Legality of Right of Self-Defense

Against Cyber-Attacks

by

Elifnur Baş

A Dissertation Submitted to the
Graduate School of Sciences and Humanities
in Partial Fulfillment of the Requirements for
the Degree of Master of Laws

KOÇ
ÜNİVERSİTESİ

August 6, 2025

Legality of Right of Self-Defense Against Cyber-Attacks

Koç University

Graduate School of Sciences and Humanities

This is to certify that I have examined this copy of a master's thesis by

Elifnur Baş

and have found that it is complete and satisfactory in all respects,
and that any and all revisions required by the final
examining committee have been made.

Committee Members:

Asst. Prof. Işıl Aral (Advisor)

Assoc. Prof. R. Murat Önok

Asst. Prof. Bilge Erson Asar

Date: 06 August, 2025

ABSTRACT

Legality of Right of Self-Defense
Against Cyber-Attacks
Elifnur Baş
Master of Laws
August 6, 2025

With the rise of technological and digital advancements, cyberattacks have emerged in our lives as a serious threat, both to individuals and the private sector. However, the risks are even greater when the target are states. States often hold some of the most sensitive and valuable information, making them frequent targets of cyber operations. Attacks against national cyber infrastructure, defense systems, and intelligence networks put public safety, economic stability, and even state sovereignty at risk.

As dependency on digital systems increases, so too do the legal and strategic challenges. Cyber operations have challenged traditional international law, particularly in terms of the use of force and the right to self-defense. Compared to conventional attacks, cyberattacks are harder to detect, attribute, and evaluate in terms of the scale and intensity required under legal frameworks such as the UN Charter. While many cyber incidents fall below the threshold of armed conflict, they are still capable of causing significant harm. This creates a legal grey area: can computer network attacks justify a state's right to self-defense under Article 51 of the UN Charter?

This thesis explores whether states can legally invoke their right to self-defense in response to cyberattacks and, if so, under what conditions such attacks would trigger Article 51. The research begins by examining the foundations of traditional international law regarding the use of force and then analyzes how these principles apply in the cyber context. This includes both doctrinal legal analysis and the study of case examples.

The thesis argues that cyberattacks can qualify as armed attacks, but only in exceptional cases, especially when their effects are comparable to those of kinetic force. However, issues such as sovereignty, attribution, and proportionality significantly complicate the lawful exercise of self-defense. Despite these challenges, international law still provides a guiding framework that can help regulate and legitimize state responses in cyberspace.

Key Words: International law, Cyber-attacks, Armed attack, Self-defense.

ÖZETÇE

Siber Saldırılara Karşı Meşru Müdafaa Hakkının Hukukiliği

Elifnur Baş

Sosyal Bilimler Enstitüsü, Yüksek Lisans

6 Ağustos 2025

Teknolojik ve dijital gelişmişliğin artmasıyla birlikte siber saldırılar, hem bireyler hem de özel sektör için ciddi bir tehdit olarak hayatımıza girmiştir. Ancak bu tehditlerin etkilediği daha önemli bir aktör daha vardır: devletler. Devletler, en kritik bilgilere sahip olmaları nedeniyle siber saldırılar karşısında büyük risk altındadır. Ulusal siber altyapılar, savunma sistemleri ve istihbarat bilgileri sıklıkla bu saldırıların hedefi hâline gelmektedir.

Artan dijital bağımlılık, kamu güvenliğinden ekonomik istikrara ve egemenliğe kadar uzanan ciddi riskleri de beraberinde getirmiştir. Siber ağ operasyonları, güç kullanımı ve meşru müdafaa hakkına ilişkin geleneksel hukuk anlayışını zorlamaktadır. Geleneksel saldırılarla karşılaştırıldığında siber saldırılar; tespiti, failinin belirlenmesi ve ölçek ile yoğunluk açısından değerlendirilmesi daha zor eylemlerdir. Genellikle silahlı çatışma eşiğinin altında kalırlar; ancak bu durum, ciddi zarar vermelerini engellemez. Bu da hukukta bir gri alan yaratır: Bilgisayar ağı saldırıları, Birleşmiş Milletler Antlaşması'nın 51. maddesi kapsamında devletlerin meşru müdafaa hakkını haklı kılabilir mi?

Bu tez, devletlerin siber saldırılara karşı meşru müdafaa hakkını uluslararası hukuk çerçevesinde kullanıp kullanamayacağını ve eğer kullanabiliyorlarsa, hangi koşullar altında 51. maddenin devreye gireceğini incelemektedir. Araştırma, öncelikle güç kullanımıyla ilgili geleneksel uluslararası hukuk kurallarını incelemekte, ardından bu ilkelerin siber saldırılara nasıl uygulanabileceğini değerlendirmektedir.

Tezin temel savı, bazı istisnai durumlarda siber saldırıların silahlı saldırı sayılabileceği yönündedir, özellikle bu saldırıların etkileri kinetik kuvvetle karşılaştırılabilecek düzeydeyse. Ancak egemenlik, atıf ve orantılılık gibi sorunlar, meşru müdafaa hakkının hukuka uygun şekilde kullanılmasını zorlaştırmaktadır. Tüm bu zorluklara rağmen, uluslararası hukuk hâlâ devletlerin siber ortamda vereceği tepkilere yön gösterebilecek bir çerçeve sunmaktadır.

Anahtar Kelimeler: Uluslararası hukuk, Siber saldırı, Silahlı Çatışma, Meşru müdafaa.

Contents

Table of Authorities

I. Cases

Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), Judgment, 2005 I.C.J. 168, (Dec. 19).

Island of Palmas Case (Neth. v. U.S.), 2 R.I.A.A. 838 (Perm. Ct. Arb. 1928).

Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, (July 8).

Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136, (July 9).

Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Merits, Judgment, 1986 I.C.J. 14 (June 27)

Oil Platforms (Iran v. U.S.), Judgment, 2003 I.C.J. 161 (Nov. 6)

Prosecutor v. Duško Tadić, Case No. IT-94-1-A, ICTY Appeals Chamber (July 15, 1999)

II. International Treaties

U.N. Charter

Convention on Cybercrime, Council of Europe, ETS No. 185, Nov. 23, 2001

Council of Europe, Explanatory Report to the Convention on Cybercrime, Nov. 23, 2001, Eur. T.S. No. 185

Additional Protocol to the Convention on Cybercrime Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems, Jan. 28, 2003, Eur. T.S. No. 189

Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence, May 12, 2022, Eur. T.S. No. 224

Int'l Law Comm'n, Draft Articles on Responsibility of States for Internationally Wrongful Acts with Commentaries, 2001, 2(2) Y.B. Int'l L. Comm'n 26, U.N. Doc. A/56/10

Int'l Law Comm'n, Draft Articles on the Law of Treaties with Commentaries, U.N. Doc. A/CN.4/SER.A/1966/Add.1 (1966)

U.N. Gen. Assembly, Declaration on Principles of International Law Concerning Friendly Relations and Cooperation Among States in Accordance with the Charter of the United Nations, G.A. Res. 2625 (XXV), U.N. Doc. A/RES/2625 (Oct. 24, 1970)

U.N. Gen. Assembly, Definition of Aggression, G.A. Res. 3314 (XXIX), U.N. Doc. A/RES/3314 (XXIX) (Dec. 14, 1974).

Vienna Convention on the Law of Treaties, May 23, 1969, 1155 U.N.T.S. 331.

U.N. General Assembly, Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from the Threat or Use of Force in International Relations, U.N. Doc. A/RES/42/22 (Nov. 18, 1987).

S.C. Res. 1368, U.N. Doc. S/RES/1368 (Sept. 12, 2001)

III. Regulations and International Documents

Regulation (EC) No. 460/2004 of the European Parliament and of the Council of 10 March 2004 Establishing the European Network and Information Security Agency, 2004 O.J. (L 77) 1

United Nations, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/70/174 (July 22, 2015).

United Nations, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/68/98 (June 24, 2013)

U.N. Secretary-General, Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, U.N. Doc. A/76/135 (July 14, 2021)

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

Abbreviations

UN	United Nations
NATO	North Atlantic Treaty Organisation
EU	European Union
US	United States
UK	United Kingdom
CCD COE	Cooperative Cyber Defense Centre of Excellence
ICJ	International Court of Justice
DoS	Denial of Service
DDoS	Distributed Denial of Service
CNA	Computer Network Attack
CNO	Computer Network Operation
CNE	Computer Network Exploitation
CND	Computer Network Defense
ICJ	Information and Communication Technologies
GGE	Group of Governmental Experts
IGE	International Group of Experts
ENISA	European Network and Information Security Agency
ICT	Information Communication Technologies
ICTY	International Criminal Tribunal for the Former Yugoslavia
FRY	Federal Republic of Yugoslavia
VPN	Virtual Private Networking

Chapter I:

INTRODUCTION

1.1.Background

In the digital age, cyberattacks have emerged as a critical concern for state security, often challenging the foundations of international law. By the end of the 20th century cybersecurity had become more and more important since the cyber space had connected the nations and civilizations through internet.[1] This integration paved the way for a new kind of battlefield.[2]

At end of 20th century cyber-attacks were newly developing and there was no law applicable to perpetrators of such crimes and due to the main principle of criminal law, "nullum crimen, nulla poena sine lege", the perpetrators had a chance to escape the law.[3] The rising digital activity and increased exchange of personal information online have heightened the risks associated with cyber-attacks. This exposure to malicious actors, whether individuals or state-sponsored entities, poses significant threats to individual autonomy and privacy. The gravity of cyber-attacks extends beyond temporary crises, as they underscore persistent vulnerabilities in our global digital infrastructure.[4] The lack of applicable law to cyber-attacks are important for comprehending the drive for contemporary international frameworks and rules that permit self-defense against cyberattacks.

The increasing frequency and sophistication of these attacks have prompted urgent questions about how existing legal frameworks apply to this new domain of conflict as the international law is still in development when it comes to cybersecurity and cyber warfare. Nevertheless, creating a legal framework is significantly more challenging under public international law, as the discipline is slow to adapt to the evolving nature of cyber-attacks and cyber warfare. As a

[1] Michael N. Schmitt ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare,* at 16 (Cambridge Univ. Press 2013).
[2] International Committee of the Red Cross**,** *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts,* at 36, U.N. Doc. 31IC/11/5.1.2 (2011).
[3] Johannes Xingan Li, *Cyber Crime and Legal Countermeasures: A Historical Analysis*, Int'l J. Crim. Just. Sci., July–Dec. 2017, at 198, https://ijcjs.com/menu-script/index.php/ijcjs/article/view/191/135.
[4] Oona A. Hathaway, Rebecca Crootof, Philip Levitz & Haley Nix, The Law of Cyber-Attack, 100 Cal. L. Rev. 817, at 841 (2012).

result of principle of the sovereign equality of states[5], establishing a rule requires the mutual consent of states, which further complicates the process.

Even though there was no cyberattack that resulted in any loss of life or unrepairable damage, the International Committee of the Red Cross stated in 2015 that the boundaries and military nature of cyberspace have not yet been fully understood and that the relevance of international humanitarian law to cyberwarfare is still up for debate.[6] States have been taking safeguards against cyberattacks since the start of the twenty-first century in order to protect themselves and their populations, even if the idea of cyberattacks is still relatively new in international law.

The first broadly accepted international framework aimed at addressing the legal dimensions of cyber operations emerged in 2013 with the publication of the Tallinn Manual on the International Law Applicable to Cyber Warfare.[7] Developed by a group of independent experts under the coordination of the NATO Cooperative Cyber Defence Centre of Excellence, the Manual does not create new legal norms but instead interprets how existing rules of international law, both jus ad bellum and jus in bello, apply to the cyber context. Although not legally binding, the Manual represents a significant step in bridging the gap between technological realities and international legal doctrine. A detailed examination of the Tallinn Manual and its relevance to the right of self-defense in cyberspace will follow in a dedicated chapter.

Although the right of states to use of force in self-defense is recognized under the Article 51 of the United Nations Charter, its application to cyber-attacks remains uncertain under public international law. The legal status of cyberspace itself is contested, as international law has not clearly defined how principles such as sovereignty, the prohibition of the use of force and the principle of self-defense apply in this domain. The definition of armed attack in cyberspace is highly controversial and the challenge of attribution further complicates the issue of state responsibility. As a result, the legal framework governing the use of self-defense in response to cyber operations contains significant gaps. Even when attribution is successful, and the necessary threshold is arguably met the scope of an appropriate and lawful response continues to be the subject of considerable debate. This thesis aims to explore these legal complexities and their implications for the right of self-defense in the context of cyber-attacks.

---

[5] U.N. General Assembly, *Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations*, G.A. Res. 2625 (XXV), U.N. Doc. A/RES/2625 (Oct. 24, 1970).

[6] International Committee of the Red Cross, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, 32nd Int'l Conf. of the Red Cross & Red Crescent, Geneva, Switz., Dec. 8–10, 2015, Doc. 32IC/15/11 (2015)

[7] Schmitt, supra note: 1, at 16.

1.2.Research Question

While the right of states to act in self-defense is firmly established under Article 51 of the UN Charter, its application in the realm of cyber operations raises novel and unresolved legal issues. The increasing frequency and severity of state-sponsored or state-enabled cyberattacks have prompted urgent questions about how traditional principles of international law apply in this emerging domain. Specifically, it remains unclear whether and under what conditions a cyber operation can trigger the right of self-defense, and how such a response must comply with existing legal frameworks. Against this backdrop, this thesis seeks to explore whether states can invoke the right of self-defense against cyberattacks under international law? In exploring this question, the thesis will analyze the key legal instruments, including Article 2(4) and 51 of the UN Charter and interpretations found in the Tallinn Manual along with relevant state practice and scholarly debates.

1.3.Thesis Objectives

The main objective of this thesis is to explore whether the states can invoke their right of self-defense against cyber-attacks under international law. To achieve that objective legal frameworks for self-defense in international law will be examined. This objective aims to provide a comprehensive understanding of the legal principles governing the right of self-defense under Article 51 of the UN Charter by first examining its traditional application to armed attacks and then assessing its applicability to cyberattacks. In doing so, it will evaluate how existing international legal frameworks-such as the Tallinn Manual and customary international law-address cyber operations, and whether these instruments sufficiently accommodate the invocation of self-defense in cyberspace, while also identifying any existing legal gaps or ambiguities.

Another objective of the thesis is investigating the nature of cyber-attacks and cyber warfare. This objective will define and classify cyberattacks, analyzing the technical and strategic characteristics that distinguish them from traditional military actions. The aim is to establish whether these cyber operations can be categorized as "armed attacks" under international law, thereby justifying the invocation of self-defense.

The thesis further aims to identify and critically examine the legal, political, and ethical challenges associated with invoking the right of self-defense in the context of cyberattacks. This includes analyzing complex issues such as attribution, the principle of proportionality, and the threshold required for an act to be considered an armed attack under international law. In addition to these legal concerns, the research also aims to explore the broader political and

ethical dilemmas that states face when determining whether to respond to a cyber operation with measures justified as self-defense.

Finally, this thesis aims to propose practical recommendations for strengthening the legal framework surrounding cyberattacks and the right of self-defense. Drawing from the findings of the previous objectives, it will suggest ways to clarify existing legal ambiguities and enhance the effectiveness of current norms and instruments, both at the international level and within domestic legal systems, to ensure a more coherent and reliable response to cyber threats.

1.4.Research Methodology

This thesis primarily employs doctrinal legal research methodology, focusing on the analysis of treaties, customary international law, general principles of law and academic literature to assess the applicability of the right of self-defense in cyberspace. In order to illustrate the operational and interpretative challenges in applying existing legal frameworks, the study also adopts a case study approach, examining state practice in incidents such as the Stuxnet attack and Russian cyber operations against Ukraine. Furthermore, a comparative legal method is used to evaluate the approaches taken by different international organizations, particularly the United Nations, the Council of Europe and the European Union as well as the NATO Cooperative Cyber Defence Center of Excellence in addressing cyber threats. These methodologies collectively enable a comprehensive and structured analysis of the legal, political, and ethical implications of invoking self-defense in response to cyberattacks.

1.5.Scope and Limitations

This thesis aims to examine the applicability of the right of self-defense in response to cyberattacks under international law, with a focus on legal interpretation rather than technical execution. This thesis does not engage in a technical categorization of cyberattacks. The focus lies solely on the legal framework governing the use of force and self-defense in cyberspace under international law. It centers on how cyber operations may fit within the scope of Article 51 of the UN Charter, especially in relation to concepts such as armed attacks, use of force, and attribution. The research includes discussion of notable incidents such as the Stuxnet operation and Russian cyber activities against Ukraine and refers to technical elements like DDoS attacks only to the extent necessary to understand their legal implications.

However, this research does not address cybersecurity at the technical level or focus on the private sector's role. Similarly, cybercrime regulation and cyber espionage in peacetime are outside the scope of this study. The study also relies on legal texts, international doctrine, and publicly available materials, and does not involve empirical or interview-based data. As such,

its scope is limited to legal and policy-based analysis of cyber operations rather than a full technical or operational assessment.

This thesis focuses solely on the right of states to exercise self-defense in response to cyberattacks under international law. It does not address the broader issue of self-defense against non-state actors acting independently. Instead, the analysis is limited to cases where the conduct of a non-state actor is attributable to a state, making that state potentially responsible under international law. Additionally, this thesis is limited to analyzing the right of states to self-defense against cyberattacks that rise to the level of an "armed attack" under international law. It does not cover responses to uses of force that fall below this threshold, such as countermeasures or retorsion.

1.6.Structure of Thesis

This thesis is divided into six chapters focusing to answer the research question; Can States lawfully invoke their right of self-defense against cyber-attacks under the United Nations Charter. Chapter I introduces the background for the research topic as well as outlining the legal problem and its relevance to international law and sets out the methodologies that have been used to answer the question. Chapter II explains the legal efforts that have been made by international communities that aims to regulate the cyberspace and the aftereffects of cyber-attacks including the process of the Tallinn Manuals, the Council of Europe's instruments and ENISA's contributions to creating an international cooperation to cyber threats. Chapter III focuses on the main legal questions surrounding how states can respond to cyber operations under international law. It starts by looking at what cyberspace is and why it's legally significant. The chapter then moves into the debate over whether cyber operations could amount to a "use of force" as prohibited by Article 2(4) of the UN Charter. After that, it explores the threshold of an "armed attack," which is what allows a state to lawfully use force in self-defense under Article 51. The chapter later goes into the core principles of self-defense and how they apply to cyber operations. Finally, it takes up the issue of attribution, showing how hard it can be to identify who's behind a cyber operation and why that matters for any legal response. Chapter IV applies the legal analyses that has been made throughout the thesis into real accidents that has happened over the decades. The case studies are going to include Stuxnet virus that targeted the Iranian nuclear facilities, power grid disruptions in Ukraine and NotPetya attacks and lastly the WannaCry ransomware that has affected a large scale of countries all across the world. Finally, Chapter V concludes the thesis by summarizing the key legal findings and identifies the areas where further research and development is needed in order to establish

more consistent and reliable foundation for evaluating self-defense claims in response to cyber-attacks.

Chapter II:

LEGAL FRAMEWORKS GOVERNING CYBERSPACE

The thesis is going to start with examining international efforts that have made across the world focusing on the international bodies. While the primary focus of this thesis is on the right of states act in self-defense against cyberattacks under international law, certain international legal instruments included in this chapter do not directly regulate use of force. Nonetheless, these frameworks are addressed here to illustrate the broader international legal efforts aimed at addressing cyber threats. Their inclusion helps contextualize the evolving legal landscape of cyberspace in which the self-defense debate takes place.

2.1.An International Research on Cyber Conflicts: The Tallinn Manual

Estonia became a key figure in shaping international legal responses to cyberattacks, largely due to its experience as the target of major cyber operations in 2007. These attacks disrupted critical infrastructure and highlighted the challenges of attribution, jurisdiction, and lawful response under existing self-defense frameworks.[8] They also sparked global debate on the application of Article 51 of the UN Charter to cyber operations, as a result, Estonia has played a leading role in efforts to clarify how international law applies in cyberspace.[9]

2.1.1 Estonian Cyber-Attacks

In 2007, Estonia faced a series of coordinated cyberattacks following the removal of a Soviet-era monument from its capital, Tallinn which triggered protests, resulting in one death and several injuries.[10] Shortly after, Estonia experienced a widespread Distributed Denial of Service (DDoS)[11] campaign that lasted 22 days, targeting both governmental and commercial

---

[8] Stephen Herzog, *Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses*, 4 J. Strat. Sec. 49, at 50, (2011)

[9] George Lucas, *Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare,* at 64 (Oxford Univ. Press 2016).

[10] Steven Lee Myers, *Estonia Removes Soviet-Era War Memorial After a Night of Violence*, N.Y. Times (Apr. 27, 2007), https://www.nytimes.com/2007/04/27/world/europe/27iht-estonia.4.5477141.html

[11] A Distributed Denial of Service (DDoS) attack is a coordinated attempt to disrupt access to a targeted system by overwhelming it with traffic from multiple sources. It typically involves a victim server, attack agents that generate traffic, a control program that manages the agents, and an attacker who directs the operation while remaining hidden. To have more information about how DDoS works see: Felix W. Lau, Stuart H. Rubin, Michael H. Smith & Ljiljana Trajkovic, *Distributed Denial of Service Attacks*, in Proc. IEEE Int'l Conf. on Systems, Man & Cybernetics, SMC 2000 (Vol. 3) 2275 (Oct. 2000).

servers.[12] These cyberattacks were politically motivated and largely launched from outside the country.[13] In response, Estonia formally requested investigative cooperation from the Russian Supreme Prosecutor's Office under the Mutual Legal Assistance Treaty (MLAT) between the two states.[14] However, Russia did not respond to the request, nor did it take any steps to prevent or halt the attacks. Although the Russian government denied responsibility, it also failed to assist in identifying the perpetrators, and no non-state actor claimed responsibility either.[15] As noted by Ottis, Russia's refusal to cooperate could be interpreted as tacit approval of the attackers' actions.[16] Similarly Estonian authorities stated that attacks are too systematic to be a work of individuals.[17] Estonia was unable to conduct a thorough legal investigation due to the lack of international cooperation and evidentiary barriers[18]; which consequently led to not being able to carry out a fair trial and judicial process. Only one individual residing in Estonia was successfully prosecuted, as local evidence was more readily accessible.[19]

2.1.2. The Process of The Tallinn Manual

In May 2008, the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) was established in Estonia by six founding member states of the North Atlantic Treaty Organization.[20] Estonia, which had initially proposed the idea, was selected as the host due to its NATO membership, strategic location and its experience with the large-scale cyberattacks of 2007.[21] The Center officially began its operations in 2009 and continues to hold annual conferences with its contracting partners to foster international cooperation and develop coordinated responses to global cyber threats.[22]

One of the most significant projects undertaken by the CCDCOE was the development of the *Tallinn Manual on the International Law Applicable to Cyber Warfare*, which represents a

---

[12] Rain Ottis, *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective*, Cooperative Cyber Defence Centre of Excellence, (2008).
[13] *Id.*
[14] Eneken Tikk, Kadri Kaska & Liis Vihul, *International Cyber Incidents: Legal Considerations*, Cooperative Cyber Defence Centre of Excellence, at 27 (2010).
[15] Ottis, *Cyber Attacks Against Estonia*, supra note 12.
[16] *Id*.
[17] Chloe Arnold, Russian Group's Claims Reopen Debate on Estonian Cyberattacks, *RFE/RL* (Mar. 30, 2009), https://www.rferl.org/a/Russian_Groups_Claims_Reopen_Debate_On_Estonian_Cyberattacks_/1564694.html.
[18] Tikk-Ringas, supra note 14, at 28.
[19] Ottis, *Cyber Attacks Against Estonia*, supra note 12.
[20] NATO Cooperative Cyber Defence Centre of Excellence, *About Us: History*, https://ccdcoe.org/about-us/ (last visited January 17 2025) Later CCDCoE has accredited as an International Military organization. This accreditation gave the CCDCoE an organizational autonomy as well as the recognition in international level as the North Atlantic Council is the highest decision making body.
[21] Rex B. Hughes**,** *NATO and Cyber Defence: Mission Accomplished*, 33 Atlantisch Perspectief 4, at 5 (2009), https://www.jstor.org/stable/45280023.
[22] Cooperative Cyber Defence Center of Excellence, supra note: 20.

collaborative effort to clarify the legal framework applicable to state conduct in cyberspace.[23] The project brought together an International Group of Experts composed of leading legal scholars, practitioners, and advisors from nearly 50 states aiming to examine how existing international law applies to cyber operations and cyber warfare.[24] Between 2009 and 2012, a group of international legal experts convened in Tallinn, Estonia, to develop a comprehensive, non-binding manual addressing how jus ad bellum and jus in bello principles apply to cyber warfare.[25] Their efforts culminated in the publication of the *Tallinn Manual on the International Law Applicable to Cyber Warfare* in 2013 by Cambridge University Press.

