SCOPE OF SELF DEFENSE IN INTERNATIONAL LAW AND THE ISSUE OF CYBER ATTACKS: A CRITICAL LEGAL ANALYSIS AND COMMENTS OF SATE PRACTICES

BY

MUHAMMAD IJAZ KHAN

LLM (International Law)

Reg# 455 -FSL/LLMIL/S21

Under the Supervision of

AFZAL AHMED

Assistant Professor

DEPARTMENT OF LAW

FACULTY OF SHARIAH & LAW

INTERNATIONAL ISLAMIC UNIVERSITY,

ISLAMABAD

2024

SCOPE OF SELF- DEFENSE IN INTERNATIONAL LAW AND THE ISSUE OF CYBER ATTACKS: A CRITICAL LEGAL ANALYSIS AND COMMENTS OF SATE PRACTICES

A thesis submitted in partial fulfillment of the requirements for Degree of LLM in International Law in the Department of Law at the Faculty of Shariah & Law, International Islamic University Islamabad.

BY

MUHAMMAD IJAZ KHAN

LLM (INTERNATIONAL LAW)

Reg# 455 -FSL/LLMIL/S21

DEPARTMENT OF LAW

FACULTY OF SHARIAH & LAW

INTERNATIONAL ISLAMIC UNIVERSITY,

ISLAMABAD

2024

IN THE NAME OF ALLAH,

THE MOST BENEFICENT,

THE MOST MERCIFUL

DEDICATION

This research work is dedicated with profound love and eternal gratitude to my beloved parents, who are no longer with me in this world. Their unwavering love, guidance, and sacrifices continue to shape my life, and their memory serves as an everlasting inspiration for my academic pursuits and personal growth.

DECLARATION

I, Muhammad Ijaz Khan Student of LLM (International Law) International Islamic University Islamabad, Registration No. 455-FSL/LLMIL/S21, hereby declare that this dissertation "Scope of Self- Defense in International Law and the Issue of Cyber Attacks: A Critical Legal Analysis and Comments of Sate Practices" is my original work and has never been presented in any other institution. Moreover, I declare that any secondary information used in this dissertation has been duly acknowledged.

Student **Muhammad Ijaz Khan**

Signature _____

Dated _____

FORWARDING SHEET

This dissertation, title "Scope of Self- Defense in International Law and the Issue of Cyber Attacks: A Critical Legal Analysis and Comments of Sate Practices", put forward by Muhammad Ijaz Khan, registration no. 455-FSL/LLMIL/S21 in partial fulfillment for the award of LLM International Law has been successfully completed under my guidance, care and supervision.

I am satisfied & contented with the excellence of scholar's research work and he is now allowed to get it submitted for the finishing pot of go forward course of section so that he may be awarded the Degree of LLM (International Law) as per modus operandi of International Islamic University, Islamabad.

AFZAL AHMAD

Assistant Professor Department of Law
Research Supervisor

TABLE OF CONTENT

ABSTRACT

This research work elucidates into the relationship between self-defense and cyber-attacks within international law. It begins by scrutinizing the United Nation Security Council's (UNSC) role in maintaining collective security and outlines the conditions for invoking self-defense in cases of armed attacks. The study then explores cyber-attacks, defining them as malicious actions conducted through cyber operations, showcasing their unique traits like indirect impact and diverse targets. It delves into various cyber-attack types and examines their classifications within cyber operations.

Furthermore, the thesis delves into the legal complexities posed by cyber-attacks to the traditional self-defense concept, assessing how these operations might breach the prohibition of force principle. It analyzes significant cyber incidents like Stuxnet, WannaCry, and SolarWinds attacks, highlighting the challenges in responding to cyber threats. Additionally, it examines the legitimacy and proportionality of cyber self-defense measures amid evolving threats, while exploring the applicability of the UN Charter's principles in this context. Ultimately, the research work emphasizes the need for a nuanced understanding of self-defense in the face of evolving cyber threats and underscores the role of state practices in shaping the legal framework.

ACKNOWLEDGEMENTS

Praise is to ALLAH, the exalted, omnipresent and sustainer of this Universe, who create man with the clot of blood, and give them honor on all the creatures, taught the human being what he knew not (before) and endowed wisdom and knowledge to mankind, and His Holy Prophet Hazrat Muhammad (PBUH) who is forever a touch guidance and knowledge for humanity as whole.

The process of earning a research degree and writing a dissertation especially when you are also simultaneously working in institute is arduous and stressful. It cannot be done single handed for which I wish to acknowledge that I have personally grown and developed in the process of the research and better understand my profession and its contextual relationship my supervisor **Afzal Ahmad** (Assistant Professor Department of Law), for his understanding, wisdom, patience and encouragement for pushing me farther than I thought I could go. I am deeply grateful for his detailed comments on the draft of my research work. The blessing, help and guidance given by him time to time shall carry me a long way in the journey of life on which I am about to embark.

I am indebted to the faculty members of Abdur Rauf Khattana and Fazal Khalique for their dedication to imparting knowledge and creating a stimulating academic environment. Their commitment to excellence, passion for their respective fields, and willingness to engage in scholarly discussions have broadened my intellectual horizons and enriched my learning experience.

I could not have accomplished the task of writing this dissertation without the support and help of my family member. I wish to acknowledge to my Mother, even though my mother is no longer physically present, her spirit and unwavering belief in my abilities continue to propel me forward. I am grateful for the lessons she taught me about perseverance, resilience, and the pursuit of excellence. Her memory remains a driving force behind my determination to achieve my goals and make a meaningful contribution to the field of law.

I would like to extend my heartfelt appreciation and gratitude to my dear brothers, Dr. Muhammad Ayaz and Muhammad Imtiaz, and my sisters for the emotional support and understanding you have shown me. You have been a source of strength, offering words of encouragement, reassurance, and motivation during moments of uncertainty

and challenges. Your unwavering presence and belief in my capabilities have instilled in me the confidence to overcome obstacles and achieve my goals. I must acknowledge the contribution of my younger brothers Dr. Muhammad Ibrahim and Rizwan Ullah (Gul G). Thank you, for being my constant cheerleaders and sources of inspiration. Your involvement in this research work, in your own unique way, has made a lasting impact, and I am truly grateful for your presence in my life.

I am also thankful to my friends Specially Raja Hamid and Muhammad Ali in Department of law International Islamic University Islamabad (IIUI), who facilitates and motivate me always for higher education. The valuable information provided by them in their respective fields. I am grateful for their cooperation during the period of my dissertation.

I would like to acknowledge the invaluable contributions of my friends Tajammul Hussain Chattah, Safdar Iqbal Khattak, and Waqas Rauf who have been my pillars of support throughout this demanding undertaking. Their unwavering belief in my abilities, words of encouragement, and understanding during moments of frustration have been an immense source of motivation. I am grateful for their presence in my life.

Last but not least, I express my heartfelt thanks to everyone who has contributed, directly or indirectly, to the successful completion of this LLM thesis, I am deeply grateful for your unwavering support, encouragement, and belief in my abilities. Your collective efforts have made a lasting impact on my academic journey and will forever be cherished.

ACRONYMS

APTs	Advanced Persistent Threats
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CNA	Computer Network Attacks
CND	Computer Network Defence
CNE	Computer Network Exploitation
CNO	Computer Network Operation
COE	Council of Europe
DNS	Domain Name Systems
DoS	Denial-of-Service
EU	European Union
FedEx	Federal Express
GCA	Global Cyber security Agenda
GGE	Groups of Governmental Experts
ICJ	International Court of Justice
ICS	Industrial Control Systems
ICT	Information and Communication Technology
ISPs	Internet Service Providers
ITU	International Telecommunications Union
ILC	International Law Commission
MitM	Man-in-the-Middle
MKO	Mujahedin-e-Khalq Organization
NATO	North Atlantic Treaty Organization
NHS	National Health Service
NSA	National Security Agency

OSCE	Organization for Security and Cooperation in Europe
OECD	Organization for Economic Cooperation and Development
OSCE PA	Organization for Security and Cooperation in Europe Parliamentary Assembly
PA	Parliamentary Assembly
PKK	Kurdistan Workers' Party
SCADA	Supervisory Control and Data Acquisition
SQL	Structured Query Language
UN	United Nation
UNGA	United Nations General Assembly
UN GGE	United Nation Groups of Governmental Experts
UNSG	United Nations Secretary-General
UNSC	United Nations Security Council
US	United States
USB	Universal Serial Bus
XSS	Cross-Site Scripting

THESIS STATEMENT

The technological revolution has changed the face of modern warfare as the cyber space has become a threat to national security, hence, there is need to examine the state practices regarding the precautionary measures in context of self-defense.

INTRODUCTION

Certainly! Scientific advancements are undeniably changing our society's progress. The rise of cyber technology has led us into a cyber-society, marked by new economic, socio-cultural, and political guidelines. With the current possibilities offered by technology, many existing norms, both within countries and internationally, are quickly becoming outdated. They can't keep up with the new challenges presented by the cyber world. Nowadays, International Law is dealing with problems that were unimaginable when its rules were first established. Specifically, it struggles with how to regulate the use of force and self-defense in relation to cyber activities. Both countries and international organizations have not ignored these new legal challenges arising from cyber technology.

As a result, the actual and potential threats that come from activities in cyberspace are significant concerns for countries, especially in developed nations that heavily rely on technology and are more vulnerable to such threats. [1]. In this sense, the US in its Assessment of International Legal Issues in Information Operations expressed its concern over cyber space threats where;

> The attacker may be a foreign State, an agent of a foreign State, an agent of a non-governmental entity or group, or an individual acting for purely private purposes. The equipment necessary to launch a computer network attack is readily available and inexpensive, and access too many computer

[1]Yoram Dinstein, "Computer network attacks and self-defense," in *Computer network attack and International Law, ed.* M. N. Schmitt and B. T. O'donnell (Newport": Monographic published in International Law Studies, 2002), 99-119.

> systems can be obtained through the Internet or another network to which access is easily obtained[2].

Furthermore, former President Obama issued an Executive Order whose Section 1 explicitly expressed its concerns that "the cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront"[3].

In the framework of the United Nations (UN), the Russian Federation introduced in 1998 a Draft Resolution in the First Committee of the United Nations General Assembly (UNGA), where pointed out its;

> Concern that these technologies and means may potentially be used for purposes incompatible with the objectives of ensuring international security and stability and the observance of the principles of non-use of force, non-interference in internal affairs and respect for human rights and freedoms[4].

Accordingly, the issue of cyber space threats has remained on the United Nations (UN) agenda since its introduction by the Russian Federation through the Draft Resolution. Subsequently, concerns regarding cyber space activities have been acknowledged in UNGA Resolution 57/239 of 2002, which recognizes that the increasing interconnectivity of information systems and networks exposes them to a growing number and wider variety of threats and vulnerabilities. This development raises new security concerns for all[5].

Additionally, both UNGA Resolution 58/199 of 2003 and UNGA Resolution 64/211 of 2009 have placed special emphasis on safeguarding critical information

---

[2] 1. Lau Francis, Simson Garfinkel Rubin, Mark Smith and Ljiljana Trajkovic, "Distributed denial of service attacks in Systems, Man, and Cybernetics*," IEEE International Conference* 3, (2000): 18-19.

[3] Ibid.

[4] Ibid.,16.

[5] Michael N. Schmitt, "Bellum American: The US view of Twenty-first Century war and its possible implications for the law of armed conflict," *Michigan Journal of International Law*, (1998): 26-28.

infrastructures from cyber threats. Furthermore, the United Nations Secretary-General (UNSG) has submitted annual reports to the UNGA, which provide the perspectives of UN Member States on developments in the field of information and telecommunications within the context of international security.

Furthermore, there have been annual reports by the United Nations Secretary-General (UNSG) to the UNGA with the views of UN Member States on the Development in the field of information and telecommunication in the context of International security[6]. In this regard some States, such as Germany, affirmed that;

Process control systems utilized in critical infrastructures have demonstrated notable vulnerability to malicious ICT operations. The potential for extensive and uncontrollable collateral damage on a global level is significant. This includes the possibility of infecting industrial control systems, potentially leading to physically destructive consequences. It is worth noting that a solitary cyber-attack targeting essential telecommunication infrastructure could result in greater global disruption compared to a single physical attack[7].

In order to address these concerns, Spain took a significant step forward in 2011 by enacting a law aimed at protecting the most critical infrastructures. Furthermore, in 2016, Spain expressed clear support for the international consensus on cyber security, highlighting the importance of ongoing deliberations on how the principles and norms of International Law, particularly those pertaining to the threat or use of force, humanitarian law, and the protection of individuals' fundamental rights and

[6] Matthew. J. Sklerov, "Solving the Dilemma of State Responses to Cyber-attacks: A Justification for the Use of Active Defenses against States Who Neglect Their Duty to Prevent." *Military Law Review*, (2009): 23-34.

[7] Ibid.

freedoms, should be interpreted and applied in the realm of cyberspace[8].

Since 2004, the United Nations (UN) has established various Groups of Governmental Experts (GGE) to examine existing and potential cyber threats, as well as explore possible cooperative measures to mitigate them. The initial 15-member GGE was formed in 2004 but did not reach a substantive agreement on a report. However, the second GGE, which issued its report in 2010, marked the first successful UN GGE report. This report placed emphasis that:

> The growing use of information and communications technologies (ICTs) in critical infrastructure creates new vulnerabilities and opportunities for disruption. Because of the complex interconnectivity of telecommunications and the Internet, any ICT device can be the source or target of increasingly sophisticated misuse. Since ICTs are inherently dual-use in nature, the same technologies that support robust e-commerce can also be used to threaten international peace and national security[9].

The Third UN GGE report, submitted to the UNGA in June 2013, stressed that "threats to individuals, businesses, national infrastructure and Governments have grown more acute and incidents more damaging. The sources of these threats comprise both State and non- State actors"[10].

The Fourth UN GGE, established in 2015 with 20 experts including all UNSC Permanent members, affirmed in its report that:

> The use of ICTs for terrorist purposes, beyond recruitment, financing,

[8] Anna Wortham, "Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent That May Violate UN Charter Provisions Prohibiting the Threat or Use of Force?," *Federal Communications Law Journal* 64, (2011): 34-37.

[9] Jensen Eric Talbot Jensen, Eric. "Computer Attacks on Critical National Infrastructure: A Use of Force invoking the Right of Self-defense." *Stanford Journal of International Law* 7, (2002) 88-96.

[10] Laura Donohue, "The Nature of War and the Idea of Cyber war," in *Cyber war, Law and Ethics for Virtual Conflicts*, ed. Jens David Ohlin, Kevin Govern, and Claire Finkelstein (New York: Oxford University Press, 2015), 67-68.

> training and incitement, including for terrorist attacks against ICTs or ICT-dependent infrastructure, is an increasing possibility that, if left unaddressed, may threaten international peace and security"[11].

The Fifth UN GGE, in its fourth and finalsession on 19-23 June 2017, ended without consensus on its final report. These reports introduced that existing International Law applies to the digital space, and developed norms and principles of responsible behavior of States in cyberspace. While such UN GGE reports carry significant influence in the field of global cyber security, the Group's future is uncertain. In its absence, it seems States may lean towards bilateral agreements, a trend which has become particularly prevalent in the last years[12].

Moreover, the UN GGE reports in 2013 and 2015 respectively, were unanimously adopted by UNGA Resolutions 68/243 of 2013 and 70/237 of 2015 expressing their concern that;

> These technologies and means can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure of States to the detriment of their security in both civil and military fields[13].

Furthermore, aiming to establish confidence and security in the use of Information and Communication Technologies (ICT), the International Telecommunications Union (ITU) initiated the Global Cyber security Agenda (GCA) in 2007. It serves as a framework for international cooperation in this domain. Additionally, various international organizations, including the Organization for Security and Cooperation

[11] Ibid.

[12] H. B Robertson, "Self-Defense against Computer Network Attack under International Law." in *Computer Network Attack and International Law*, ed. Michael. N. and O 'Donell, B. T. (Newport: Naval War College Newport press, 2002): 43-50.

[13] Michael N. Schmitt, "Cyber Activities and the Law of Countermeasures," in Peacetime Regime for State Activities in *Cyberspace ed. Katharina Ziolkowski* (Tallinn: International Law, International Relations and Diplomacy, *NATO CCD COE Publication*, 2013): 55-68.

in Europe (OSCE), the North Atlantic Treaty Organization (NATO), the European Union (EU), the Organization for Economic Cooperation and Development (OECD), and the Council of Europe (COE), have engaged with the challenges posed by cyber space.

The OSCE Parliamentary Assembly (PA) recognized the severity of threats originating from cyber space in its 2008 Resolution on Cyber Security and Cyber Crime. It acknowledged that such threats could endanger the modern way of life and civilization as a whole. The Minsk Declaration expressed similar concerns about ongoing security challenges, including cyber security threats and violent extremism. It urged the adoption of measures to enhance cyber security between states, prevent tensions and conflicts arising from the use of information and communication technologies, and protect critical infrastructure from cyber threats[14]. Furthermore, during the Lisbon conference on Digital Resilience of a Democratic State, the OSCE PA emphasized the importance of cyber threat protections while upholding fundamental freedoms[15].

NATO has been addressing cyber operations as part of its political agenda since the Prague Summit in 2002. The cyber-attacks against Estonia in 2007 marked a turning point in the Alliance's attention towards cyber defense. In 2008, NATO formulated its First Cyber Defense Policy, followed by its inclusion in NATO's Strategic Concept at the Lisbon Summit in 2010[16]. In 2013, the NATO Cooperative Cyber Defense Centre of Excellence convened a group of international experts to establish principles for addressing cyber-attacks, which were outlined in the Tallinn Manual.

[14] D. Momtaz, "Did the Court miss an opportunity to denounce the erosion of the principle prohibiting the use of force?," *Yale Journal of International Law*, (2004): 25-27.

[15] Nicolo Bussolati, "The Rise of Non-State Actors in Cyber warfare," in *Cyber war, Law and Ethics for Virtual Conflicts*, Ed. J. D Ohlin, K. Govern, C. Finkelstein (New York: Oxford University Press, 2015), 46.

