journal of International law (Vol. 107-3) (p. 563). https://doi.org/10.5305/amerjintelaw.107.3.0563

Byers, M., (2003). Preemptive Self-defense: Hegemony, Equality and Strategies of Legal Change. In Journal of Political Philosophy (Vol.11-2) (p.181). https://doi.org/10.1111/1467-9760.00173 .

Carr, J., (2012). Responding to International Cyber Attacks as Acts of War. In Inside Cyber Warfare (p. 49) O'Reilly Media.

Dinstein, Y., (2002). Computer Network Attacks and Self-defense. In International law Studies (Vol 76) (p. 110). US Naval War College.

Dinstein, Y., (2011). Controversial consequences of the change in the legal status of war. In War, Aggression and Self-Defence. (pp. 181-182). Cambridge University Press. https://doi.org/10.1017/CBO9780511920622

Dinstein, Y., (2011). The Concept of Self-Defence. In War, Aggression and Self-Defence. (p. 203) (p. 204) (p. 205). Cambridge University Press. https://doi.org/10.1017/CBO9780511920622

Finlay, L., & Payne, C., (2019). The Attribution Problem and Cyber Armed Attacks." In American Journal of International Law Unbound (Vol. 113) (pp. 202-206). Cambridge University Press. https://doi.org/10.1017/aju.2019.35.

Gray, C., (2018). The Use of Force and the International Legal Order. In International law (pp. 601-635). Oxford University Press. https://doi.org/10.1093/he/9780198791836.003.0020

International Committee of the Red Cross (ICRC), Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 8 June 1977, 1125, UNTS 609

Legality of the Use by a State of nuclear weapons in Armed Conflict, Advisory Opinion, ICJ. Reports (1996) (p. 39)

Mayer, L., (2018) Defining cyberterrorism. In Revista Chilena de derecho y tecnología (Vol.7-2) (p.6) Centro de Estudios en Derecho Informático de la Facultad de Derecho de la Universidad de Chile. https://doi.org/10.5354/0719-2584.2018.51028

Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States), Merits, (1986) ICJ Rep1986 (p.14) (p. 195) (p. 191) (p.194) (p. 115) (pp. 194 -195)

Non-State Actors in International law, Final Report of the ILA Committee on Non-State Actors (2016) (pp. 4-6)

Oil Platforms (Islamic Republic of Iran v. United States of America), Mertis, (2003) ICJ Rep. 2003. (p. 161 para.1) (p. 161 paras 51,64)

Oorspronga, F., Ducheineband, P., & Pijpers, P. (2023) Cyber-attacks and the right of self-defense: a case study of the Netherlands. In Policy Design and Practice (Vol.6-2023) (p.2 20). Taylor & Francis. https://doi.org/10.1080/25741292.2023.2179955

Pangrazzi, S. (2021) Self-Defence against Cyberattacks? Digital and Kinetic Defence in Light of Article 51 UN-Charter (Policy Brief). ICT for Peace Foundation (pp. 18-19) https://ict4peace.org/publications/self-defence-against-cyberattacks-digital-and-kinetic-defence-in-light-of-article-51-un-charter/

Proulx, V. (2005). Babysitting Terrorists: Should States be Strictly Liable for Failing to Prevent Transborder Attacks? In Berkeley Journal of International law. (Vol.23-3) (p.615). Berkeley Law. https://doi.org/10.15779/Z38CK90

Roscini, M. (2014). Cyber Operations and the jus ad bellum. In Cyber Operations and the Use of Force in International law. (p. 43) (p. 91). Oxford Academic. https://doi.org/10.1093/acprof:oso/9780199655014.003.0002.

Schmitt, M. (2014). The Law of Cyber Warfare: Quo Vadis? In Stanford Law & Policy Review (Vol 25-2) (pp. 273-274). Stanford University. https://ssrn.com/abstract=2320755

Schmitt, M. (2017). Due Diligence. In Tallinn Manual 2.0 on the international law Applicable to Cyber Operations. (p. 48). Cambridge University Press. https://doi.org/10.1017/9781316822524

Schmitt, M. (2017). Jurisdiction. In Tallinn Manual 2.0 on the international law Applicable to Cyber Operations. (p. 54). Cambridge University Press. https://doi.org/10.1017/9781316822524

Schmitt, M. (2017). Law of international responsibility. In Tallinn Manual 2.0 on the international law Applicable to Cyber Operations. (p. 94). Cambridge University Press. https://doi.org/10.1017/9781316822524

Schmitt, M. (2017). The use of force. In Tallinn Manual 2.0 on the international law Applicable to Cyber Operations. (pp. 334-337) (pp. 330-333), (p. 339) (p. 345) (p. 348) (p. 351). Cambridge University Press. https://doi.org/10.1017/9781316822524

Schmitt, M. (2022). The Law of Cyber Conflict: Quo Vadis 2.0? In The Future Law of Armed Conflict. (p. 222). Oxford Academic https://doi.org/10.1093/oso/9780197626054.003.0007

Sigholm, J. (2016). Non-State Actors in Cyberspace Operations. In Journal of Military Studies. Vol 4(1) (p. 11). The Finnish Society of Military Sciences. https://doi.org/10.1515/jms-2016-0184

United Nations. (2004). A more secure world: our shared responsibility: report of the High-level Panel on Threats, Challenges, and Change. (pp. 53-64) United Nations Dept. of Public Information.

White House. (2002). The national security strategy of the United States of America. https://history.defense.gov/Portals/70/Documents/nss/nss2002.pdf?ver=oyVN99aEnrAWijAc_O5eiQ%3d%3d