This influential document has become a cornerstone in the field, offering guidance on how existing international law governs state behavior in cyberspace. Building on its foundation, *Tallinn Manual 2.0*, published in 2017, expanded the analysis to include peacetime cyber operations, reflecting the need to regulate cyber activities beyond armed conflict.[26] As of today, further work is underway on *Tallinn Manual 3.0*, which aims to address emerging challenges in cyberspace governance and further refine the legal framework applicable to evolving technological threats.[27]

Experts from the CCDCOE and legal scholars from around the world spent years discussing how existing rules of international law could apply to the fast-changing world of cyber operations.[28] The long and careful preparation process behind the Manual not only reflects the complexity of the topic but also shows how the international legal system tries to keep up with new and evolving threats.[29] Throughout the drafting of the Tallinn Manual, the group of experts faced various ethical and technical challenges that required thoughtful discussion.[30] A key issue they set out to resolve was whether existing international law, including treaties and customary norms, could meaningfully apply to the fast-changing and unique field of cyber warfare.[31] In the end, the experts agreed that current international law was sufficient to address cyber

[23] Schmitt, supra note 1, at 22.
[24] *Id.*
[25] Oliver Kessler & Wouter Werner, Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare, 26 Leiden J. Int'l L. 793, at 797, (2013).
[26] Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* at 2 (2d ed. 2017, Cambridge Univ. Press).
[27] NATO Cooperative Cyber Defence Centre of Excellence, *CCDCOE to Host the Tallinn Manual 3.0 Process* (Dec. 14, 2020), https://ccdcoe.org/news/2020/ccdcoe-to-host-the-tallinn-manual-3-0-process/.
[28] Schmitt, supra note 1, at 22.
[29] Sandra Braman, *Cyber Security Ethics at the Boundaries: Systems Maintenance and the Tallinn Manual*, in Proceedings: 1st Workshop on Ethics of Cyber Conflict 49, at 49 (Ludovica Glorioso & Anna Maria Osula eds., NATO CCD COE 2014).
[30] Kessler, supra note 25, at 796-797.
[31] Schmitt, supra note 1, at 18.

warfare.[32] Building on this consensus, they outlined 95 core rules reflecting treaty law and customary international law to help guide how warfare should be conducted in cyberspace.[33] This approach shows that the general rules of public international law are meant to apply to cyber conflicts between states, highlighting how traditional legal frameworks can adapt to new technological realities.

The CCDCOE brought together a group of experts to research cyber conflicts between states, with the goal of producing a reference for how international law applies in such situations. To stay focused, the International Group of Experts deliberately chose not to revisit issues already well covered by existing legal frameworks, such as cyberattacks triggered by traditional military operations.[34] Scenarios where physical force targets cyber infrastructures are already governed by international humanitarian law, including treaties on armed conflict and customary legal norms.[35] By focusing specifically on cyber-to-cyber operations, the experts aimed to fill an important gap in how international law applies to the evolving realities of cyberspace.[36] This targeted approach allowed the Tallinn Manual to tackle areas of legal uncertainty and challenges instead of repeating principles already settled in the context of conventional warfare.

The first challenge that the Manual tackles is practical limitations of cyberspace which complicate the application of existing norms.[37] These challenges, as will be discussed in upcoming sections, take its root from the intangible nature of digital data, the quickly evolving pace of cyber operations which often leaves no room for traditional diplomatic measures. This problem is particularly relevant for this thesis since Rule 13 of the Manual, Rule 71 in Tallinn Manual 2.0, addresses self-defense and recognizes the need for swift responses to cyberattacks, even when usual intermediary steps are unfeasible.[38] To address these ontological challenges, the first part of the Tallinn Manual sets out jus ad bellum rules specifically tailored to cyber conflicts. These provisions outline when states may lawfully invoke self-defense in response to cyberattacks, aiming to adapt international law to the urgency and speed of cyber operations while keeping its core principles intact.[39]

Secondly, the Manual addresses challenges that the "ontological issues" which is rooted from the borderless nature of cyberspace poses for applying the principle of state sovereignty,

[32] *Id*.
[33] Braman, supra note 29, at 49.
[34] Id. at 50.
[35] Schmitt, supra note 1, at 18.
[36] *Id*. at 18.
[37] Braman, supra note 29, at 51.
[38] Schmitt, supra note 1, rule 13.; *Tallinn Manual 2.0,* supra note 26, rule 71.
[39] Lucas, supra note 9, at 65.

particularly the difficulty of tracing cyberattacks to a specific state.[40] This poses a direct problem for the lawful exercise of self-defense, as the fast-moving nature of cyberattacks often leaves little time for reliable attribution. To respond to these difficulties, the jus ad bellum section of the Manual includes rules on attribution and how the right to self-defense may be invoked in cyber contexts.[41] Through these rules, the Manual attempts to adapt traditional legal standards to the realities of cyber operations that frequently defy national boundaries.[42]

Finally, the Manual acknowledges that the lack of centralized control in cyberspace complicates governance and the creation of clear norms for state conduct.[43] To address this, Part II of the Tallinn Manual 1.0 focuses on jus in bello, adapting the established principles of armed conflict to guide conduct during cyber operations.[44] However, since this concern falls under jus in bello, which regulates conduct during conflict, it lies outside the scope of this thesis.

The success of Tallinn Manual 1.0 drew significant international attention and sparked new questions about how international law applies to cyberspace and as cyber operations became more complex, the need for clearer legal guidance grew which led to the development of Tallinn Manual 2.0, published in 2017.[45] Unlike the first version, which focused on cyber warfare, the second edition also addressed peacetime cyber operations, expanding the number of rules from 95 to 154. By doing so, it aimed to help states better understand how international law applies across the full spectrum of cyber activities.[46] Just like its predecessor, Tallinn Manual 2.0 is not a legally binding document, but it continues to serve as a valuable guide for states navigating cyber operations under international law.

Tallinn Manual 1.0 focused mainly on cyber operations during armed conflict, due to the legal background of its contributors as most of the experts were in the law of armed conflict. However, the nature of cyber operations evolved, especially in peacetime scenarios which as a result this narrow focus was seen as a limitation.[47] In response, Tallinn Manual 2.0 expanded both its scope and depth. It addressed legal gaps related to peacetime operations broadening its relevance to cover a wider range of cyber activities.[48] One of the main criticism of Manual 1.0

---

[40] Braman, supra note 29, at 51.
[41] *Tallinn Manual 2.0,* supra note 26, at 3.
[42] *Id*.
[43] Braman, supra note 29, at 51.
[44] Schmitt, supra note 1, at 19.
[45] Dan Efrony & Yuval Shany, *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*, 112 Am. J. Int'l L. 583, at 584 (2018).
[46] *Tallinn Manual 2.0,* supra note 26, at 2.
[47] Dieter Fleck, *Searching for International Rules Applicable to Cyber Warfare—A Critical First Assessment of the New Tallinn Manual*, 18 J. Conflict & Security L. 331, at 335 (2013).
[48] *Tallinn Manual 2.0,* supra note 26, at 2.

has got is the rules were not detailed enough and not explained thoroughly.[49] To fix this criticism Manual 2.0 has added more rules in order to cover any left out legal points to deserve a consideration.[50] Another important criticism is that the Manual's focus on specific, state-on-state conflict scenarios leaves substantial gaps in addressing the full range of contemporary cyber threats, particularly those falling below the threshold of armed conflict.[51] Moreover, the pace of technological development has outstripped the Manual's coverage, leaving certain operational realities of cyberspace either underexplored or entirely absent.[52] Some authors criticized Manual 1.0 for being too complex, arguing that it reads not like a practical roadmap but rather like a treaty.[53] Unlike Tallinn Manual 1.0, which primarily addressed the law of armed conflict in cyber warfare, Tallinn Manual 2.0 is structured into four parts to offer a broader legal framework, including the legal rules that apply during peacetime.[54]

2.2.The Council of Europe Efforts

The Council of Europe adopted the Convention on Cybercrime in Budapest in 2001 and the Convention was opened for signature in the same year and entered into force in 2004.[55] In the preamble, the Council stated that the aim for Convention on Cybercrime is fighting against cybercrime with well-organized international cooperation.[56] The Convention on Cybercrime is the first international binding document which the drafting process has taken over 16 years, going back to 1995 due to cybercrimes quick evolving nature.[57] In order to fulfill the aim of the Convention on Cybercrime, an organized international cooperation, some level of harmonization between States are necessary.[58] The Convention on Cybercrime has intended to be applicable globally[59] thus was open to the non-member of the Council of Europe and it has been signed by 82 States, 80 of those States have also ratified the Convention.[60]

---

[49] Fleck, supra note 47, at 334.
[50] Tallinn Manual 2.0, supra note 26, at xxxviii.
[51] James E. McGhee, Cyber Redux: The Schmitt Analysis, Tallinn Manual and US Cyber Policy, 2 J.L. & CYBER WARFARE 64, at 83-84 (Spring 2013).
[52] Id., at 97.
[53] Terence Check, *Book Review: Analyzing the Effectiveness of the Tallinn Manual's Jus Ad Bellum Doctrine on Cyberconflict: A NATO-Centric Approach*, 63 Clev. St. L. Rev. 495, at 511 (2015).
[54] *Tallinn Manual 2.0*, supra note 26, at xxxviii.
[55] Convention on Cybercrime, Council of Europe, ETS No. 185, Nov. 23, 2001 (entered into force July 1, 2004).
[56] *Id*.
[57] Jonathan Clough, *A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation*, 40 Monash U. L. Rev. 698, at 699 (2014), https://ssrn.com/abstract=2615789.
[58] *Id*. at 701.
[59] Council of Europe, *Explanatory Report to the Convention on Cybercrime*, Nov. 23, 2001, Eur. T.S. No. 185, at 1–2, https://rm.coe.int/16800cce5b
[60] Council of Europe, *Chart of Signatures and Ratifications of Treaty 185* (Budapest Convention), https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185

Following the adoption of the Convention on Cybercrime, both the digital landscape and the nature of cyber threats have evolved significantly, prompting calls for further legal development.[61] In response, two additional protocols have been introduced. The first, the Additional Protocol to the Convention on Cybercrime Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems, was adopted in 2003 and entered into force in 2006.[62] It focuses on hate crimes committed online. The second protocol was the Second Additional Protocol on Enhanced Cooperation and Disclosure of Electronic Evidence, was adopted in 2022. It aims to strengthen cross-border cooperation and improve access to electronic evidence in cybercrime investigations.[63] However, as of 2025, this protocol has not yet entered into force due to an insufficient number of ratifications.[64]

Just as the Tallinn Manual offers guidance for applying international law to cyber operations between states, the Council of Europe supports harmonizing domestic cybercrime laws through the Budapest Convention and its T-CY Committee Guidelines. Although these efforts focus on national legal systems, they reflect a broader international recognition that cyber threats require both domestic and global legal coordination, making them relevant to the overall framework of cyber self-defense. For example in the 9th Plenary Cybercrime Convention Committee had dealt with Denial of Service(DoS) and Distributed Denial of Service(DDoS) attacks.[65] Article 2 of the Budapest Convention on Cybercrime requires contracting states to criminalize unauthorized access to computer systems.[66] According to the Convention Committee's Guidance Notes, DoS and DDoS attacks are considered forms of such unauthorized access, reinforcing their relevance under international cybercrime norms.[67] The Committee has made another important evaluation under Article 13 of the Convention pointing out how dangerous these attacks can be when they

---

[61] Council of Europe, *Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence*, opened for signature May 12, 2022, C.E.T.S. No. 224, at 2, https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224

[62] Council of Europe**,** *Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems*, Jan. 28, 2003, Eur. T.S. No. 189, https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=189

[63] Communication from the Commission to the European Parliament and the Council, *The EU Internal Security Strategy in Action: Five Steps Towards a More Secure Europe*, COM (2010) 673 final, at 4-5 (Nov. 22, 2010), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52010DC0673

[64] Council of Europe, *Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence*, opened for signature May 12, 2022, C.E.T.S. No. 224, at 2, https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224

[65] Denial of Service attacks are malicious attempts to disrupt the normal operation of a computer or network by preventing legitimate users from accessing it by flooding the system with an excessive amount of traffic. To have more information on the DoS and DDoS attacks see: Christos Douligeris & Aikaterini Mitrokotsa, *DDoS Attacks and Defense Mechanisms: Classification and State-of-the-Art*, 44 COMPUT. NETWORKS 643 (2004).

[66] *Convention on Cybercrime,* supra note 55, art 2.

[67] Council of Europe, Cybercrime Convention Committee (T-CY), Guidance Notes, adopted by the 8th, 9th, 12th, 16th, and 21st Plenary Sessions, at 18 (July 8 2019), https://rm.coe.int/t-cy-guidance-notes-compilation/16809fc22c

target critical systems like hospitals or government services.[68] In the same plenary, critical infrastructure was defined as systems so vital that their disruption could seriously affect national security, public health, or safety.[69] Based on this, cyberattacks targeting such infrastructure can be seen as falling under the Convention, which supports the argument that some of these attacks might be in a position to raise self-defense considerations under international law.

2.3.European Network and Information Security Agency (ENISA)

By requiring member states to align their national laws with EU directives, the European Union plays a key role in building a unified legal framework across Europe, particularly in areas like cybersecurity. This harmonization helps create more consistent responses to cyber threats throughout the continent. Beyond Europe, the EU has also influenced other regions to adopt similar regulatory approaches. Looking at how the EU addresses cyberattacks and cybersecurity in general is essential for understanding how European states are shaping their legal response to challenges in cyberspace.

The European Union established the European Network and Information Security Agency (ENISA) in March 2004 to support its efforts in strengthening cybersecurity across member states by acting as a central point of reference, aiming to build trust through its independence, the quality of its advice, and the transparency of its operations.[70] When looking at the role of institutions like ENISA in cybersecurity governance, it's clear that such bodies play an important part in shaping coherent and reliable approaches.

ENISA's independence is crucial: it lets the agency give impartial, expert advice that member states can trust. Its transparent procedures and clear operational methods supports accountability, making ENISA's work predictable and reliable.[71] By sharing timely information and diligently carrying out its tasks, ENISA helps build confidence at both national and EU levels.[72] The Agency's management board who is responsible for setting the budget, defining working procedures, and overseeing implementation and ensures these standards are maintained.[73] The management structure of ENISA is designed to ensure accountability and

---

[68] *Convention on Cybercrime,* supra note 55, art 13.
[69] *Guidance Notes,* supra note 67, at 7.
[70] Regulation (EC) No. 460/2004 of the European Parliament and of the Council of 10 March 2004 Establishing the European Network and Information Security Agency, para 11, 2004 O.J. (L 77), http://data.europa.eu/eli/reg/2004/460/oj/eng
[71] Karin Attström et al., *Study on the Evaluation of the European Union Agency for Network and Information Security (ENISA),* at 36, (Ramboll Group & CARSA 2017), https://digital-strategy.ec.europa.eu/en/library/final-report-evaluation-european-union-agency-network-and-information-security-enisa
[72] Regulation No. 460/2004, supra note 70, art 3(e).
[73] *Id.,* para 21.

effective coordination among member states, which is essential in developing coherent responses to cyber threats. The Executive Director may form ad hoc Working Groups to bring in technical or scientific expertise, often including both private sector actors and national authorities which helps ENISA stay updated on emerging cyber risks and support the EU and its members in strengthening their cybersecurity posture.[74] While ENISA does not deal directly with questions of use of force or self-defense, its role in promoting cyber resilience and legal harmonization contributes to the broader capacity of states to respond to serious cyberattacks.

Chapter III:

CYBER-ATTACKS AND JUS AD BELLUM FRAMEWORK IN INTERNATIONAL LAW

In order to assess whether states can lawfully respond to cyber operations through the right of self-defense, it is necessary to examine how cyber operations fit within the broader jus ad bellum framework which is the body of international law that governs the use of force between states. This chapter begins by introducing cyberspace as the operational environment in which cyber operations happen and outlines how the nature of cyber domain complicates legal assessments under international law. It then proceeds to examine how Article 2(4) of the UN Charter may apply to cyber operations and can cyber operations be considered as use of force. After making the assessment of Article 2(4) the thesis will analyze the conditions under which a cyber operation may cross the threshold of an armed attack, triggering the right of self-defense under Article 51. The definitional ambiguity surrounding what qualifies as a cyber-attack will be addressed within that section, emphasizing the lack of a unified legal standard and its implications for the application of armed conflict thresholds before discussing the armed attack threshold.

Tom Ruys analyzes the concept of an “armed attack” under international law under three key dimensions: *ratione materiae* explaining what kind of acts qualify as armed attacks, *ratione temporis* explaining when such attacks occur in a way that triggers the right of self-defense, and *ratione personae* explains who must carry out or be responsible for the attack.[75] This thesis will also follow that structure when assessing the legality of self-defense against cyber-attacks: the

[74] Id., para 24.
[75] Tom Ruys, *The Intangible 'Armed Attack': Evolutions in Customary Practice Pertaining to the Right of States to Self-Defence and the Quest for a Definition of 'Armed Attack' under Article 51 UN Charter,* at 220 (unpublished doctoral dissertation, Katholieke Universiteit Leuven 2009) (on file with Ghent Univ. Library).

question of *ratione materiae* will be discussed in Cyber-Attacks as Armed Attacks section by assessing whether cyber operations can reach the threshold of armed attacks. The aspect of *ratione temporis* will be addressed in the Right of Self-Defense section, focusing on when and how states may lawfully respond. Finally, *ratione personae* considerations will appear in the Attribution of Cyber-Attacks section, where the issue of who is responsible for cyberattacks will be analyzed.

3.1. The Nature of Cyberspace in International Law

Cyberspace is the fundamental domain where cyber operations take place, it is the virtual environment that enables the existence, transfer, and disruption of digital information.[76] In the context of international law and cyber conflict, cyberspace is not just a technical construct but also a legally significant one. It is the terrain where sovereignty, jurisdiction, and state responsibility are increasingly being tested. Defining cyberspace provides a foundational framework for determining the applicable legal rules when invoking the right of self-defense in response to cyber operations. This section aims to explore the nature of cyberspace to lay the groundwork for understanding how cyberattacks unfold and why legal debates around the right of self-defense in this domain are especially complex. Before examining specific incidents or legal doctrines, it is essential to understand the cyberspace in which all these interactions occur.

The shift from traditional methods of information collection to cloud-based systems has fundamentally transformed how information is stored, accessed, and secured. This technological evolution, combined with the increasing reliance of states on digital infrastructure, has highlighted the importance of clearly defining cyberspace not only as a domain of state activity[77], but also as a legally relevant space under international law. While cyberspace was once seen as beyond the reach of legal regulation due to its intangible and borderless nature, it is now widely recognized as subject to both domestic and international legal frameworks.[78] The contemporary consensus acknowledges the need to govern cyberspace through legal frameworks to address emerging challenges and ensure accountability in this

[76] Julie E. Cohen, Cyberspace as/and Space, 107 Colum. L. Rev. 210, at 211 (2007).
[77] NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit, NATO Cooperative Cyber Defence Centre of Excellence (July 21, 2016), https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/. NATO member states recognized cyberspace as a distinct domain of operations—alongside land, air, and sea—allowing for enhanced coordination and strategic planning in the cyber realm among allies.
[78] Nicholas Tsagourias, *The Legal Status of Cyberspace*, in Research Handbook on International Law and Cyberspace, at 12 (Nicholas Tsagourias & Russell Buchan eds., 2d ed. 2021)

increasingly critical domain.[79] Defining cyberspace therefore provides a foundational basis for determining the applicable legal rules when assessing a state's right of self-defense in response to cyber operations.[80]

As a major actor in cyberspace and a key practitioner of international law, the United States plays a significant role in shaping how cyberspace is understood and regulated, as reflected in the U.S. Department of Defense's definition of cyberspace grounds itself in operational utility as "global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers".[81] This definition reflects the growing recognition that, unlike traditional physical domains, cyberspace's intangible and interconnected nature requires a tailored legal framework, one that accounts for state sovereignty over cyber infrastructure, regardless of where that infrastructure is physically located.[82]

On the other hand, there are different approaches that avoids to stick to one definition and adopts three layered approach. Tallinn Manuals are one of those sources that adopt three layered approach; first layer of cyberspace has been physical layer, which covers infrastructures and hardware, second layer is logical layer that covers protocols and connections that keeps the system running, finally social layer, third layer, covers the cyber actors that are relevant in cyber activities.[83] Physical layer is the only layer that its elements are existing in other physical domains like the undersea internet cables or fiber-optic infrastructures located in lands of States or routers located in the air or space also some of those physical assets might be fixed to the physical location like the wires and some can be moving like the computers.[84] The logical layer is the non-physical layer where the aspects do not locate in any physical domain; the systems that run the physical infrastructure in the physical layer would be included in the logical layer or any other protocols that decides the streaming of the data, the assets in this layer is not fixed to a physical location since they do not exist in the physical realm the detection of their location

---

[79] Rain Ottis & Peeter Lorents, *Cyberspace: Definition and Implications*, in Proceedings of the 5th International Conference on Information Warfare and Security, at 267-268 (Academic Publishing Ltd. 2010).
[80] *Id.*
[81] U.S. Dep't of Def., Department *of Defense Dictionary of Military and Associated Terms*, Joint Pub. 1-02 (Nov. 8, 2010).
[82] Katarzyna Chałubińska-Jentkiewicz, Filip Radoniewicz & Tadeusz Zieliński, eds., *Cybersecurity in Poland: Legal Aspects,* at 12, (Springer 2022).
[83] *Tallinn Manual 2.0,* supra note 26, at 12.
[84] Nicholas T. Pantin, Key Terrain: Application to the Layers of Cyberspace, at 45, (Mar. 2011) (unpublished M.S. thesis, Naval Postgraduate School), https://calhoun.nps.edu/server/api/core/bitstreams/f3e5cfcd-de3b-40b0-bda1-ae3e9803308b/content

needs monitoring the activities.[85] Social layer involves the non-physical identities and actors that we see in cyber operations like the hackers or even the account that has been created by the users.[86] Detecting activities in social layer is harder than the rest of the cyberspace layers because it requires the real identities behind the accounts since a normal account in the first glance can be controlled by hackers and the actual owner of the account might not be aware of such activities of their account's.[87]

Earlier, in 2011, Tabansky proposed a comparable framework originally developed by the RAND Corporation, a U.S.-based research organization known for its extensive work in defense, security, and public policy.[88] RAND's model, widely used in cybersecurity and defense strategy, divides cyberspace into layers that help analyze state capabilities and vulnerabilities. Tabansky adapted this approach to emphasize the strategic implications of cyber power within these layers, demonstrating the interplay between technological and legal perspectives.[89]

In this model the first layer of cyberspace includes the physical infrastructure that makes cyber activities possible, such as cables and the energy sources that power these systems.[90] The second layer is the software logic, which involves the coded systems and human created protocols that keep these activities running.[91] Lastly the third layer focuses on information, referring to the data that is gathered from those cyber processes.[92] While the first two layers generally align with the Tallinn Manual's understanding, a key difference arises in the third. Tabansky's model puts emphasis on the information itself and how it is used, whereas the Manual focuses more on the individuals or entities carrying out the operations. This difference shows how even seemingly similar approaches can reflect different priorities; Tabansky highlights the strategic dimension of cyber activities, particularly how cyber power can be exercised through control over information. For example, under the Tallinn Manual's social layer view, a state investigating a cyber incident might focus on attribution, identifying the human or organizational actors responsible for the intrusion.[93] Under Tabansky's information layer approach, however, the priority might shift toward assessing how the compromised or manipulated data itself could be weaponized, regardless of the actor's identity. [94] This

[85] Id., at 47.
[86] Id., at 49.
[87] Id., at 50.
[88] For further information on RAND Corporation and its research focus, see *About RAND*, RAND Corporation, https://www.rand.org/about.html
[89] Lior Tabansky. *Basic Concepts in Cyber Warfare*. 3 Mil. & Strategic Aff. 75, at 75 (2011).
[90] Id., at 76.
[91] Id.
[92] Id.
[93] Tallinn Manual 2.0, supra note 26, rule 2 para 7.
[94] Tabansky, supra note 85, at 78.

difference is not just academic it could change how states use resources between forensic attribution and countering the operational use of stolen or falsified information.

3.2. Sovereignty in Cyberspace

Another major area of uncertainty in cyberspace, especially when evaluating a state's right of self-defense under Article 51 of the UN Charter, is the question of sovereignty. The non-physical, decentralized nature of cyberspace makes it difficult to determine how sovereignty should apply or be exercised in this domain. In general terms, sovereignty is a fundamental principle of international law that defines a state's authority within its own territory and limits external interference.[95] Applying this concept to cyberspace, however, raises several challenges due to its borderless and human-made structure.

One of the clearest and most influential definitions of sovereignty in international law comes from the *Island of Palmas* arbitration (1928), where Judge Max Huber stated that "sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State."[96] This definition captures the essence of state sovereignty which is the authority of a state to govern its territory without external interference.[97] The principle of sovereignty has long been a cornerstone of the international legal order, forming the basis for key rules such as non-intervention, jurisdiction, and the prohibition of the use of force.[98] The United Nations Charter reflects the principle of state sovereignty both in its recognition of sovereign equality and non-intervention, and in the voluntary limitation of certain sovereign rights by States through their consent to be bound by a universally accepted legal framework representing the collective will of the international community.[99] Understanding sovereignty is therefore essential when discussing any legal framework that involves the rights and responsibilities of states, including the right of self-defense under Article 51 of the UN Charter.