[16] Gerhard Nolte, Multipurpose Self-Defence, Proportionality Disoriented: A Response to David Kretzmer," *European Journal of International Law*, (2013): 14-18.

This manual focused on the most disruptive and destructive cyber operations, classifying them as armed attacks and allowing states to respond in self-defense[17]. The Tallinn Manual was subsequently updated in 2017 as Tallinn Manual 2.0, examining the international legal framework applicable to cyber operations and exploring general principles of International Law[18].

At the Wales Summit in September 2014, NATO approved an enhanced Cyber Defense Policy, affirming that a significant digital attack on a member state could be covered by Article 5 of the NATO Treaty[19]. It also emphasized the need for dialogue and cooperation between NATO and the EU on common security challenges, including cyber defense, proliferation of weapons of mass destruction, counter-terrorism, and energy security. Recognizing the shared challenges in cyberspace, NATO and the EU adopted a Joint Declaration on July 8, 2016, establishing cooperation in the field of cyber security and defense as a strategic priority. Subsequently, the Council of the EU approved a Conclusion on the implementation of this declaration on December 6, 2016[20].

The EU has been actively engaged in the field of cyber space since the nineteenth century, particularly due to the increasing number of cyber-attacks on individuals, companies, and critical infrastructures[21]. The Council of the EU adopted a decision on attacks against information systems in 2005, and the European Commission and the High Representative of the EU published their first cyber security strategy in 2013[22]. In terms of legislation, the EU introduced the Network and Information Security (NIS) Directive in 2016, the most comprehensive instrument to date. This

[17] Michael, Cyber Activities and the Law of Countermeasures, 68.
[18] Ibid.
[19] Nicolo, The Rise of Non-State Actors in Cyber warfare, 65.
[20] Mary Ellen O'Connell, "Cyber Security without Cyber War," *Journal of Conflict and Security Law* (New York: Oxford University Press 17, 2012): 51-54.
[21] Ibid.22.
[22] Ibid.

directive includes incident reporting obligations for the private sector, including operators of essential services and digital service providers. In 2017, the Council of the EU approved Draft Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities, aiming to reinforce the EU's activities in this field and enhance coordinated responses in the event of cyber-attacks on European targets[23].

Furthermore, as a response to the rise of cyber threats, the Council of Europe adopted the Convention on Cybercrime to harmonize national laws in this area. It recognizes the need for a common criminal policy to protect society against cybercrime, emphasizing the importance of appropriate legislation and international cooperation[24]. It is essential to note that this research focuses on Public International Law related to cyber activities, particularly those falling under the right of self-defense according to Article 51 of the UN Charter, especially when the attackers are non-state actors. Therefore, it does not address cyber activities related to cyber warfare, cyber responsibility, international telecommunications law, human rights, diplomatic law, law of the sea, air law, or space law.

RESEARCH QUESTIONS

1. Whether a cyber-operation can violate the principle of the prohibition of the threat, particularly when such operations give rise to high level of economic and political intensity.
2. To what extent do the principles of self-defense, as articulated in international law, accommodate and respond to the complexities posed by

[23] Michael N. Schmitt, "Cyberspace and International Law: The Penumbral Mist of Uncertainty," *Harvard Law Review* 126, (2013):67-73.
[24] David Sanger, "Obama Order Sped up Wave of Cyber-attacks Against Iran," *New York Times*, Apr. 9. 2012. Retrieve from https://www.nytimes.com. Last accessed 9/4/2022.

cyber-attacks, considering the evolving nature of technological capabilities and the global threat landscape?

3. Whether cyber-attacks constitute a “use of force” and “armed attack” that reflects the traditional goals of the UN Charter, while taking into account the present realities of the use of cyber-attacks
4. Under which conditions can cyber operations amount to an armed attack to justify resorting to the right of self-defense?
5. Whether in front of an imminent cyber-attack is, in contemporary International Law, applicable the anticipatory or pre-emptive right of self-defense.

SIGNIFICANCE OF THE STUDY

This research work will discuss to what extent existing international law is adequate to regulate the issue of cyber-attacks in relations to self-defense. More specifically, this research will cover an examination of what legal authority states have to respond with forcible measure to cyberattacks or cyber threats by states or non state actors. Initially, the legal framework surrounding self-defense and use of force in international law will be presented. It will be explained that the fundamental principle of Article 2 (4) and Article 51 of the Charter of the United Nations are sufficient to meet the new challenges which cyber-attacks pose.

The threshold for legal self-defense will be examined and it will be explained that whether a cyber-attack can be categorized as an armed attack will defense on the damage and effect the attack causes more than the type of weapon which has been launched. Thus, it has to be respected to ensure certainty, peace and stability in the international order. If it was considered irrelevant or ignored by cyber actors, the world would be less safe. The absence of specific norms customary principles or State practice regulating cyber operations in International Law drives many scholars to

pursue answers based on analogies and to elaborate proposals of new rules. Our task, in this research, will be to focus on finding out in which way has the International Law been modified to cope with cyber activities threats.

REVIEW OF RELATED LITERATURE

Kanuck argues that since state behavior is a major contributor to interpretation of international law, the lack of consensus leads to the initial conclusion that cyber-related attack is a relatively new development. Therefore, the issue lacks adequate historical context and is in need of a clear delineation of the norms that define the phenomena and what acceptable responses might entail.25 British Foreign Secretary Hague has called for nations to discuss "norms for state behavior in cyberspace".[26]

Hathaway and explain that following the documented cyber-attack on Estonia of 2007, the North Atlantic Treaty Organization (NATO) was unable to act, lacking a previously agreed upon response to such an incident; however, at the 20th NATO Summit in 2008 in Bucharest, the group formally addressed cyber-attacks.[27]

Hughes notes that following the summit, two new NATO divisions were created in order to focus on the threat of cyber-attacks: The Cyber Defense Management Authority and the Cooperative Cyber Defense Centre of Excellence. The example of NATO and its cyber defense initiatives created as a result of the 2008 Bucharest Summit do not necessarily qualify as a widespread and inclusive endeavor. Still, it does highlight the possibility of multilateral cooperation and agreement among states

[25] Sean Kanuck, "Sovereign Discourse on Cyber Conflict under International Law," Tax Law Review 88, no.7, (2010): 71-79.

[26] Timothy Farnsworth, "UK Calls for International Cyber Conference," *Arms Control Today* l42, no.1, (2011): 7

[27] Anne Hathaway Oona, Rebecca Crootof, Paul Levitz, H. Nowlan Alden, W. Perdue and J. Spiegel "The Law of Cyber Attack," California Law Review 100, (2012): 21-26.

regarding the issue of cyber war. Agreement on application is vague at this stage, but members continue dialogue on the matter.[28]

As pertains to cyber-attack, **Benatar** shows that a broad interpretation of Article 2(4) of the UN Charter could lead one to "…demonstrate that cyber-attacks are perhaps not a new kind of force but instead a new kind of armed force". Interestingly, jus ad bellum (the right to war) does not categorize which weaponry is authorized, and Benatar states that the legality or the question thereof with regards to cyber force is difficult to ascertain. However, Benatar does reference the International Telecommunications Convention, the laws of neutrality, and international humanitarian law as those norms that may be challenged by the use of cyber force.[29]

Muir, Lawrence L. argue against an international convention on cyber-warfare. These challengers claim that independent and autonomous efforts on the parts of states should be the main prospect[30]. Any international convention only serves to limit state opportunity to create its own framework to handle cyberwar. In addition, there is the question of, "…ambiguities that will prevent any meaningful international discourse and resolution from taking place". Muir sees the issue strictly from an American perspective, as the world leader in cyber operations. He claims that unilateral action on the part of the United States is the correct course of action in attaining what he sees as the four goals for, "…The development of a legal regime around cyber warfare.[31]

---

[28] J. Richmond, "Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict," Fordham International Law Journal 35, (2011): 11-20.

[29] Marco Benatar, "The Use of Cyber Force: Need for Legal Justification?," *Goettingen Journal of Int Law* 1, no. 3, (2009): 375-396.

[30] Ibid.

[31] Lawrence L Muir, "The Case against an International Cyber Warfare Convention," *Wake Forest Law. Rev*. (2011) Online available at https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf. Last accessed 26/10/2022.

However, enlightened realists **Rid, Thomas** argue that it may be in the best interests of the state to enter into international agreements on cyber-warfare. The realist perspective will be briefly described later in this paper. Conversely, some argue that the issue of cyberwar is not a relevant issue. Rid argues that cyberwar is not a separate threat at all. He claims that cyberwar is simply, "sophisticated versions of three activities that are as old as warfare itself: subversion, espionage and sabotage".[32] Citing Clausewitz on "the most concise concept of war," Rid claims that past cyber-attacks do not meet the criteria of an act of war: violent character, instrumentality as a means to an end and political nature. Rid does not believe that there will be any comparatively large-scale event on the scale of the Hiroshima attack or the Pearl Harbor attack of World War II, and to compare cyberwar to nuclear war is "misplaced and problematic".[33]

Kanuck points to the 1990s as the decade in which "efforts to analyze 'information warfare' under international law" took shape. He argues that states try to "exercise their sovereignty over cyberspace". The challenge of cyberspace to the conception of physical boundaries that is so endemic to international law makes the effort to exercise sovereignty a unique undertaking. It is not simply a question of state government influence, but also that of private companies and sometimes a combination of the two entities. **Kanuck** states, "Once one appreciates that governments seek to extend their sovereign authority into this new realm, it then becomes necessary to analyze how their interests may align or conflict in regard to

[32] Thomas Rid, Cyber War Will Not Take Place," *The Journal of Strategic Studies* 35, no.1, (2012): 5-31

[33] Ibid.

nonexclusive resources". Therefore, Kanuck argues in favor of collective standards where unilateral action is not the answer.[34]

The literature to date has only obliquely dealt with the issue of State responsibility for cyber-attacks in international law. Some works note that armed coercion is generally chargeable to States more so than other forms of coercion, but do not address the degree of proof needed to constitute State responsibility. The one recent collection of essays on cyber warfare entirely ignores the topics of State responsibility, attribution, sovereignty and management of the information commons, all of which are central to countering cyber-attacks. There is thus a paucity of literature dealing with cyber-attacks from the lens of international law and relations, to say nothing of the ethical and human rights implications of cyber-attacks on national and international security[35]. Treatments of cyber-attacks and information warfare outside the orthodox international humanitarian law framework are also nearly non-existent. In particular, the literature to date has been silent on the appropriate legal regime to use as a baseline for regulatory responses to cyber-attacks despite the fact that a developed system of treaties on the law of war now governs many aspects of the conduct of modern warfare, from weapons of mass destruction to the treatment of POWs and non-combatants[36]. Nor has the growing literature on the rise of Internet law and the information commons applied its findings to the question of State responsibility for cyber-attacks. Consequently, there is an important gap in the international law literature that this work addresses by explicitly laying out the increase of military or cyber operations by non-State actors constitute serious threats to the State sovereignty

[34] Sean Kanuck, "Sovereign Discourse on Cyber Conflict under International Law," Tax Law Review 88, no.7, (2010): 71-79.

[35] Ibid.

[36] Nicholas Tsagourias, "Necessity and the Use of Force: A Special Regime," *Netherlands Yearbook of International Law* 3, (2010): 12-20.

and arise the issue of whether cyber operations by non-State actors with high gravity can justify the right of self-defense against such actors, especially when any State is substantially involved in such operations. Moreover, it raises the question of whether States have the authorization to use kinetic weapons in the right of self-defense in response to cyber operations that amount to an armed attack. In relation to other requirements, particularly to the immediacy condition, we attempt to give appropriate answer whether in front of an imminent cyber-attack is, in contemporary International Law, applicable the anticipatory or pre-emptive right of self-defense. Also whether it is possible to resort to preventive self-defense against a future cyber-attack. Finally, in which situations can a State use the right of self-defense a posteriori against a cyber-attack.

RESEARCH METHODOLOGY

In this thesis, the legal method was applied to describe, systematize, and analyze the existing rules in force. Given the relatively new nature of this legal domain, the thesis primarily relied on a comprehensive examination and systemization of previous adjudications. It involved an independent analysis of customary international law, state practices, and the actions of the United Nations. The legal framework for analyzing these issues was drawn from the provisions regarding the use of force and self-defense in international law, as outlined in the Charter of the United Nations.

The research primarily drew analogies within existing law, particularly examining the classic use of self-defense as a response to an armed attack. This approach was necessitated by the absence of specific precedents or well-defined sources within international law regarding cyber-attacks as constituting an armed attack.

Furthermore, this examination encompassed a review of legal literature, reports, UN Security Council resolutions, and General Assembly resolutions to provide comprehensive insights into the subject matter.

CHAPTER NO 1

THE RIGHT OF SELF-DEFENSE IN INTERNATIONAL LAW

1.1 INTRODUCTION

The core principle behind self-defense is rooted in self-help, a concept found in early legal systems across civilizations. According to the International Law Commission Self-Defense can be seen as a form of armed self-help or self-protection, allowing modern States to exercise this right directly[37]. This fundamental right of self-defense is universally recognized in customary international law, also known as the law of nations. The UN Charter, which is the primary codification of these customs and practices, does not create or restrict this right; it simply acknowledges its existence[38]. Both the French version of the UN Charter and the International Court of Justice (ICJ) affirm that the right of self-defense is inherent. Through the actions and customary practices of States, particularly evident within the United Nations Security Council (UNSC), a customary law has developed regarding the implementation of self-defensive actions. Some scholars argue that Article 51 of the UN Charter has solidified this customary norm. Moreover, Article 51 encompasses both customary and conventional aspects of self-defense[39].

The ICJ emphasizes that Article 51 can only be properly understood within the

[37] A State responsible for an internationally wrongful act is under an obligation to make restitution, that is, to re-establish the situation which existed before the wrongful act was committed, provided and to the extent that restitution: 1. Is not materially impossible; 2. Does not involve a burden out of all proportion to the benefit deriving from restitution instead of compensation. ILC, "State responsibility" ll, (1980): 2.

[38] William J. Haynes, "Legal Distinction between preemption, preventive self-defense and anticipatory self-defens*e", Office of General Counsel*, (2002). available at http://library.rumsfeld.com/doclib/sp/2564/2002-10-16%20from%20William%20Haynes%20re%20Legal%20Distinction%20Between%20Preemption,%20Prev entive%20and%20Anticipatory%20Self-Defense.pdf. Last accessed 23/12/2022.

[39] ICJ, *Nicaragua case*, par. 176

context of a 'natural' or 'inherent' right of self-defense[40], most likely of a customary nature, even though the Charter may have influenced its current content.

As per Article 51 of the UN Charter:

> Any armed attack against a Member of the United Nations shall not infringe upon the inherent right of both individual and collective self-defense. This right remains valid until the Security Council has implemented measures to uphold international peace and security. Member States exercising this right of self-defense are obligated to promptly report their actions to the Security Council. These actions taken in self-defense shall not undermine the authority and responsibility of the Security Council, as outlined in the present Charter, to take any necessary action at any time to preserve or reinstate international peace and security.[41]

The right of self-defense recognizes the inherent entitlement of both individual and collective self-defense against armed attacks. Article 51 of the UN Charter confirms that the right of self-defense can be exercised individually or collectively. This provision offers assurance to UN member States that they are legally authorized to use force in self-defense if the UN's enforcement mechanisms fail[42]. There are two perspectives or approaches to understanding what collective self-defense entails.

1. The first modality involves a pre-established agreement in a bilateral or multilateral treaty for mutual self-defense or military alliance.
2. The second modality requires a prior and urgent request from a State that has fallen victim to an armed attack by other States[43].

In the case of the first modality, various treaties explicitly establish collective

[40] Bruno Simma, *The Charter of the United Nations (*A Commentary. New York: Oxford University Press, 2002), 51-59.

[41] Article 51 of UN Charter 1945.

[42] The requirement of the request is firmly reaffirmed by the IDI, 10A Resolution on "Present problems of the use of armed force in International Law. Additionally, State practice has provided evidence supporting this condition, as seen in Vietnam's case when facing aggression from the North with the support of the US in 1965.

[43] Ibid.

responses in the event of an armed attack on one of the State parties, outlining the conditions under which such States commit to providing assistance[44]. For instance, examples of such treaties include Article 5 of the North Atlantic Treaty Organization (NATO) signed on 4 April 1949, Article 42(7) of the European Union Treaty signed on 7 February 1992, or Article 2 of the Treaty of Joint Defense and Economic Cooperation among the States of the Arab League dated 17 June 195o[45].

In the context of the second modality, the exercise of the collective right of self-defense is subject to two conditions laid out by the International Court of Justice (ICJ) in the Nicaragua case. Firstly, the State facing an armed attack must openly declare itself a victim and has the sole authority to determine whether an armed attack has occurred. It can then seek assistance from other States in its quest for help. Secondly, the victim State, after being subjected to an armed attack, must formally request assistance based on the right of self-defense. Fulfilling these requirements is essential, in addition to meeting other criteria, such as necessity, proportionality, immediacy, and notifying the United Nations Security Council (UNSC) of the action taken[46].

The primary purpose, as stated in Article 51 of the UN Charter, is to safeguard the existence of a state. Self-defense is an inherent right intertwined with a state's sovereignty, signifying its foremost duty to ensure its survival. The International Court of Justice (ICJ) underscored that every state possesses the fundamental right to

[44] Furthermore, the requirement of the request is unequivocally reaffirmed by the IDI, 10A Resolution on "Present problems of the use of armed force in International Law. A. Self-defence", Tenth Commission, 27 October 2007.

[45] UN Charter, Article 51. “Until the Security Council has implemented the necessary measures to uphold international peace and security.”

[46] Actions carried out by Member States in exercising the right of self-defense shall not, in any manner, diminish the authority and responsibility of the Security Council to undertake, at any moment, such actions as it considers necessary to uphold or restore international peace and security" (Article 51 of the UN Charter).

survival and the right to resort to self-defense, in line with Article 51 of the Charter, particularly when its survival is at risk[47].