When cyber activities first emerged as a challenge in international law, scholars offered divergent views on whether the principle of sovereignty could be meaningfully applied to cyberspace. The core concern for those who questioned its applicability stemmed from the

---

[95] *Declaration on Friendly Relations*, supra note 5.
[96] *Island of Palmas Case (Neth. v. U.S.)*, 2 R.I.A.A. at 838 (Perm. Ct. Arb. 1928).
[97] *Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Merits, Judgment*, 1986 I.C.J. 14, para 202 (June 27). https://www.icj-cij.org/sites/default/files/case-related/70/070-19860627-JUD-01-00-EN.pdf
[98] *Tallinn Manual 2.0, Supra* note 26, at 13.
[99] Winston P. Nagan & Craig Hammer, *The Changing Character of Sovereignty in International Law and International Relations*, 43 Colum. J. Transnat'l L. 141, at 154 (2004).

inherently borderless, human-constructed, and decentralized nature of cyberspace.[100] These features, they argued, distinguished it from traditional physical domains, such as land, sea, and air, that sovereignty has historically governed. As a result, some legal scholars contended that cyberspace should not be subject to traditional sovereignty rules.[101] However the applicability of international law to cyberspace was affirmed by the United Nations in successive Group of Governmental Experts (GGE) reports.[102] The most authoritative among them, the 2015 GGE report, recognized sovereignty as a governing principle in cyberspace, stating that *"State sovereignty and international norms and principles that flow from sovereignty apply to the conduct by States of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory."*[103] This recognition signals the international community's view that cyberspace, despite its unique characteristics, falls within the scope of traditional international legal principles.

3.2.1. Sovereignty in The Tallinn Manual

An evolving interpretation of sovereignty in cyberspace can be observed in the Tallinn Manuals. While both Manuals agree that no State can claim sovereignty over cyberspace as a whole[104], their understanding of how sovereignty applies in this domain differs significantly. Tallinn Manual 1.0 treats sovereignty primarily as a guiding principle of international law and reflects considerable debate among experts regarding its applicability to cyberspace. The consensus was that States' exercise of sovereignty remains largely confined to their physical territory, allowing jurisdiction only over cyber infrastructure located within their borders.[105] In contrast, Tallinn Manual 2.0 recognizes sovereignty as a legally binding rule of international law that can extend beyond physical territory in a context-dependent manner.[106]

---

[100] Tsagourias, *supra* note 78, at 9.
[101] John Perry Barlow, *A Declaration of the Independence of Cyberspace*, 18 Duke L. & Tech. Rev. 5, at 5–7 (2019) (reprinting 1996 version). Barlow issued this declaration in response to the Communications Decency Act, part of the Telecommunications Act of 1996, which he saw as an overreach of governmental authority into the emerging digital space.
[102] See also: the 2013 GGE report, which first addressed these issues, though the 2015 report provides a more detailed and explicit affirmation of sovereignty and other international law principles in cyberspace. United Nations, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/68/98 (June 24, 2013) https://dig.watch/wp-content/uploads/A_68_98_E.pdf
[103] United Nations, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, para 27, U.N. Doc. A/70/174 (July 22, 2015), https://docs.un.org/en/A/70/174 ICT=Information Communications Technologies.
[104] Schmitt, *supra* note 1, at 25; *Tallinn Manual 2.0, supra* note 26, at 11.
[105] Schmitt, *supra* note 1, at 25.
[106] *Tallinn Manual 2.0, supra* note 26, at 11.; Rain Liivoja, Maarja Naagel & Ann Väljataga, *Autonomous Cyber Capabilities under International Law*, at 16, (NATO Cooperative Cyber Defence Centre of Excellence 2019), https://ccdcoe.org/library/publications/autonomous-cyber-capabilities-under-international-law/. Shows that the

To better understand how Tallinn Manual 2.0 treats sovereignty as a binding rule of international law, it is useful to examine Rules 2, 3, and 4. Rule 2 addresses internal sovereignty, affirming that states have the right to exercise control over cyber infrastructure, persons, and activities within their territory.[107] Rule 3 concerns external sovereignty, reflecting the principle of sovereign equality by acknowledging that states may engage in cyber activities without requiring prior consent, provided they respect the sovereignty of other states.[108] Most importantly, Rule 4 outlines the violation of sovereignty, establishing that certain cyber operations may amount to internationally wrongful acts if they breach another state's sovereignty.[109] This framework demonstrates that the experts view sovereignty not merely as a general principle, but as a legal rule applicable to cyberspace, whose violation can trigger state responsibility under international law.[110] Sovereignty in cyberspace shapes how the UN Charter, particularly the principle of non-intervention, applies to state conduct in cyber activities.

3.2.2. States Opinions on Governance of Cyberspace

The conceptualization of cyberspace and the application of international legal terms and rules remain problematic within the international community. As in other areas of international law, achieving consensus between states is relatively difficult due to differing strategic interests, technological capabilities, and interpretations of sovereignty. It is useful to gain a general understanding of how various nations approach cyberspace and the application of international principles to incidents involving cyber operations.

The United States adopts a proactive cyber defense strategy, emphasizing the necessity of defending forward to disrupt malicious cyber activities at their source.[111] This approach is encapsulated in the Department of Defense's 2018 Cyber Strategy, which asserts that the U.S. will "defend forward to disrupt malicious cyber activity at its source, including activity that

---

experts drafted The Manual 2.0 sees sovereignty both as a principle that is the root of many other international rules and as an international rule on its own as well.

[107] *Id.*

[108] *Id.*

[109] *Id.*

[110] This view, while authoritative within the Tallinn framework, is not universally accepted. Tsagourias notes that despite this legal recognition, there is insufficient opinio juris and consistent State practice to support sovereignty as a standalone rule in cyberspace under customary international law. See: Tsagourias, supra note 78, at 19

[111] Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States, submitted by participating governmental experts in the GGE established pursuant to G.A. Res. 73/266, U.N. GAOR, 76th Sess., U.N. Doc. A/76/136, at 136, (2021).

falls below the level of armed conflict."[112] This strategy reflects a commitment to preemptive actions to safeguard national interests in cyberspace.

The United Kingdom consistently emphasizes that international law already governs cyber operations, treating cyberspace as part of the established rules-based order.[113] In his 2018 Chatham House speech, Attorney General Jeremy Wright stated that cyber operations causing or threatening "death and destruction on an equivalent scale to an armed attack"[114] can invoke Article 51 showing that the UK aligns cyber thresholds with conventional use of force standards. Also in its 2021 U.N. Group of Governmental Experts national contribution, the Foreign & Commonwealth Office reiterated that there is no separate cyber-specific rule under international law; instead, both cyber and kinetic operations fall under existing norms such as the prohibition of force, necessity, and proportionality.[115]

The European Union and its Member States maintains that existing international law applies fully to state behavior in cyberspace.[116] This was underlined again in a November 2024 declaration by the Council of the European Union, saying that the UN Charter and its prohibitions on the use of force, sovereignty, and the regulation of self-defense governs cyberspace.[117] To translate these norms into action, the EU has developed frameworks and tools that reflect a commitment to both normative clarity and practical cooperation.[118] Their Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities empowers the bloc to coordinate diplomatic, legal, and restrictive responses to malicious cyber behavior, effectively allowing a collective reaction that stays grounded in international law.[119] Along with their legal frameworks ENISA, as discussed above, was established to enhance the cooperation

---

[112] U.S. Dep't of Defense, Fact Sheet: 2018 DoD Cyber Strategy and Cyber Posture Review—Sharpening Our Competitive Edge in Cyberspace, at 4-5, (Sept. 19, 2018)

[113] United Kingdom, Application of International Law to States' Conduct in Cyberspace: UK Statement (Nov. 25 ,2021), https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement.

[114] UK Attorney General Speech (2018) Jeremy Wright, Cyber and International Law in the 21st Century, Speech at Chatham House (May 15, 2018), https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

[115] UK GGE National Statement (2021), United Kingdom of Great Britain and Northern Ireland, Application of International Law to States' Conduct in Cyberspace: UK Statement, U.N. Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (Nov. 25, 2021), https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement.

[116] European Union, *EU Statement – United Nations First Committee: Thematic Discussion on Other Disarmament Measures and International Security* (Oct. 26, 2018), https://www.eeas.europa.eu/node/52894_en?utm

[117] Council of the European Union, *Cyberspace: Council Approves Declaration on a Common Understanding of Application of International Law to Cyberspace*, Press Release (Nov. 18, 2024)

[118] László Kovács, Cyber Security Policy and Strategy in the European Union and NATO, 23 Land Forces Acad. Rev. 16, at 19 (2018).

[119] Council of the European Union, Council Document No. 10474/17, at 3-4, (Brussels, June 19, 2017).

between the Union States. Their statements at UN OEWG sessions affirm respect for state sovereignty, non-intervention, state responsibility, and peaceful dispute settlement in cyber contexts.[120]

Russia recognizes that core principles of international law like sovereignty, prohibition of use of force, apply to cyberspace, as affirmed in various UN reports and resolutions. However, it argues that due to the unique and often anonymous nature of ICT activities, applying existing law should not be automatic.[121] Instead, Russia calls for developing a universal, UN-led framework clarifying how international law operates in the cyber domain. Official doctrines consistently frame cyberspace as part of the broader "information space," merging cyber capabilities with psychological and information operations.[122] This approach rejects the Western model of a global, open internet, instead favoring what Moscow calls "information security" a concept that includes controlling domestic information flows and shaping external narratives.[123] Russian strategic documents and official statements underscore that cyber capabilities are vital for both national defense and influence abroad, portraying information confrontation as a constant condition in international relations rather than a wartime exception.

Another important actor in the global cyber arena is China, which emphasizes the principle of cyber sovereignty and stresses that international law, including the UN Charter, applies in cyberspace.[124] However, it urges that these norms be applied with prudence to avoid escalation and militarization of the digital domain.[125] China supports developing new international legal instruments tailored to the unique characteristics of ICTs, particularly to address issues like cyber terrorism.[126] Beyond its formal statements to the UN on sovereignty in cyberspace, China has undertaken an unparalleled effort to construct a comprehensive governance regime for information and communications technology (ICT). This framework integrates cybersecurity, digital economy regulation, critical infrastructure protection, and content control under a single sovereignty-based vision.[127] This approach reflects Beijing's belief that cyberspace governance

---

[120] European Union, EU Statement – UN Open-Ended Working Group on ICT: International Law (Dec. 19, 2023), https://www.eeas.europa.eu/node/52894_en
[121] U.N. Doc. A/76/136, supra note 111, at 80.
[122] *Russia's Strategy in Cyberspace*, NATO StratCom COE 7, at 5, (June 2021).
[123] Id., at 6-7.
[124] People's Republic of China, Chinese Position Paper on the Application of the Principle of Sovereignty in Cyberspace, U.N. Office for Disarmament Affairs, at 2, (Dec. 2021), https://documents.unoda.org/wp-content/uploads/2021/12/Chinese-Position-Paper-on-the-Application-of-the-Principle-of-Sovereignty-ENG.pdf.
[125] Id., at 3.
[126] Id., at 4.
[127] Samm Sacks, China's Emerging Cyber Governance System, China Cyber Outlook, Center for Strategic & International https://www.csis.org/programs/strategic-technologies-program/resources/china-cyber-outlook/chinas-emerging-cyber (last visited Aug. 2025).

and sovereignty are inseparable and may contribute to the emergence of divergent regulatory spheres globally.[128]

Lastly this is going to look at how the African Union approaches the application of international rules to cyberspace. The African Union's position on cyberspace governance, as reflected in its Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace (2024), affirms a strict interpretation of state sovereignty in the digital domain.[129] They emphasized that cyber operations conducted without a state's consent constitute a violation of international law. This view aligns with what Kevin Jon Heller describes as a "pure sovereignty" approach, which rejects the more restrictive "sovereignty as a principle" model advanced by some Western states.[130] In practice, the AU's stance asserts that sovereignty operates as a binding rule in cyberspace, prohibiting any form of unauthorized cyber intrusion, interference with data, or disruption of infrastructure within a state's jurisdiction.[131] This approach places the African Union alongside states such as Iran and China, which similarly recognize sovereignty as an enforceable legal norm in the cyber context, and contrasts with the positions of states like the United Kingdom that treat sovereignty as a non-binding principle.[132]

3.3.Problem of Defining Cyber-Attack

Before starting to explain the legal evaluations of cyber-attacks and the required thresholds for invoking the right of self-defense it is important to highlight that there is not an agreed upon definition for cyber-attacks thus the absence of an internationally agreed definition of cyberattacks complicates efforts to develop a cohesive legal framework.[133] This challenge stems from the fact that different states, organizations, and stakeholders approach the concept with varying interpretations and priorities. This lack of agreement on the definition of a cyber-attack highlights the need to consult international legal documents, such as General Assembly resolutions, to understand how the term "attack" has been traditionally interpreted. By analyzing these foundational definitions, we can gain insights into how existing legal norms might be applied to the unique characteristics of cyberspace, providing a starting point for developing a comprehensive understanding of cyberattacks. Establishing such a definition is

---

[128] Id.
[129] African Union Peace & Security Council, *Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace* (Jan. 29, 2024).
[130] Kevin Jon Heller, *The African Union (Rightly) Endorses Pure Sovereignty in Cyberspace*, Opinio Juris (Feb. 5, 2024), https://opiniojuris.org/2024/02/05/the-african-union-rightly-endorses-pure-sovereignty-in-cyberspace/.
[131] Id.
[132] Id.
[133] Hathaway, supra note 4, at 822-823

essential for addressing questions of state responsibility, attribution, and the invocation of the right of self-defense in response to cyber threats.[134]

The UN General Assembly have an interpretative guidance in its resolutions like Definition of Aggression. It is especially important when evaluating whether certain cyber operations could reach the threshold necessary to invoke a state's right of self-defense. However, it is important to note that jus ad bellum itself does not contain a formal definition of attack. Rather, it centers on the notion of "armed attack", as outlined in Article 51 of the UN Charter, without further specifying what exactly constitutes such an act.[135]

The term cyber-attack covers a wide range of hostile cyber operations in technical and policy literature to describe a broad range of malicious cyber operations, this thesis does not attempt to define or classify such operations in technical terms. Instead, it focuses on identifying the legal thresholds under international law at which certain cyber operations may trigger the right of self-defense. This requires a closer examination of when a cyber operation may amount to a use of force within the meaning of Article 2(4) or an armed attack under Article 51 of the UN Charter.

3.3.1. Possible Definition for Cyber-Attack

Even though the frequency and the advancement of the cyber-attacks have increased over the years a proper definition of what cyber-attack remains unknown. Cyber-attacks can range from a disturbing the day to day life to actually cause a loss of life and not having a proper definition for it further complicates the application of international rules to cyber-attacks.[136] There are different definitions for cyber-attacks that have been made the legal scholars and examining those definitions would help us to understand the terminology that has been used in cyberspace and to create a framework on applying the international legal rules.

Owens defines cyber-attacks as "…a deliberate actions to alter, disrupt, deceive, degrade or destroy adversary computer systems or networks or the information and/or resident in or transiting these systems or networks."[137] On the other hand Hathaway claims cyber-attacks "ny action taken to undermine the functions of a computer network for a political or national

---

[134] Reese Nguyen, *Navigating Jus Ad Bellum in the Age of Cyber Warfare*, 101 Cal. L. Rev. 1079 (2013).
[135] Michael N. Schmitt, *"Attack" as a Term of Art in International Law: The Cyber Operations Context*, in Proceedings of the 4th International Conference on Cyber Conflict (Christian Czosseck, Rain Ottis & Katharina Ziolkowski eds., NATO CCD COE 2012).
[136] Joseph N. Madubuike-Ekwe, Cyberattack and the Use of Force in International Law, 12 BEIJING L. REV. 631, at 633-634, (June 2021).
[137] William A. Owens, Kenneth W. Dam & Herbert S. Lin, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES, at 10-11, (Nat'l Acads. Press 2009).

security purpose."[138] The United States have made an official definition of cyber-attack in their Joint Chiefs of Staff in 2010 by defining cyber-attack as "A hostile act using computer or related networks or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions."[139]

When comparing these definitions, it becomes clear that Owens adopts a broad, technical perspective, emphasizing the range of actions targeting computer systems or the information they contain without limiting the motivation behind them. Hathaway, by contrast, narrows the scope by focusing on actions that specifically undermine computer network functions for political or national security purposes and assessing them in the geopolitical context. The U.S. Joint Chiefs of Staff definition combines elements of both, retaining the hostile, disruptive, or destructive nature of Owens' view while also introducing the explicit element of "hostile act" and tying it to adversaries' "critical" cyber assets, which reflects a national defense and operational security orientation. Taken together, the three definitions shows that cyber-attacks involve deliberate, harmful interference with computer systems, but they differ in their coverage of conducts, the emphasis on intent and motivation, and the degree to which they frame such acts within a political or military context.

3.4. Use of Force and Cyber Operations

The prohibition of use of force is established in Article 2(4) of the United Nations Charter. Article 2(4) states that, *"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."*[140] Under international law, the prohibition on the use of force in Article 2(4) of the UN Charter sets a broad framework for what states may not do. Within this framework, the concept of 'armed attack' in Article 51 occupies a narrower and higher threshold: while all armed attacks are uses of force, not all uses of force amount to armed attacks. Armed attacks refer to the gravest forms of force, serious enough to trigger the inherent right of self-defense. The Friendly Relations Declaration (1970) reinforces the importance of respecting the territorial integrity and political independence of states.[141] It expands on Article 2(4) by offering more detail on what kinds of actions may constitute a breach of this fundamental rule and, in doing so, provides a legal

[138] Hathaway, supra note 4, at 821.
[139] United States Joint Chiefs of Staff. 2010. Memorandum: Joint Terminology for Cyberspace Operations, at 5, Washington, DC: United States Department of Defense.
[140] *U.N. Charter*, art. 2, para 4.
[141] *Declaration on Friendly Relations*, supra note 5.

framework that helps interpret which acts may amount to an attack, emphasizing respect for state sovereignty and the prohibition of forcible conduct.[142] As a reflection of the prohibition of use of force principle, the UN General Assembly Resolution on the Definition of Aggression (1974) further portrays the types of conduct that may constitute aggression which are the most grave forms of use of force.[143] By identifying actions such as invasion, military occupation, bombardment, and the use of armed force by irregular groups or proxies, the resolution helps define the outer limits of what may constitute an unlawful and forceful intervention.[144] However, international law recognizes two main exceptions to the prohibition of use of force: actions authorized by the United Nations Security Council under Chapter VII of the Charter, and the right of self-defense as defined in Article 51 of the UN Charter. As previously discussed, the UN Charter emphasizes the sovereign equality of states. In the specific context of Article 2(4), subsequent General Assembly Resolutions further clarify that this provision aims to uphold international peace and security through strict limitations on the use or threat of force.[145] In order to understand when a cyber operation might justify a response in self-defense, it is essential to first explore what use of force means under international law. This section will examine how the concept of force is interpreted in legal terms and whether it can apply to cyber operations. It will also consider existing international legal documents and scholarly opinions to assess how the prohibition of force might apply in the face of modern cyber threats.

Article 2(4) of the UN Charter prohibits the use or threat of force in international relations. In order to hold a state responsible for conduct that threatens another state's territorial integrity or political independence, it is essential to determine what types of actions actually amount to force within the meaning of Article 2(4). As prohibition of the use of force under Article 2(4) of the UN Charter is widely considered one of the most fundamental principles in international law. The United Nations General Assembly emphasizes that, for the purpose of maintaining international peace and security, states must refrain from the use or threat of force as set out in Article 2(4) of the UN Charter, and that all states should avoid such conduct within the framework of peaceful relations.[146] Moreover, the General Assembly has stated that the use of force cannot be considered a legitimate method for resolving international disputes, and that any use of force, unless explicitly permitted by international law, constitutes a violation of that

[142] *Id.*
[143] It is important to remember that not every use of force constitutes agression; not every armed attack even constitutes agression. Agression is the most grave form of acts that a State can do.
[144] *Definition of Aggression*, G.A. Res. 3314 (XXIX), U.N. Doc. A/RES/3314 (Dec. 14, 1974).
[145] *Declaration on Friendly Relations*, supra note 5.
[146] *Id.*

law regardless of its justification.[147] Under the U.N. Charter, "aggression" is distinct from the general prohibition of the use of force in Article 2(4). While all acts of aggression involve an unlawful use of force, not all uses of force amount to aggression. The United Nations' General Assembly defines aggression as the most extreme form of unlawful use of force.[148] It also provides examples of conduct that can qualify as aggression, especially when these acts threaten a state's territorial integrity or political independence.[149] International courts have followed a similar line of reasoning in their interpretation of the use of force. In Nicaragua v. US Case, the International Court of Justice confirmed that the prohibition of the use of force under Article 2(4) of the UN Charter reflects a peremptory norm of international law[150], a similar approach made by the International Law Commission in 1966.[151]

The UN General Assembly has repeatedly underlined how important Article 2(4) is for maintaining international peace and security. Among the many declarations made on this issue, the Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from the Threat or Use of Force in International Relations stands out. This declaration is especially important because it does not just restate the general rule. Instead, it tries to improve on how the rule is applied in practice.[152] It also makes it clear that the use of force cannot be justified for political or strategic reasons unless it is clearly allowed under the UN Charter.[153] On the other hand International Law Commission (ILC) takes a stricter stance on countermeasures in the Articles on State Responsibility (ARSIWA) framework as Article 50 explicitly limits countermeasures by stating that they cannot be used to justify or circumvent the prohibition on the use of force.[154]

Certain core points of the prohibition of the use of force under Article 2(4) of the UN Charter will be examined in order to better understand the legal framework that prevents states from unlawful uses of force. As the prohibition on the use of force constitutes a core principle that gives rise to the legal conditions for invoking self-defense, the next few paragraphs will focus on unpacking the elements of Article 2(4), so that the later discussion on the threshold of an

---

[147] *Id.*
[148] *Definition of Aggression,* supra note 144.
[149] *Id.*
[150] *Nicaragua Judgment*, supra note 97, para 190.
[151] Int'l Law Comm'n*, Draft Articles on the Law of Treaties with Commentaries,* art. 50, para. 1 U.N. Doc. A/CN.4/SER.A/1966/Add.1 (1966).
[152] U.N. General Assembly, *Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from the Threat or Use of Force in International Relations*, U.N. Doc. A/RES/42/22 (Nov. 18, 1987).
[153] *Id.*cl. 14
[154]Int'l Law Comm'n, Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries, art. 50, 2001, 2(2) Y.B. Int'l L. Comm'n 26, U.N. Doc. A/56/10. ARSIWA is going to be discussed more in detail under Attribution Rules.

armed attack and the conditions for invoking self-defense can rest on a more structured foundation. The binding nature of this rule is evident for UN member states through their treaty obligations, the prohibition is not limited to Charter signatories. This norm has attained the status of a peremptory norm (jus cogens) so the obligation to refrain from the threat or use of force also stems from customary international law, it applies to all states regardless of UN membership.[155]

To determine whether an act qualifies as a use of force under Article 2(4) of the UN Charter, several factors must be considered. These include the nature of the act, its consequences, and the means used to carry it out. The scale and effects of the conduct help assess whether it crosses the threshold of prohibited force. The political context and the intention behind the act can also influence the evaluation.[156] If the act shows signs of being coercive or hostile, it is more likely to be viewed as a use of force.

Actions that are not intended to amount to a use of force, such as soldiers accidentally crossing into another State's territory would not qualify as a prohibited use of force; yet it is important to note that if such actions may constitute use of force if that State does not comply with other States' requests to stop that action.[157] The intention behind the act can be understood by looking at the political tensions between the states, the location of the act in relation to the other state's strategic assets, the frequency of such incidents even if they cause no actual harm, and whether the act creates the impression of a potential attack.[158]

3.4.1 Consent in International Law

States may allow foreign military forces to operate within their territory through consent, which can limit the legal characterization of such presence as a use of force.[159] However, this consent does not give the guest state unlimited freedom to act as it pleases. Any activities exceeding the agreed terms between States may still be considered a use of force under international law. Also, the territorial state holds the authority to withdraw its consent at any moment. This point was highlighted in the *Armed Activities on the Territory of the Congo (DRC v. Uganda)* case, where Uganda relied on the Congo's earlier consent to justify its military

---

[155] *Nicaragua Judgment*, supra note 97, para 190.
[156] Erin Pobjie, *Prohibited Force: The Meaning of 'Use of Force' in International Law,* at 93 (Cambridge Univ. Press 2024).
[157] Tom Ruys, *The Meaning of "Force" and the Boundaries of the Jus ad Bellum: Are "Minimal" Uses of Force Excluded from UN Charter Article 2(4)?,* 108 Am. J. Int'l L., at 173 (2014).
[158] *Id.* at 175-176.
[159] Ashley S. Deeks, *Consent to the Use of Force and International Law Supremacy*, 54 Harv. Int'l L.J. 1, at 15 (2013).; for further references, see the sources cited therein.

operations.[160] The International Court of Justice found that Uganda's actions went beyond the scope of that consent and therefore breached both the prohibition on the use of force and constituted armed attack.[161] It is however important to keep in mind that while states may give consent to foreign military operations on their territory, such consent cannot override the jus cogens prohibition on the use of force as Article 53 of the Vienna Convention on the Law of Treaties renders void any agreement that permits acts of aggression, requiring a narrow interpretation of consent that does not justify force beyond its lawful scope.[162] A similar limitation is apparent in Articles on State Responsibility where the International Law Commission highlights the limit of the consent would be the customary international law.[163]

These evaluations are especially important when assessing cyber operations, where intent and methods play a central role. While there is ongoing scholarly debate regarding whether a certain scale or gravity must always be present for an act when assessing state response to that act, such questions become more significant when determining whether an act amounts to an armed attack under Article 51. These discussions will therefore be revisited in the next section, which focuses on the threshold of armed attacks and the lawful exercise of self-defense.

3.4.2 Prohibition of Use of Force in Cyber Operations

Building on the traditional understanding of the prohibition of the use of force under Article 2(4) of the UN Charter, the analysis now turns to its application in the context of cyber operations. This part will consider whether cyberattacks can qualify as force under international law and how the principles developed in the conventional framework can apply to cyber-attacks. To understand this better, it is important to remember that Article 2(4) of the UN Charter was primarily created to prohibit the use of military force and to maintain global peace and security in the aftermath of World War II.[164] While originally intended to regulate traditional, kinetic forms of force, the rapid development of technology and the emergence of cyberspace have raised the question of whether certain cyber operations may also fall within its scope. This consideration arises because some cyberattacks, depending on their scale and effects, can cause

---

[160] *Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda)*, Judgment, 2005 I.C.J. 168, para 52, (Dec. 19). Uganda claimed that the consent granted by the DRC remained valid even after the operations against rebel groups had concluded, despite the agreement being limited in scope. However, in paragraph 47 of the judgment, the Court clarified that while the 1998 Protocol might be interpreted as implying ongoing cooperation, it was not the legal basis for Uganda's military presence. The actual legal authorization preceded the Protocol, and the DRC retained the sovereign right to withdraw that consent at any time without formalities.
[161] *Id.* at 170
[162] *Vienna Convention on the Law of Treaties,* art. 53, May 23, 1969, 1155 U.N.T.S. 331.
[163] ARSIWA, supra note 154, at 73-74.
[164] Matthew C. Waxman, *Cyber Attacks as "Force" Under UN Charter Article 2(4)*, 87 Int'l L. Stud., at 46 (2011).

damage comparable to conventional armed force. Therefore, international legal scholars and states have increasingly examined whether severe cyber operations should be regarded as a "use of force" under Article 2(4).

Cyber-attacks became frequent[165] and more complex throughout the time since the first time they came into consideration of the world[166] even if they do not cause serious harm to the State.[167] Due to the multi-national nature of cyber-attacks detecting the perpetrators of such attacks becomes harder[168] thus risks becomes more advanced.[169] As a result of the frequent occurrence of cyber incidents and the possible risk of future attacks States are motivated to have a solid defense mechanisms.[170] While defending against individual cyber-attacks is important; a cyber operation that amounts to an armed attack at the State level can trigger the right of self-defense under international law.[171] In its 2021 report, the UN Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace reaffirmed that states must refrain from engaging in ICT (Information and Communication Technologies) activities that intentionally damage another state's critical infrastructure, such infrastructure is considered part of a state's national assets.[172] The report also emphasized that states remain responsible for their actions in cyberspace and that their obligations under the UN Charter.[173] Ultimately the actions that significantly interfere with the functionality of a nation's infrastructure through attacks on its controlling information systems, regardless of whether they cause immediate physical damage, can be regarded as uses of force.[174]

---

[165] In their National Security Strategy the United Kingdom mentions that during the 2008 Olympic Games Beijing had faced 12 million cyber-attacks per day. See: HM Gov't, *A Strong Britain in an Age of Uncertainty: The National Security Strategy* , at 29 (Cm. 7953, 2010), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf.

[166] The Morris Worm attack in 1988 is considered the first known cyberattack. It was launched by a university student who was later convicted under the U.S. Computer Fraud and Abuse Act. For an in-depth examination of the Morris Worm attack, see Eugene H. Spafford, *The Internet Worm Program: An Analysis* (1988), https://spaf.cerias.purdue.edu/tech-reps/823.pdf.

[167] One of the most knowns cyber-attack was ILOVEYOU Bug in 2000 that has affected millions of computers via e-mail. Since than cyber-attacks have taken much more complex and sever forms. See: Mark Ward, *A Decade on from the ILOVEYOU Bug*, BBC News (May 4, 2010), https://www.bbc.com/news/10095957

[168] Australian Gov't, *Cyber Security Strategy,* at3 (Nov. 23, 2009), https://apo.org.au/sites/default/files/resource-files/2009-12/apo-nid19945.pdf.

[169]Australian Gov't, *2023–2030 Australian Cyber Security Strategy,* at 12 (Nov. 22, 2023), https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf.

[170] U.S. Government, *National Cybersecurity Strategy,* at 22 (Mar. 2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

[171] Nicholas Tsagourias, *Cyber Attacks, Self-Defence and the Problem of Attribution*, 17 J. Conflict & Sec. L. 229, at 230 (2012).

[172] U.N. Secretary-General, *Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, para 42, U.N. Doc. A/76/135 (July 14, 2021).

[173] *Id.* para 70.

[174] Herbert S. Lin, Offensive Cyber Operations and the Use of Force, 4 J. NAT'l SEC. L. & POL'y 63, at 74, (2010).

The risks posed by cyberattacks have become increasingly evident to States across the globe. This raises a critical question: Can cyber operations breach Article 2(4) of the UN Charter? As stated in Rule 69 of the Tallinn Manual 2.0, the threat or use of force being carried out through cyber operations does not make any difference, and an act may constitute the use of force regardless of the types of weapons used.[175] For example some scholars argue that cyberattacks targeting critical infrastructure, such as hospitals, schools, or military and intelligence systems, may amount to a use of force under Article 2(4), even in the absence of kinetic effects. Article 2(4) does not require the same level of harm as Article 51, which is about self-defense after an armed attack. In cyber cases, causing serious disruption can be enough.[176] One of the examples of this approach can be seen in the 2007 Estonia cyberattacks, which has been discussed in detail above in the context of the Tallinn Manual. Despite the lack of physical damage, the attacks had widespread disruptive effects, demonstrating how cyber operations can meet the threshold of a use of force under Article 2(4). So, whether cyber-attacks constitute a use of force the effects of the cyber-attacks should be the main focus rather than their means[177], meaning that when the effect of the cyber operation meets the effects that can be reached using a traditional kinetic force.[178] ICJ supports this claim in its Nuclear Weapons Advisory Opinion by repeating that The UN Charter applies to all uses of force "regardless of the weapons employed."[179] This shows an important principle; the legality of using force is assessed based on its effects, not the type of weapon.

To understand how this approach applies to the cyber operations, it is first necessary to distinguish the different types of operations in cyberspace. Computer network operations (CNO) groups into three categories: computer network attacks (CNA), computer network exploitation (CNE), and computer network defense (CND).[180] CNAs involve activities intended to disrupt, deny, degrade, or destroy information or systems[181]; CNEs are focused on gathering information and they fall more under cyber espionage and do not aim to cause physical or functional harm; CNDs are designed to protect systems against external cyber threats[182]. Since CNEs and CNDs are defensive or espionage-related in nature, they fall outside the scope of this

[175] *Tallinn Manual 2.0,* supra note 26, at 329.
[176] Marco Roscini, *World Wide Warfare – Jus ad Bellum and the Use of Cyber Force*, 14 Max Planck Y.B. U.N. L. 85, at 107, (2010).
[177] *Id,* at 117.
[178] Michael N. Schmitt, *The Evolution of Cyber Jus ad Bellum Thresholds*, Articles of War (July 28, 2022).
[179] L*egality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, 1996 I.C.J. 226, at 244 (July 8).
[180] *Roscini,* supra note 176, at 92.
[181] Joint Chiefs of Staff, *Joint Doctrine for Information Operations*, Joint Publication 3-13, at I-9 (Oct. 9, 1998), https://www.c4i.org/jp3_13.pdf
[182] Andrew Rathmell, *Controlling Computer Network Operations*, 26 Stud. Conflict & Terrorism, at 215 (2003).

thesis. The focus here is on CNAs, which are more commonly referred to as cyberattacks, because they have the potential to cause damage comparable to conventional military force.[183] Depending on the scale and consequences, CNAs might reach the threshold of an "armed attack" required to invoke the right of self-defense under Article 51.[184] However, even if they cannot provide that, they can still constitute a prohibited "use of force" under Article 2(4) of the UN Charter. This means that when a cyber operation does not cause serious harm or loss and therefore does not reach the threshold of an armed attack, its qualification as a use of force can still be evaluated by looking at certain factors including the scale or severity of the operation, how directly it impacts the target, and whether the operation is repeated or sustained over time.[185] Since only armed attacks give a state the right to respond with self-defense under Article 51 of the UN Charter, it's important to look at what actually makes a cyber operation cross that line. So now, the focus will shift to understanding when a cyberattack can count as an armed attack under international law. In sum, while all armed attacks involve a use of force, not all uses of force qualify as armed attacks. For example, a cyber operation that disrupts a country's stock exchange for several days, causing serious economic loss but no physical damage or casualties, would likely constitute a use of force without crossing the armed attack threshold.[186]

3.5. Cyber-Attacks as Armed Attacks

The term "armed attack" appears in Article 51 of the UN Charter. Under international law, the concept of armed attack occupies a narrower and higher threshold than the general prohibition on the use of force in Article 2(4). While both concern hostile actions between states, an armed attack is reserved for the gravest forms of force that are serious enough to trigger the inherent right of self-defense. In other words, all armed attacks are uses of force, but not all uses of force amount to armed attacks. The key distinction lies in the *scale and effects* of the action: measures that cause inconvenience, temporary disruption, or minor physical damage may qualify as uses of force without crossing into armed attack territory. So acts causing large-scale destruction, significant loss of life, or damage comparable to major kinetic attacks can meet the armed attack threshold. This section will first explain what "armed attack"

---

[183] Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 Colum. J. Transnat'l L. 885, at 900 (1999), https://ssrn.com/abstract=1603800.
[184] *Id.,* at
[185] Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 Yale J. Int'l L. 421, at 435, (2011).
[186] Lin, supra note 174, at 75.

means under traditional international law before assessing whether cyber operations can meet this higher threshold.

As reflected in the language of the United Nations Charter, not every use of force triggers the right of self-defense under Article 51. As previously discussed, Article 51 sets a specific threshold: the state must be the target of an armed attack to lawfully exercise this right. This establishes a clear distinction between Article 2(4) and Article 51, where Article 51 adopts a stricter approach than the general prohibition of threat or use of force.[187]

The need for a certain level of gravity for an act to qualify as an armed attack is also affirmed by the International Court of Justice in the Nicaragua case.[188] The Court emphasized that not every use of force amounts to an armed attack, stating that for a use of force to constitute an armed attack, it must reach a certain scale and produce effects serious enough to trigger the right of self-defense.[189] A similar approach is reflected in the Definition of Aggression, which in Article 1 defines aggression as the use of armed force by a state.[190] When read together with the assertion that acts of aggression are among the gravest forms of the use of force, this supports the view that such acts may fall at the higher end of the spectrum of armed attacks capable of triggering the right of self-defense under Article 51. The ICJ reaffirmed its approach in the Nicaragua judgment during the Oil Platforms judgment, holding that claims of individual self-defense under Article 51 of the UN Charter must be assessed according to whether the attack in question meets the threshold for an "armed attack" as established in Nicaragua.[191] Having a distinct requirement in scale when considering an act of force as armed attack is important to support the peaceful coordination between the international community as it prevents the conflicts that might arise between States in minor uses of forces.[192]

In contrast to the ICJ's approach, many legal scholars have disagreed with how the Court defined armed attacks, especially in the Nicaragua case. In that judgment, the Court recognized that Nicaragua had supported rebel groups who are against the government of El Salvador and even described these actions as one of the most serious forms of using force.[193] However, the Court still decided that merely supporting those groups did not reach the level of an "armed

---

[187] Yoram Dinstein, *War, Aggression and Self-Defence,* at 206, (7th ed. 2017).
[188] ICJ specified that most grave forms of use of force needs to be distinguished from other forms of use of force. Then refers to the list that has been made in Declaration on Friendly Relations as less grave forms of force. See: *Nicaragua Judgment,* supra note 97, para 191
[189] *Id.,* para 195.
[190] *Definition of Aggression*, supra note 144, at art I.
[191] *Oil Platforms (Iran v. U.S.), Judgment*, 2003 I.C.J. 161, para 51, (Nov. 6).
[192] Christine Gray, *International Law and the Use of Force*, 3d ed. Oxford Univ. Press, at 148, (2008).
[193] *Nicaragua Judgment*, supra note 97, para 191.

attack"[194], explaining that even if the aid was significant, helping rebel groups was not the same as directly carrying out an armed attack.[195] Hargrove criticizes the ICJ's approach by pointing out that the Court accepts and even supports the idea that states can take forceful countermeasures in response to grave uses of force.[196] However, by refusing to classify these grave acts as armed attacks and having a strict interpretation may end up with uses of force that are not covered by Article 51.[197] Dinstein states that the small-scale armed attacks would still constitute armed attacks and there is no reason for Court to remove small-scale armed attacks under Article 51 of the Charter.[198]

3.5.1 Armed Attack Threshold Assessments

Tom Ruys summarizes three main views on how the armed attack threshold is categorized under international law.[199] The first is that only large-scale, serious attacks qualify as armed attack; the second allows for some smaller, but still significant attacks to count; the third approach closes the gap between Articles 2(4) and 51 of the UN Charter by considering any use of armed force as enough to trigger the right of self-defense.[200] Depending on which view is taken, the legal consequences differ regarding when states can lawfully invoke self-defense or instead rely on countermeasures under the Charter.[201]

Computer network attacks can be employed alongside conventional weapons during an international armed conflict, or they can be used independently during peacetime without any accompanying traditional military action.[202] Although when computer network attacks are used during an international armed conflict they would be treated under international humanitarian law.[203] As discussed in the previous chapter, such operations may amount to a violation of the prohibition on the use of force under Article 2(4) of the UN Charter. This chapter will now examine whether certain computer network attacks can meet the threshold of an "armed attack" and therefore give rise to the right of self-defense under international law. It is now well recognized that cyberattacks can have effects similar to conventional weapons, with the

---

[194] *Id.* para 230.
[195] *Id.* para 247.
[196] John Lawrence Hargrove, The Nicaragua Judgment and the Future of the Law of Force and Self-Defense, 81 Am. J. Int'l L. 135 (1987).
[197] *Id.*
[198] Yoram Dinstein, *'War, Aggression and Self-Defence',* at 195 (4th ed., Cambridge Univ. Press 2005).
[199] Ruys, supra note 75, at 236.
[200] *Id.*
[201] *Id.*
[202] Schmitt, *Computer Network Attack,* supra note 183, at 901.
[203] Yoram Dinstein, *Computer Network Attacks and Self-Defense*, 76 Int'l L. Stud. 99, at 102 (2002).

potential to destroy infrastructure, disrupt systems, and even take control of another State's military programs, potentially causing physical damage.[204]

When assessing how a computer network attack (CNA) fits within the UN Charter's framework, three possibilities can be identified: first, the CNA may fall below the threshold of the use of force, in which case the Charter is not engaged; second, it may constitute a use of force but not rise to the level of an armed attack, thereby raising questions about the range of countermeasures a state may lawfully take and finally, the CNA may amount to an armed attack, thus triggering Article 51 and the right to self-defense under international law.[205] Classifying a computer network attack (CNA) under international law can be particularly challenging, as the effects and consequences of such operations vary significantly.[206] Some cyber operations may merely cause disruption or inconvenience without damaging physical assets[207] which will fall short on the armed attack scale; others, may result in significant destruction, including damage to critical infrastructure or even loss of life, thus constitutes an armed attack.[208] In other cases, a similar technical method may be used either to collect sensitive information, typically analyzed under the framework of cyber espionage, or to irreversibly destroy that information, which could carry far more serious legal implications.[209] This variability necessitates a careful case-by-case assessment when determining whether a particular CNA may amount to an armed attack.

When evaluating whether a cyber operation may constitute an armed attack under international law, three main approaches can be considered.[210] The instrument-based approach focuses on the means used in the attack, requiring that they resemble traditional military instruments such as armed forces, missiles, or bombs.[211] For *use of force*, this approach can be satisfied with lower-grade tools even if the effects are not catastrophic. For *armed attack*, however, the instruments must be employed in a way that produces large-scale, destructive consequences, comparable to major conventional strikes[212]. In cyber contexts, this often leads to the conclusion that most CNAs do not qualify, as digital code lacks the physical destructive

---

[204] Nguyen, supra note 134, at 1116.
[205] Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense*, 38 Stan. J. Int'l L. 207, at 222 (2002).
[206] Schmitt, *Computer Network Attack,* supra note 183, at 901.
[207] See: *U.N. Charter* art. 41, which lists non-forcible measures such as the interruption of means of communication as lawful countermeasures not amounting to the use of force.
[208] Jensen, supra note 205, at 223 (quoting Walter Gary Sharp, Sr.)
[209] *Id.*
[210] Nguyen, supra note 134, at 1118.
[211] Schmitt, *Computer Network Attack,* supra note 183, at 901.
[212] Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 Lewis & Clark L. Rev. 1023, at 1041, (2007), https://ssrn.com/abstract=1083889.

qualities of traditional weapons.[213] It is because, in most cases, this approach concludes that such attacks do not amount to an armed attack, as the digital code used in cyber operations does not share the same characteristics as conventional weapons.[214] Not only the CNAs cannot reach the armed attack threshold they cannot even reach for use of force threshold that since in traditional meaning even lower-grade tools are more effective than the numbers that creates the codes of the attacks.[215]

The target-based approach shifts the focus to the target of the attack.[216] Under this view, if a cyber operation is directed at critical infrastructure and poses the risk of serious disruption, it qualifies as an armed attack.[217] Targeting a state's critical infrastructure through a computer network attack (CNA) may reveal an intent to cause significant harm.[218] To give an example, if the attack disables a state's hospital systems, it could meet the threshold of an armed attack under the target-based approach, thereby triggering the victim state's right to self-defense. The classification of assets as "critical infrastructure" largely depends on how each state defines and identifies them.[219] For instance, the United States has designated sixteen sectors as critical infrastructure that must be protected under any circumstances.[220] However, this broad categorization has been criticized. Nguyen points out that these sixteen sectors encompass both essential services, such as defense and healthcare which are vital to a state's survival, and less essential, primarily private sectors, such as commerce.[221] This raises concerns about whether all components of so-called critical infrastructure should be afforded the same level of protection or trigger the same legal consequences in the event of a cyberattack.[222]

Lastly, the consequence-based approach focuses on the outcome of the operation.[223] According to this perspective, the nature or target of the attack is less important than its effects; if the cyber operation results in significant damage or destruction comparable to that caused by conventional attacks, it could be classified as an armed attack under Article 51 of the UN Charter. For use of force, the necessary consequences might include temporary loss of

---

[213] Nguyen, supra note 134, at 1120.
[214] *Id.* at 1118.
[215] Marco Roscini, Cyber Operations and the Use of Force in International Law, Oxford University Press, at 47, (2014).
[216] Schmitt, *Computer Network Attack,* supra note 183, at 901.
[217] Nguyen, supra note 134, at 1117.
[218] Jensen, supra note 205, at 224.
[219] Nguyen, supra note 134, at 1120.
[220] U.S., Presidential Policy Directive 21: Critical Infrastructure Security and Resilience, PPD-21 (Feb. 12, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil
[221] Nguyen, supra note 134, at 1121.
[222] *Id.*
[223] *Id*. at 1117.

functionality or moderate economic damage. For armed attack, the effects must be on a scale equivalent to major kinetic operations like destruction of infrastructure, loss of life, or crippling of national defense capabilities. Schmitt argues that a computer network attack specifically designed to cause physical destruction or serious injury can be considered a use of armed force, and potentially an armed attack, under international law.[224] He emphasizes that what matters is not whether kinetic weapons are used, but whether the operation directly results in physical damage or harm to human beings.[225] In other circumstances, it is the actual effects of the cyber operation that will determine whether it qualifies as an armed attack under international law.[226] Michael Schmitt identifies six key factors that help determine whether a form of coercion qualifies as an armed attack under international law: severity, immediacy, directness, invasiveness, measurability, and presumptive legitimacy.[227] According to Schmitt, these indicators can also be applied to computer network attacks (CNAs) to assess whether a particular operation amounts to armed coercion, as opposed to merely economic or political coercion.[228] He argues that armed attacks are typically characterized by observable physical harm caused directly by the act itself, without relying on additional supporting circumstances, and within a relatively short time frame thus for such harm to qualify as an armed attack, the operation must cross into the territorial domain of another state, and do so in a manner that is illegitimate, including potentially under the domestic law of the targeted state.[229]

While both use of force and armed attack assessments may look at similar factors the thresholds are distinct. The use of force covers a broad range of hostile actions prohibited under Article 2(4), including those causing temporary or limited harm. Armed attacks, by contrast, represent only the most serious violations, which scale and effects rival traditional military assaults, capable of triggering the right to self-defense under Article 51. This distinction is particularly important in cyber operations, where many hostile acts may breach the use of force prohibition without ever crossing into the armed attack category.

---

[224] Schmitt, *Computer Network Attack,* supra note 183, at 901.
[225] Michael N. Schmitt, *Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts*, in Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy 151, at 163-164 (Nat'l Research Council ed., Nat'l Acads. Press 2010).
[226] *Id.* at 934.
[227] *Id*. at 914. Schmitt explains the application of these factors in this article with a cyber-attack scenario that targets an aircraft CNA attack causes the plane to crash due to this attack. A similar accident happened in in Malaysia in 2014 later Russia has founded responsible for that incident. U.N. News, *U.N. aviation council finds Russia responsible for downing of Malaysia Airlines flight*, May 13, 2025, https://news.un.org/en/story/2025/05/1163161.
[228] Schmitt, *Computer Network Attack,* supra note 183, at 901.
[229] *Id*.

3.5.2 The Tallinn Manual's Armed Attack Classification

After discussing the various scholarly approaches to determining whether a cyber operation may constitute an armed attack, it is now essential to turn to the Tallinn Manual 2.0. As a product of the International Group of Experts (IGE), the Manual represents a consolidated view of how existing international law may apply to cyber operations, particularly in relation to the threshold of an armed attack under Article 51 of the UN Charter. Rule 71 of the Tallinn Manual 2.0 acknowledges the cross-border nature of an armed attack and states that a cyber operation must meet this criterion to qualify as such. This condition can be satisfied either when the cyber operation is directly conducted by a state or when a non-state actor carries out the attack with a sufficient nexus to a state, thereby allowing the action to be attributed to that state under international law.[230] Experts agreed that cyber operations may amount to an armed attack, drawing parallels to the ICJ's Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons, which acknowledged that certain non-kinetic means, such as biological or radiological weapons, could reach the threshold of an armed attack due to their destructive consequences.[231]

The Tallinn Manual 2.0 acknowledges that experts were divided on whether cyber operations that do not result in immediate physical destruction or loss of life can amount to an armed attack. While some members of the International Group of Experts argued that the threshold should be assessed based on whether the cyber operation caused severe damage, others maintained that cumulative or long-term negative consequences could also suffice for classifying an act as an armed attack.[232] Another important debate that has been made by the Experts in the Tallinn Manual 2.0 over 'bleed-over' scenarios, where a cyber-attack produces effects on a third, unintended state. They debate the third state's right to defend itself if the consequences of the attack reach the threshold of an armed attack.[233] Some experts argue that, since the effects meet the required standard, the third state may invoke the right of self-defense. Others contend that, because the attack was not intended against the third state, the operation cannot be classified as an armed attack.[234]

---

[230] *Tallinn Manual 2*.0, supra note 26, at 340.
[231] *Id*.; *Nuclear Weapons,* supra note 179, para 39.
[232] *Tallinn Manual 2.0*, supra note 26, at 343. See: Irène Couzigou, *The Challenges Posed by Cyber Attacks to the Law on Self-Defence*, Eur. Soc'y Int'l L., 10th Anniversary Conf., Vienna, Sept. 4–6, 2014, Conference Paper No. 16/2014, at 10 (Dec. 1, 2014), https://ssrn.com/abstract=2593868. The author highlights that such accumulation approach can be abused by States thus the attacks that happened needs to happen in short amount time to be able to create a nexus as well as the timing of the effects needs to be close to the actual attack.
[233] *Tallinn Manual 2.0*, supra note 26, at 344.
[234] Id.