In the realm of International Law, certain prerequisites must be met to apply either individual or collective self-defense. Firstly, this right can only be utilized in a provisional and subsidiary manner when the collective security system is unable to address the threat effectively. Secondly, a crucial condition is the existence of an armed attack, as explicitly outlined in Article 51 of the UN Charter. Lastly, the right of self-defense must satisfy three requirements established by customary International Law: necessity, proportionality, and immediacy[48].

1.2 THE ROLE OF THE UN SECURITY COUNCIL IN THE FRAMEWORK OF THE COLLECTIVE SECURITY SYSTEM

The conditions governing the integration of self-defense with the collective security system are specifically outlined in Article 51 of the UN Charter. As per this article, self-defense actions are provisional and subsidiary to the actions of the UN Security Council (UNSC), which aligns with the primary responsibility of the UNSC to maintain international peace and security.

The UN Charter conceptualizes self-defense as a provisional measure, applicable when the Chapter VII collective defense system is ineffective. Consequently, during the implementation of self-defense measures, States must promptly inform the UNSC and assess whether the actions are in line with Article 51 and whether the need for collective measures outweighs individual actions. Nonetheless, the UNSC has never paralyzed such actions through unanimity; usually, the veto has been used

[47] According to the International Court of Justice (ICJ), in the case Legality of nuclear weapons, the Court confirmed that "In addition to the requirements of necessity and proportionality, Article 51 specifically mandates that States promptly report the measures taken in the exercise of the right of self-defense to the Security Council."

[48] Y. Arai-Takahashi, "Shifting boundaries of the right of self-defense. Appraising the impact of the September 11 attacks on jus ad bellum," *The International Lawyer* 36, no. 4 (2002): 1081-1102.

beforehand[49].

While States do not require prior authorization from the UNSC to engage in self-defense, they must cease their armed responses once the UNSC adopts necessary measures to maintain or restore international peace and security. This serves as a contribution to complying with the general prohibition of the use of force, as stated in Article 2(4) of the UN Charter.

The obligation to report to the UNSC is independent of the correctness of the acts taken in self-defense. It is a formal requirement explicitly provided in the Charter to enable the UNSC to oversee the use of force allowed by the Charter. This obligation centers on three aspects: First, the timing of the report, which must occur immediately after the adoption of defensive measures and should not be confused with the application of those measures. This obligation is not always fulfilled; for instance, Iran did not report the Iraq attack on 22 September 198 to the UNSC until 1st October 198[50].

Second, the content of the communication to the UNSC. The Charter does not specify any particular characteristics or content that States must include in the report. The variety of content ranges from precise descriptions of actions to mere notifications of measures taken under the exception of the right of self-defense. The UNSC does not penalize States for not providing precise descriptions, a circumstance that has been criticized for hindering the determination of the nature of the actions.

Third, the consequences of non-compliance with the communication to the UNSC.

[49] D. W. Greig, "Self-defense and the Security Council: what does article 51 require?," *International and Comparative Law Quarterly* 40, no. 2 (1991): 366-402.

[50]The Iran invasion of Iraq's territory, justified by invoking the right of self-defense to pursue Kurdish armed groups, managed to evade international criticism. However, there was insufficient evidence to link the conduct of the MKO (Mujahedin-e Khalq Organization) to Iraq. For more information, refer to Th. M. Franck's, *threats and armed attacks*, (Cambridge University Press, 2002), 64.

Initially, the UNSC placed greater emphasis on this duty, but over time, it has become less stringent in its requirements. However, States claiming self-defense tend to provide more or less accurate information about their actions. Nonetheless, it is excessive to claim that non-compliance with this requirement renders any immediate action in the right of self-defense illicit. It represents a violation of procedural duties according to Article 51 of the UN Charter, as "such failure is not itself a substantive breach that invalidates the exercise of the right to self-defense[51]."

Under the right of self-defense, the reaction of a victim State would be considered fulfilled once the aggressor State's armed attack, as defined in Article 51 of the UN Charter, is neutralized, the aggressor State withdraws, or the UNSC adopts necessary measures. Although States do not need authorization from the UNSC to act in self-defense, they must refrain from such actions as soon as the UNSC takes the necessary measures to maintain or restore international peace and security.

According to Article 51 of the UN Charter, the failure to report to the UNSC about self-defense actions does not constitute a substantive breach that invalidates the exercise of the right to self-defense[52]. Under the right of self-defense, a victim State's response would be considered fulfilled when the armed attack by the Aggressor State[53], as defined in Article 51 of the UN Charter, is neutralized, the Aggressor State withdraws, or the UNSC takes the necessary measures. Although States do not

[51] According to the Court's perspective, every State bears the responsibility of ensuring that its territory is not knowingly utilized for activities that violate the rights of other States (ICJ, Corfu Channel case, paragraph 4). This principle is further reinforced by UNGA Resolution 2625 (XXV), particularly in paragraphs 8 and 9, which emphasize the prohibition of the threat or use of force.

[52] As an example, in the African Union Non-Aggression and Common Defence Pact dated 1st January 2005, aggression is defined in article 1, c (xi) as "the act of encouraging, supporting, harboring, or providing any assistance for the commission of terrorist acts and other violent trans-national organized crimes against a member State."

[53] An aggressor state refers to a country or nation that initiates or launches an aggressive action against another country, often using military force or engaging in hostilities. In international relations and law, an aggressor state is seen as the one that commits an act of aggression, which may include invasion, attack, or any other use of armed force against the territorial integrity, political independence, or sovereignty of another state.

require authorization from the UNSC to act in self-defense, they must immediately refrain from further actions under this right as soon as the UNSC adopts measures to maintain or restore international peace and security.

1.3 REQUIREMENTS FOR THE EXERCISE OF THE RIGHT OF SELF-DEFENSE

The exercise of the right of self-defense is a fundamental principle of international law, permitting a state to employ force in response to an armed attack. However, the exercise of this right is subject to several requirements, which encompass the following:

1.3.1 Armed Attack

According to international law, the right to self-defense is only permissible as a response to an armed attack. The concept of an "armed attack" is a critical element within the right to self-defense and has been subject to diverse interpretations by the international community. The most authoritative definition of an "armed attack" can be found in Article 51 of the United Nations Charter, stating that the right to self-defense can only be exercised when a state faces an armed attack. The use of force must be necessary and proportional, and the self-defense measures taken must be immediately reported to the UN Security Council[54].

The International Court of Justice (ICJ) has also offered some clarification on the definition of an "armed attack." In the case of Nicaragua v. United States, the ICJ stated that an "armed attack" is fundamentally characterized by the use of force by one state against another state and that the form of such an attack may vary. This

[54] To demonstrate the legality of its actions in exercising the right of individual self-defense, the United States must prove that it faced attacks attributed to Iran, and that these attacks met the criteria of 'armed attacks' as defined in Article 51 of the United Nations Charter and customary law on the use of force. This requirement is emphasized in the ICJ's Oil Platforms case, as stated in paragraph 51.

implies that an armed attack can take different forms, such as a military invasion, bombing, or even a cyber-attack, as long as it involves one state using force against another[55].

Furthermore, the ICJ has established that the threshold for an armed attack is relatively high, and minor acts of violence or incursions into a state's territory may not necessarily qualify as an armed attack. In the case of oil Platforms (Islamic Republic of Iran v. United States of America), the ICJ emphasized that the use of force must be "of such a degree as to amount to an actual armed attack" and that not every use of force, even if in violation of international law, will be considered an armed attack. It is essential to note that the requirement of an armed attack does not apply to non-state actors, such as terrorist groups. There has been an ongoing debate in recent years about whether a state can exercise the right to self-defense against non-state actors carrying out attacks on its territory. The ICJ's stance is that a state can invoke the right to self-defense against non-state actors only if they are operating under the direction or control of another state.

1.3.2 Necessity

Traditionally, the necessity requirement has been recognized as a condition to exercise the right of self-defense against an armed attack by a state in inter-State conflict. However, this requirement is not explicitly mentioned in Article 51 of the UN Charter. In this context, necessity and proportionality have customary character, supplementing the UN Charter provisions.

Necessity is one of the prerequisites for the exercise of the right of self-defense,

[55] D. M. Momtaz, "Did the Court Miss an Opportunity to Denounce the Erosion of the Principle Prohibiting the Use of Force," *Yale Journal of International Law* 29, no. 2, (2004): 19. The author explores whether the court missed a chance to condemn the weakening of the principle prohibiting the use of force. The article delves into this topic and presents a critical analysis of the Court's stance on the matter.

implying that the use of force must be essential to repel an armed attack or prevent an imminent one. The principle of necessity dictates that the use of force must be proportional to the threat faced by the state and must not go beyond what is necessary to repel or prevent the attack. It is rooted in the idea that force should be a last resort, used only when all other peaceful means of resolution have been exhausted. In other words, the state must demonstrate that the use of force was necessary to protect itself and its citizens from an imminent or ongoing armed attack and that no other means of resolving the situation were available or effective.

The principle of necessity is closely related to the principle of proportionality, which requires that the use of force must not be excessive or go beyond what is necessary to repel the attack. Together, these principles ensure that the use of force in self-defense is limited to what is necessary to protect the state and its citizens and does not lead to unnecessary harm or escalation of the conflict. It is evident that the necessity to act in the right of self-defense against an armed attack aligns with the defense of a state, the realization of state rights, or provocation[56].

To exercise the right of self-defense against an armed attack by states, assessing the necessity criteria is comparable between forcible and non-forcible use of force. However, discerning necessity criteria in the right of self-defense against an armed attack by non-state actors in the territory of another state entails a comparison between unilateral actions by a victim state or unilateral actions by a host state. If an armed attack occurs by non-state actors, according to the necessity condition, before resorting to the right of self-defense, the victim state must request the host state to suppress the non-state actors' acts[57]. Alternatively, the victim state might cooperate with the host state to repress such groups or acquire the host state's consent to

[56] Th. Graham, "National Self-Defense, International Law, and Weapons of Mass Destruction," *Chicago Journal of International Law*, 4 (2003): 1-17.

[57] Ibid., 18.

activate extraterritorial measures against non-state actors[58].

Thus, to justify the right of self-defense against an armed attack by non-state actors, the victim state's reaction is not subject to the primacy of the host state[59]. This notion is implied in recent state practice, where countries like Turkey, the US, and Israel frequently justified acts of self-defense against terrorist groups in other states' territory by alleging that the host state had taken no action or that its respective state is unwilling or unable to eliminate threats.

In this context, there appear to be the following scenarios: first, if the host state supports non-state actors, enforcement action by the host state against such groups seems unlikely. In this case, the victim state's reaction in the right of self-defense against an armed attack by non-state actors seems necessary. This approach was evidenced by the international community's support for military action against Al-Qaeda in Afghanistan after realizing the relationship between the Taliban regime and the Al-Qaeda organization since 199[60]. Second, when the host state merely tolerates non-state actors and does not actively support them or at least shows no evidence of support, this case seems a little more complicated.

In practice, there are instances of the international community resorting to the right of self-defense in some sporadic cases; for instance, Turkey against PKK in the territory of Iraq and recently in Syria. Moreover, Russia has tried to justify such a right of military interference in the territory of Georgia against the Chechen rebel group or Iran in front of the Mujahedin-e-Khalq organization (MKo) into the

[58] B. J Foley, "Avoiding a death dance: adding steps to the International Law on the use of force to improve the search for alternatives to force and prevent likely harms", *Brooklyn Journal of International Law*, 29(1), 2003: 129-173.

[59] S. Verhoeven, "Attacks by private actors and the right of self-defence", *Journal of Conflict and Security Law* 10, no 3, (2005): 289-320,

[60] Among others, the following United Nations Security Council resolutions provide relevant examples: UNSC Resolution 188, 9 April 1964; UNSC Resolution 228, 25 November 1966; UNSC Resolution 248, 24 March 1968; UNSC Resolution 256, 16 August 1968; UNSC Resolution 265, 1 April 1969; UNSC Resolution 270, 26 August 1969; UNSC Resolution 487, 19 June 1981; UNSC Resolution 567, 20 June 1985; and UNSC Resolution 567, 20 June 1985

territory of Iraq, claiming that the right of self-defense is applicable against terrorist groups inside the territory of another state when host states tolerate such groups in their territories[61].

This approach might have derived from the duty of states to not allow their territories to be used to infringe the rights of other states, according to the ICJ jurisprudence and UNGA Resolutions or implicitly in modern international conventions that explicitly forbid giving shelter to terrorists or any action of support to any act of aggression[62]. In order to repel armed attacks by non-state actors from the territory of another state, there is unanimity in the priority of host state action[63]. In the case that this state is unable to suppress attacks by non-state actors, the victim state, in each case, should obtain the consent of the host state and explore if there is an opportunity to work cooperatively with the territorial state to repress the threat. Thus, the preference of a victim state must be to obtain consent or cooperation with the host state, instead of acting unilaterally.

1.3.3 Proportionality

Proportionality is an essential requirement for the exercise of the right of self-defense. It stipulates that the force used in self-defense must be commensurate with the threat posed by the aggressor and the harm being defended against. In simpler terms, the use of force in self-defense should not exceed what is necessary to repel the attack and should not cause greater harm than the attack itself. The principle of proportionality plays a crucial role in balancing the competing interests of self-defense and the protection of human rights. The right of self-defense is not absolute

[61] Verhoeven, Attacks by private actors and the right of self-defense, 317.

[62] T. Mori, "Origins of the right of self-defense in International Law*," Caroline incident to the United Nations Charter*, (Brill, 2018): 5-6.

[63] Corten, O., "The controversies over the customary prohibition on the use of force: a methodological debate", *EJIL* 16, no. 5, (2005):803-822.

and must be exercised within the bounds of international law[64]. The use of excessive force or indiscriminate attacks can lead to violations of international human rights laws and may result in unnecessary loss of life and property. In practice, the principle of proportionality requires considering the following aspects:

The nature and extent of the attack: The force used in self-defense must correspond to the nature and extent of the attack. For instance, a minor attack would not justify the use of lethal force[65]. The military objectives: The force used must be directed towards achieving the military objectives of repelling the attack and protecting the state's security. It must not target civilian or non-military objectives[66]. The means of attack: The force used must be proportional to the means of attack used by the aggressor. For example, using nuclear weapons to repel a minor attack would not be considered proportional. The overall circumstances: The use of force must take into account the overall circumstances of the situation, including the potential consequences of the force's use and the likelihood of success in repelling the attack[67].

Regarding acts of self-defense under international law, three criteria must be respected. Firstly, the defensive action does not have to mirror the means used by the attacker but must focus on defending the territory[68]. Secondly, the response in self-defense must not exceed the level of necessity required to defend against the armed attack; it must not serve as an excuse to initiate a large-scale attack. The proportionality refers to the quantum of force that the Victim State is authorized to

[64] Ibid.

[65] Ruys, Verhoeven, Attacks by private actors and the right of self-defense, 317.

[66] For instance, African Union Non-Aggression and Common Defence Pact, 1st January 2005, where according to article 1, c (xi), aggression means "the encouragement, support, harbouring or provision of any assistance for the commission of terrorist acts and other violent trans-national organized crimes against a member State".

[67] Ibid

[68] Ibid., 23.

use to counter the aggressor's force, and it aligns with the type and purpose of the self-defense, not necessarily the exact material means used[69].

Thirdly, the immediate nature of the response, necessity, and proportionality are conditions that must be assessed case-by-case based on the circumstances of each particular case. The proportionality requirement is not a fixed legal formality; it is determined according to the extent of hostilities, the duration of military operations, the choice of means and methods of conflict, or geographical operations[70]. In the third criterion, one of the limits to the right of self-defense is the territory of the other State. However, in cases where the conflict persists in the border area, the defending State may temporarily enter the aggressor's territory to defend itself. This temporary penetration into the foreign territory by the defender must cease when the aggressor stops using armed force.

In addition to these criteria, in some cases, we must observe that the remoteness of the self-defense action, based on the nature of the original attack, can violate the principles of proportionality and necessity. As the ICJ confirmed, The Court cannot fail to observe that the taking of airports and towns many hundreds of kilometers from Uganda's border would not seem proportional to the series of trans border attacks it claimed had given rise to the right of self-defense, nor to be necessary to that end[71].

1.3.4 Immediacy

To justify the right of self-defense, States must fulfill the criterion of immediacy, in addition to other closely related requirements, which are interconnected with

[69] Anne Hathaway Oona, Rebecca Crootof, Paul Levitz, H. Nowlan Alden, W. Perdue and J. Spiegel "The Law of Cyber Attack," *California Law Review* 100, (2012): 21-26.

[70] D. Momtaz, "Did the Court miss an opportunity to denounce the erosion of the principle prohibiting the use of force", *Yale Journal of International Law* 29, no. 2, (2004):307-313.

[71] Ibid., 320.

necessity. As confirmed by the International Law Commission (ILC):

The fourth requirement is that armed resistance to an armed attack should occur immediately, meaning while the attack is still ongoing, and not after it has concluded. A State cannot claim to be acting in self-defense if, for instance, it launches bombings on a country that conducted an armed raid into its territory after the raid has ceased and the troops have withdrawn beyond the border[72].

Self-defense must constitute an immediate response in both time and space to the aggressive action, as the use of force in self-defense is justified only to the extent necessary to counteract the attack. Otherwise, self-defense would turn into an armed retaliation, which is prohibited by Article 2(4) of the UN Charter[73]. This would be exemplified by US air raids against Iranian oil platforms in the Persian Gulf[74], where other conditions were also violated. Thus, the requirement of immediacy distinguishes the use of force under the right of self-defense from mere retaliation. Additionally, the temporal proximity factor is crucial between the attack and response. Moreover, it is worth noting that the reaction to an armed attack must be immediate and excludes the necessity of a formal declaration of war, which may be subject to lengthy internal procedures[75].