To sum up the Experts have agreed that cyber-attacks indeed may count as an armed attack under right conditions and therefore can be evaluated under Article 51 of the UN Charter. After exploring whether cyber operations can be considered armed attacks that trigger the right to self-defense, the next section will examine the principles that apply when a cyber-attack does meet the armed attack threshold.

3.6. Right of Self-Defense

This section focuses on how the right to self-defense works under international law and how it can be applied to cyberattacks. First, it looks at the traditional understanding of self-defense as outlined in Article 51 of the UN Charter, especially focusing on key principles like necessity, proportionality, and timing. After explaining how these principles work in the conventional use of force context, the chapter will then explore how they might apply when a state is responding to a cyber operation that reaches the level of an armed attack.

The right of self-defense is codified in Article 51 of the UN Charter which states *"Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security."*[235] The right of self-defense is not evident only in the treaty law but also in customary international law, the International Court of Justice has highlighted this aspect of the Article 51 of the Charter in paragraph 178 of the Nicaragua Judgment stating that "… the Charter, having itself recognized the existence of this right, does not go on to regulate directly all aspects of its content…"[236]

As explained above there are certain requirements that need to be met in order to lawfully invoke the right of self-defense. There has to be an armed attack against the State which is using the right of self-defense. Article 51 includes a procedural requirement for states to report acts of self-defense to the Security Council. Although this obligation stems from treaty law, the ICJ addressed it in the Nicaragua Judgment, noting that the United States' failure to report its actions raised doubts about whether it genuinely believed it was acting lawfully under the right of

[235] *UN Charter*, supra note 140, art. 51.
[236] *Nicaragua Judgment*, supra note 97, para 178.

collective self-defense.[237] An applicable situation under the Charter arose in the DRC v. Uganda case, where the ICJ included the requirement of reporting to the Security Council in its reasoning on the lawfulness of Uganda's exercise of self-defense.[238] As can be seen this requirement is important when evaluating the legality of a self-defense under the UN Charter; meaning that a lawful self-defense under customary international law, since there is not a report requirement to any authority, it can still be unlawful under the treaty law.[239]

3.6.1 Individual and Collective Self-Defense

The first question that we face when dealing with self-defense is who is going to react to an ongoing attack. The UN Charter indicates that states can use their right of self-defense individually or collectively and that use of force does not constitute a breach of prohibition of use of force. Individual self-defense is where States directly responds to armed attack that is targeting them.[240] As for collective self-defense this is where a third state, or more states, get involved with the armed attack and responds with or in name of the victim state.[241] It should be noted that there is not an additional requirement based on the Article 51 for collective self-defense to be valid however the International Court of Justice has stated two requirements specifically needed for collective self-defense. In Nicaragua judgment the Court have stated that in order to resort to collective self-defense the victim State needs to make a public declaration that it has been targeted by an armed attack and also needs to make a request to the third State.[242]

3.6.2 Temporal Categorizations of Self-Defense

Legal doctrine identifies three time-based categories of self-defense that shape when states may lawfully exercise their right under Article 51 of the UN Charter: self-defense exercised before an armed attack, during an armed attack, or after an armed attack.[243] Reactive self-defense occurs when an armed attack has already struck the victim state, and that state responds to defend itself.[244] Interceptive self-defense takes place when an attack has been launched but has not yet reached its target, allowing the victim state to act in the narrow window before the

---

[237] Due to Vandenberg reservation the Court cannot apply the UN Charter to the case. *Id*., at para 200. Also See for more information on the reservation: Louis B. Sohn, American Acceptance of the Jurisdiction of the International Court of Justice: Experiences and Prospects, 18 Ga. J. Int'l & Comp. L. 1 (1988).
[238] *DRC v. Uganda Judgment*, supra note 160, at 5- para 147.
[239] Ruys, supra note 75, at 172.
[240] Dinstein, *War, Agression and Self-Defense*, supra note 198, at 252.
[241] James A. Green**,** *Collective Self-Defence in International Law*, Cambridge Univ. Press, at 18 (2024).
[242] *Nicaragua Judgment*, supra note 97, para 195, 199.
[243] James A. Green, *The 'Ratione Temporis' Elements of Self-Defence*, 2 J. Use of Force & Int'l L. 97, at 98 (2015).
[244] Ruys, supra note 75, at 327.

impact.[245] Finally, anticipatory self-defense is invoked even before the attack is launched. Depending on how imminent the threat is, anticipatory self-defense can be further divided into pre-emptive self-defense, where there is clear evidence like a visible preparations that an attack is about to occur, and preventive self-defense, where no concrete evidence exists of an immediate attack, but a state takes action based on the belief that a threat may emerge in the future.[246] In most of the legal literature, the terms anticipatory and pre-emptive self-defense are used interchangeably to describe a response to an imminent armed attack. This thesis adopts that interchangeable usage for simplicity and consistency.

Reactive self-defense is the most established and least controversial form of self-defense in international law. It refers to a state's right to respond to an armed attack after it has occurred, as clearly outlined in Article 51 of the UN Charter. In traditional settings, this form of self-defense is generally unproblematic in terms of legality, as long as the response meets the requirements of necessity and proportionality. While it does not raise many interpretative issues in conventional warfare, applying it to cyber operations becomes more complex due to attribution problems and the difficulty in identifying the precise moment when an 'attack' has occurred.[247] Article 51 of the United Nations Charter refers to the occurrence of an "armed attack" as a precondition for exercising the right of self-defense.[248] However, legal scholars have criticized the Charter for not incorporating anticipatory self-defense as a legitimate form of self-defense, even though customary international law has recognized it under certain circumstances, particularly when an attack is imminent.[249]

Interceptive self-defense is often confused with pre-emptive self-defense by scholars on both sides of the anticipatory self-defense debate. For instance, Brownlie explains the root cause of these debates to modern mechanisms that are being used which separates the time of the attack and the actual damage.[250] According to Ruys, the distinction between the two is relatively narrow. Interceptive self-defense refers to situations where an armed attack has already been launched but has not yet crossed the borders of the target state making this form of defense only justifiable within a very limited timeframe, making it particularly difficult to establish, as the attack must have begun but not yet crossed the victim state's borders.[251] In contrast, pre-emptive

[245] *Id*.
[246] T.D. Gill, The Temporal Dimension of Self-Defence: Anticipation, Pre-Emption, Prevention and Immediacy, 11 J. Conflict & Sec. L. 361, at 363 (2006).
[247] Dinstein, *War, Aggression, Self-Defence*, supra note 198, at 247.
[248] *UN Charter*, supra note 140, Art 51.
[249] Ruys, supra note 75, at 329.
[250] Ian Brownlie, The Use of Force in Self-Defense, 37 Brit. Y. B. Int'l L. 183, at 259, (1961).
[251] Ruys, supra note 75, at 336.

self-defense is invoked based on evidence that preparations for an attack are underway, requiring a different burden of proof.[252]

Anticipatory self-defense is traditionally traced back to the Caroline incident, which has become foundational in customary international law. In 1837, during the Canadian rebellion against the British rule, the American ship Caroline was used to supply insurgents from U.S. territory; in response, British forces crossed into American waters and destroyed the ship.[253] The United States protested this violation of its sovereignty. Britain justified its actions by asserting that the Caroline posed an imminent threat, thereby invoking the right of self-defense.[254] After this incident, U.S. Secretary of State Daniel Webster and Lord Ashburton, the representative of the British Crown, articulated the principles that known as Caroline Doctrine, setting out strict criteria for anticipatory self-defense based on the principles of imminence, proportionality, and necessity.[255] These principles will be examined in greater detail in the following paragraphs of this chapter. Authors that accept anticipatory self-defense as a legitimate form of self-defense explain their view as the letter of the UN Charter is not supposed to mean if and only in that circumstance, but rather to show if an armed attack occurs, the right of self-defense would be available.[256] Brownlie highlights the application of this doctrine should be careful since it is very vague and might find a very large application situations.[257]

ICJ on the other hand has openly avoided to give its opinion on the debates on the anticipatory self-defense in the Nicaragua case, stating that the anticipatory self-defense was not relevant to the case and it was not going to address it.[258] As set out in the Caroline Doctrine there are four conditions to using self-defense in other States' territory in international law: to begin with there should be an illegal action coming from that States' territory, that action should be an existing grave danger to national security which necessitates the defense action, there should not be any other solution to end the risk other than defending itself in other States' territory and lastly the reaction should be proportionate with the action that justifies the self-defense.[259] Although anticipatory self-defense is traditionally limited to strict conditions and requires the

---

[252] *Id.*
[253] Louis-Philippe Rouillard, *The Caroline Case: Anticipatory Self-Defense in Contemporary International Law*, 1 Miskolc J. Int'l L. 104, at 106 (2004).
[254] Id. at 108.
[255] Gill, supra note 246, at 366 (2006). The Caroline incident is particularly important for showing the anticipatory self-defense was a customary international law before the UN Charter.
[256] Ruys, supra note 75, at 329 (quoting F.P. Feliciano); Also See: *Id.,* at 364.
[257] Ian Brownlie, The Rule of Law in International Affairs: International Law at the Fiftieth Anniversary of the United Nations, at 203, (1998).
[258] *Nicaragua Judgment*, supra note 97, para 35.
[259] Bin Cheng, *Pre-emptive or Similar Type of Self-Defense in the Territory of Foreign States*, 12 Chinese J. Int'l L. 1, at 5 (2013).

presence of an imminent armed attack, an increasing number of scholars advocate for a broader interpretation of the concept.[260]

The traditional opinion on how to apply imminence to cyber operations is the about to be launched approach where if the where a state may lawfully act in self-defense if it has clear evidence that a cyberattack is imminent and would occur very shortly, leaving no time for other preventive measures.[261] One of the most debated aspects of anticipatory self-defense is the so-called "last window of opportunity" test, which suggests that a state may lawfully use force preemptively only when an attack is imminent and no other means of prevention remain.[262] Kevin Jon Heller critically challenges this test, arguing that it is neither firmly established in customary international law nor supported by consistent state practice.[263] He warns that relying on such a narrow and rigid criterion risks encouraging unlawful preemptive strikes and escalating conflicts unnecessarily.[264] In determining imminence, the prevailing view is that two key criteria must be met: the attackers must have clearly manifested hostile intent, and they must be materially preparing to carry out the attack. [265] While this approach aims to clarify imminence, the debate shows that states differ widely on how strictly these conditions should be interpreted, especially in the fast-evolving cyber context. This tension underlines the urgent need for clearer legal standards on anticipatory self-defense in cyberspace to prevent misuse and preserve international stability. There are also scholars that ties the imminence of an attack to previous actions that have happened consistently named as elongated imminence.[266] The important part of this approach is the likelihood of an attack, similar to the last possible window approach it focuses on the actions that led to the potential attack.[267]

Preventive self-defense gained prominence following the 9/11 terrorist attacks, most notably through the 2002 U.S. National Security Strategy, widely referred to as the Bush Doctrine. In this document, the United States asserted a broader interpretation of the right to self-defense, claiming the right to act even in the absence of an imminent threat, based on the assumed

---

[260] *Id*. at 335.
[261] Ryan J. Hayward, Evaluating the Imminence of a Cyber Attack for Purposes of Anticipatory Self-Defense, 117 COLUM. L. REV. 399, at 414, (March 2017).
[262] Tallinn Manual 2.0, supra note 26, rule 73.
[263] Kevin Jon Heller, *The "Last Window of Opportunity" Test Is Unlawful and Dangerous*, Opinio Juris (June 24, 2025), https://opiniojuris.org/2025/06/24/the-last-window-of-opportunity-test-is-unlawful-and-dangerous/.
[264] Id.
[265] Michael N. Schmitt, *Responding to Transnational Terrorism under the Jus ad Bellum: A Normative Framework*, 56 Naval L. Rev. 1, at 19 (2008)
[266] Michael W. Lewis, Elongated Imminence and Operational Realites, Opinio Juirs, (Jan. 29, 2013), https://opiniojuris.org/2013/01/29/elongated-imminence-and-operational-realities/
[267] Daniel Klaidman, *Kill or Capture: The War on Terror and the Soul of the Obama Presidency,* at 219-220, (Crown Publishers 2009).

existence of potential future attacks.[268] However, this approach has faced significant criticism from legal scholars and governments worldwide. For example, scholars from Canada[269] and the United Kingdom[270] have argued that invoking the right to self-defense against a speculative or non-imminent threat, one that may occur in the unknown future, would constitute a clear violation of international law. A non-imminent approach cannot be justified under customary international law, as the doctrine of anticipatory self-defense relies on the Caroline Doctrine, which clearly requires the threat to be imminent; this approach also undermines the UN Charter's purpose of existence as the Charter aims to stop States from acting on their own.[271] Knowing until when the self-defense is going to end is as important as knowing when it will begin; Article 51 limits the duration of self-defense until the Security Council takes necessary measures.[272]

Having analyzed the temporal classifications of self-defense and their legal standing under both customary and treaty law, the next step is to examine the core principles that govern the lawful exercise of self-defense which plays a crucial role in determining whether a state's use of force is justified under international law. Necessity, immediacy and proportionality are the main principals for evaluating the legality of right of self-defense under international law, as previously mentioned they are the core principles that shapes the Caroline Doctrine.

3.6.3 Temporal Categorization of Self-Defense in Cyber-Attacks

In light of the existing international law framework, this thesis will now explore the temporal categories into which cyber-attacks may fall. As discussed in the previous chapter, cyber-attacks can constitute a use of force, and therefore may fall under Article 2(4) of the UN Charter and potentially qualify as an armed attack.[273] The right of self-defense is regulated in Rule 71 of the Tallinn Manual 2.0 where the Manual acknowledges the right of using self-defense when a cyber-attack has reached the armed attack threshold.[274] States may invoke their right of self-defense either in response to a cyberattack directed against them or, under certain conditions discussed above, when they are aware of an imminent attack and it constitutes their last

---

[268] U.S., *The National Security Strategy of the United States of America* (Sept. 2002), at 14 https://2009-2017.state.gov/documents/organization/63562.pdf.
[269] *Military Action in Iraq Without Security Council Authorization Would Be Illegal*, 34 Ottawa L. Rev. 1, 2 (2002-03).
[270] War Would Be Illegal, *The Guardian* (London), Mar. 7, 2003, https://www.theguardian.com/politics/2003/mar/07/highereducation.iraq.
[271] Thomas M. Franck, *Preemption, Prevention and Anticipatory Self-Defense: New Law Regarding Recourse to Force*, 27 Hastings Int'l & Comp. L. Rev. 425, at 433 (2004).
[272] *UN Charter*, supra note 140, art 51.
[273] Dinstein, *Computer Network Attacks,* supra note 203, at 102.
[274] *Tallinn Manual 2.0,* supra note 26, rule 71.

opportunity to prevent it.[275] However Schmitt highlights that last opportunity to take action does not allow States to use preventive self-defense.[276] Anticipatory self-defense may be considered when a cyber-attack is part of a larger plan, the attack poses an unavoidable threat, and the defending state acts immediately before the attack occurs.[277] As for how the Manual handles the anticipatory self-defense in cyber context we need to look at Rule 73 as the rule states that a self-defense can be invoked when "a cyber armed-attack has occurred or imminent"[278] while tracing it back to the Caroline Doctrine.[279] After looking at the Manual's approach to anticipatory self-defense we will be look at how the principles of self-defense apply to cyber-attacks. Hayward visualizes the difference between anticipatory self-defense approaches with hypothetical examples.[280] Where an adversary has fully developed cyber capabilities to shut down a critical infrastructure system but has not yet initiated the attack. Under the traditional about to be launched view, a state may not act because the attack is not immediately imminent.[281] In contrast, under the last window of opportunity approach, the state may lawfully respond preemptively, as the window to prevent a potentially devastating attack is closing.[282] From the elongated imminence perspective, the state could justify defensive action even earlier than the last window of opportunity approach. The reasoning is that the adversary's capability to strike critical infrastructure, even without immediate intent, represents a continuing and evolving threat.

3.6.4 Leading Principles of Self-Defense

Necessity, as a core principle of lawful self-defense under international law, requires that the use of force be a last resort,[283] undertaken only when no other peaceful means remain to protect the state's national security and sovereignty.[284] However the application of necessity as a principle is mostly apparent in anticipatory self-defense where States use self-defense when there is not a direct attack but rather a threat of an attack.[285] In State practice, the principle of

---

[275] Schmitt *Cyber Operations in International Law,* supra note 225, at 166.
[276] Id.
[277] Schmitt, *Computer Network Attack,* supra note 183, at 932.
[278] *Tallinn Manual 2.0,* supra note 26, rule 73.
[279] Gábor Kajtár, *The Caroline as the 'Joker' of the Law of Self-Defence – A Ghost Ship's Message for the 21st Century*, 21 Austrian Rev. Int'l & Eur. L. 3, at 5 (2016), https://ssrn.com/abstract=3394124.
[280] Hayward, supra note 261, at 417.
[281] *Id*.
[282] *Id*., at 418-419.
[283] *Id.* art 2(3).; ARSIWA, supra note 154, art. 25.
[284] Ruys, supra note 75, at 194.
[285] Dapo Akande & Thomas Liefländer, *Clarifying Necessity, Imminence and Proportionality in the Law of Self-Defence*, 107 EJIL 563, at 564 (July 2013).

necessity is generally not applied strictly once an armed attack has already occurred.[286] As Article 51 of the UN Charter recognizes the inherent right of a State to use force in self-defense in response to such attacks. The focus at that stage shifts from avoiding force to ensuring that any defensive action is proportionate and directed at repelling the aggression.[287] When assessing whether a self-defense action meets the requirement of necessity, the nature and potential impact of the weapons likely to be used in the anticipated attack are crucial. If the expected use of such weapons would cause severe and immediate harm, this may support the lawfulness of anticipatory self-defense.[288]

Another principle that governs the legality of self-defense is immediacy, meaning that there should be an appropriate time between the original attack and the defense act that has been taken by the victim State.[289] It is important to note that the appropriate timing for taking action cannot be determined in advance.[290] The International Court of Justice addressed the element of immediacy in the Nicaragua case, emphasizing that the timing of the United States' alleged acts of self-defense occurred well after the actual armed attack against Nicaragua had taken place. As a result, the Court found that these actions did not satisfy the principle of necessity, as the temporal gap undermined the justification for invoking self-defense under Article 51 of the UN Charter.[291] However the immediacy assessment should be made case by case as there are different scenarios that can be happen.[292] The principle of immediacy serves to ensure that self-defense measures are taken as a direct response to an armed attack, rather than as a delayed act of retaliation or punishment.[293]

Proportionality is the final principle of self-defense examined in this thesis. Under jus ad bellum, it requires that the forceful response to an armed attack must not be excessive in scale, duration, or intensity relative to the initial attack.[294] This means that the assessment considers the response as a whole, including strategic and political decisions, rather than evaluating the legality of individual strikes.[295] There are two main approaches in determining what constitutes a proportionate response under the principle of proportionality in jus ad bellum. The quantitative approach argues that the defensive response should mirror the original attack in

---

[286] Oscar Schachter, *The Right of States to Use Armed Force*, 82 Mich. L. Rev. 1620, at 1629 (1984).
[287] Ruys, supra note 75, at 196 (with further citations)
[288] Leo Van den hole, *Anticipatory Self-Defence Under International Law*, 19 Am. U. Int'l L. Rev. 69, at 101 (2003).
[289] *Id. at 104*
[290] Ruys, supra note 75, at 197.
[291] *Nicaragua Judgment*, supra note 97, para 237.
[292] Dinstein, War, Aggression, Self-Defence, supra note 198, at 243.
[293] Van den hole, supra note 288, at 104.
[294] Ruys, supra note 75, at 206.
[295] *Id*.

terms of the type of weapons used, the scale of damage caused, and the overall effects.[296] However, this view has been widely criticized and rejected by many scholars, who argue that proportionality does not require the same kind of weapons or an equal level of destruction.[297] Instead, a more widely accepted functional approach focuses on whether the self-defense action is necessary to effectively repel or neutralize the threat posed by the original armed attack.[298] In this view, proportionality is assessed in terms of achieving the legitimate defensive objective, rather than matching the attack on a one-to-one basis.[299]

The International Court of Justice has made it clear in several key cases that the principles of "necessity" and "proportionality" are essential when evaluating whether a state's use of force can be justified as "self-defense under jus ad bellum". In the Nicaragua case, the Court explained that even when a state faces an armed attack, any response must still meet the standards of necessity and proportionality and found that United States' actions failed to meet these conditions however the Court did not make a clear explanation on which approach its taking when assessing the proportionality test.[300] This view was later reaffirmed in the Oil Platforms case, where the Court stated that even if the attacks on United States vessels could be seen as armed attacks, the United States response still needed to be necessary and proportionate.[301] The same approach was taken in DRC v. Uganda, where the Court found that Uganda did not prove its actions met either the necessity or proportionality test, and therefore could not rely on self-defense as a legal justification.[302] These cases show that necessity and proportionality are not just secondary requirements, but the core elements that must be satisfied for a lawful exercise of self-defense under Article 51 of the UN Charter.

The ICJ has maintained the same approach in its advisory opinions. For example, in its Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons, the International Court of Justice also addressed the principles of necessity and proportionality in the context of self-defense.[303] The Court acknowledged that the inherent right of self-defense under Article 51 of the UN Charter applies even in extreme cases, but it stressed that any use of force in response to an armed attack must still meet the criteria of necessity and proportionality regardless of the

---

[296] *Id*. at 207.
[297] *Id*. (with further citations)
[298] Natalia Ochoa & Esther Salamanca-Aguado, *Exploring the Limits of International Law Relating to the Use of Force in Self-Defence,* 16 Eur. J. Int'l L. 499, at 520 (2005)
[299] Ruys, supra note 75, at 207.
[300] *Nicaragua Judgment*, supra note 97, para 237.
[301] *Oil Platforms Judgment*, supra note 191, para 76.
[302] *DRC v. Uganda Judgment*, supra note 160, para 147.
[303] Sara Fallegård, *The ICJ Advisory Opinion on the Israeli Wall,* at 31-32 (unpublished student paper, Univ. of Lund, Faculty of Law [2008]).

weapons used.[304] This suggests that even in extreme self-defense situations, the legal limits imposed by necessity and proportionality still apply. The Court stated that the use of nuclear weapons might be lawful in extreme circumstances of self-defense where the very survival of a state is at stake but it carefully highlighted that even the use of nuclear weapons in self-defense would still need to satisfy the legal tests of Article 51.[305] Similarly in the Wall Advisory Opinion, the International Court of Justice discussed the limits of self-defense in international law, particularly under Article 51 of the UN Charter. The Court acknowledged that Israel had invoked its right to self-defense in justifying the construction of the wall but ultimately rejected this argument. The Court stated that Article 51 only applies when there is an armed attack by another state, and since Israel did not claim that the attacks originated from a foreign state, the legal conditions for invoking self-defense were not met.[306] While the opinion did not go into detailed analysis of necessity and proportionality in this case, it implicitly reinforced the idea that these principles must be applied within a clear legal framework meaning that firstly there must be an armed attack attributable to another state. The Court's conclusion highlights that necessity and proportionality cannot even be considered unless the threshold requirement of an armed attack by a state is satisfied.

3.6.5 Core Principles of Self-Defense in Cyber Context

Applying necessity, immediacy, and proportionality to cyber-attacks can be tricky, since identifying the real perpetrator often takes longer than in conventional armed attacks, and the immediacy principle can be debated when there is a time gap between the original attack and the response.[307] Jensen explains that the United States has addressed this attribution issue in its Rules of Engagement by allowing defensive force to be used based on the characteristics of the target, rather than on confirmed identification of the attacker.[308] This approach appears to conflict with the Department of Defense's earlier position in 1999, which recognized that lawful self-defense requires proper attribution.[309] Schmitt also discusses this in Bellum Americanum noting that 21st century attacks often originate from non-state actors. He argues that the identification process for such attackers should be adapted or that the rules governing lawful

---

[304] *Nuclear Weapons*, supra note 179, para 41.
[305] *Id*., para 46.
[306] Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136, para 139 (July 9).
[307] Heather Harrison Dinniss, *Cyber Warfare and the Laws of War,* at 103 (Cambridge Univ. Press 2012), https://research.ebsco.com/linkprocessor/plink?id=074b99e4-1240-3c32-ab0b-c23ef8fb66f8.
[308] Jensen, supra note 205, at 235.
[309] U.S. Dep't of Def., Office of the Gen. Counsel, *An Assessment of International Legal Issues in Information Operations,* at 22 (May 1999), https://fas.org/irp/eprint/io-legal.pdf.

responses should be more flexible.[310] Roscini on the other hand strongly opposes to the idea saying that adopting this approach would be illogical even before being illegal as there cannot be a self-defense if you do not know who you are defending yourself against.[311]

Another issue that needs to be taken into consideration is that what kinds of peaceful or non-use of force actions can be taken before invoking the right of self-defense. In Rule 72, the Manual highlights that if cyber-defense systems are sufficient to stop a cyber-attack, then retaliatory actions such as hacking back, causing damage, or destroying infrastructure would be unlawful.[312] Under Article 51, self-defense against an armed attack must meet the requirements of necessity, proportionality, and immediacy. Necessity asks whether non-forceful alternatives exist, while proportionality limits the response to what is reasonably required without demanding symmetry of means. So, a cyberattack could, in principle, justify a kinetic response. Immediacy is interpreted flexibly, allowing a state to act even days or weeks after the initial incident.[313] The Manual emphasizes that the assessment of necessity and proportionality should be made from the perspective of the victim state for example in circumstances where the perpetrator state has stopped the attack but the victim state is not aware of that that would not make the self-defense action unlawful.[314]

The Manual mentions the accumulation of effect theory meaning that instead of a single highly effective cyber-attack smaller scaled but connected attacks coming from the same source can reach the required threshold for self-defense under Article 51.[315] This is particularly important for evaluating the proportionality of the self-defense– as explained earlier this aligns with the principle in jus ad bellum perspective as the overall effect of the armed attack should be taken into consideration. Imagine an adversary launches multiple coordinated cyber-attacks targeting a country's power grid, water supply systems, and emergency services over a short period. The attacks simultaneously cause widespread blackouts, disrupt access to clean water, and incapacitate emergency response systems, leading to severe harm to civilians and critical infrastructure. Even if each individual cyber operation might not meet the threshold of an armed attack, the combined and simultaneous effects clearly create the kind of destruction and

[310] Michael N. Schmitt, *Bellum Americanum: The U.S. View of Twenty-First Century War and Its Possible Implications for the Law of Armed Conflict*, 19 Mich. J. Int'l L. 1051, at 1074 (1998).
[311] Roscini, supra note 176, at 119.
[312] *Tallinn Manual 2.0,* supra note 26, rule 72.
[313] Jay P. Kesan & Carol M. Hayes, Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace, 25 HARV. J. L. & TECH. 429, at 526, (Spring 2012).
[314] Tallinn Manual 2.0, supra note 26, rule 14.
[315] *Id*. art 71 para 11.

disruption recognized under Article 51 as an armed attack, thereby justifying self-defense measures.[316]

Cyber-attacks usually do not affect its target in a short amount of time when its launched and they produce both direct and indirect consequences. As a result of this uncertain nature of cyber-attacks they are harder to evaluate the proportionality of the cyber-attack response in self-defense.[317] Proportionality assesses the extent and type of force, including cyber operations, that a state may lawfully employ when acting in self-defense. This principle constrains the appropriate level of force is determined by what is necessary to effectively repel the ongoing attack or to prevent an imminent one.[318] Depending on the circumstances, a greater or lesser degree of force may be justified to achieve a successful defense. The force that has been used in self-defense might be non-cyber if it fits the proportionality of the overall effect of the original attack.[319] To give an example that is aligned with the Tallinn Manual's explanation of the proportionality principle let's say a state suffers a cyber-attack that temporarily disables its water supply management system, causing limited disruption to residents but no widespread physical damage. A proportionate response under jus ad bellum would not involve launching a large-scale offensive cyber operation that shuts down the attacker's entire national grid. Instead, a proportionate response could involve a targeted cyber operation that neutralizes the specific malicious code, blocks further intrusions, or disables the attacker's ability to continue the assault.

Under international law principle of immediacy means a defensive action must occur sufficiently close to the original attack so that it is recognized as a direct response rather than delayed retaliation or punishment.[320] In the context of cyber-attacks, assessing immediacy can be challenging because the effects of a cyber operation often unfold over time, and identifying the actual perpetrator may take days or even weeks. In cyber self-defense, the end of an attack does not automatically mean the situation is over.[321] If a state has reason to believe additional cyber operations are likely, it can treat the attacks as part of a continuing campaign and respond accordingly.[322] If no further attacks are expected, any additional action could be seen as

[316] Michael Gervais, Cyber Attacks and the Laws of War, 1 J.L. & Cyber Warfare 8, at 60, (2012).
[317] Titiriga Remus, Cyber-Attacks and International Law of Armed Conflicts: A *Jus ad Bellum* Perspective, 8 J. Int'l Com. L. & Tech. 179, at 187 (2013).
[318] Tallinn Manual 2.0, supra note 26, rule 72 commentary; Nazanin Baradaran & Homayoun Habibi, Cyber Warfare and Self-Defense from the Perspective of International Law, 10 J. POL. & L. 40, at 44, (2017).
[319] Dinniss, supra note 307, at 105.
[320] Tallinn Manual 2.0, supra note 26, rule 73 para 12.
[321] Id., rule 73 para 13.
[322] Matthew Hoisington, Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense, 32 B. C. INT'l & COMP. L. REV. 439, at 450, (Spring 2009).

retaliation rather than legitimate self-defense. In practice, immediacy is judged by what is reasonable given the circumstances at the time.

Cyber-attacks can also be slow to reveal their origin or impact.[323] For example, sophisticated malware like Stuxnet caused damage long before its source or full effects were understood. In such situations, a state may still act in self-defense if it is reasonable to respond promptly despite these uncertainties. Imagine a state's national energy grid control systems start experiencing unexplained slowdowns and glitches. At first, engineers think it's just a technical fault. Over the next 48 hours, the glitches spread to multiple power plants, and in one region the system suddenly overloads, causing a localized blackout. Investigators later discover that malicious code has been quietly sitting in the network for months, but it only became active now, triggered remotely by the attackers. The problem is, no one can be sure whether this blackout was the final stage of the attack or just a test run for something bigger in the coming days. Now, if the principle of immediacy says self-defense should be exercised right after the attack, the question becomes: when did the "attack" occurred here? Was it the moment the malware was planted months ago, the moment the blackout happened, or when analysts finally figured out this was an external hostile act?

Taken together, these principles illustrate the tension between adapting existing jus ad bellum rules to cyberspace and maintaining the clarity needed for lawful self-defense. While necessity and proportionality can be flexibly applied, immediacy remains the most context-sensitive, especially when attribution and impact unfold gradually, as is often the case in cyber operations.

3.7. Problem of Attribution

Attribution plays a crucial role in determining whether a state may lawfully invoke the right of self-defense under Article 51 of the United Nations Charter, as it establishes whether a cyberattack can be legally imputed to a state. Since self-defense under international law must be directed against a responsible state actor, attribution forms the basis of the *ratione personae* element, identifying who the use of force is directed against. One of the main issues that we face when evaluating the right of self-defense is attributing the internationally wrongful acts to a State and without attribution, the legal framework for invoking self-defense cannot be properly applied. Although the concept of attribution originates in the broader law of state responsibility, this thesis focuses on attribution as it is necessary to establish the legal permissibility of using force in self-defense. It does not address the technical or evidentiary

[323] Tallinn Manual 2.0, supra note 26, rule 73 para 14.

challenges involved in proving attribution but rather explains the general international rules that determine when a cyber operation can legally be treated as an act of the state.

3.7.1 International Law Aspects of Attribution

Attribution in international law determines when conduct can be legally considered an act of a State, thereby engaging its international responsibility. The Declaration on Principles of International Law concerning Friendly Relations affirms that States have a duty not to organize, instigate, assist, or participate in acts of armed force by irregulars, armed bands, or other groups to invade the territory of another State.[324] The authoritative framework for attribution is set out in the Articles on the Responsibility of States for Internationally Wrongful Acts (ARSIWA), adopted by the International Law Commission in 2001. Although the Articles on the Responsibility of States for Internationally Wrongful Acts (ARSIWA) have not entered into force as a treaty and are formally non-binding, they are widely regarded as reflecting customary international law. This view is reinforced by their frequent invocation by the International Court of Justice and other international tribunals as authoritative guidance on the law of state responsibility. ARSIWA codifies customary rules on when conduct is attributable to a State and the circumstances precluding wrongfulness.[325] According to ARSIWA States are responsible for their internationally wrongful acts which constitutes a breach of customary international law attributable to the State.[326] That international law can take its reasoning from both the customary international law and treaty law.[327]

Under the Articles on the Responsibility of States for Internationally Wrongful Acts (ARSIWA), attribution can arise in a variety of circumstances. Article 4 covers conduct of the State's organs or personnel acting in that capacity.[328] This principle ensures that actions by official bodies, such as military cyber units, remain attributable even if carried out without express political authorization. Article 5 extends attribution to entities empowered by the State to exercise elements of governmental authority.[329] In practice, this could include private contractors managing cyber operations under a State's instruction, or public–private arrangements that place critical infrastructure control in private hands but under State mandate.

---

[324] *Declaration on Friendly Relations,* supra note 5, at 123.
[325] ARSIWA, supra note 154, para 1, 3.
[326] *Id.*, art.2.
[327] *Id.,* art.2.
[328] *Id.* art.4.
[329] *Id*., art 5.

Article 6 concerns organs of one State placed at the disposal of another.[330] Attribution applies when one State places its organs at the disposal of another, provided the receiving State directs their conduct within the scope of the functions conferred. It can be a foreign cyber unit operating under another State's military command structure. Article 7 provides that conduct remains attributable even when an organ exceeds its authority or contravenes instructions.[331] This prevents States from evading responsibility on the basis of internal disciplinary breaches. Article 8 addresses acts of non-State actors acting under the instructions, direction, or control of the State,[332] while Article 9 covers situations where persons exercise governmental authority in the absence or default of official authorities.[333]

Article 10 concerns conduct by movements that become the new government of a State or form a new State.[334] In such cases, their prior conduct becomes retrospectively attributable. Article 11 allows attribution where a State acknowledges and adopts conduct as its own after the fact.[335] These provisions, read alongside the remaining parts of ARSIWA that establishes the existence of a breach, lawful circumstances precluding wrongfulness, and related consequences, form the core framework for determining when conduct can be legally considered an act of the State.

Article 8 of the ARSIWA which is the main topic of this thesis, states that the non-state actors' actions needs to meet a certain criteria in order to be attributable to a State.[336] The conditions that can create a link between a non-state actor's action and a State have been argued over the course of time. Brownlie explained that States' governments can; organize the non-state groups inside of its own territory to violate other States' sovereignty, organize the non-state groups outside of its own territory to use them to violate other States' sovereignty, supporting the groups while that groups are conflicting with other State, tolerate those groups in its own territory even though being fully aware of their organizations in its own territory or their wrongful actions towards other States, not be able to stop those groups' violence towards the other State.[337] However as he highlighted all of those possibilities invoke different levels of responsibilities.[338] Only actions that are attributable to the State can raise a state's responsibility.

---

[330] *Id*., art 6.
[331] *Id*., art 7.
[332] Id., art 8.
[333] Id., art 9.
[334] Id., art 10.
[335] Id., art 11.
[336] Ruys, supra note 75, at 419.
[337] Ian Brownlie, International Law and the Activities of Armed Bands, 7 INT'L & COMP. L.Q. 712, at 713 (1958).
[338] *Id*.

If an armed group does not act based on a State's instructions or if the State is not involved in controlling that armed group their actions cannot be attributed to that State.[339]

Regarding of the involvement of the State government when the connection between the State and the group may be treated as a de facto agent of the State thus that groups actions targeting the victim state would be considered as the armed attack.[340] When States are not willing to or be able to prevent the attacks that are coming from their territory, this can constitute the violation of due diligence obligations.[341] The ICJ has acknowledged that the Declaration on Friendly Relations constitutes customary law.[342] In DRC v. Uganda judgment the Court has examined both incidents, the armed groups outside of Ituri[343] and the armed groups on Zaire[344], stated that inability on its own does not constitutes a violation of customary international law with regards to Friendly Relations Declaration where States failure of duty of prevention would invoke State responsibility.

The International Court of Justice has examined whether the usage of non-state actors constitute a violation of prohibition of use of force in the Nicaragua Judgment. In paragraph 205 of the judgment the Court emphasized that intervention is prohibited when it uses coercive methods, including support for subversive or terrorist armed groups operating within another state so if those acts include use of force they would be considered under the Declaration of Friendly Relations.[345] In the Nicaragua case, Nicaragua claimed that the United States had violated the prohibition on the use of force by supplying, financing, and training armed groups to act against Nicaragua.[346] The United States justified these actions as a form of collective self-defense on behalf of El Salvador. However, the ICJ held that, even if the collective self-defense justification of the US was accepted, the acts of training and arming the contras already amounted to a breach of the prohibition on the use of force.[347] Later the Court did not hold the United States accountable for the actions of those armed contras due to lack of effective control of the United States over the contras.[348] The court acknowledged the heavy support of the United States to contras but cannot found the control to the degree that would be assumed that

---

[339] ARSIWA, supra note 154, art 8, para 1.
[340] Ruys, supra note 75, at 423.
[341] Joanna Kulesza, *Due Diligence in International Law,* at 136-137 (Brill Nijhoff 2016) [ISBN 978-90-04-28310-7].
[342] DRC v. Uganda Judgment, supra note 160, para 162.
[343] *Id*., para 247.
[344] *Id*., para 300-301. The court has highlighted that the area where the armed groups are located is a mountain and Congo did not have physical control over that mountain.
[345] Nicaragua Judgment, supra note 97, para 205.
[346] Id.
[347] Id., para 228.
[348] Id., para 105.

the contras were "acting behalf of the United States."[349] The reasoning for this decision is explained as, in order to attribute the groups actions to the State the link between them needs to be more major than just financing or training the contras but supporting them to a point where the contras are dependent to the United States and the United States would need to have control over every action of the contras.[350] This shows that responsibility does not always require direct attribution; states can be held accountable for their support of armed groups without the need to establish a direct nexus for attribution.[351]

However in Prosecutor v. Tadić Case, International Criminal Tribunal for the former Yugoslavia (ICTY) found the ICJ's approach to effective control test is being too strict and stated that the logic behind the state responsibility is to prevent States from using private individuals to conduct armed attacks.[352] The ICTY used the overall control test on the Bosnian Serb armed forces where the Federal Republic of Yugoslavia (FRY) had overall control over the armed forces and international law does not requires action based control or command in order to held the State accountable.[353] However in Article on State Responsibility, the Commission highlighted the differences between those two cases in front of the Courts where in Tadić Case the Tribunal was trying individuals for criminal responsibility; the ICJ on the other hand was trying to answer State responsibility under the UN Charter.[354] This interpretation was subsequently reaffirmed by the ICJ in Bosnia and Herzegovina v. Serbia and Montenegro, where the Court found that the atrocities committed at Srebrenica could not be attributed to Serbia because there was no evidence that Serbia had exercised effective control over the operations in which the massacres occurred.[355] By confirming Nicaragua and rejecting ICTY's broader overall control standard in the context of State responsibility, the Court reinforced the high evidentiary threshold required to link the conduct of non-State actors to a State under Article 8 ARSIWA. Regardless of whether the effective control or overall control test is applied, a certain level of gravity must be met for a state's involvement with non-state actors to qualify their actions as an armed attack. This threshold is essential to trigger the right of self-defense under Article 51 of the UN Charter. Both the ICJ and the ICTY have made clear that merely

[349] Id.
[350] Id., para 109.
[351] Michał Kowalski, Armed Attack, Non-State Actors and a Quest for the Attribution Standard, 30 Pol. Y.B. Int'l L. 101, at 110 (2010), https://ssrn.com/abstract=2173000.
[352] *Prosecutor v. Duško Tadić*, Case No. IT-94-1-A, Appeals Chamber, Int'l Crim. Trib. for the Former Yugoslavia, para 117, (July 15, 1999).
[353] Id., para 145.
[354] ARSIWA, supra note 154, art 8, para 5.
[355] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Monten.)*, Judgment, 2007 I.C.J. 43, para 400, (Feb. 26).

supporting or financing armed groups is not sufficient to attribute their actions to a state. Instead, they require the state to exercise a specific level of control over the non-state actors involved.[356]

Effective control was widely accepted until 9/11 when Al Qaeda attacked the United States, where the attacks have attracted all the attention UN Security Council have adopted a resolution which condemned the attacks.[357] The United States has claimed that these attacks have reached the armed attack threshold and, therefore, it will exercise its right of self-defense under the UN Charter.[358] The United States defended that Taliban was harboring the Al Qaeda's executives thus claimed that the attribution criteria has been met with that support without the need of effective control or even overall control.[359] Later on the United States gave an ultimatum to the Taliban where the United States have requested the extradition of Al-Qaeda leaders and the dismantling of their operations in Afghanistan stating that it was not open to discussion; however Taliban has rejected this request. On the following October 7th UK and the United States have started Operation Enduring Freedom on Afghanistan.[360] The operation has gained support from most of the international community. [361] For example, some scholars have argued that the Taliban was the de facto government at that time, and thus the operation can be considered under Article 9 of the Articles on State Responsibility, which allows states to use force when no state has effective control over the territory.[362] Regardless of the international support that the United States and the United Kingdom received for their operation, it does not satisfy the requirements of Article 8 or Article 11 of the Articles on State Responsibility. As regulated in the Article 8 of the Articles on State Responsibility a state must exercise effective control over the armed group in order to be held responsible for their actions however harboring Al-Qaeda does not amount to effective control.[363] Similarly Article 11 of the Articles on State Responsibility requires that state must acknowledge and adopt the conducts as its own and Taliban never acknowledged the attack of Al-Qaeda as its own.[364]

---

[356] Kowalski, supra note 351, at 107
[357] S.C. Res. 1368**,** U.N. Doc. S/RES/1368 (Sept. 12, 2001).
[358] Derek Jinks, *State Responsibility for the Acts of Private Armed Groups*, 4 Chi. J. Int'l L. 83, at 89 (2003).
[359] Ruys, supra note 75, at 477.
[360] CNN, "Bush Delivers Ultimatum," CNN (Sept. 21, 2001), https://edition.cnn.com/2001/WORLD/asiapcf/central/09/20/ret.afghan.bush/
[361] Letter dated 7 October 2001 from the Permanent Representative of the United States of America to the United Nations addressed to the President of the Security Council, U.N. SCOR, U.N. Doc. S/2001/967 (Oct. 15, 2001); Res. 1368, supra note 357.
[362] Yutaka Arai-Takahashi, Shifting Boundaries of the Right of Self-Defence—Appraising the Impact of the September 11 Attacks on Jus Ad Bellum, 36 Int'l Law. 1081, at 1097 (2002)
[363] Ruys, supra note 75, at 481. (with further citations)
[364] *Id*.

Creating a nexus between the State and the armed groups is necessary when the State does not accept the responsibility for the armed groups action. Having addressed the core principles of attribution under general international law, including relevant case law and the ILC's Articles on State Responsibility, it is now necessary to assess how these rules apply in the cyber domain.

3.7.2 Attribution in Cyberspace

The Tallinn Manual states that international law applies in cyberspace, including the attribution standards used to determine state responsibility for cyber operations.[365] According to Rule 14 of the Tallinn Manual 2.0, a cyber operation can be attributed to a state if it is carried out by its organs or by people or organizations operating under its guidance, control, or orders even if the act in question is not technically a cyber operation, the Manual also applies this attribution framework to certain cyber-related conduct, such as organizing, directing, or aiding a cyber operation.[366] Since neither intent nor physical damage is required for an act to be internationally wrongful, actions taken by states in cyberspace, whether in peacetime or during an international armed conflict, can still constitute internationally wrongful acts.[367] The attribution of actions that can categorize as internationally wrongful act, is sometimes related to geographical aspects of the State yet some of the cyber operations are not that strictly tied with geographical territory of States by their nature.[368]

On the other hand when a cyberattack originates from the territory of another state, Dinstein identifies four possible types of computer network attacks that can occur in such circumstances: the attackers might be on their own without any support of the host state; suspects can be located in the host state but not under control of that states' government; suspects that are located in the host state as well as under support of that states' government; lastly the attackers might be the official organs or personnel of the attacking state.[369] In the first two possibilities the host state is only under obligation to take necessary steps to stop or prevent those attacks based on its obligation of due diligence.[370] However the kinds of measures that can be taken to prevent such attacks are not in the scope of this thesis.

Schmitt mentions that one of the most challenging part of attribution of cyber-attacks in order to hold States responsible for hacking activities is creating a nexus between States authorities and non-official hacker groups because of Article 8 of the ARSIWA as the article lacks clarity

[365] Tallinn Manual 2.0, supra note 26, sec. 1 para 4.
[366] Id., Rule 14 para 8-9.
[367] Id., Rule 14 para 4.
[368] Id., Rule 14 para 11.
[369] Dinstein, *Computer Network Attacks,* supra note 203, at 103.
[370] *Id*.

on describing the required factors it counts.[371] Before starting to examine under which conditions the link between the State and non-state actors can be established it is important to put out the more easy to apply principles of attribution to computer network attacks. Using the categorization that Dinstein has showed in the last scenario where the attackers are the organs or personnel of the State it is evident that the State is responsible for its organs' actions– this also applies to computer network attacks so if the hackers are the personnel of a State than the actions that are committed by hackers would be attributed to the State.[372] As an example to the organs of States, some States have cyber operation centers under their military organizations employing hackers to use in cyberwarfare.[373] Also when a private entity is using governmental authority or power to function it will be treated as an organ of that State.[374] States are responsible of the behaviors of private entities that are acting on behalf of that State when this relationship is publicly open like a public-private partnership it is easier to hold that State responsible for the actions of that private entity.[375]

Attribution becomes a particularly important problem, as discussed under self-defense section, when discussing lawful self-defense against computer network attacks because of the fast-occurring nature of computer network attacks than conventional attacks which take some time whereas computer network attacks can occur within a second.[376] Jensen argues that even detecting the location of attackers is usually difficult, let alone discovering the hacker's identity, and that establishing a nexus between the hacker and a state is highly unlikely.[377] However, sometimes computer network attacks may carry the hacker's signature or a specific coding pattern that can be linked to a single state.[378] Under those circumstances, the attacks can be attributed to the perpetrator, including the state itself.[379]

In cases of cyber operations where the relationship between a non-state actor and a state is unclear, it becomes difficult to determine whether the actor is operating under the control of that state. As a result, such operations often remain unattributed under international law.[380] Pirker claims that the root problem in the difficulty of attribution of cyber-attacks are the lack

---

[371] Michael N. Schmitt, *Grey Zones in the International Law of Cyberspace*, 42 Yale J. Int'l L. Online, at 9 (2017), https://ssrn.com/abstract=3180687.
[372] Tallinn Manual 2.0, supra note 26, art 15.
[373] Roscini, supra note 176, at 96.
[374] Benedikt Pirker, *Territorial Sovereignty and Integrity and the Challenges of Cyberspace,* 189, at 210(Katharina Ziolkowski ed., NATO Cooperative Cyber Defence Centre of Excellence 2013).
[375] *Id*. This approach takes its' roots from the ICTY approach of overall control test.
[376] Jensen, supra note 205, at 232-233.
[377] *Id*., at 234.
[378] Dinniss, supra note 307, at 99.
[379] Id.
[380] Schmitt, *Grey Zones*, supra note 371, at 9.

of proof that can showcase the link between the State and the non-state actors.[381] In relation to the ICJ's approach that can be seen in its judgments the mere support or low level of control does not make the actions of that group attributable.

Beyond these legally grounded approaches, some scholars and policymakers have proposed a virtual attribution doctrine. This concept suggests that, in the cyber domain, states could respond to cyberattacks based on strong technical and circumstantial indicators, even where full legal attribution is lacking.[382] While it reflects the operational challenges of attribution in cyberspace, virtual attribution lacks a firm legal basis under existing international law and raises concerns regarding misuse and undermining state responsibility standards.[383] Accordingly, reliance on virtual attribution may not meet the threshold required for invoking the right of self-defense under Article 51 of the U.N. Charter. Virtual attribution is particularly discussed in cybersecurity literature, where the urgent and covert nature of cyber operations can make traditional legal attribution unworkable. Organizations such as Microsoft and research bodies like RAND have supported this approach, highlighting the need for timely and credible attribution mechanisms.[384] It remains a policy-oriented suggestion rather than a legally recognized attribution doctrine. When a States involvement of cyber operations led by a non-state hacker group stays at supporting or giving them technical equipment that they need would not be attributed to the State.[385] At this point Schmitt asks an important and unresolved question: if the non-state actors are really dependent to that State's support to a point that when the State withdraws that support the hackers become unable to continue their activities would this support still be counted as merely supporting since the State did not use effective control over the operations?[386] Although Schmitt does not offer a definitive answer, the question itself highlights a significant gap in the current attribution framework. It challenges the sufficiency of the effective control test, particularly on cyber operations where State involvement may be indirect but functionally essential. This uncertainty complicates the legal assessment of whether cyber operations by non-state actors can be attributed to States under international law.