The notion of immediacy must be assessed based on the time required to prepare the armed response, the continuation of the attack or foreign occupation of the territory, and the possibilities that can be provided by the collective security system. In this

[72] Ibid.

[73] Article 2(4) of the United Nations Charter is a fundamental provision that deals with the use of force by states. It states that, "Article 2(4): All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."

[74] Operation Nimble Archer was the 19 October 1987 attack on two Iranian oil platforms in the Persian Gulf by United States Navy forces. The attack was a response to Iran's missile attack three days earlier on MV Sea Isle City, a reflagged Kuwaiti oil tanker at anchor off Kuwait.

[75] International Court of Justice, “Case Concerning Oil Platforms (Islamic Republic of Iran v. United States of America)” Judgment of 6 November 2003.

context, there have been instances within the UNSC where the concept of immediacy has been interpreted to encompass not only the time factor but also the spatial element, requiring an immediate and proximate response in the same location relative to the attack. Indeed, given the complexity of modern conflicts, a flexible interpretation of the immediacy requirement is now considered advisable.

1.4 PREVENTIVE SELF-DEFENCE IS UNLAWFUL

According to the UN Charter, contrary to the imminent threat already covered by article 51, other latent that are not imminent threats are under the authority of the UNSC to use military force to preserve international peace and security[76]. Literally, although all terms (preventive, pre-emptive, and anticipatory self-defence) refer to the use of force prior occurring an armed attack, in International Law there is a distinction between them in light of imminent threat.

In this field, there are rhetorical distinctions among scholars to address the right of self-defence against threat and imminent threat. For instance, often pre-emptive and anticipatory self-defence are used to refer to the same concept, while preventive self-defence is used to refer to another concept. However, this rule is not followed by some authors that literally made distinctions between pre-emptive and anticipatory self-defence. For instance, Murphy claims that "Pre-emptive self-defence is used to refer to the armed coercion by a State to prevent another State or (non-State actors) from pursuing a course of action that is not yet directly threatening"[77].

The conception of preventive self-defence as an international political measure of a State does not have place in the Charter[78]. In this regard, Pastor exposes that there

[76] UNGA "In larger freedom: towards development, security and human rights for all," General's report, (2005): 124-125.

[77] J. F. Murphy, "Cyber war and International Law: does the International Law process constitute a threat to U.S vital interests?," *International Law Studies* 89, no. 1, (2013):309-340.

[78] Ibid. 390.

are three arguments:

First, an interpretation in this sense of article 51 of the UN Charter would blur the boundary between what would be a real preventive self-defence and an armed retaliation which are prohibited by International Law.

Second, the unilateral uses of force not submitted to any institutional control, easily leading to strategic errors as, for instance, the killing in Afghanistan on 1 July 2002 of forty natives who celebrated a wedding and they made outbursts of joy, that the US air force interpreted as a Taliban attack.

Third, the admission of this kind of defense would be a real damage to the principle of sovereign equality of States; only the great powers could benefit from the detriment of the less powerful States of the diffused and inaccurate limits that exist between the preventive self- defense and the armed retaliation[79].

Gonzalez adds that admitting preventive self-defence would mean, first, to open the door to arbitrary qualification of States to legitimate the use of force in the face of an attack that still is non-existent, leading to a rise in the risk to international peace and security; and second, it is completely against the responsibility of the UNSC to control the use of force in the context of article 51[80]. Gutiérrez also emphasizes that "the doctrine of preventive war can be very dangerous"[81].

Moreover, in the Oil platforms, although US claimed that their attacks were means to prevent new Iranian armed attacks, the Court did not take these allegations into account. Gutiérrez sets out two reasons why preventive self-defence does not reconcile with the jurisprudence established by the ICJ. First, the Court is expressed

[79] Ibid.
[80] Ibid., 1018.
[81] Albrecht Randelzhofer, "Article 2(4), the Charter of the United Nations," in *A Commentary*, Ed. Simma, Bruno (New York: Oxford University Press 1, no 2, 2002): 93-99.

in such a way that self- defense seems only possible when there is already a victim of a use of armed force, not when only there is a danger or threat of such force[82]. Second, the ICJ is very classic in the treatment of the self-defence: it demands all the related requirements, with particular demands on certain occasions[83]; in addition, it insist that only the most serious uses of armed force can give rise to the right of self-defence[84]. Even some authors pointed out that the sentence offers a "restrictive" interpretation of what must be understood as armed attack[85]. Despite all these notable concerns, it seems these arguments are convincing, however, when the forcible counter-proliferation theory can destroy any semblance of stability in international relations and the rule of law[86].

1.5 ANTICIPATORY RIGHT OF SELF-DEFENCE AGAINST AN IMMINENT ATTACK

Immediacy is a main requirement of the right of self-defence and is used in two different contexts: first, it is often seen as one of the requirements of the exercise of the self-defence alongside the necessity and proportionality; and second, in relation to an imminent or immediate threat of an act within the field of the anticipatory self-defence[87].

Anticipatory self-defence refers to the use of armed force by a State to halt an imminent armed attack by another State. Hence, the State has not yet been victim of

[82] ICJ, *Oil Platforms case*, 51. In order to establish that it was legally justified in attacking the Iranian platforms in exercise of the right of individual self-defence, the United States has to show that attacks had been made upon it for which Iran was responsible; and that those attacks were of such a nature as to be qualified as 'armed attacks' within the meaning of that expression in article 51 of the United Nations Charter, and as understood in customary law on the use of force".

[83] Ibid.

[84] Ibid.

[85] D. Momtaz, "Did the Court miss an opportunity to denounce the erosion of the principle prohibiting the use of force," *Yale Journal of International Law* 29, no. 2, (2004): 307-313.

[86] Th. Graham, "National self-defense, International Law, and weapons of mass destruction," *Chicago Journal of International Law* 4, (2003):1-17.

[87] S. Bellier, "Unilateral and multilateral preventives self-defense," *Maine Law Review* 58, no. 2, (2006): 508- 542.

an attack but perceives that an act will occur in the imminent future. In fact, anticipatory self-defence is the right in the classic term of the use of force under customary International Law against an imminent threat. Under general International Law, anticipatory self-defence is inferred from Caroline case in 1937 which was later affirmed in the Nuremberg Tribunal in1946[88].

International Law accepts that States do not need to suffer an armed attack to take lawful action to defend themselves against imminent danger of attack. In this field, legal scholars often conditioned the legitimacy of the response to an imminent threat to the visible mobilization of armies, navies, and air forces preparing to attack, such as threat was done by Iraq in the border of Kuwait in 1990. It seems international community generally admitted that the right of self-defence can be exercised against an imminent armed attack. However, the pre-emptive self-defence is only supported by a minority.

1.6 THE RIGHT OF SELF-DEFENCE A POSTERIORI

After the events of terrorist attacks in September 2001, the US permanent representative in the UN made a declaration of intentions where it implicitly expresses that the US reserves the right to exercise the self-defence a posterior. A posteriori self-defence would not fulfil the requirement of necessity. It provided that without respecting the necessary, temporal connection between attack and response, what would the need be for a victim State to protect itself?[89]

In this context, it raises the question of what kind of reaction against the attacks of 9/11 would have it been according to International law. The answer seems to lie in the UNSC enforcement actions pursuant to Chapter VII of the UN Charter. If the US had reached unanimity to adopt UNSC Resolutions 1368 and 1373, among others,

[88] Mary Ellen O'Connell, "Cyber Security without Cyber War." *Journal of Conflict and Security Law* (New York: Oxford University Press 17, 2012): 51-54.

[89] Ibid.

then it would have obtained the due authorization to activate article 42, but according to its interests the US preferred to despise the UNSC and act unilaterally. That is, to provoke a loss of authority and credibility of the UN in its primary function of maintaining international peace and security[90].

In addition, where is the requirement of proportionality in the purposes? As Vacas points out that, the objective of employing force in self-defense must solely be to counteract the armed attack that necessitated such action. Once this objective has been accomplished and the threat neutralized, the use of force must cease; otherwise, it would no longer constitute self-defense but rather a new armed attack, signifying the initiation of a fresh episode of the use of force.[91] Several resolutions of the UNSC have indicated the illegality of various armed actions. There it was alleged that the exercise of self-defence once after an armed attack had occurred, did not comply with the requirement of immediacy[92].

1.7 CONCLUSION

In conclusion, the right to self-defense is a fundamental principle of international law that is inherent in the right of every state to defesnd itself against an armed attack. The UN Charter provides for the collective security system, which governs the exercise of the right to self-defense, requiring that it be provisional and subsidiary to the UNSC, which has the primary responsibility to maintain international peace and security. The exercise of the right of self-defense requires that the use of force be necessary and proportionate to the armed attack faced. This necessity requirement applies to both inter-state and non-state actors, while the

[90] Ibid.
[91] Ibid.
[92] UN General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, (24 June 2013), UN Doc A/68/98.

proportionality requirement is more complex and is often the subject of debate.

States have a duty to report to the UNSC immediately after taking measures in the exercise of self-defense. While failure to report to the UNSC does not necessarily invalidate the exercise of the right of self-defense, it is a procedural duty of states under Article 51 of the UN Charter. The UNSC plays a crucial role in the collective security system and may take collective measures to maintain international peace and security, including authorizing the use of force. The exercise of the right of self-defense is a complex issue in international law. However, it is important to adhere to the principles of necessity and proportionality, while working within the framework of the collective security system established by the UN Charter. By doing so, the international community can work towards maintaining international peace and security while respecting the inherent right of states to defend themselves.

CHAPTER NO 2

CYBER-ATTACKS AND THEIR IMPLICATIONS FOR SELF-DEFENSE

2.1 INTRODUCTION

This chapter focuses on the implications of cyber-attacks in the context of self-defense. The increasing reliance on the internet and information technology has brought about new forms of threats, including cyber-attacks[93]. The world has witnessed a rise in cyber-attacks in recent years, which has brought significant economic and social losses to individuals, businesses, and governments.

Cyber-attacks have become a major threat to national security and international stability. The use of computers and the internet has revolutionized the way people communicate, do business, and conduct warfare. However, this technological advancement has also led to an increase in cyber-attacks, which can cause significant damage to critical infrastructure and disrupt daily activities. As cyber-attacks become more sophisticated and prevalent, the question of how to respond to them arises[94]. The traditional notions of armed attacks and self-defense are no longer sufficient in the context of cyber operations. States must now consider the implications of cyber-attacks on their security and the international community as a whole[95].

This chapter aims to explore the legal framework governing the use of force in cyberspace and how it relates to the right of self-defense. It will examine the challenges and limitations of applying traditional concepts of international law to cyber operations. Furthermore, it will discuss the importance of establishing clear

[93] M. C.Waxman, "Self-defensive force against cyber-attacks: legal, strategic and political dimensions", *International Law Studies* 89, (2013): 109-122.

[94] Y. Dinstein, "Computer network attacks and self-defense," in Schmitt, M. N.; O'DonnelL, B. T. (eds.), *Computer network attack and International Law*, Naval War College 76, (2002): 99-119.

[95] H. B. Robertson, "Self-defense against computer network attack under International Law," in *Computer network attack and International Law*, ed. M. N Schmitt, B. T. O'Donnell, (Newport: Naval War College Newport press, 2002): 121-145.

rules of engagement and the need for international cooperation in addressing cyber threats. Overall, this chapter will provide insights into the complexities of cyber operations and their implications for self-defense. It highlights the importance of understanding the legal framework governing cyber operations and the need for states to adopt effective measures to protect themselves and the international community from cyber threats.

2.2 DEFINITION OF CYBER-ATTACK

Cyber-attack, which falls within the broader category of cyber operation, has been broadly defined as "the use of deliberate actions, perhaps over an extended period of time to alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks or the information and/or programs resident in or transiting these systems or networks[96].

According to Tallinn Manual "A cyber-attack 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"[97]. This definition equally applies in international and non- international armed conflict. In addition, non-violent operations, such as psychological cyber operation or cyber espionage, do not qualify as attack. There are no consistent terminology or widely accepted definitions"[98]. In this sense, the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) affirms that;

> There are no common definitions for cyber terms - they are understood to mean different things by different nations/organizations, despite prevalence in mainstream media and in national and international

[96] L. R. Blank, "International Law and cyber threats from non-State Actors," *International Law Studies* 89, (2013): 406-437.
[97] Ibid., 92.
[98] Ibid.

> organizational statements. Given this ambiguity and regardless of caveats, the glossary aims to provide a picture on how nations/States and different institutions, interpret and approach to "cyber". The majority of definitions provided, are from The Tallinn Manual and strategic or policy documents such as National Strategies, therefore the information contained in this glossary does not represent a nation's position in a legal context[99].

In accordance with the feature of this approach, cyber-attacks are limited to hostile acts that are intended to harm critical cyber system. Thus, this definition restricts cyber-attacks based on the objective of the attack. In this sense, some scholars prefer a narrower definition of cyber-attack and affirm that "a cyber-attack consists of any action taken to undermine the functions of a computer network for a political or national security purpose"[100]. For instance, using a computer network to operate a predator drone for kinetic attack is not a cyber-attack but a technologically advanced conventional warfare. On the contrary, using a regular explosive to cut the undersea network cables which carries the information packets between continents is a cyber-attack[101].

2.3 CYBER OPERATIONS

Cyber operations, contrary to conventional weapons, have unique and incomparable characteristics. We can identify four features to describe cyber operations that differ from conventional attacks in the field of the use of force: indirectness, intangibility, locus factor and result[102].

[99] NATO, CCDCOE, *Cyber definitions*, https://ccdcoe.org/cyber-definitions.html, 8/01/2023.
[100] Ibid.
[101] Antolin-Jenkins, V. M., "Defining the parameters of cyber war operations: looking for law in all the wrong places", *Naval Law Review* 51, (2005):132-40,
[102] H. H. Dinniss, "Cyber warfare and the laws of war," *Journal of Learning and Teaching in Digital Age* 2, no. 2, (2017): 46-53.

2.3.1 The Indirectness

The first feature of cyber-attacks is their indirectness. Unlike conventional attacks that involve the use of physical force and weapons, cyber-attacks rely on the exploitation of vulnerabilities in computer systems, networks, and software. Cyber-attacks can be conducted remotely, making it difficult to trace the source of the attack[103]. The attacker can use a range of techniques, such as malware, phishing emails, and social engineering, to gain unauthorized access to computer systems and networks.

The indirect nature of cyber-attacks makes them difficult to detect, as the attacker can often remain hidden for long periods of time, gathering sensitive information and causing damage without being detected. The anonymity and deniability that cyber-attacks provide can be attractive to state and non-state actors seeking to engage in malicious activities without fear of retaliation or accountability[104]. The indirectness of cyber-attacks also makes it difficult to respond to them with traditional military means. In some cases, it may not be clear who is responsible for the attack, and attribution can be a challenge. This can make it difficult for states to determine an appropriate response to a cyber-attack and can complicate the application of the law of armed conflict to cyber operations[105].

An example of the indirectness of cyber-attacks is the Stuxnet worm, which was discovered in 2010 and targeted Iran's nuclear program. The attack was indirect because the worm was not designed to cause direct physical damage to the targeted facility. Instead, it was designed to disrupt the operation of specific equipment used in

[103] T. Ruys, S. Verhoeven, "Attacks by private actors and the right of self-defence," *Journal of Conflict and Security Law* 10, no. 3, (2005):289-320

[104] Ibid.

[105] R. N. Ochoa, E. Salamanca-Aguad, "Exploring the limits of International Law relating to the use of force in self-defense", *EJIL* 16, no. 3, (2005): 499-524.

the uranium enrichment process[106]. This disruption would cause the equipment to malfunction, leading to a decrease in the efficiency of the enrichment process. The indirect nature of the attack was necessary to avoid detection and prevent a direct military response from Iran. The Stuxnet worm was able to spread throughout the facility's computer network and infect the targeted equipment without being detected for a significant amount of time. This allowed the attack to achieve its objectives before it was discovered and removed[107].

2.3.2 The Intangibility

The second feature of cyber-attacks is intangibility. The intangibility refers to a feature which neither the target of the attack nor the weapon used might exist in the real world. Its damages might be unphysical as well; for example, a cyber-attack on a stock exchange. Even those attacks that have physical consequences targeting the computer data, such as the *Stuxnet* attack to Iranian atomic facilities in 2009, can be an appropriate example in this field that of attacks which modified the spinning frequencies of the centrifuges and, as a result led to physical damage to them[108].

The intangibility of cyber-attacks also makes it difficult to respond with conventional military force. A physical attack may require a military response, but a cyber-attack may not warrant a similar response, particularly if the damage is not immediate or visible. The intangibility of cyber-attacks creates unique challenges for both attribution and response. It requires a new approach to understanding the nature of the damage caused by cyber-attacks and the appropriate measures to respond to them.

---

[106] D. Momtaz, "Did the Court miss an opportunity to denounce the erosion of the principle prohibiting the use of force," *Yale Journal of International Law* 29, no. 2, (2004): 307-313.

[107] S. Bellier, "Unilateral and multilateral preventives self-defense," *Maine Law Review* 58, no. 2, (2006): 508- 542.

[108] S. Chien, Stuxnet: a breakthrough, Symantec Blog, 2010, available at https://www.symantec.com/connect/blogs/stuxnet-breakthrough. Last accessed 2/01/2023.

2.3.3 The Locus

The locus factor is related to the fact that, in some cyber operations, it may be difficult to find out of the origin of the attacks[109], because such attacks may be routed from several pointsin different countries in order to hide the true source; for instance, during the cyber-attack to Estonia in 2007, the malicious traffic was originated from 178 countries[110]. Hence, in the field of cyber-operations, anonymity is one of the most important characteristics[111]. In this regard, it seems that the identification and attribution of attacks provide a serious evidentiary problem. Moreover, a cyber-attack can be launched without any warning[112].

2.4 TYPES OF CYBER-ATTACKS

There are several types of cyber-attacks that can be carried out by hackers and cybercriminals. Here are some of the most common types:

2.4.1 Malware

Malware is a type of software designed to harm a computer system or steal sensitive data. It includes viruses, trojans, worms, and ransomware.