For attributing the cyber actions of non-state actors to a State those three points should be established: the object that has been used in that cyber activity, the perpetrator that has been

---

[381] Pirker, supra note 374, at 211.
[382] Brad Smith, *The Need for a Digital Geneva Convention*, MICROSOFT ON THE ISSUES (Feb. 14, 2017), https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/.
[383] John S. Davis II et al., Stateless Attribution: Toward International Accountability in Cyberspace, RAND CORPORATION (June 2, 2017), https://www.rand.org/pubs/research_reports/RR2081.html.
[384] Kristen E. Eichensehr, *The Law and Politics of Cyberattack Attribution*, 67 UCLA L. Rev. 520, at 554-556 (2020).
[385] Schmitt, *Grey Zones*, supra note 371, at 10.
[386] Id., at 10.

committing those activities and the body of the State that perpetrator is working on behalf of.[387] The internet transfers data separately meaning that the original data that wants to be transferred is going to be broken into much smaller data and be sent through different layers of the internet when those smaller datas reach the target computer they build again in that host computer to become the original data.[388] The way the internet transfers data from one computer to another through multiple layers was originally intended to make user tracing difficult, which allows individuals or groups to conceal their tracks within those layers and supports anonymity.[389] In order to gain information on Lin's three points to attribute the cyber operations to a State the address of the original data, before it has broken into smaller data, should be known and moreover that address needs to belong to the actual perpetrators of that cyber operation.[390] There are techniques that allows to disrupt or redirect the IP address of the computer in which cases it would be almost impossible to reach the original attacker.[391] Dinniss highlights that 'masking' IP addresses also allowed States to reject the responsibility by defending that the attacks were not launched by them and they were framed by the original attackers.[392] Sometimes the attacks are made by using the VPN tunnels which changes all the journey that the main and end data takes.[393] Another method that is used frequently by hackers is the "onion routing" where the attackers uses multiple devices and every attack follows a different path between the devices before reaching to the final target.[394]

Even though the evidentiary issues are not in the scope of this thesis it is important to mention the party that has to bear the burden of proof is the State that claims its right of self-defense.[395] According to the ICJ's interpretation of burden of proof when a State faces a computer network attack and wants to invoke its right of self-defense under Article 51 of the UN Charter, it has to provide evidence of attribution regarding the country against which it intends to invoke its right of self-defense.[396]

---

[387] Tsagourias, *Cyberattacks,* supra note 171, at 233; Herbert Lin, *Attribution of Malicious Cyber Incidents: From Soup to Nuts*, 70 J. Int'l Aff. 75, at 89 (2016) ; Michael J. Glennon, *The Dark Future of International Cybersecurity Regulation,* 6 Journal of National Security Law and Policy, 563, at 567 (2012).
[388] Howard F. Lipson, *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues*, CMU/SEI Special Report No. 2002-SR-009, at 7 (Nov. 1, 2002).
[389] *Id*. at 13.
[390] Duncan B. Hollis, *An e-SOS for Cyberspace*, 52 Harv. Int'l L.J. 373, at 398 (2011).
[391] Lipson, supra note 388, at 13.
[392] Dinniss, supra note 307, at 100-101.
[393] Kriangsak Kittichaisaree, *Public International Law of Cyberspace*, Law, Governance and Technology Series 32, Springer, at 32 (2017).
[394] Id.
[395] *Oil Platforms,* supra note 191, para
[396] Dinniss, supra note 307, at 101.

It is important to remember however that attribution does not only carry technical difficulties when invoking the right of self-defense under Article 51 but also a political challenge in international law.[397] Banks notes, attribution is not merely a technical step but a legal prerequisite for determining whether a cyber operation may lawfully trigger a response under Article 51 of the UN Charter, since the right to self-defense can only be exercised against a state to which the act is imputable.[398] This legal complexity has been the subject of various international discussions, including those led by the United Nations Group of Governmental Experts (UN GGE). The GGE, established by the UN General Assembly, brings together experts to examine how international law applies to state behavior in cyberspace.[399] For example the failure of the Fifth UN GGE to produce a conclusive report, largely due to disagreements over the applicability of self-defense and international humanitarian law to cyber operations, has drawn criticism for reflecting political divisions rather than fostering legal clarity.[400] The difficulty in applying traditional attribution rules to cyberattacks often leads to a gap in the attribution of state responsibility, making it even more complex to satisfy the ratione personae requirement necessary for invoking lawful self-defense.[401] Schmitt also agrees that in order to invoke right of self-defense the attribution and armed attack discussions needs to be made thus the international rules on attribution, particularly the ones that are related to proxies, needs to be adjusted for computer network attacks so that States would not prefer using hackers to intervene to other State's territory.[402]

Chapter IV:

CASE STUDIES OF IMPORTANT CYBER-ATTACKS

So far, this thesis has discussed the main principles and international rules on self-defense and their application to cyber-attacks along with international legal frameworks that has aimed to regulate the cyberspace, such as Convention on Cybercrime and the Tallinn Manual. These

---

[397] Brian J. Egan, *International Law and Stability in Cyberspace*, 35 Berkeley J. Int'l L**.** 169, 176-177 (2017).
[398] William C. Banks, *Cyber Attribution and State Responsibility*, 97 Int'l L. Stud. 1039, at 1051 (2021).
[399] U.N. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Report of the Group of Governmental Experts, para 1–3, U.N. Doc. A/68/98 (June 24, 2013).
[400] Ann Väljataga, *Back to Square One? The Fifth UN GGE Fails to Submit a Conclusive Report at the UN General Assembly*, (September 1 2017), https://ccdcoe.org/back-square-one-fifth-un-gge-fails-submit-conclusive-report-un-generalassembly.html
[401] Nicholas Tsagourias & Michael Farrell, *Cyber Attribution: Technical and Legal Approaches and Challenges*, 31 Eur. J. Int'l L**.** 941, at 955 (2020).
[402] Michael N. Schmitt & Liis Vihul, *Proxy Wars in Cyberspace: The Evolving International Law of Attribution*, 1 Fletcher Sec. Rev. 53, at 67-68 (2014).

instruments have shown State's approach to computer network attacks especially in invoking the right of self-defense under the UN Charter. Chapter Five will examine how states have responded to computer network attacks in practice, and whether, according to scholarly opinion, such responses can be justified as acts of self-defense under Article 51 of the UN Charter. The case selection has been made accordingly that each incident involves widely recognized or strongly suspected state involvement and raises important legal questions regarding the use of force, the threshold of armed attack, and the conditions for invoking the right of self-defense.

4.1.Stuxnet Case

In 2010 Iranian nuclear centrifuges located in Natanz were attacked by a computer worm named Stuxnet, which was sophistically designed with the intention of collecting the data from the computers and destroy that data to make the centrifuges unable to work.[403] The sophistication of this virus was lying within its working mechanism where the virus would damage only certain target and not anywhere else of the computer.[404] A side note that is going to be important in the upcoming discussion of Stuxnet attack and its legal consideration will be that in 2008 the United States and Israel have made statements that they are not happy with Iran's new nuclear facilities.[405] After the discovery of the Stuxnet virus, Iranian authorities reported that approximately 60.000 computers were affected and over 9.000 centrifuges were damaged causing significant delays in Iran's nuclear program.[406]

The Stuxnet attack drew significant international attention. It was the first cyber operation to cause physical damage to a State's critical infrastructure, specifically a nuclear facility. This has led scholars to debate whether a computer worm could violate the prohibition on the use of force under the UN Charter and trigger the right of self-defense under Article 51. As explained above, there are different techniques for assessing whether the force used constitutes an armed attack. If the instrument-based approach is applied, a computer worm may not possess the characteristics of a traditional weapon; however, under the target-based approach, Stuxnet could be considered an armed attack under international law.[407] When applying Schmitt's method where if the consequences of the force are similar to conventional weapons the force that is used will considered as an armed attack; Hollis highlights that even the effects of Stuxnet

---

[403] John Richardson, *Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield*, 29 J. Marshall J. Computer & Info. L. 1, at 4 (2011).
[404] Id.
[405] Id., at 5.
[406] Sean Collins & Stephen McCombie, *Stuxnet: The Emergence of a New Cyber Weapon and Its Implications*, 7 J. Policing, Intell. & Counter Terrorism 80, at 87 (2012).
[407] Duncan B. Hollis, *Could Deploying Stuxnet Be a War Crime?*, *Opinio Juris* (Jan. 25, 2011), https://opiniojuris.org/2011/01/25/could-deploying-stuxnet-be-a-war-crime/

was great it did not effect Iran like a bomb or military invasion would effect; the target was so specific and the attack did not kill anyone therefore it might fall below the armed attack threshold.[408] Stuxnet is evaluated as a use of force under Rule 68 of the Tallinn Manual as the experts explained that physical damage and injury is not a precondition for use of force however the experts could not reach a consensus whether it meets the armed attack threshold.[409] Schmitt on the other hand supports that Stuxnet was indeed a weapon thus if the attributability of that act might have been made, it would trigger the right of self-defense under the UN Charter.[410] Jenkins argued the physicality of Stuxnet in *'Is Stuxnet Physical? Does It Matter?'* and claimed that even though the Stuxnet does not have a physicality it still needed to cross the border of Iran and attack the computers. He also states that when evaluating whether Stuxnet should be considered as a weapon the effects should be considered rather than the means.[411] Some scholars have argued that, in order to qualify a computer virus as an armed attack, its consequences should be irreversible. Stuxnet, they contend, did not cause irreparable damage nor long-term effects. However, some accept that Natanz could be considered a legitimate target due to the potential for significant damage.[412]

After the discovery of Stuxnet Iranian authorities did not accept any damage that has been done to nuclear centrifuges at first but later on the President Mahmoud Ahmadinejad have stated that some of their nuclear program was affected by the computer virus.[413] Later New York Times made an analogy where it revealed that Stuxnet was launched by the United States and Israeli intelligence agencies.[414] Iran officially attributed the Stuxnet attack to Israeli and American intelligence agencies reasoning that they had underlying political motives and especially targeted the nuclear program.[415] However neither the United States nor Israel have made any statements on accepting or rejecting the attack and there was no proof provided by Iran to make a proper attribution to either Israel or the United States.[416] Nonetheless both as

---

[408] Hollis, *Stuxnet be a War Crime*?, supra note 407.
[409] *Tallinn Manual 2.0*, supra note 26, at 342 para 10.
[410] Michael N. Schmitt, *Classification of Cyber Conflict*, 89 Int'l L. Stud. 233, at 240 (2013)
[411] Ryan Jenkins, *Is Stuxnet Physical? Does It Matter?*, 12 J. Mil. Ethics 68, at 75 (2013).
[412] James P. Farwell & Rafal Rohozinski, *Stuxnet and the Future of Cyber War*, 53 Survival 23, at 30,34 (2011).
[413] Gary D. Brown, *Why Iran Didn't Admit Stuxnet Was an Attack*, 63 Joint Force Q. 70, at 71 (2011).
[414] William J. Broad, John Markoff & David E. Sanger, *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*, N.Y. TIMES (Jan. 16, 2011), https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html. ; David E. Sanger**,** *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES (June 1, 2012), https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html
[415] Efrony, supra note 45, at 599. ; *RNA: Stuxnet a Product of US and Israel*, Jpost.com Staff, *Jerusalem Post* (Apr. 16, 2011), https://www.jpost.com/breaking-news/irna-stuxnet-a-product-of-us-and-israel (lastly visited March 21 2025)
[416] Dennis Broeders, Els de Busser, Fabio Cristiano & Tatiana Tropina, Revisiting Past Cyber Operations in Light of New Cyber Norms and Interpretations of International Law: Inching towards Lines in the Sand?, 7 J. Cyber Pol'y 97, at 100 (2022).

regards the problem of attribution and speculations that whether Stuxnet could constitute an armed attack or not, Iran could not use its right to self-defense under Article 51 of the UN Charter. Although no state has officially accepted responsibility for the Stuxnet operation, many scholars and investigators presume it was a state-sponsored act due to its technical complexity, strategic target, and political context.[417] This does not lessen the importance of Stuxnet, as it raises the question of whether cyber-attacks can be considered a weapon under international law, as Singer concluded "*Do you focus on the fact that this new kind of weapon permitted a preemptive attack? Or do you focus on the fact that the cyber strike caused far less damage than any previous comparable attack and was so discriminating it essentially gave new meaning to the term?*" (P.W. Singer, 2015).[418]

4.2. Power Grid and NotPetya Attacks

While Stuxnet raised early questions about covert cyber operations that cause physical damage, the cyberattacks on Ukraine's power grid and the global NotPetya incident brought new dimensions to the legal discussion particularly in terms of sustained disruption, economic consequences, and attribution linked to ongoing armed conflict.

4.2.1 Power Grid Attacks

Two highly advanced cyberattacks carried out by Russian hackers targeted Ukraine's power grids in 2015 and 2016, with the 2015 attack severely disrupting the country's electrical infrastructure by compromising industrial control systems and causing widespread blackouts.[419] The attacks against Ukraine's power grids are considered to be the first cyber-attack that has aimed at power grids.[420]

The attacks were sophistically planned denial of service attacks (DoS) and the 2015 attack lasted 6 months.[421] Those attacks have resulted in 225.000 individuals losing their connection in their telecommunications.[422] The United States Department of Homeland Security has helped

---

[417] Panayotis A. Yannakogeorgos & Eneken Tikk, *Stuxnet as Cyber-Enabled Sanctions Enforcement*, in 2016 Int'l Conf. on Cyber Conflict (CyCon U.S.) 1, at 2 (IEEE 2016).
[418] P.W. Singer, *Stuxnet and Its Hidden Lessons on the Ethics of Cyberweapons*, 47 Case W. Res. J. Int'l L. 79, at 85 (2015).
[419] ICS-CERT, *Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case,* at 1,3 (Mar. 18, 2016), https://us-cert.cisa.gov/sites/default/files/documents/ICS-Cyber-Attack-Ukraine-Defense-Use-Case-S508C.pdf.
[420] Andrea Peterson, *Hackers Caused a Blackout for the First Time, Researchers Say*, Wash. Post (Jan. 5, 2016), https://www.washingtonpost.com/news/the-switch/wp/2016/01/05/hackers-caused-a-blackout-for-the-first-time-researchers-say/
[421] Afra Ansaria, *A Decision Model on Optimising Cybersecurity Controls Using Organisation Preferences,* at 50 (June 2021) (unpublished Master's thesis, Mass. Inst. of Tech.) (on file with Mass. Inst. of Tech. Libraries).
[422] Donghui Park & Michael Walstrom, *Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks* (Oct. 11, 2017), Henry M. Jackson School of Int'l Studies, Univ. of Wash.,

Ukraine to investigate the attacks and have founded that the attacks were launched from a Russian hacker group named Sandworm, however the United States have not officially attributed the power grid attacks to Russian government since they could not find any link that ties Sandworm to Russia.[423] States did not made any official attributions to Russia including Ukraine and the reason for that is the attacks were not in the threshold of armed attack and was particularly designed that way so that international responsibility requirements would not have risen.[424] The ones that were affected by the power grid attacks were private infrastructures in Ukraine and the Tallinn Manual claims that the private infrastructure will be covered under States sovereignty as well.[425] The attacks have occurred during an armed conflict between Russia and Ukraine thus it could have been considered under that armed conflict and could be included in Russia's use of force campaigns.[426] The discussion have been made especially under international humanitarian law where scholars like Schmitt and Tsagourias argued that those attacks could have been counted under Article 49 of the Additional Protocol I of Geneva Conventions however the aim of this thesis is to evaluate the jus ad bellum rules, thus in regards to states right of self-defense.[427]

4.2.2 NotPetya Cyber-Attack

After the power grid attacks Ukraine has faced a cyber-attack in 2017, NotPetya, which was launched by Russian hackers allegedly backed by the Russian government, initially targeting Ukrainian accounting software. The malware quickly spread globally through secondary attacks, causing an estimated 10 billion dollars in damages and making NotPetya one of the most costly cyberattacks in history.[428] NotPetya was designed to mimic the ransomware Petya and distributed through the Ukrainian accounting software company MEDoc; however, it functioned as a wiperware, permanently destroying data rather than merely encrypting it for

https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/ (last visited March 15 2025).

[423] Broeders, supra note 416, at 109.

[424] Id. ; Marie Baezner, *Hotspot Analysis: Cyber and Information Warfare in the Ukrainian Conflict*, Version 2, at 13-14 (Oct. 2018), Risk & Resilience Team, Ctr. for Sec. Studies (CSS), ETH Zürich

[425] Tallinn Manual 2.0, supra note 26, rule 2.

[426] Baezner, supra note 424, at 17.

[427] To have more information on Russia's cyber interference to Ukraine see: Michael N. Schmitt & Liis Vihul, *Respect for Sovereignty in Cyberspace* (text originally titled *Sovereignty in Cyberspace: Lex Lata Vel Non?*), 95 Tex. L. Rev. 1639 (2017); Nicholas Tsagourias, *Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace*, Univ. of Sheffield Legal Rsch. Pap. No. 159652 (Apr. 17, 2019)

[428] Josephine Wolff, *How the NotPetya Attack Is Reshaping Cyber Insurance*, Brookings (Dec. 1, 2021), https://www.brookings.edu/articles/how-the-notpetya-attack-is-reshaping-cyber-insurance/ (last visited March 15, 2025).

ransom.[429] Although the malware specifically targeted MEDoc users, it caused global disruption due to the widespread use of the software, and it was primarily built on two tools: EternalBlue and Mimikatz.[430] EternalBlue is a malware tool originally developed by the United States National Security Agency and leaked in early 2017, it exploits a vulnerability in a Windows protocol that allows attackers to remotely execute malicious code on unpatched systems.[431] Mimikatz is a program that enables hackers to extract passwords from a system's RAM. Together, these tools gave NotPetya the ability to spread rapidly and compromise secure networks.[432]

The impact of NotPetya was not limited to Ukraine, on the same day, it spread to many countries, including the United States and parts of Europe, and affected several companies.[433] Officials from some victim states claimed that the Russian government should be held responsible, arguing that the malware was too advanced to be developed without state involvement and that the hackers were allegedly funded by Russia.[434] However, the Russian Ministry of Foreign Affairs denied these claims.

Again, with regards to NotPetya's legal evaluation, it was argued under international humanitarian law just like the power grid attacks. However, if we evaluate such autonomous cyber-attacks under jus ad bellum, the existing regulations are not sufficiently clear to determine liability or legality when the virus operates independently.[435]

4.3.WannaCry Case

Petya was not the only computer virus that has originated from EternalBlue, it was faced again in the same year, 2017, WannaCry virus has affected over 150 State across the world and thousands of computer systems including United Kingdom's healthcare system.[436] WannaCry was a ransomware that infected computers running the Windows operating system, encrypting users' data and demanding payment for access.[437] Victims were initially asked to pay 300 USD

---

[429] Andy Greenberg, *The Untold Story of NotPetya — The Most Devastating Cyberattack in History*, *Wired* (Aug. 22, 2018), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world
[430] *Id*.
[431] Sean Steinberg, Adam Stepan & Kyle Neary, *NotPetya: A Columbia University Case Study*, SIPA Case Study No. 21-022.1 (Columbia Univ. Sch. Int'l & Pub. Affairs, Oct. 2021)
[432] *Id*.
[433] Broeders, supra note 416, at 117.
[434] Sarah Marsh, *US Joins UK in Blaming Russia for NotPetya Cyber-Attack*, *The Guardian* (Feb. 15, 2018), https://www.theguardian.com/technology/2018/feb/15/uk-blames-russia-notpetya-cyber-attack-ukraine (last visited March 16, 2025).
[435] Broeders, supra note 416, at 119- 120-121.
[436] Da-Yu Kao & Shou-Ching Hsiao, *The Dynamic Analysis of WannaCry Ransomware*, in Proc. Int'l Conf. on Advanced Communications Technology (ICACT), 159, at 159-160 (2018).
[437] Jakub Vostoupal, *Stuxnet vs WannaCry and Albania: Cyber-Attribution on Trial*, 54 Comput. L. & Sec. Rev. 106008, at 16 (2024)

in Bitcoin within three days, after which the demand increased to 600 USD.[438] The ransomware threatened to delete the encrypted data if payment was not made within seven days, but it was later discovered that access was not restored even when payments were made.[439] In December 2017, the United States publicly attributed the attack to North Korea.[440] The National Security Agency assessed that the WannaCry attack was carried out by a hacker group known as the Lazarus Group, which is also believed to be behind the 2014 cyberattack on Sony Pictures Entertainment.[441] Although this thesis does not examine the Sony incident in detail, it is worth noting that both attacks have been linked to the same group, which is reportedly backed by North Korea cause the Lazarus Group have demanded from the company to film a movie about North Korea's dictator Kim Jung Un.[442]

The WannaCry ransomware attack has also sparked legal debate over whether such cyber operations can meet the threshold of an armed attack under international law. Although the attack caused significant global disruption, especially by affecting essential public services like hospitals, it remains unclear whether the effects were serious enough to qualify as a use of force or an armed attack. As Eichensehr points out, cyber incidents like WannaCry often fall into a legal grey zone where they interfere with critical state functions but do not always rise to the level traditionally required for invoking self-defense.[443] In addition to the threshold issue, WannaCry raises questions about possible violations of state sovereignty and due diligence obligations, especially if the state involved either directly sponsored the attack or failed to prevent it.[444] Lastly, the attack highlights the ongoing challenges in legally attributing cyber operations to states, since open-source evidence may suggest state involvement but still fall short of meeting the international legal standards for attribution.[445]

---

[438] Shou-Ching Hsiao & Da-Yu Kao, *The Static Analysis of WannaCry Ransomware*, in *Proceedings of the 2018 20th International Conference on Advanced Communications Technology (ICACT)* 153, at 154 (IEEE 2018)
[439] Vostoupal, supra note 437, at 16.
[440] Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea, James S. Brady Press Briefing Room (Dec. 19, 2017), https://trumpwhitehouse.archives.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/
[441] Ellen Nakashima, *The NSA Has Linked the WannaCry Computer Worm to North Korea*, Wash. Post (June 14, 2017), https://www.washingtonpost.com/world/national-security/the-nsa-has-linked-the-wannacry-computer-worm-to-north-korea/2017/06/14/101395a2-508e-11e7-be25-3a519335381c_story.html (last visited March 16, 2025).
[442] To have more in depth information on Sony attack see: Sean Steinberg, Adam Stepan & Kyle Neary, *The Hacking of Sony Pictures: A Columbia University Case Study*, SIPA Case Study No. 21-0023.1 (Columbia Univ. Sch. Int'l & Pub. Affairs Oct. 2021), https://www.sipa.columbia.edu/sites/default/files/2022-11/Sony%20-%20Written%20Case.pdf
[443] Kristen Eichensehr, *Questions About WannaCry Attribution to North Korea*, Just Security (Dec. 19, 2017), https://www.justsecurity.org/49889/questions-wannacry-attribution-north-korea/.
[444] Id.
[445] Id.

As for the assessments on the whether WannaCry attack can be considered under Article 2(4) of the UN Charter Schmitt claimed that the attack has affected UK's healthcare systems which is considered as critical infrastructure. Even without that fact the WannaCry attack can be considered as a use of force since– as explained in the Tallinn Manual– destruction or injury is not a requirement for cyber operations to constitute use of force.[446] Schmitt also adds that even if attribution claims have been made there is not an open source that proves those claims, North Korea has denied the accusations.[447] For any self-defense claims regarding the WannaCry ransomware attack, many scholars argue that its disruptive effects, though significant, do not reach the gravity necessary to qualify as an armed attack. Furthermore, the principle of immediacy, which requires a self-defense response to be timely and directly linked to an ongoing attack, further limits the use of force as a lawful response.[448] Since WannaCry was a discrete incident that had ended before any retaliatory action could be considered, it fails to satisfy this immediacy requirement therefore it is unlikely that states such as the United Kingdom could invoke Article 51 to justify a use of force in self-defense against the WannaCry attack.[449]

CHAPTER V:

CONCLUSION

The cases that have been studied in the previous chapter reflect the different forms and consequences of cyber-attacks. Those incidents show that while some cyber-attacks cause important damage to critical infrastructure like it happened in the power grid attacks on Ukraine other can interfere with national security like how Stuxnet has effected Iran's nuclear facilities. However, some cyber-attacks may not meet the armed attack threshold that is required for invoking the right of self-defense under Article 51 of the UN Charter. The blurred lines between activities like espionage or use of force in cyberspace raise serious challenges for applying traditional jus ad bellum principles. Against this background, this thesis has sought to answer the central question of whether states may lawfully invoke the right of self-defense in response

[446] Michael N. Schmitt & Sean A. Fahey, *WannaCry and the International Law of Cyberspace*, Just Security (May 16, 2018), https://www.justsecurity.org/50038/wannacry-international-law-cyberspace/.
[447] Id.
[448] Efrony, supra note 45, at 635.
[449] Schmitt, *WannaCry*, supra note 446.

to cyberattacks, and under what conditions such a response would be consistent with international law.