2.4.2 Phishing

Phishing is a type of social engineering attack that aims to trick victims into revealing sensitive information such as passwords, usernames, or credit card details. This is usually done via email or a fake website that looks like a legitimate one.

---

[109] M. N. Schmitt, "Cyber operations and the jus ad bellum revisited," *Villanova Law Review* 56, (2011): 569-605.

[110] E. Tikk, "International cyber incidents: legal considerations," *NATO CCDCE* 112, (2010): 23. Available at https://ccdcoe.org/publications/books/legalconsiderations.pdf, last accessed 1/01/2023.

[111] S. W. Brenner, "At light speed': attribution and response to cybercrime/terrorism/ warfare," *Journal of Criminal Law and Criminology* 97, (2007): 379-475.

[112] Ibid.

2.4.3 Denial-of-Srvice (DoS) Attacks

DoS attacks aim to disrupt the availability of a website or service by flooding it with traffic, making it impossible for legitimate users to access it.

2.4.4 Man-in-the-Middle (MitM) Attacks

In MitM attacks, a hacker intercepts communication between two parties and can steal sensitive information or even alter it[113].

2.4.5 SQL Injection Attacks

This type of attack targets databases that use Structured Query Language (SQL) and allows the attacker to access or manipulate sensitive data[114].

2.4.6 Cross-Site Scripting (XSS) Attacks

XSS attacks inject malicious code into legitimate websites, allowing the attacker to steal user data or take control of their accounts[115].

2.4.7 Advanced Persistent Threats (APTs)

APTs are long-term attacks that target specific individuals or organizations, with the aim of stealing sensitive data or intellectual property.

2.4.8 Zero-Day Attacks

Zero-day attacks exploit vulnerabilities in software or hardware that are unknown to the vendor or the public, allowing the attacker to gain unauthorized access to a system. It's important that cyber-attacks are constantly evolving, and new types of attacks are discovered regularly. Therefore, it's crucial to keep your systems and

[113] Nicholas Tsagourias, "Necessity and the Use of Force: A Special Regime," Netherlands Yearbook of International Law 3, (2010): 12-20.
[114] Ibid.
[115] Ibid.

software up-to-date and to stay informed about the latest security threats[116].

2.5 CLASSIFICATIONS OF CYBER OPERATIONS

The different classifications of cyber operations have been known by the US documents. According to the US National Military Strategy for Cyberspace Operations, computer networkoperation (CNO) includes:

2.5.1 Computer Network Attacks (CNA)

Computer Network Attacks (CNA), which are explained as "operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves"[117]. A more accurately definition of CNA is "actions taken through the use of computer networks to disrupt, deny, degrade, manipulate, or destroy information resident in the target information system or computer networks, or the systems/networks themselves"[118]. Hence, the concept of CNA is narrower than cyber-attack, which can operate not only through computer networks, but also through close access to systems with evil intentions[119]; for example, attacks on computer systems which are intended to degrade or destroy the infrastructure capability.

2.5.2 Computer Network Defence (CND)

Computer Network Defence is defined as "actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within DOD information systems and computer networks"[120]. In this sense, CND employs information assurance,

---

[116] Ibid.

[117] US "The National Military Strategy for Cyberspace Operations*,"* 2006. Available at file:///C:/Users/hamed/Downloads/AAP-06%202017%20(1).pdf/ Last accessed 2/01/2023.

[118] US, *"Joint Terminology for Cyberspace Operation,"* 2010. available at http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf, Last accessed 01/01/2023[.

[119] Ibid.

[120] Ibid., 45.

capabilities, intelligence, counterintelligence, and law enforcement, military capabilities, which include both active cyber defences and passive cyber defences[121].

2.5.3 Computer Network Exploitation (CNE)

Computer Network Exploitation are conceptualized as "enabling operations and intelligence collection to gather data from target or adversary automated information systems or networks"[122], which must occur through the use of computer networks. Also, more ambiguously, NATO defines CNE as action taken to make use of a computer or computer network, as well as the information hosted therein, in order to gain advantage[123]. NATO's *Glossary of Terms in Definitions* only distinguishes between CNA and CNA and does not include CND.

2.6 NATURE OF CYBER-ATTACKS AND ATTRIBUTION CHALLENGES

The rapid development of information and communication technologies (ICT) has brought about various benefits to society, such as increased efficiency and convenience in various aspects of life. However, it has also brought new challenges in the field of international security. One of these challenges is the nature of cyber-attacks and the difficulties in attributing them to a specific state or non-state actor.

Cyber-attacks can be defined as any intentional and unauthorized attempt to access, manipulate, or destroy information or computer systems through electronic means. These attacks can target various sectors, such as government agencies, military institutions, financial institutions, critical infrastructure, and private businesses.

[121] Ibid.
[122] David Sanger, "Obama Order Sped Up Wave of Cyber-attacks Against Iran," *New York Times*, Apr. 9. 2012, https://www.nytimes.com/9/4/2022.
[123] Ibid.

Cyber-attacks can take various forms, such as malware, phishing, denial-of-service attacks, and hacking.

One of the unique features of cyber-attacks is their ability to hide the identity of the attacker. Unlike traditional forms of attacks, such as military strikes or terrorist attacks, cyber-attacks can be launched from anywhere in the world and can be routed through multiple countries to hide the true origin. This makes it difficult to attribute the attack to a specific state or non-state actor[124]. Attribution challenges in cyber-attacks arise from several factors. First, the anonymity of the internet and the use of encryption and other obfuscation techniques make it difficult to identify the origin of an attack. Second, cyber-attacks can be launched from compromised third-party systems, such as botnets, which further obscure the origin of the attack. Third, attackers can use false flags, such as using the language or tools of another state or non-state actor, to mislead investigators[125].

The difficulties in attributing cyber-attacks to a specific state or non-state actor have significant implications for the exercise of the right of self-defense under international law. The inability to identify the attacker may prevent a state from responding to a cyber-attack, leading to a perception of impunity for the attacker and potentially increasing the risk of further attacks. Therefore, the development of effective attribution techniques and the establishment of norms and rules for the attribution of cyber-attacks are critical for international security[126].

[124] J. F. Murphy, "Cyber war and International Law: does the International Law process constitute a threat to U.S vital interests?," *International Law Studies* 89, no. 1, (2013): 309-340

[125] N. Decoulare-Delafontaine, "Cyber-attacks on nuclear facilities and nuclear responses to cyber-attacks in International Law," 2015. available at http://lcnp.org/pubs/studentpapers/2016/Cyber%20Attacks%20-%20Nina.pdf, Last accessed 12/12/2022.

[126] Ibid.

2.7 LEGAL CHALLENGES POSED BY CYBER-ATTACKS TO THE TRADITIONAL CONCEPT OF SELF-DEFENSE

The first legal challenge posed by cyber-attacks is the difficulty of attributing responsibility for the attack. Unlike physical attacks, which leave visible traces and can be more easily traced to a specific state actor, cyber-attacks can be carried out by non-state actors, using anonymous or disguised methods[127]. This makes it difficult to identify the perpetrator of the attack and respond appropriately in a manner consistent with international law. Attribution of cyber-attacks requires sophisticated technical analysis and intelligence gathering, which can be time-consuming and may not always yield definitive results. This makes it challenging for states to determine who is responsible for a cyber-attack and to hold them accountable under international law[128].

The second legal challenge posed by cyber-attacks is the potential for unintended consequences. If a state responds to a cyber-attack with military force, it could escalate the situation and lead to a broader conflict, potentially violating international law. Cyber-attacks often target non-military targets such as critical infrastructure, financial systems, and private companies. This raises questions about whether such attacks constitute an armed attack under international law and whether a state has the right to use force in response to such attacks[129].

The third legal challenge posed by cyber-attacks is the lack of clarity in international law on how the principles of necessity, proportionality, and immediacy apply in the

[127] E. Tikk, "International cyber incidents: legal considerations," *NATO CCDCE* 112, (2010): 23. Available at https://ccdcoe.org/publications/books/legalconsiderations.pdf, last accessed 1/01/2023.

[127] S. W. Brenner, "At light speed': attribution and response to cybercrime/terrorism/ warfare," *Journal of Criminal Law and Criminology* 97, (2007): 379-475.

[128] Ibid.

[129] Ibid., 477.

context of cyber-attacks. The use of force in self-defense must be necessary, proportional, and immediate to the attack, but it is not clear how these principles apply in the context of cyber-attacks. For example, if a state is the victim of a cyber-attack that causes significant economic damage, it may be tempted to respond with military force, even though the attack may not rise to the level of an armed attack under international law. This raises questions about whether the use of force in response to a cyber-attack is necessary and proportional, and whether it is consistent with international law[130].

The legal challenges posed by cyber-attacks to the traditional concept of self-defense in international law require a rethinking of the traditional framework for self-defense. This includes developing new rules and norms that address the unique characteristics of cyber-attacks and providing clarity on the legal principles that apply in the context of cyber-attacks[131].

2.8 CYBER OPERATIONS AS VIOLATION OF THE PRINCIPLE OF THE PROHIBITION OF THE THREAT ORUSE OF FORCE

Cyber operations can potentially violate the principle of the prohibition of the threat or use of force, as outlined in international law. This principle, often associated with the United Nations Charter, prohibits states from using or threatening to use force against each other. Cyber operations involve the use of digital technologies to infiltrate, disrupt, or damage computer systems, networks, or data. While cyber operations generally lack the physicality associated with traditional military force,

[130] M. N. Schmitt, "Cyber operations and the jus ad bellum revisited" *Villanova Law Review* 56, (2011): 569-605.
[131] Ibid., 608

they can still have significant disruptive effects on a nation's infrastructure, economy, or security[132].

In the context of the prohibition of the threat or use of force, cyber operations that cause substantial harm, destruction, or disruption to another state's critical systems or infrastructure could be considered as acts of force. Such operations may include cyber-attacks targeting military installations, government networks, or essential services like power grids or financial systems. However, it is important to note that there is ongoing debate and legal ambiguity regarding the precise application of the principle of the prohibition of the threat or use of force in cyberspace. The lack of a universally accepted definition and the difficulty in attributing cyber operations to specific actors make it challenging to establish clear boundaries for what constitutes a violation. States and the international community are actively engaged in discussions to clarify and develop norms, rules, and frameworks for responsible behavior in cyberspace. Efforts are underway to establish guidelines regarding the use of cyber operations and to determine the threshold at which they may be considered as a violation of the principle of the prohibition of the threat or use of force[133].

2.9 CYBER OPERATIONS AS USE OF FORCE

Cyber operations can be considered as a form of the use of force under certain circumstances. The concept of the use of force is a fundamental principle in international law, primarily governed by the United Nations Charter. Traditionally, the use of force refers to actions that involve physical violence or coercion, such as military operations or armed attacks. However, in the context of cyberspace, the use

[132] Ibid.

[133] V. M. Antolin-Jenkins, "Defining the parameters of cyber war operations: looking for law in all the wrong places," *Naval Law Review* 51, (2005): 132-140.

of force has been expanded to include certain types of cyber operations that result in significant harm or damage[134].

When cyber operations cause effects comparable to those produced by traditional kinetic force, they can be considered as a use of force. For example, if a cyber-operation results in physical damage, loss of life, or significant disruption to a state's infrastructure or essential services, it may be deemed as a use of force. Determining whether a specific cyber operation constitutes a use of force involves assessing factors such as the scale, intensity, and consequences of the operation. The effects must be substantial enough to be considered a coercive act that infringes upon the territorial integrity or political independence of a state[135].

However, it is important to note that there is ongoing debate and interpretation regarding the threshold at which a cyber-operation qualifies as a use of force. The inherently intangible and non-physical nature of cyberspace presents challenges in applying traditional definitions of force to this domain. Efforts are underway within the international community to develop norms, rules, and frameworks to address the use of force in cyberspace. These discussions aim to establish clearer guidelines and consensus on when cyber operations can be considered as a use of force and how to respond to such actions in a manner consistent with international law[136].

2.10 CYBER OPERATION AS THREAT OF FORCE

Cyber operations can be seen as a threat of force in certain situations. The principle of the prohibition of the threat of force, also known as the threat of the use of force, is a key component of international law, particularly outlined in the United Nations

[134] H. KURU, "Prohibition of use of force and cyber operations as force," *Journal of Learning and Teaching in Digital Age* 2, no. 2, (2017): 46-53.

[135] Chien, Stuxnet: a breakthrough, Symantec Blog, 2010, available at https://www.symantec.com/connect/blogs/stuxnet-breakthrough. Last accessed 2/01/2023.

[136] Ibid.

Charter. While cyber operations themselves may not involve physical violence, they can still have significant coercive effects and can be employed as a means of signaling an intention to use force. The use of cyber capabilities to infiltrate, disrupt, or damage computer systems, networks, or data can serve as a demonstration of power and a warning of potential future aggression[137].

When cyber operations are conducted with the explicit or implicit purpose of intimidating or coercing another state, they can be regarded as a threat of force. Such operations may include activities like reconnaissance, probing, or displaying capabilities that could be used to inflict harm or disruption. Determining whether a specific cyber operation constitutes a threat of force requires an evaluation of factors such as the nature, scale, and intent of the operation. The perceived capability and credibility of the threat, as well as the context in which it occurs, also play a role in assessing its significance[138]. It is important to note that the assessment of whether a cyber-operation constitutes a threat of force can be subjective and context-dependent. There are ongoing discussions within the international community to establish clearer norms, rules, and frameworks regarding the use of cyber operations as a threat of force and to define appropriate responses in accordance with international law[139].

2.11 CYBER OPERATIONS AS AN ARMED ATTACK IN THE CONTEXT OF THE RIGHT OF SELF-DEFENCE

In the context of the right of self-defense, cyber operations can be considered as an armed attack under certain circumstances. The right of self-defense is a fundamental

[137] J. Richmond, "Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict," *Fordham International Law Journal* 35, (2011): 11-20.

[138] Ibid.

[139] L. R. Blank, "International Law and cyber threats from non-State actors," *International Law Studies* 89, (2013):406-437.

,

principle of international law, enshrined in Article 51 of the United Nations Charter. It allows states to use force in response to an armed attack against them.

Traditionally, an armed attack has been understood as a physical act of violence or coercion involving the use of weapons, such as military operations or acts of aggression[140]. However, with the increasing significance of cyberspace, the concept of armed attack has expanded to include cyber operations that meet certain criteria. To be considered an armed attack, a cyber-operation must fulfill certain requirements. These include:

2.11.1 Severity

The cyber operation must result in significant consequences, causing extensive destruction, loss of life, or grave damage to a state's essential infrastructure or vital interests[141]. The effects should be comparable to those caused by traditional kinetic attacks.

2.11.2 Attribution

It must be possible to attribute the cyber operation to another state or non-state actor. Establishing clear attribution is crucial in determining who is responsible for the attack and justifying a response.

2.11.3 Intent

The cyber operation must be intentional, meaning it is conducted with the purpose of causing harm or coercion. Accidental or unintentional cyber incidents, while disruptive, may not necessarily constitute an armed attack.

[140] Y. Dinstein, Computer network attacks and self-defense, 76.

[141] M. C. Waxman, "Self-defensive force against cyber-attacks: legal, strategic and political dimensions," *International Law Studies* 89, (2013): 109-122.

When these conditions are met, a state may invoke the right of self-defense to respond to a cyber-operation as it would to a conventional armed attack. However, it is important to note that self-defense measures must be necessary and proportionate, taking into account the principles of necessity and proportionality in international law[142]. The determination of whether a specific cyber operation qualifies as an armed attack and triggers the right of self-defense can be complex. The inherently intangible and transnational nature of cyberspace poses challenges in attribution and assessing the severity of effects. As a result, there is ongoing discussion and debate among states and international legal scholars to establish clearer guidelines and criteria for applying the right of self-defense in cyberspace[143].

2.11.4 Infrastructures and those damages that can be object of cyber-attacks

Infrastructure refers to the fundamental systems and facilities necessary for the functioning of a society, economy, or organization. These infrastructures can be targeted in cyber-attacks, which can cause significant damage and disruption. Here are some examples of infrastructures that can be objects of cyber-attacks:

2.11.5 Critical Infrastructure

This includes sectors such as energy, transportation, water supply, telecommunications, financial systems, and healthcare. Cyber-attacks targeting these sectors can have far-reaching consequences, such as power outages, transportation disruptions, financial instability, compromised healthcare services, or compromised communication networks.

[142] Ibid.

[143] Momtaz, "Did the Court miss an opportunity to denounce the erosion of the principle prohibiting the use of force," *Yale Journal of International Law* 29, no. 2 (2004): 307-313.

2.12 INDUSTRIAL CONTROL SYSTEMS (ICS) AND SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) SYSTEMS

These systems are used to monitor and control industrial processes in sectors like manufacturing, utilities, and transportation. Cyber-attacks against these systems can disrupt operations, manipulate controls, or cause physical damage to industrial equipment, potentially leading to industrial accidents or environmental disasters.

2.12.1 Government Networks

Governments rely on secure information and communication technology infrastructure to carry out essential functions and provide public services. Cyber-attacks against government networks can compromise sensitive information, disrupt operations, or even undermine national security.

2.12.2 Defense Systems

Military infrastructure, including command and control systems, weapons systems, and communication networks, can be targeted in cyber-attacks. Such attacks can compromise operational readiness, disrupt military capabilities, or lead to unauthorized access to classified information.

2.12.3 Financial Systems

Cyber-attacks against financial institutions, banking systems, or payment networks can disrupt financial transactions, compromise customer data, or facilitate fraudulent activities, causing significant economic damage and loss.

2.12.4 Healthcare Systems

Cyber-attacks targeting healthcare systems can disrupt patient care, compromise medical records, or even disrupt critical medical devices, potentially endangering lives.

2.12.5 Internet Infrastructure

The core infrastructure of the internet, including internet service providers (ISPs), domain name systems (DNS), and routing infrastructure, can be targeted. Attacks on these systems can result in widespread internet outages, disruption of online services, or manipulation of internet traffic.

The damages caused by cyber-attacks on these infrastructures can range from financial losses, operational disruptions, compromised data and privacy, physical harm to individuals, and societal and economic instability. Protecting and securing these infrastructures against cyber threats is crucial for ensuring the resilience and safety of modern societies.

2.13 CONCLUSION

In conclusion, cyber-attacks pose significant challenges to the traditional concept of self-defense in international law. The unique nature of cyber warfare, which often involves attacks that are difficult to attribute and may not result in physical harm, has led to a range of legal and policy debates surrounding the appropriate response to such attacks. The UN Charter's framework for the use of force in self-defense has been challenged by the emergence of cyber-attacks as a new form of aggression. While some states have sought to expand the definition of armed attack to include cyber-attacks, others have argued for a more cautious approach, emphasizing the need for greater international cooperation and the development of new legal frameworks to address the unique characteristics of cyber warfare.

Cyber operations can be considered as a violation of the principle of the prohibition of the threat or use of force when they cause significant harm or disruption to a state's critical systems or infrastructure, signaling an intention to use force or coercion. Cyber Operations as Use of Force: Cyber operations can be regarded as a use of force

when they result in effects comparable to traditional kinetic force, such as physical damage, loss of life, or significant disruption to a state's infrastructure or essential services. Cyber Operation as Threat of Force: Cyber operations can be seen as a threat of force when they are conducted with the explicit or implicit purpose of intimidating or coercing another state, demonstrating the capability and intent to cause harm or disruption.

Cyber operations can be considered as an armed attack, triggering the right of self-defense, when they meet certain criteria, including severity of consequences, attribution to another state or non-state actor, and intent to cause significant harm or coercion. Infrastructures and Damages Object of Cyber-attacks: Various infrastructures, such as critical infrastructure (energy, transportation, water supply, etc.), government networks, financial systems, and healthcare systems, can be targeted in cyber-attacks.

The damages caused can include financial losses, operational disruptions, compromised data and privacy, physical harm, and societal and economic instability. These systems are used to monitor and control industrial processes. Cyber-attacks against ICS and SCADA systems can disrupt operations, manipulate controls, or cause physical damage, potentially leading to industrial accidents or environmental disasters. Applicability of the UN Charter in the Cyber Context: The UN Charter's principles, such as state sovereignty, non-intervention, prohibition of the use of force, the right to self-defense, and state responsibility, apply in the cyber context. However, challenges exist in interpreting and applying these principles due to the unique characteristics of cyberspace, such as attribution difficulties and the intangible nature of cyber operations. Ongoing efforts are underway to clarify the application of the UN Charter and develop norms and rules specific to cyberspace.

Overall, the implications of cyber-attacks for self-defense in international law are complex and multifaceted. As such, it is important for policymakers, legal experts, and other stakeholders to continue to engage in a constructive dialogue on these issues in order to develop effective and responsible strategies for responding to cyber-attacks and maintaining international security in the digital age.

CHAPTER 3

THE SELF-DEFENSE IN THE CONTEXT OF CYBER-ATTACKS

3.1 INTRODUCTION

The use of force in self-defense is a well-established principle of international law, enshrined in the United Nations Charter and customary international law. However, the emergence of cyber warfare as a new form of aggression has challenged the traditional concept of self-defense and raised a range of legal and policy questions surrounding the appropriate response to cyber-attacks.

This chapter presents a critically examines the legal challenges posed by cyber-attacks to the traditional concept of self-defense, including issues related to attribution, proportionality, and necessity. Furthermore, it also analyses state practices and responses to cyber-attacks as acts of aggression or armed attacks, highlighting the different approaches taken by states depending on the circumstances of the attack and their own national interests. It also examines the implications of cyber-attacks for international security, including the potential for cyber-attacks to undermine the stability of states and the international system as a whole. This chapter seeks to provide a comprehensive and critical analysis of the various cyber-attacks, highlighting the legal and policy challenges posed by this emerging threat and exploring potential solutions for addressing these challenges.

3.2 EXAMINATION OF RELEVANT CASES AND STATE PRACTICES

Cyber-attacks have become increasingly prevalent in recent years, targeting various sectors and entities around the world. While I can provide an overview of some relevant cases of cyber-attacks, it's important to worth mention that state practices in

response to cyber-attacks can vary depending on the country and its policies. There are some cyber-Attacks cases which is explain as under:

3.2.1 Stuxnet Case

The Stuxnet case is one of the most notable cyber-attacks in history. It was a sophisticated malware that targeted industrial control systems, specifically those used in Iran's nuclear program[144]. Stuxnet was discovered in 2010 and had a significant impact on the cyber warfare landscape[145]. Stuxnet was first identified by security researchers in June 2010. It quickly gained attention due to its unprecedented complexity and advanced capabilities. The malware targeted Windows computers and sought to exploit zero-day vulnerabilities, which are unknown and unpatched security flaws.

Stuxnet was designed to target Supervisory Control and Data Acquisition (SCADA) systems used in critical infrastructure, particularly the Natanz nuclear[146] facility in Iran. Its main objective was to damage the uranium improvement process by manipulating industrial control systems. Stuxnet employed multiple propagation methods, including USB drives and network vulnerabilities, to spread within the targeted network and beyond. It used both worm-like features to infect other computers and rootkit techniques to remain hidden and avoid detection. Stuxnet was incredibly sophisticated, incorporating several zero-day exploits and employing multiple layers of encryption and complication[147]. It also employed stolen digital

[144] David Kushner, "The Real Story of Stuxnet," *IEEE Spectrum* 50, no. 3 (2013): 48–53.

[145] In the cyber warfare landscape, different state and non-state actors may be engaged in activities such as cyber espionage, cyberattacks, information warfare, and cyber sabotage. These actors can include nation-states, criminal organizations, hacktivists, and other groups with varying motivations and capabilities.

[146] The Natanz nuclear facility is a significant nuclear enrichment site located in Iran. It is one of the key facilities in Iran's nuclear program and is situated approximately 250 kilometers south of Tehran.

[147] Anne Hathaway Oona, Rebecca Crootof, Paul Levitz, H. Nowlan Alden, W. Perdue and J. Spiegel "The Law of Cyber Attack," *California Law Review* 100, (2012): 21-26.

certificates to appear legitimate and bypass security measures. These characteristics made it difficult to detect and analyze[148].

Stuxnet employed a combination of unique techniques that indicated a deep understanding of the targeted control systems. It focused on disrupting the centrifuges used for uranium enrichment by altering their operating parameters without raising suspicion. Stuxnet was successful in its mission, causing significant damage to Iran's nuclear program. It reportedly destroyed a large number of centrifuges, delaying Iran's nuclear ambitions. The attack demonstrated the potential for cyber weapons to cause physical destruction and disrupt critical infrastructure[149].

The true origin of Stuxnet remains officially undisclosed, it is widely believed to be a joint effort between the United States and Israel. The attack required substantial resources, expertise, and intelligence on the targeted systems, leading to speculation about state involvement. Stuxnet raised awareness about the vulnerabilities of industrial control systems and the potential consequences of cyber-attacks on critical infrastructure. It prompted organizations to invest in stronger cyber security measures and encouraged the development of more resilient systems[150]. The Stuxnet case stands as a landmark event, showcasing the use of advanced cyber weapons for sabotage purposes. It highlighted the potential risks associated with cyber warfare and the need for improved security in critical infrastructure sectors worldwide.

[148] Ellen Nakashima, "Stuxnet was work of U.S. and Israeli experts, officials say," *The Washington Post*, June 2, 2012, archived https://www.washingtonpost.com/sports/tv-and-radio-listings-june-2/2012/06/02/gJQAbheI8U_story.html. Last accessed September, 2022.

[149] Ronen Bergman and Mark Mazzetti, "The Secret History of the Push to Strike Iran," *The New York Times*, September 4, 2019, archived from https://www.nytimes.com/issue/todayspaper/2019/09/04/todays-new-york-times. Accessed March 23, 2023.

[150] Ibid.

3.2.2 Wannacry Case

Wannacry was a devastating ransomware[151] attack that occurred in May 2017. It quickly spread across the globe, infecting hundreds of thousands of computers and causing widespread disruption. WannaCry exploited a vulnerability in the Windows operating system known as EternalBlue, which was originally discovered and developed by the U.S. National Security Agency (NSA). The malware spread rapidly by scanning the internet for vulnerable systems and using the Eternal Blue exploit to gain unauthorized access and execute the ransom ware[152] payload. The WannaCry attack had a significant global impact, infecting organizations and individuals in over 150 countries[153]. It targeted a wide range of victims, including government institutions, healthcare organizations, businesses, and regular users. Some of the notable victims included the United Kingdom's National Health Service (NHS), Spanish Telecommunications Company Telefonica, and FedEx.

The rapid and widespread nature of the attack led to significant disruption of critical services. For example, the NHS experienced canceled appointments, delayed surgeries, and the temporary shutdown of computer systems. Numerous other organizations faced similar challenges, resulting in financial losses, reputational damage, and compromised data. Microsoft had released a security patch for the EternalBlue vulnerability prior to the WannaCry attack, but many organizations had not applied the update. The attack highlighted the importance of regular patching and prompt security updates to protect against known vulnerabilities. Subsequently,

[151] Ransomware is a category of malicious software (malware) designed to encrypt a victim's files or lock their computer system, effectively rendering it inaccessible until a ransom is paid. This cyber extortion tactic involves attackers demanding payment, often in cryptocurrency like Bitcoin, as a condition for restoring access to the encrypted files or unlocking the compromised system.

[152] After infiltrating a system, WannaCry proceeded to encrypt the files on the compromised computer, making them inaccessible. Subsequently, a ransom note appeared, demanding a payment in Bitcoin in return for the decryption key required to recover the files. The attackers issued a threat to permanently delete the files if the ransom was not paid within a specified timeframe.

[153] Nicholas Tsagourias, "Cyber-attacks, self-defense and the problem of attribution." *Journal of Conflict and Security Law* 10, (2012): 98-112.

Microsoft released emergency patches even for older, unsupported Windows versions to mitigate the impact[154].

WannaCry was attributed to the Lazarus Group, a hacking group believed to have ties to North Korea. While attribution in the cyber realm is challenging, evidence such as code similarities and infrastructure analysis led cybersecurity experts to associate the attack with this group. The WannaCry attack served as a wake-up call to the global community regarding the risks and consequences of ransomware attacks. It emphasized the importance of cyber security best practices, including regular software updates, robust backup systems, and employee awareness training to prevent and mitigate such incidents. The WannaCry attack underscored the potential scale and impact of ransomware attacks, prompting increased focus on cybersecurity and improved collaboration between governments, organizations, and security experts to prevent and respond to such threats[155].

3.2.3 Notpetya Case

The attack started with the compromise of the update mechanism of a popular Ukrainian accounting software called MeDoc. The attackers managed to insert malicious code into the software's updates, which were then distributed to users who downloaded and installed them[156]. Once a computer was infected with the malicious software update, the malware spread rapidly within the local network using various techniques, including the Eternal Blue exploit, which was originally developed by the

[154] Ibid., 4.

[155] Jakub Kroustek, "Avast reports on WanaCrypt0r 2.0 ransomware that infected NHS and Telefonica," *Avast Security News*, May 12, 2017, archived from https://www.avast.com/c-wannacry. Last accessed May 14, 2022.

[156] Mary Ellen O'Connell, "Dangerous Departures." *American Journal of International Law*, (2013): 34-37.

.

U.S. National Security Agency (NSA) and later leaked by a hacking group known as the Shadow Brokers[157].

NotPetya employed a combination of techniques from the Petya ransom ware and a disk-wiping malware called KillDisk. It encrypted the master file table of infected computers, rendering them inaccessible. The attackers demanded a ransom in Bit coin for the decryption key. The attack quickly spread beyond Ukraine, affecting numerous organizations worldwide. Companies in various sectors, including shipping, logistics, manufacturing, and energy, were hit hard. Notable victims included Maersk (the world's largest shipping company), Merck (a pharmaceutical company), and the Chernobyl nuclear power plant[158].

While the attack initially appeared to be a typical ransom ware campaign, it is widely believed to have been a deliberate act of disruption rather than a financially motivated attack. The main target seemed to be Ukraine, where the attack caused significant damage to the country's infrastructure. The NotPetya attack caused extensive financial losses, with estimates ranging from hundreds of millions to billions of dollars. Many affected organizations faced operational disruptions and incurred substantial recovery costs. It also highlighted the vulnerability of critical infrastructure to cyber threats and sparked discussions about cyber security measures and the responsibility of nation-states in cyber operations[159]. It's worth noting that the NotPetya attack was a significant wake-up call for governments, organizations, and the cyber security community, highlighting the need for improved security measures and better response strategies against sophisticated cyber threats.

---

[157] Anne Hathaway Oona, Rebecca Crootof, Paul Levitz, H. Nowlan Alden, W. Perdue and J. Spiegel "The Law of Cyber Attack," *California Law Review* 100, (2012): 21-26.

[158] I. Lachow, "Stuxnet Enigma: Implications for the Future of Cyber Security," *Georgetown Journal of International Affairs*11, (2010): 19-24.

[159] Olivia Solon and Alex Hern, "'Petya' ransomware attack: what is it and how can it be stopped?," *The Guardian*, June 28, 2017, archived from https://www.theguardian.com/theguardian/2017/jun/28. Last accessed June 29, 2022.

3.2.4 Solarwinds Case

The SolarWinds cyber-attack, also known as the SolarWinds supply chain attack, was a sophisticated cyber-attack that came to light in December 2020[160]. It involved the compromise of the software supply chain of SolarWinds, a prominent IT management software company based in the United States. The attack had significant implications for both government and private sector organizations. The attackers infiltrated SolarWinds' software development environment and injected a malicious code into a software update package called "Orion." Orion is widely used by organizations for network and IT infrastructure monitoring[161].

The compromised software update, which contained a backdoor named "Sunburst" or "Solorigate," was unknowingly distributed to SolarWinds' customers as a legitimate software update[162]. This allowed the attackers to gain unauthorized access to the networks of organizations using the compromised version of Orion. Once inside the targeted networks, the attackers conducted reconnaissance, moved laterally, and escalated privileges to gain access to sensitive systems and data. They carefully selected their targets and focused on high-value assets, including government agencies, technology companies, and other organizations of strategic importance[163].

The attackers demonstrated patience and sophistication, remaining undetected within compromised networks for an extended period, often several months. They employed various techniques to evade detection, including mimicking legitimate network traffic and encrypting their malicious communications. The cyber-attack has been widely

[160] Ibid.

[161] David E. Sanger, Nicole Perlroth, and Eric Schmitt, "Scope of Russian Hack Becomes Clear: Multiple U.S. Agencies Were Hit," *New York Times*, December 15, 2020, archived from https://www.nytimes.com/issue/todayspaper/2019/09/04/todays-new-york-times. Last accessed December 18, 2022.

[162] Ibid.

[163] Barry Harrell, "Fast-growing Austin software maker Solarwinds acquires Idaho company," *Austin American-Statesman*, July 5, 2011, archived from https://www.newspapers.com/newspage/435038741. Last accessed January 23, 2023.

attributed to a state-sponsored group believed to be affiliated with Russia, often referred to as APT29, Cozy Bear, or Nobelium. The motive behind the attack is believed to be espionage and intelligence gathering, rather than financial gain[164].

The SolarWinds attack had far-reaching consequences, affecting numerous organizations worldwide, including U.S. government agencies, defense contractors, critical infrastructure operators, and private sector companies. Notable victims included the U.S. Department of Defense, the Department of Homeland Security, and major technology companies. Once the attack was discovered, affected organizations took steps to mitigate the damage. This involved removing the compromised versions of Orion, patching vulnerabilities, conducting forensic investigations, and enhancing security measures to prevent similar incidents in the future[165]. The SolarWinds cyber-attack highlighted the vulnerability of software supply chains and the potential for sophisticated threat actors to exploit trusted software vendors to gain access to target networks. It has prompted increased scrutiny of supply chain security and emphasized the importance of robust cyber security practices, including supply chain risk management and continuous monitoring of network environments.

3.3 APPLICABILITY OF THE CRITERIA FOR SELF-DEFENSE TO CYBER-ATTACKS

An analysis of the applicability of the criteria for self-defense to cyber-attacks is a crucial component of the critical legal analysis of the scope of self-defense in the context of cyber-attacks. The criteria for the use of force in self-defense under

[164] Ibid.
[165] Ibid.

international law require that the use of force must be necessary, proportional, and immediate in response to an armed attack[166].

However, the application of these criteria to cyber-attacks is complex and raises several challenges. For example, it may be difficult to determine the identity of the attacker, the extent of the damage caused, and the intent behind the attack. These challenges can make it difficult to establish whether a cyber-attack constitutes an armed attack that triggers the right to self-defense. Moreover, the concept of proportionality in the context of cyber-attacks is complicated by the fact that cyber-attacks can have far-reaching and unpredictable consequences. For instance, a cyber-attack on critical infrastructure, such as a power grid or water treatment plant, can result in widespread disruption and even loss of life. In such cases, it may be difficult to determine what constitutes a proportionate response in self-defense[167].

The analysis of the applicability of the criteria for self-defense to cyber-attacks thus requires a careful consideration of the unique characteristics of cyber warfare and the challenges they pose for the traditional concepts of self-defense. It involves an examination of relevant cases and state practices, as well as a critical analysis of the existing legal framework and its applicability to cyber-attacks. By analyzing the applicability of the criteria for self-defense to cyber-attacks, the thesis can contribute to the development of a more coherent and effective legal and policy framework for addressing cyber-attacks in the context of self-defense. It can help identify gaps and

[166] The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations" by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). This manual provides a comprehensive analysis of how international law applies to cyber operations, including discussions on self-defense.

[167] International Law and the Use of Force in Cyberspace" by Michael N. Schmitt and Liis Vihul. This article explores the applicability of the law of armed conflict to cyber operations, including the criteria for self-defense.

limitations in the existing framework and propose solutions to address these challenges[168].

3.4 STATE PRACTICES AND RESPONSES TO CYBER-ATTACKS

The statement State practices and responses to cyber-attacks as acts of aggression or armed attacks have varied widely, with different states adopting different approaches depending on the circumstances of the attack and their own national interests reflects the fact that there is no uniform approach among states when it comes to responding to cyber-attacks. Some states have taken a very aggressive approach, treating cyber-attacks as the equivalent of traditional military attacks and responding with military force. For example, in 2007, Russia was accused of carrying out a cyber-attack on Estonia, which disrupted government and commercial websites for several weeks[169]. Estonia responded by activating its cyber defense unit and shutting down internet traffic from Russia[170]. Similarly, in 2010, the US and Israel were reported to have carried out a cyber-attack on Iran's nuclear program, using the Stuxnet worm to damage centrifuges. This attack was widely viewed as an act of aggression, but neither state acknowledged responsibility[171].

Other states have taken a more cautious approach, treating cyber-attacks as a form of espionage or crime rather than an act of aggression. For example, China has been accused of carrying out cyber-attacks on a range of targets, including US government agencies and private companies. However, China has generally denied involvement in these attacks and has not responded aggressively to accusations of cyber-attacks

[168] Michael N .Schmitt, "Cyber Operations and the Jus ad Bellum Revisited," *Villanova Law Review*, (2011): 37-38.

[169] Ibid.

[170] Ellen Nakashima, Michael Birnbaum & William Booth, "US and its allies target Russian cyber spies with indictments, public shaming," *Washington Post*, 4 October 2018. Retrieve http://nssarchive.us/wp-content/uploads/2015/02/2015.pdf. Last accessed march12, 2023.

[171] Lau Francis, Simson Garfinkel Rubin, Mark Smith and Ljiljana Trajkovic, "Distributed denial of service attacks in Systems, Man, and Cybernetics," *IEEE International Conference* 3, (2000): 18-19.

against it[172]. The variation in state responses to cyber-attacks reflects the complexity of the issue. Cyber-attacks can be carried out by a wide range of actors, including state-sponsored groups, criminal organizations, and individual hackers. The targets of cyber-attacks can also vary widely, ranging from government agencies and critical infrastructure to private companies and individuals. The motivations for cyber-attacks can also be diverse, including political, economic, and strategic objectives[173].

Given this complexity, it is not surprising that states have taken different approaches to responding to cyber-attacks. Some states may view cyber-attacks as a serious threat to national security and respond with force, while others may see cyber-attacks as a more manageable problem that can be addressed through diplomacy or law enforcement. Ultimately, the effectiveness of different approaches to responding to cyber-attacks will depend on a range of factors, including the nature of the attack, the capabilities of the attacker, and the strategic interests of the responding state[174].

The lack of a clear legal framework for cyber warfare has been a major challenge for states in responding to cyber-attacks as acts of aggression or armed attacks. While the UN Charter and customary international law provide some guidance on the use of force in self-defense, they were developed in the context of traditional warfare and may not fully capture the unique characteristics of cyber warfare. This has led to uncertainty and inconsistency in state practice, with some states adopting a more aggressive approach to responding to cyber-attacks while others have been more cautious[175].

---

[172] Ibid.

[173] Michael N. Schmitt, "Preemptive Strategies in International Law," *Michigan Journal of International Law* 24 (2003): 513–34.

[174] William F. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89 (2010): 97, 99.

[175] Leon E. Panetta, "Cybersecurity to the Business Executives for National Security," *New York City*, October 11, 2012, https://www.hsdl.org/?view&did=724128. Last access January 01, 2023.

The lack of a clear legal framework has also created challenges for international cooperation in responding to cyber-attacks. Unlike traditional forms of warfare, which are often carried out by states, cyber-attacks can be carried out by non-state actors or through proxy actors. This can make it difficult to attribute responsibility for cyber-attacks and to hold those responsible accountable under international law[176]. The need for a more robust and consistent approach to the legal regulation of cyber warfare has been recognized by many states and international organizations. Efforts to develop such a framework have included proposals for a new treaty or additional protocols to the UN Charter, as well as initiatives by states and international organizations to develop norms and principles for responsible state behavior in cyberspace. However, progress in this area has been slow, and there is still a significant amount of work to be done to develop a more comprehensive and effective legal framework for cyber warfare[177].

Other states have taken a more cautious approach to classifying cyber-attacks as acts of aggression or armed attacks. For example, China has argued that cyber-attacks are not covered by the UN Charter's definition of armed attack, and that the international community needs to develop a new legal framework to address the unique characteristics of cyber warfare" reflects the fact that some states, such as China, have taken a more nuanced approach to classifying cyber-attacks and have called for a more comprehensive legal framework to address the unique challenges of cyber warfare. China has argued that cyber-attacks should not be considered acts of aggression or armed attacks under international law because they do not involve the use of physical force. Instead, China has advocated for the development of a new legal framework that takes into account the unique characteristics of cyber warfare,

[176] Ibid.

[177] John P. Carlin, "Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats," *Harvard National Security Journal* 7 (2016): 396–97.

such as the potential for anonymity, the difficulty of attribution, and the risk of unintended consequences[178].

China's position is not unique, and other states have also called for a more comprehensive legal framework to address the challenges posed by cyber warfare. For example, in 2015, the United Nations Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security recommended the development of norms, rules, and principles for responsible state behavior in cyberspace[179].

The debate over the legal classification of cyber-attacks reflects the fact that the traditional legal framework governing the use of force was developed in the context of traditional military conflicts and may not be well-suited to address the unique challenges of cyber warfare. As the use of cyberspace continues to grow and become increasingly intertwined with global politics and national security, there is likely to be continued debate over how best to regulate and respond to cyber-attacks[180].

Russia has been accused of using cyber-attacks to influence foreign political affairs and to spread disinformation. These allegations stem from a number of high-profile incidents, including Russia's alleged interference in the 2016 US presidential election and its involvement in the 2017 NotPetya cyber-attack, which caused widespread disruption to businesses around the world. Russia has consistently denied these allegations, and has argued that it is unfairly targeted by Western governments who seek to undermine its legitimacy and influence in the global arena[181]. Russian officials have also argued that cyber-attacks are a legitimate tool of statecraft and that all

[178] Herbert Lin, "Attribution of Malicious Cyber Incidents: From Soup to Nuts," *Journal of International Affairs* 75, (2016): 82–83.

[179] Ibid.

[180] Ibid.

[181] Gerhard Nolte, Multipurpose Self-Defence, Proportionality Disoriented: A Response to David Kretzmer," *European Journal of International Law*, (2013): 14-18.

countries engage in such activities to some degree. Russia's position on cyber-attacks is consistent with its broader approach to international relations, which emphasizes the use of non-military means to achieve strategic objectives. This approach, which is often referred to as "active measures," involves the use of propaganda, disinformation, and other covert means to influence foreign governments and public opinion[182].

Critics of Russia's approach to cyber-attacks argue that it undermines the integrity of democratic institutions and violates international norms governing the use of force. They also point to the potential for unintended consequences, such as the escalation of tensions between states or the unintentional spread of malware to unintended targets. Despite these concerns, Russia's use of cyber-attacks as a tool of statecraft is likely to continue, particularly as the global political landscape becomes increasingly competitive and the stakes of cyber warfare continue to rise. As such, it is important for the international community to develop a comprehensive legal framework governing the use of cyber-attacks in order to mitigate the risk of unintended consequences and ensure that such attacks are used in a responsible and transparent manner[183].

The responses of states to cyber-attacks have also varied widely. Some states have responded to cyber-attacks with military force, while others have pursued diplomatic or legal remedies. For example, in 2018, Israel reportedly carried out a military strike against a Syrian air defense site in response to a cyber-attack on its water supply system. Similarly, the United States has reportedly conducted cyber operations against foreign targets in response to cyber-attacks against U.S. interests. Other states have

[182] William Banks, "State Responsibility and Attribution of Cyber Intrusions After Tallinn," *Texas Law Review* 95, (2017): 1494–97.

[183] Michael N .Schmitt, "Cyber Operations and the Jus ad Bellum Revisited," *Villanova Law Review*, (2011): 37-38.

pursued diplomatic or legal remedies in response to cyber-attacks[184]. For example, in 2020, the European Union imposed sanctions on individuals and entities involved in a cyber-attack on the Organization for the Prohibition of Chemical Weapons. The EU also created a cyber-sanctions regime in 2020 to target individuals and entities involved in cyber-attacks against EU member states[185].

Overall, the responses of states to cyber-attacks as acts of aggression or armed attacks have been complex and varied. The lack of a clear legal framework for cyber warfare has contributed to uncertainty and inconsistency in state practice, highlighting the need for a more robust and consistent approach to the legal regulation of cyber warfare.

3.5 LEGITIMACY AND PROPORTIONALITY OF CYBER SELF-DEFENSE RESPONSES

The evaluation of the legitimacy and proportionality of cyber self-defense responses is another important aspect of the critical legal analysis of the scope of self-defense in the context of cyber-attacks. As noted earlier, the principles of necessity and proportionality are critical in determining the legitimacy of self-defense responses to cyber-attacks. In evaluating the legitimacy of cyber self-defense responses, the analysis must consider whether the response was necessary to counter the attack and whether it was proportionate to the harm caused. This involves an assessment of the nature, scope, and severity of the attack, as well as the response's intended objectives[186].

[184] Ibid.
[185] Ibid.
[186] Jens David Ohlin, "Did Russian Cyber Interference in the 2016 Election Violate International Law?," *Texas Law Review* 95, (2017): 1579.

Moreover, the analysis must also consider the potential consequences of the self-defense response, including the risk of escalation, collateral damage, and unintended consequences[187]. This requires a consideration of the broader geopolitical context and the implications of the response for regional and global security. The evaluation of the proportionality of cyber self-defense responses is particularly challenging given the unpredictable and far-reaching consequences of cyber-attacks. The analysis must consider whether the response was proportional to the harm caused by the attack, taking into account the potential for the attack to cause widespread disruption and even loss of life[188].

To evaluate the legitimacy and proportionality of cyber self-defense responses, the analysis may draw on relevant case studies and state practices, as well as legal and policy frameworks. The analysis must also consider the evolving nature of cyber warfare and the challenges it poses to traditional concepts of self-defense[189].

By evaluating the legitimacy and proportionality of cyber self-defense responses, the thesis can help identify best practices and principles for responding to cyber-attacks in a manner that is consistent with international law and promotes regional and global security. It can also help address concerns regarding the potential abuse of the right to self-defense in the context of cyber-attacks and contribute to the development of a more coherent and effective legal and policy framework for addressing cyber threats[190].

---

[187] Ibid.

[188] James Stavridis, "How to Win the Cyberwar Against Russia," *Foreign Policy* (October 12, 2016), https://foreignpolicy.com/2016/10/12/how-to-win-the-cyber-war-against-russia/. Last accessed May 12, 2023.

[189] Ibid.

[190] George Norman and Joel P. Trachtman, "The Customary International Law Game," *American Journal of International Law* 99, (2005): 22-26.

3.6 APPLICABILITY OF THE UN CHARTER IN THE CYBER CONTEXT

The United Nations Charter serves as a foundational document of international law, providing a framework for the conduct of states and promoting peace and stability. While the Charter was adopted in 1945, it remains applicable in the context of cyberspace, despite the unique challenges posed by this evolving domain. Here are key aspects regarding the applicability of the UN Charter in the cyber context:

3.6.1 Sovereignty and Non-Intervention

The principles of state sovereignty and non-intervention, enshrined in the UN Charter, apply to cyberspace. States have the right to exercise control over their own territory, including their information and communication infrastructure. Cyber operations conducted by one state within the territory of another without consent may violate these principles[191].

3.6.2 Prohibition of the Use of Force

The UN Charter prohibits the threat or use of force by states against each other. This principle applies to cyber operations as well, particularly when cyber operations cause significant harm or disruption to the targeted state's essential systems or infrastructure. Determining the threshold at which a cyber-operation constitutes a use of force can be challenging and is subject to ongoing discussion[192].

3.6.3 Right of Self-Defense

The UN Charter recognizes the inherent right of self-defense. If a cyber-attack constitutes an armed attack, as defined under international law, the targeted state may

[191] Jack Kenny, "France, Cyber Operations and Sovereignty: The 'Purist' Approach to Sovereignty and Contradictory State Practice," *Lawfare*, https://www.lawfareblog.com/france-cyber-operations-and-sovereignty-purist-approach-sovereignty-and-contradictory-state-practice. last accessed March 12, 2021

[192] Kofi Annan, "Two Concepts of Sovereignty," *The Economist*, 1999, [Online], available at http://www.economist.com/node/3247. Last accessed January 3, 2023.

invoke its right to self-defense in response. However, determining when a cyber-operation meets the threshold of an armed attack can be complex, especially given the intangible nature of cyberspace[193].

3.6.4 State Responsibility

The principles of state responsibility, as outlined in the UN Charter, apply to cyber operations. States are responsible for their actions in cyberspace and are obligated to prevent, investigate, and address cyber operations originating from their territory that violate international law[194].

3.6.5 Role of the Security Council

The UN Security Council has the mandate to address threats to international peace and security. In the cyber context, the Security Council can play a role in responding to significant cyber incidents that pose a threat to international peace. However, the Security Council's involvement in cyber-related matters has been limited thus far, with most discussions and actions occurring at the national or regional levels[195].

The applicability of the United Nations (UN) Charter to cyber-attacks is a topic of ongoing debate and interpretation. The UN Charter is a foundational document that establishes the principles and framework for international relations, including the maintenance of peace and security among nations[196]. While the Charter does not explicitly mention cyber-attacks or cyberspace, its principles and provisions can be relevant to addressing cyber threats. Under the UN Charter, the use of force is generally prohibited, except in cases of self-defense (Article 51) or when authorized by the UN Security Council (Chapter VII). The concept of self-defense traditionally

[193] Kofi Annan, "We the Peoples: The Role of the United Nations in the Twenty-First Century," *report of the United Nations*, A/54/2000, (2000).

[194] Noam Chomsky, "Humanitarian Intervention," *Boston Review*, (1994), [Online], available at http://bostonreview.net/BR18.6/chomsky.html. Last accessed January 2, 2023.

[195] Ibid.

[196] Ibid.

pertains to physical aggression or armed attacks. However, the increasing prevalence and disruptive potential of cyber-attacks have raised questions about how the principles of self-defense outlined in the Charter apply to this domain[197].

States differ in their interpretation of the Charter's application to cyber-attacks. Some argue that cyber-attacks may qualify as a use of force if they meet certain thresholds of severity, impact, and intent. These proponents suggest that a cyber-attack causing significant damage, disruption, or loss of life could be considered an armed attack, triggering the right to self-defense under Article 51. On the other hand, there are those who argue that cyber-attacks do not meet the traditional criteria for armed attacks, as they lack the physicality and directness associated with traditional military aggression. They argue that a different legal framework may be required to address cyber-attacks adequately[198].

The UN has acknowledged the challenges posed by cyber-attacks and has undertaken efforts to address them. Various UN bodies, including the General Assembly and the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, have examined the issue and provided recommendations on responsible state behavior in cyberspace[199]. However, there is no universally agreed-upon interpretation of the UN Charter's application to cyber-attacks. Given the evolving nature of cyberspace and the ongoing discussions at the international level, the interpretation and application of the UN Charter to cyber-attacks may continue to evolve. States and international organizations are actively working to establish norms, rules, and frameworks for

[197] Ibid.

[198] Oram Dinstein, "War, Aggression and Self-Defence," (New York: Cambridge University Press, 2011).

[199] Costas Douzinas, *"The End of Human Rights,"* (Oxford/Portland: Hart Publishing, 2000).

responsible behavior in cyberspace, seeking to ensure international peace and security while addressing the unique challenges presented by cyber threats[200].

3.7 ARTICLE 51 OF THE UN CHARTER

There are two generally accepted exceptions to the prohibition of the use of force under public international law, the first being the use of force authorised by the UNSC when there exists a threat to the peace, breach of the peace, or acts of aggression. The second exception is the 'inherent' right to self-defence of sovereign states under UN Charter Article 51 and customary international law.[201]

It has been argued that Article 51 provides the only legitimate exception of any significance for the unilateral (or collective) use of force.[202] Within treaty law, the right to self-defence is enshrined in UN Charter Article 51. That article is part of Chapter VIII, which confers upon the Security Council the responsibility to maintain peace and security and respond to threats to and breaches of the peace. Article 51 states in 102 words the conditions on which the contracting party has the right to act in self-defence. With Article 51 the drafters intended to restrict the use of self-defence and put a threshold in place by deliberately using armed attack instead of the much broader terminology (threat or use of force) in Article 2(4).[203]

The wording of the first sentence of Article 51 shows that the contracting parties have the right to use individual (or collective self-defence) if an armed attack occurs against a member of the United Nations. The usage of the words *inherent right* suggests that the UN Charter recognises the existent right but does not 'create'

[200] Ibid.
[201] ICJ Report, "Case Nicaragua v United States of America" (1986): 193.
[202] Rudiger Wolfrum and Christiane Philipp, "United Nations: Law and Policies and Practice," *Verlag C.H. Beck Munchen* II, (1995): 1162.
[203] *Ibid*.

the right to self-defence, nor tries to regulate all aspects of its content directly.[204] The *travaux preparatoires* leaves it ambiguous as to whether 'inherent right' refers to all forms of self-defence permitted under customary international law or just limits the use of self-defence to all actions permitted by the UN Charter.[205]

3.8 ANALYZING THE ELIGIBILITY OF CYBER-ATTACKS

In principle, cyber-attacks between States—without taking enabling attacks in support of conventional attacks into account can be categorized in three different types: "cyber espionage,"[206] manipulation of the information environment," and "disruption, degradation or destruction of core security assets"[207] For each type, an analysis will take place to determine whether it is eligible to qualify as an armed attack.

Due to the large scale at which modern "cyber espionage" also referred to as information exfiltration takes place, this first type has become a real concern and a kind of intrusion that is too disturbing and too big to ignore. An illustrative example is the blueprint information for the F-35 fighter aircraft that—according to the Snowden Leaks was among the more than 50 TB of information that China stole from the United States (US) government in a years-long theft operation.[208] However, even the most relentless "close access cyber espionage operations" (Schmitt Citation2017, 171, Rule 32, para. 8 + 9) would not be graded as "cyber warfare"[209], regardless of their severity or the method employed (Schmitt Citation2017, 171, Rule 32, para. 8). In

[204] Leland M Goodrich, Edvard Hambro and Anne P Simons, "Charter of the United Nations – Commentary and Documents" *(Columbia: Columbia University Press*, 1969): 344.

[205] Rudiger and Christiane, United Nations: Law and Policies and Practice, 1995.

[206] Ibid.

[207] Cyber Espionage is the non-consensual collection of confidential information. Whilst cyber espionage can be executed in peacetime or during armed conflict, it does not reach the threshold of the use of force.

[208] Aleriano, Brandon, and Ryan C. Maness, Cyber War versus Cyber Realities: cyber Conflict in the International System (*New York, NY: Oxford University Press*. 2015): 95.

[209] Ducheine, P. A. L., and B. M. J. Pijpers, "The Notion of Cyber Operations." In *Research Handbook on International Law and Cyberspace*, ed. Nicholas Tsagourias and Russell Buchan, (Cheltenham: Edward Elgar Publishing, 2021): 271–295.

fact, cyber espionage is to be considered as (merely) an intelligence or counter-intelligence operation (Ducheine and Pijpers Citation2021, 287–288). Therefore, cyber espionage operations do not violate Article 2(4) and will not be considered eligible for qualification as an armed attack.

With regard to the second cyber-attack type, an illustrative example of "manipulation of the information environment" is the way Russia and (perhaps even more impressively) Cambridge Analytica (contracted by the Republican Party) displayed their methods during the US elections in 2016. Especially the combined use of social media and big data to massively target and influence individual voters, demonstrated that modern techniques can manipulate the information environment and harm the democratic integrity of Western countries[210]. Moreover, while manipulation of the information environment is not an obvious expression of force, it could be regarded as a psychological instrument or "weapon". Nevertheless, despite its harmfulness, both the UK and the Netherlands have explicitly designated "manipulating electoral systems" and "altering election outcomes" as (merely) a potential breach of the nonintervention principle[211]. Therefore, for the purpose of this research in which the authors focus on the Netherlands' right of self-defense, it does not amount to a violation of the prohibition of the use of force and is, thus, not considered eligible to qualify as an armed attack, regardless of its scale and effect.

The third type refers to "disruption, degradation or destruction of core security assets." The most straightforward analogy regarding the qualification of cyber-attacks as an armed attack,[212] is when cyber-attacks create effects comparable to traditional kinetic weapons. A cyber-attack directed at critical infrastructure, including a nuclear

[210] Hakim, Danny, and Matthew Rosenberg, "Data Firm Tied to Trump Campaign Talked Business with Russians." *The New York Times*, March 17. 2018.

[211] Ibid.

[212] Ibid.

powerplant to trigger a meltdown, or the system control station of a dam (upstream a populated area) could arguably fall in that category[213]. The possibility of this qualification would especially, but perhaps not exclusively, arise if "loss of life or significant destruction of property" are involved[214]. Therefore, the "disruption, degradation or destruction of core security assets" is the type of cyber-attack that is considered eligible for qualification as an armed attack[215].

3.9 CONCLUSION

It is concluded that the use of force in self-defense is a well-established principle of international law, enshrined in the United Nations Charter and customary international law. However, the emergence of cyber warfare as a new form of aggression has challenged the traditional concept of self-defense and raised a range of legal and policy questions surrounding the appropriate response to cyber-attacks.

The examination of relevant cases and state practices sheds light on the diverse range of cyber-attacks experienced globally and the various approaches taken by states to defend themselves. This section underscores the importance of understanding different state practices to develop effective self-defense strategies. Also it delves into the applicability of criteria for self-defense to cyber-attacks. By exploring the principles of necessity, immediacy, and proportionality, the chapter highlights the complexities involved in determining when a cyber-attack warrants a self-defense response.

---

[213] Ill, Terry D, "Legal Basis of the Right of Self-Defence under the UN Charter and under Customary International Law," In *The Handbook of the International Law of Military Operations*, ed. Terry D. Gill and Dieter Fleck, (Oxford: Oxford University Press. 2015): 444

[214] Dinstein, Yoram. "Cyber War and International Law: Concluding Remarks at the 2012 Naval War College International Law Conference," *International Law Studies* 89, 2021: 276–287

[215] Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," *Columbia Journal of Transnational Law*, (1999): 14-18.

Further it is concluded that that this chapter focuses on state practices and approaches to cyber self-defense. It explores the range of defensive measures employed by states, such as active defense, deterrence strategies, and collective defense initiatives. This section emphasizes the importance of a multi-faceted and adaptive approach to cyber self-defense. Also it is examines state practices and responses to cyber-attacks as acts of aggression or armed attacks. By analyzing different perspectives and legal frameworks, the chapter highlights the challenges in defining cyber-attacks as traditional acts of aggression and the implications for self-defense responses. The applicability of the UN Charter in the cyber context has been subject to ongoing debate and interpretation. The principles of sovereignty, non-intervention, prohibition of the use of force, and the right of self-defense outlined in the Charter form the basis for international relations. However, their application to cyber-attacks, which may not fit traditional notions of armed aggression, remains a complex issue.

Finally, this chapter explores the legitimacy and proportionality of cyber self-defense responses. It delves into the ethical and legal considerations surrounding the use of force in cyberspace, emphasizing the need for proportionate and justifiable actions. Overall, this chapter underscores the importance of developing a comprehensive understanding of self-defense in the context of cyber-attacks. By examining relevant cases, state practices, and legal frameworks, it provides valuable insights into the complexities of cyber self-defense and offers a foundation for further research and policy development in this critical field.

CHAPTER NO 4

CONCLUSION AND RECOMMENDATIONS

CONCLUSION

The profound advancements in cyber technology have ushered in a new era fraught with unprecedented challenges to the traditional constructs of international law and the United Nations Charter. Designed before the advent of the internet, these frameworks primarily catered to kinetic activities, facing an uphill struggle in encompassing and addressing the complexities introduced by cyber operations. The rapid evolution of technology surpassing the pace of legal adaptation, positions international law at a pivotal juncture, necessitating a paradigm shift in its fundamental rules to accommodate and regulate the intricacies posed by cyber-attacks.

The gap between existing international laws and the pressing demands of cyber technology is stark, leaving a void where explicit solutions to multifaceted cyber threats remain elusive. Proposing universal treaties emerges as a promising avenue to regulate the burgeoning sphere of cyberspace activities. However, reluctance among developed nations to establish clear-cut universal rules stems from the delicate balance between leveraging cyber operations to safeguard national interests and preventing potential abuses of the right of self-defense against cyber-attacks.

Embedded within international law, the right to self-defense stipulates the imperative of necessity and proportionality in responding to armed attacks. Yet, the emergence of cyber warfare challenges the orthodox notions of self-defense, instigating legal and policy debates on the appropriate recourse to counter cyber-attacks. The intricate nature of cyber operations allows for interpretation as a use of force, a threat of force,

or an armed attack, contingent upon the severity, attribution, and intent underlying these acts. These attacks target critical infrastructures, inflicting financial losses, operational disruptions, privacy breaches, and social upheaval, underscoring their far-reaching implications.

While the principles of the UN Charter ostensibly apply to the cyber realm, their adaptation faces significant hurdles owing to the distinct attributes of cyberspace—manifesting as attribution complexities and the intangibility of cyber operations. The chapter concludes by advocating for a holistic comprehension of cyber self-defense, stressing the necessity for ethical and proportionate responses within the ever-evolving cyber threat landscape. Understanding diverse state practices and the intricate legal frameworks surrounding cyber warfare serves as the cornerstone for crafting efficacious cyber self-defense strategies and charting a path for comprehensive research and policy development in this critical domain.

RECOMMENDATIONS

Impact on the traditional concepts of self-defense within the framework of international law, several key recommendations emerge which are:

1. Need for Modernized International Laws

Recognize the pressing need for updated international laws explicitly addressing cyber-attacks. The emergence of cyber warfare demands nuanced translations and adaptations of fundamental international law principles to aptly govern cyberspace activities.

2. Advocate for Universal Treaties

Encourage the establishment of universal treaties tailored to regulate cyber activities. Universal agreements can offer a structured approach, although navigating diverse state interests remains a challenge. Despite this challenge, the international community must strive for clarity and consensus to address cyber threats.

3. Embrace Collective Responsibility

Acknowledge the pivotal role of the UN Security Council (UNSC) in maintaining international peace and security. Emphasize the importance of reporting self-defense measures to the UNSC as a procedural duty, respecting the collective security system outlined in the UN Charter.

4. Clarify and Adapt Legal Frameworks

Urgently address the complexities surrounding cyber-attacks' categorization as use of force, threats of force, or armed attacks. Develop clearer criteria based on severity, attribution, and impact on critical infrastructures to determine the applicability of the right to self-defense.

5. Promote Ethical Cyber Responses

Stress the ethical considerations in responding to cyber threats, emphasizing proportionality and justifiability in self-defense measures. Encourage a multi-faceted approach to cyber self-defense, encompassing strategies like active defense, deterrence, and collective defense initiatives.

BIBLIOGRAPHY

Books

Brownlie, Ian. *Principles of Public International Law*. New York: Oxford University Press, 2008.

Dinstein, Yoram. *War, Agression and Self-Defence*. Cambridge: Cambridge University Press, 2005.

Franck, Thomas Martin. *Recourse to force: state action against threats and armed attacks*. Cambridge: Cambridge University Press, 2002.

Gray, Christine Dean. *International law and the use of force*. New York: Oxford University Press, 2008.

Harrison Dinnis, Heather. *Cyber Warfare and the Laws of War*. Cambridge: Cambridge University Press, 2012.

Rid, Thomas. *Cyber War will not take place*. New York: Oxford University Press, 2013.

Simma, Bruno. *The Charter of the United Nations, A Commentary*. New York: Oxford University Press, 2002.

Articles

Bussolati, Nicolo. "The Rise of Non-State Actors in Cyber warfare." in *Cyber war, Law and Ethics for Virtual Conflicts*, Edited by J. D Ohlin, K. Govern, C. Finkelstein. New York: Oxford University Press, 2015.

Donohue, Laura. "The Nature of War and the Idea of Cyber war", in *Cyber war, Law and Ethics for Virtual Conflicts*, Edited by Jens David Ohlin, Kevin Govern, and Claire Finkelstein. New York: Oxford University Press, 2015.

Francis Lau, Simson Garfinkel Rubin, Mark Smith & Ljiljana Trajkovic. "Distributed denial of service attacks in Systems, Man, and Cybernetics", *IEEE International Conference* 3. (2000).

Lachow, I. "Stuxnet Enigma: Implications for the Future of Cyber Security." *Georgetown Journal of International Affairs*11, (2010): 322-345.

Momtaz, D. "Did the Court miss an opportunity to denounce the erosion of the principle prohibiting the use of force?." *Yale Journal of International Law*, (2004): 307-313.

Nolte, Gerhard. Multipurpose Self-Defence, Proportionality Disoriented: A Response to David Kretzmer, *European Journal of International Law*, (2013): 455-478.

O'Connell, Mary Ellen. "Cyber Security without Cyber War." *Journal of Conflict and Security Law*, New York: Oxford University Press 17, (2012): 510-524.

O'Connell, Mary Ellen. "Dangerous Departures." American Journal of International Law, (2013): 344-357.

Oona Anne Hathaway, Rebecca Crootof, Paul Levitz, H. Nowlan Alden, W. Perdue, J. Spiegel "The Law of Cyber Attack." *California Law Review* 100, (2012): 211-236.

Randelzhofer, Albrecht. “Article 2(4), the Charter of the United Nations, A Commentary.” Edited by. Simma, Bruno., New York: Oxford University Press 1, no 2 (2002): 934-956.

Randelzhofer, A. “Article 51, The Charter of the United Nations, A Commentary.” Edited by Simma, Bruno., New York: Oxford University Press 1, no 2 (2002): 1012-1032.

Richmond, J. “Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict.” *Fordham International Law Journal* 35, (2011): 711-732.

Robertson, H. B. “Self-Defense against Computer Network Attack under International Law.” in *Computer Network Attack and International Law*, Edited by Michael. N. and O 'Donell, B. T. Rhode Island: Naval War College Newport press, 2002.

Sanger, David. “Obama Order Sped Up Wave of Cyber-attacks Against Iran.” *New York Times,* April. 9. 2012.

Schmitt, Michael. N. “Bellum American: The US view of Twenty-first Century war and its possible implications for the law of armed conflict.” *Michigan Journal of International Law,* (1998): 267-281.

Schmitt, Michael. “Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework” *Columbia Journal of Transnational Law*, (1999): 914-915.

Schmitt, Michael. N. “Bellum Americanum Revisited: US Security Strategy and the Jus ad Bellum” *Military Law Review*, (2003): 178-191.

Schmitt, Michael. “Cyber Operations and the Jus ad Bellum Revisited.” *Villanova Law Review,* (2011): 376-381.

Schmitt, Michael. “Cyberspace and International Law: The Penumbral Mist of Uncertainty.” *Harvard Law Review* 126, (2013):267-283.

Schmitt, Michael. N. “Cyber Activities and the Law of Countermeasures.” in *Peacetime Regime for State Activities in Cyberspace* Edited by Katharina Ziolkowski, *International Law, International Relations and Diplomacy, NATO CCD COE Publication,* (2013): 455-470.

Sklerov, Matthew. J. “Solving the Dilemma of State Responses to Cyber-attacks: A Justification for the Use of Active Defenses against States Who Neglect Their Duty to Prevent.” *Military Law Review*, (2009): 723-740.

Talbot Jensen, Eric. “Computer Attacks on Critical National Infrastructure: A Use of Force invoking the Right of Self-defense.” *Stanford Journal of International Law* 7, (2002) 788-96.

Tsagourias, N. “Necessity and the Use of Force: A Special Regime.” *Netherlands Yearbook of International Law* 3, (2010): 1202-1220.

Tsagourias, Nicholas. “Cyber-attacks, self-defense and the problem of attribution.” *Journal of Conflict and Security Law* 10, (2012): 1098-1112.

Wortham, Anna. “Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent That May Violate UN Charter Provisions Prohibiting the Threat or Use of Force?.” *Federal Communications Law Journal* 64, (2011): 784-898.

Treaties

Charter of the United Nations, 1945.

Statute of the International Court of Justice, 1945.

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.

Vienna Convention on the law of treaties, 23 May 1969.

United Nations Documentation

The International Law Commission's Draft Articles on Responsibility of States for Internationally Wrongful Acts, in Report of the International Law Commission, 53rd session, (Apr. 23-June 1,July 2-Aug. 10, 2001), General Assembly Official Records, 56th session, supp. no. 10, UN Doc. A/56/10.

United Nation Report of the High-level Panel on Threats, Challenges and Change, A more secure world: our shared responsibility, (2004), UN Doc A/59/565.

United Nations Report of the Secretary-General, In larger freedom: towards development, security and human rights for all, (2005), UN Doc A/59/2005.

UN General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, (24 June 2013), UN Doc A/68/98.

Resolutions

UN Security Council resolution 1368, Threats to international peace and security caused by terrorist acts, UN Doc S/RES/1368 (12 September 2001).

UN Security Council resolution 1373, Threats to international peace and security caused by terrorist acts, UN Doc S/RES/1373 (28 September 2001).

UN Security Council resolution 2170, Threats to international peace and security caused by terrorist acts, UN Doc S/RES/2170 (15 August 2014).

Cebrowski, Vice Admiral, at the US Naval War Collage Symposium, Computer Network ”Attack” and International Law, convened at the Naval War Collage, Newport, Rhode Island, 22-25 June, 1999.

Godwin III, J. B., Kulpin, A., Rauscher, K. F., Yaschenko, V., (2014), Policy report, Russia-U.S. Bilateral on Cyber security: Critical Terminology Foundations 2, East West Institute and the Information Security Institute.

National Research Council, Eds. Owens, W., Dam, K., and Lin, H., (2009), Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyber-attack Capabilities.

NATO Standardization Agency, NATO Glossary of Terms and Definitions (AAP-6) (2010), at 2-C-12.

Ed. Schmitt, M. N., (2013), Tallinn manual on the international law applicable to cyber warfare, Cambridge University Press.

US Department of Defense, Dictionary of Military and Associated Terms, 8 November 2010 (as Amended Through 15 November 2012), Washington DC.

Internet Sources

Falliere, N., Murchu O. L., Chien, E., (2011), W32 Stuxnet Dossier, Symantech, version 1.4, available at: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

Graham Harrison, E., (2015), Could Isis's 'cyber caliphate' unleash a deadly attack on key targets?, The Guardian, available at: http://www.theguardian.com/world/2015/apr/12/isis-cyber-caliphate-hackingtechnology-arms-race.

Letter from U.S. Secretary of State, Daniel Webster, to Lord Ashburton (Aug. 6, 1842) available at: http://avalon.law.yale.edu/19th_century/br-1842d.asp.

Matrosov, A., Rodionov, E., Harley, D., & Malcho, J., (2010), Stuxnet under the microscope, ESET LLC, revision 1.31, available at: http://www.eset.com/us/resources/white-papers/Stuxnet_Under_the _ Microscope . pdf.

White House, The National Security Strategy of the United States of America, (2002), available at: http://www.state.gov/documents/organization/63562.pdf.

White House, The National Security Strategy of the United States of America, (2006), available at: http://www.state.gov/documents/organization/64884.pdf.

White House, The National Security Strategy of the United States of America, (2015), pp. 12-13, available at: http://nssarchive.us/wp-content/uploads/2015/02/2015.pdf.