As explored in this thesis, cyberattacks present a uniquely modern challenge to the international legal system, particularly when it comes to the right of self-defense. While the UN Charter's rules were created before the rise of cyberspace, states and legal scholars are actively working to interpret and apply these principles to this new domain. This raises the critical question at the center of this research: can states lawfully invoke their right to self-defense under international law in response to cyberattacks? States concern of cyber operation has grown over the years as cyber threats have emerged rapidly.[450] In order to solve the absence of universally binding legal framework Cooperative Cyber Defence Center of Excellence has been established by NATO aiming to regulate the operations in cyber domain.[451] NATO is not the only international organization that has concerns over cyber operations. The Council of Europe and European Union also developed other instruments to regulate cyber-crimes[452] and enhance the cooperations between States.[453]

Before making any legal assessment of cyber operations we must first understand the layered nature of cyberspace itself. As outlined in the Tallinn Manual, cyberspace consists of a physical layer, a logical layer, and a social layer.[454] This conceptualization helps clarify how cyberattacks may target different aspects of the digital domain and why this diversity complicates the application of traditional international legal norms, such as the prohibition on the use of force.[455] Article 2(4) of the UN Charter prohibits the threat or use of force, it does not define what "force" means in the cyber context. As a result, much of the legal reasoning has been shaped by analogy to traditional armed force, focusing on whether the effects of a cyber operation are comparable to armed attacks.[456] Cyber operations that interfere with critical infrastructures may have effects comparable to conventional attacks, however cyber operations do not always involve physical destruction.[457] However, legal uncertainty persists when such operations cause no visible damage, raising the question of whether non-physical harm alone can satisfy the criteria for a use of force.[458] Determining whether a cyber operation constitutes a use of force under Article

[450] Remus, supra note 317, at 179.
[451] CCDCOE, supra note 20.
[452] Amalie M. Weber, *The Council of Europe's Convention on Cybercrime*, 18 Berkeley Tech. L.J. 425, at 429 (2003).
[453] Regulation (EC) No. 460/2004, supra note 70.
[454] *Tallinn Manual 2.0,* supra note 26, at 11-13.
[455] Noah Simmons, *A Brave New World: Applying International Law of War to Cyber-Attacks*, 4 J.L. & Cyber Warfare 42, 52 (Winter 2014).
[456] Waxman, supra note 185, at 425.
[457] Id.
[458] *Tallinn Manual 2.0*, supra note 26, at 331.

2(4) depends on a range of contextual factors. The Congo v. Uganda judgment confirms that non-consensual interventions may amount to a use of force.[459] The Tallinn Manual 2.0 provides further guidance on how to assess the action as a use of force in a cyber context under Rule 69, stating that a cyber operation may amount to a use of force when its scale and effects are comparable to those caused by kinetic force.[460] This approach does not require physical destruction or injury but instead focuses on the consequences of the act, such as disrupting critical infrastructure or disabling essential state functions. By evaluating the impact rather than the means, Rule 69 offers a functional test that aligns with the evolving nature of cyber conflict.

To invoke the right of self-defense under Article 51 of the UN Charter, the underlying act must meet the threshold of an "armed attack."[461] As the Nicaragua judgment emphasized, not every use of force amounts to an armed attack. The Court makes a distinction between more serious acts and "mere frontier incidents," which do not trigger the right of self-defense.[462] As this thesis has demonstrated, and consistent with the ICJ's approach in the Nicaragua judgment, cyber operations must reach a certain scale and gravity in their effects to qualify as armed attack.[463] However, determining when a cyber operation crosses this threshold remains legally uncertain.[464] To solve this uncertainty, legal scholars have proposed different approaches to help determine whether the threshold under Article 51 has been met.

Instrument-based approach emphasizes the type of means employed in a cyber operation, suggesting that only those resembling traditional kinetic weapons can meet the armed attack threshold.[465] Target-based approach, on the other hand, shifts the focus to the object of the attack, arguing that operations directed at vital state functions or critical infrastructure may qualify as armed attacks even without kinetic force.[466] The widely accepted approach among legal scholars and in the Tallinn Manual 2.0 is the consequence-based approach. This approach assesses whether the effects of a cyber operation are comparable to those caused by conventional armed force.[467] While these approaches offer useful analytical tools, the lack of consensus reinforces the complexity of applying the right of self-defense in cyberspace and highlights the need for clearer legal standards. Even after a cyber-attack has passed this

[459] *DRC v. Uganda*, supra note 160, para 47.
[460] Tallinn Manual 2.0, supra note 26, Rule 69.
[461] *U.N. Charter*, supra note 140, art. 51.
[462] *Nicaragua Judgment*, supra note 97, para 191.
[463] Id.
[464] Waxman, supra note 185, at 435.
[465] Hollis, *Stuxnet be a War Crime?*, supra note 407.
[466] Id.
[467] David E. Graham, Cyber Threats and the Law of War, 4 J. NAT'l SEC. L. & POL'y 87, at 91, (2010).

threshold, the lawful invocation of self-defense under Article 51 is possible under strict principles set out by international law.[468]

The lawful exercise of self-defense under Article 51 of the UN Charter depends on several elements, including ratione personae (the identity of the attacker), ratione temporis (the timing of the response), and ratione materiae (the gravity and nature of the attack).[469] In this framework, self-defense can be exercised either individually or collectively. While individual self-defense allows a state to respond to an armed attack against itself, collective self-defense requires a request or consent from the state under attack.[470] Furthermore, states invoking self-defense are obliged to report such actions to the UN Security Council under Article 51.[471]

The right of self-defense under international law involves important temporal dimensions, commonly grouped into three categories: reactive, interceptive, and anticipatory self-defense. Reactive self-defense occurs after an armed attack has already taken place, while interceptive self-defense responds to an attack that has begun but is not yet complete.[472] Anticipatory self-defense, on the other hand, aims to prevent an imminent attack before it occurs.[473] These distinctions become difficult to apply to cyber operations due to the often hidden and delayed nature of cyber operations. Invoking the right of self-defense must also comply with principles of necessity, immediacy, and proportionality under international law. Necessity requires that self-defense should be the last resort when no peaceful alternatives exist[474], however this is complicated because of the uncertainty about the nature and scope of ongoing cyber operations. Immediacy requires that the response to an armed attack happens within a short time after the attack occurs.[475] When it comes to cyber-attacks, applying this principle becomes difficult. The time gap between the original cyber operation and the defensive response can raise questions about whether the response is still considered timely under international law. I think that, in cyber cases, immediacy should be linked to when the damage is actually noticed rather than when the attack was launched. Since detecting and tracing cyber operations is often slow and complex, focusing on the damage date feels more realistic and fair for allowing a state to respond in self-defense. Proportionality limits the response of the self-defense acts to what is

[468] *Nicaragua Judgment*, supra note 97, para 194; Dinstein, *War, Aggression and Self-Defense*, supra note 198, at 195.
[469] Ruys, supra note 75, at 220.
[470] Dinstein, *War, Agression and Self-Defense*, supra note 198, at 252.
[471] *U.N. Charter*, supra note 140, art 51.
[472] Ruys, supra note 75, at 327.
[473] Gill, supra note 246, at 363.
[474] Ruys, supra note 75, at 194.
[475] Van den hole, supra note 288, at 101.

necessary to stop the attack.[476] However, the effects of cyber-attacks may not be visible or immediate; therefore, deciding the necessary actions are harder to determine. These debates become more visible after 9/11 when the international community began to argue that the traditional principles of the Caroline doctrine should be applied more flexible.[477] Given the complexity of modern threats, strictly requiring an immediate attack might delay necessary responses and leave states vulnerable.

Even though attribution is not the focus of this thesis, it plays a critical role in determining whether a state can lawfully invoke self-defense under international law.[478] Identifying the attackers in computer network attack is harder than conventional armed attacks because States deny their involvement of the attack and most of the time acts through proxies to avoid attribution.[479] According to the International Court of Justice in the Nicaragua judgment, a state can only be held responsible if it exercises effective control over the actors and their specific operations.[480] However, this is a very high threshold and difficult to meet in cyberspace. Some have argued for a lower standard, like the overall control test applied by the ICTY,[481] but there is no consensus on which should apply in cyber cases. As a result, the attribution problem remains one of the most significant legal challenges to invoking the right of self-defense in response to cyberattacks.[482]

Looking at everything together it is clear that the current rules for self-defense and attribution work well on paper but they do not always fit the way cyber operations happen. The effects-based approach mostly focuses on the damage that has already occurred. In the cyber context I believe we should also think about what could reasonably be expected to happen. Some attacks might not cause immediate destruction, but they are designed in a way that could lead to major harm if not stopped early. This is especially true for operations against critical systems. Including foreseeability in the assessment would make it easier for states to act before the situation becomes unmanageable. For attribution the effective control test can be too strict for the realities of cyberspace. Cyber operations are often complex, and actors may hide behind many layers. A state may not direct every step but can still be closely involved in the operation.

[476] Ruys, supra note 75, at 206.
[477] Franck, supra note 271, at 433.
[478] Eichensehr, supra note 384, at 522.
[479] Tallinn Manual 2.0, supra note 26, at 89.
[480] Nicaragua Judgment, supra note 97, para 115.
[481] Tadić Judgment, supra note 352, para 145.
[482] Stephen Petkis, Rethinking Proportionality in the Cyber Context, 47 GEO. J. INT'l L. 1431, at 1456 (Summer 2016).

In such situations the overall control approach could give us a more realistic way to link cyber actors to states while still keeping the burden of proof high enough to prevent misuse.

These legal uncertainties are also visible in actual cyber incidents. As analyzed in this thesis, the attacks that were given as case study examples demonstrate both the disruptive potential of cyber operations and the difficulty in applying traditional self-defense frameworks to them. Stuxnet attack was a turning point for computer network attacks as it was the first attack that has led to the question whether cyber-attacks amount to an armed attack under Article 51 of the UN Charter.[483] It is also important in demonstrating the damaging potential of cyberattacks, as it targeted the Iranian nuclear program and damaged over 9,000 centrifuges.[484] That proved that a cyber-attack could provide a damage that is comparable to traditional conventional armed attacks.[485] In those aspects, Stuxnet challenged the prohibition on the use of force under Article 2(4) of the UN Charter, and further raised the question of whether cyber-attacks can reach the armed attack threshold required by Article 51 of the Charter.[486] The Tallinn Manual classified Stuxnet as a use of force. However, the Experts could not reach a consensus on whether the virus was sufficient to be considered an armed attack.[487] Iran publicly attributed the attack to the U.S. and Israeli intelligence agencies; however, due to the lack of formal evidence and the absence of acknowledgment by the U.S. and Israeli authorities, proper attribution could not be established.[488] For both its disruptive outcomes and legal challenges Stuxnet has opened a new chapter in cyberwarfare.

Two cyber-attacks on Ukraine's power grid in 2015 and 2016 disrupted communications and caused widespread blackouts across Ukraine.[489] The attacks are attributed to Russian hacker group however there was no public attribution that has been made by States.[490] Those incidents have shown the potential harm that cyber-attacks are capable of as the effects have lasted up to 6 months.[491] As those attacks have happened during the war between Russia and Ukraine, they are classified under Geneva Conventions and international humanitarian law.[492] Regardless of the area of law that has been applied the attacks raise important questions about attribution, legal thresholds, and the blurring line between civilian and military targets in cyberspace.

---

[483] Hollis Stuxnet be a War Crime?, supra note 407.
[484] Collins, supra note 406, at 87.
[485] Schmitt, *Classification of Cyber Conflict,* supra note 410, 240.
[486] Tallinn Manual, supra note 26, at 342.
[487] Id.
[488] Broeders, supra note 416, at 100.
[489] ICS-CERT, supra note 419.
[490] Ansaria, supra note 421, at 50.; Broeders, supra note 416, at 109.
[491] ICS-CERT, supra note 419, at 1-3.
[492] Schmitt, *Respect for Sovereignty in Cyberspace,* supra note 427.

Lastly, this thesis examined the NotPetya and WannaCry attacks as key examples of how cyber operations can originate from the same technical root but led to different legal and practical consequences. NotPetya caused extensive harm to financial systems and infrastructure. This raises questions about state responsibility and whether the attack reached the armed attack threshold.[493] WannaCry, by contrast, appeared less targeted and more financially motivated, yet still disrupted critical services, including the UK's National Health Service.[494] These examples were chosen because they show the varying legal complexities in assessing scale, intent, attribution, and ultimately, the possibility of invoking the right to self-defense under international law.

In response to the legal and practical challenges of asserting cyber self-defense, several initiatives have emerged to provide much-needed clarity. The Tallinn Manual 2.0 offers a structured legal commentary, though its nonbinding nature limits adoption.[495] The challenges surrounding the lawful exercise of self-defense in cyberspace have prompted several international proposals and initiatives aimed at clarifying how international law applies in this domain. Microsoft's 2017 proposal for a Digital Geneva Convention advocates for a multilateral treaty that commits governments to protecting civilians from nation-state cyberattacks during peacetime, drawing parallels to the Fourth Geneva Convention's protection of civilians during armed conflict.[496] A key component of Microsoft's proposal is the establishment of an independent, multistakeholder attribution organization, tasked with publicly identifying the perpetrators of cyberattacks to enhance accountability and deter future violations.[497] Complementing Microsoft's call for a multistakeholder attribution mechanism, RAND's Global Cyber Attribution Consortium proposes a structured framework for improving the accuracy, transparency, and reliability of attributing cyber operations to responsible state actors.[498] By providing a standardized methodology for assessing technical, contextual, and behavioral evidence, RAND's model aims to reduce misattribution and support the lawful exercise of self-defense in cyberspace, reinforcing the accountability goals envisioned by Microsoft's Digital Geneva Convention.[499]

Another important initiative aimed at clarifying the application of international law in cyberspace is the *Handbook on Developing a National Position on International Law and*

[493] Broeders, supra note 416, at 117.
[494] Kao, supra note 436, at 160.
[495] *Tallinn Manual 2.0,* supra note 26, at 1-2.
[496] Smith, supra note 382.
[497] Id.
[498] Davis, supra note 383, at 33-34.
[499] Id., at 27.

Cyber Activities, published in May 2025 by the NATO Cooperative Cyber Defence Centre of Excellence in collaboration with the University of Exeter and the Ministries of Foreign Affairs of Estonia and Japan.[500] The Handbook provides practical guidance for states to formulate or refine their official positions regarding how international law applies to cyber operations.[501] A key feature of the Handbook is its set of structured checklists, which prompt states to systematically consider legal, technical, and policy factors when developing their positions.[502] These checklists are designed to reduce ambiguity, promote internal consistency, and ensure that all relevant aspects of cyber operations, including thresholds for armed attacks and criteria for lawful self-defense, are carefully evaluated.[503] The Handbook's development involved consultations with officials from 46 states across four continents, ensuring a broad and inclusive perspective.[504] For the purposes of this thesis, the Handbook is particularly significant because it encourages states to articulate clear national positions, enhancing the predictability and legitimacy of responses to cyberattacks and supporting a more lawful and measured exercise of the right to self-defense.

These international efforts are important because they help create an environment where states are encouraged to respond to cyberattacks through lawful means rather than relying on proxies, which can obscure accountability and complicate attribution. Developing clearer thresholds for what constitutes a use of force and an armed attack in cyberspace by flexing the consequence-based approach to include the attacks that have potential to cause great harm and not wait for an actual loss of life happen. As well as improving the speed and reliability of attribution processes by adopting more flexible approaches, states would be better positioned to exercise their right of self-defense in a manner consistent with international law. This approach reinforces the fundamental objectives of the UN Charter, promoting both state security and the preservation of international peace and order.

As explained in this thesis, cyber operations that reach a certain scale and effect may qualify as armed attacks under international law under strict conditions. However, the lack of universally accepted definitions, evolving nature of cyber threats and the challenges of timely attribution and proportional response remain critical barriers to the reliable invocation of Article 51 of the UN Charter.[505] This thesis underlines the need for greater international consensus on

[500] Handbook on Developing a National Position on International Law and Cyber Activities: A Practical Guide for States, at 14, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), May 2025.
[501] Id., at 24.
[502] Id., at 21.
[503] Id., at 169.
[504] Id., at 6.
[505] Schmitt, *Grey Zones*, supra note 371.

the interpretation of existing legal norms in cyberspace, particularly regarding the threshold for an armed attack and the attribution of cyber operations.[506] In conclusion, while international law does not prohibit invoking self-defense against cyberattacks, the challenges that have been mentioned narrows its application in real cyber-attack incidents.

[506] Hathaway, supra note 4, at 877.

BIBLIOGRAPHY

Australian Gov't, *Cyber Security Strategy,* (Nov. 23, 2009), https://apo.org.au/sites/default/files/resource-files/2009-12/apo-nid19945.pdf.

Australian Gov't, *2023–2030 Australian Cyber Security Strategy,* (Nov. 22, 2023), https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf.

Arnold, Chloe. Russian Group's Claims Reopen Debate on Estonian Cyberattacks, *RFE/RL* (Mar. 30, 2009), https://www.rferl.org/a/Russian_Groups_Claims_Reopen_Debate_On_Estonian_Cyberattacks_/1564694.html.

Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), Judgment, 2005 I.C.J. 168, (Dec. 19).

Akande, Dapo. & Thomas Liefländer, *Clarifying Necessity, Imminence and Proportionality in the Law of Self-Defence*, 107 EJIL 563 (July 2013)

Arai-Takahashi, Yutaka. Shifting Boundaries of the Right of Self-Defence—Appraising the Impact of the September 11 Attacks on Jus Ad Bellum, 36 Int'l Law. 1081 (2002)

Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Monten.), Judgment, 2007 I.C.J. 43 (Feb. 26).

Afra Ansaria, *A Decision Model on Optimising Cybersecurity Controls Using Organisation Preferences* (June 2021) (unpublished Master's thesis, Mass. Inst. of Tech.) (on file with Mass. Inst. of Tech. Libraries).

Barlow, John Perry. *A Declaration of the Independence of Cyberspace*, 18 Duke L. & Tech. Rev. 5, (2019) (reprinting 1996 version)

Baradaran, Nazanin & Homayoun Habibi, Cyber Warfare and Self-Defense from the Perspective of International Law, 10 J. POL. & L. 40, (2017).

Brownlie, Ian. *The Use of Force in Self-Defense*, 37 Brit. Y. B. Int'l L. 183 (1961).

Braman, Sandra. *Cyber Security Ethics at the Boundaries: Systems Maintenance and the Tallinn Manual*, in Proceedings: 1st Workshop on Ethics of Cyber Conflict 49 (Ludovica Glorioso & Anna Maria Osula eds., NATO CCD COE 2014).

Brownlie, Ian. International Law and the Activities of Armed Bands, 7 INT'L & COMP. L.Q. 712 (1958).

Brownlie, Ian. *The Rule of Law in International Affairs: International Law at the Fiftieth Anniversary of the United Nations* (1998).

Banks,William C. *Cyber Attribution and State Responsibility*, 97 Int'l L. Stud. 1039 (2021).

Broad, William J. John Markoff & David E. Sanger**,** *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*, N.Y. TIMES (Jan. 16, 2011), https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html.

Brown, Gary D. *Why Iran Didn't Admit Stuxnet Was an Attack*, 63 Joint Force Q. 70, 71 (2011), https://ssrn.com/abstract=2485181.

Broeders, Dennis. Els de Busser, Fabio Cristiano & Tatiana Tropina, Revisiting Past Cyber Operations in Light of New Cyber Norms and Interpretations of International Law: Inching towards Lines in the Sand?, 7 J. Cyber Pol'y 97 (2022).

Baezner, Marie. *Hotspot Analysis: Cyber and Information Warfare in the Ukrainian Conflict*, Version 2, (Oct. 2018), Risk & Resilience Team, Ctr. for Sec. Studies (CSS), ETH Zürich

Couzigou, Irène. *The Challenges Posed by Cyber Attacks to the Law on Self-Defence*, Eur. Soc'y Int'l L., 10th Anniversary Conf., Vienna, Sept. 4–6, 2014, Conference Paper No. 16/2014 (Dec. 1, 2014).

Cheng, Bin. *Pre-emptive or Similar Type of Self-Defense in the Territory of Foreign States*, 12 Chinese J. Int'l L. 1 (2013).

Convention on Cybercrime, Council of Europe, ETS No. 185, Nov. 23, 2001 (entered into force July 1, 2004).

Collins, Sean. & Stephen McCombie, *Stuxnet: The Emergence of a New Cyber Weapon and Its Implications*, 7 J. Policing, Intell. & Counter Terrorism 80 (2012).

Cohen, Julie E. Cyberspace as/and Space, 107 Colum. L. Rev. 210, (2007).

NATO Cooperative Cyber Defence Centre of Excellence, *About Us: History*, https://ccdcoe.org/about-us/

Check, Terence. *Book Review: Analyzing the Effectiveness of the Tallinn Manual's Jus Ad Bellum Doctrine on Cyberconflict: A NATO-Centric Approach*, 63 Clev. St. L. Rev. 495 (2015).

Clough, Jonathan. *A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation*, 40 Monash U. L. Rev. 698 (2014).

Council of Europe, *Chart of Signatures and Ratifications of Treaty 185* (Budapest Convention), https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185

Council of Europe, *Additional Protocol to the Convention on Cybercrime (CETS No. 224)*, https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224

Council of Europe, *Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence*, opened for signature May 12, 2022, C.E.T.S. No. 224, https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224

Council of Europe, *Explanatory Report to the Convention on Cybercrime*, Nov. 23, 2001, Eur. T.S. No. 185, https://rm.coe.int/16800cce5b

Council of Europe, *Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems*, Jan. 28, 2003, Eur. T.S. No. 189, https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=189

Council of the European Union, Council Document No. 10474/17 (Brussels, June 19, 2017).

Communication from the Commission to the European Parliament and the Council**,** *The EU Internal Security Strategy in Action: Five Steps Towards a More Secure Europe*, COM (2010) 673 final (Nov. 22, 2010), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52010DC0673

Council of Europe, Cybercrime Convention Committee (T-CY), Guidance Notes, adopted by the 8th, 9th, 12th, 16th, and 21st Plenary Sessions (July 8 2019), https://rm.coe.int/t-cy-guidance-notes-compilation/16809fc22c

Handbook on Developing a National Position on International Law and Cyber Activities: A Practical Guide for States, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), May 2025

CNN, "Bush Delivers Ultimatum," CNN (Sept. 21, 2001), https://edition.cnn.com/2001/WORLD/asiapcf/central/09/20/ret.afghan.bush/

Davis, John S. II et al., Stateless Attribution: Toward International Accountability in Cyberspace, RAND CORPORATION (June 2, 2017), https://www.rand.org/pubs/research_reports/RR2081.html.

Deeks, Ashley S. *Consent to the Use of Force and International Law Supremacy*, 54 Harv. Int'l L.J. 1, (2013).

Dinstein, Yoram. *War, Aggression and Self-Defence*, (4th ed. 2005).

Dinstein, Yoram. *War, Aggression and Self-Defence,* (7th ed. 2017).

Dinstein, Yoram. Computer Network Attacks and Self-Defense, 76 Int'l L. Stud. 99 (2002).

Dinniss, Heather Harrison. *Cyber Warfare and the Laws of War,* (Cambridge Univ. Press 2012), https://research.ebsco.com/linkprocessor/plink?id=074b99e4-1240-3c32-ab0b-c23ef8fb66f8.

Douligeris, Christos & Aikaterini Mitrokotsa, *DDoS Attacks and Defense Mechanisms: Classification and State-of-the-Art*, 44 COMPUT. NETWORKS 643 (2004).

Efrony, Dan. & Yuval Shany, *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*, 112 Am. J. Int'l L. 583 (2018).

European Union, *EU Statement – United Nations First Committee: Thematic Discussion on Other Disarmament Measures and International Security* (Oct. 26, 2018), https://www.eeas.europa.eu/node/52894_en?utm

European Union, EU Statement – UN Open-Ended Working Group on ICT: International Law (Dec. 19, 2023), https://www.eeas.europa.eu/node/52894_en

Regulation (EC) No. 460/2004 of the European Parliament and of the Council of 10 March 2004 Establishing the European Network and Information Security Agency, 2004 O.J. (L 77) 1, http://data.europa.eu/eli/reg/2004/460/oj/eng

Egan, Brian J. *International Law and Stability in Cyberspace*, 35 Berkeley J. Int'l L. 169 (2017).

Eichensehr, Kristen E. *Questions About WannaCry Attribution to North Korea*, Just Security (Dec. 19, 2017), https://www.justsecurity.org/49889/questions-wannacry-attribution-north-korea/.

Eichensehr, Kristen E. *The Law and Politics of Cyberattack Attribution*, 67 UCLA L. Rev. 520, (2020).

Franck,Thomas M. *Preemption, Prevention and Anticipatory Self-Defense: New Law Regarding Recourse to Force*, 27 Hastings Int'l & Comp. L. Rev. 425 (2004).

Fallegård, Sara. *The ICJ Advisory Opinion on the Israeli Wall* (unpublished student paper, Univ. of Lund, Faculty of Law [2008]).

Fleck, Dieter. *Searching for International Rules Applicable to Cyber Warfare—A Critical First Assessment of the New Tallinn Manual*, 18 J. Conflict & Security L. 331 (2013), https://www.jstor.org/stable/26296259

Farwell, James P. & Rafal Rohozinski, *Stuxnet and the Future of Cyber War*, 53 Survival 23 (2011).

Graham, David E. Cyber Threats and the Law of War, 4 J. Nat'l Sec. L. & Pol'y 87 (2010).

Gray, Christine. International Law and the Use of Force, 3d ed. Oxford Univ. Press, (2008).

Gervais, Michael. Cyber Attacks and the Laws of War, 1 J.L. & Cyber Warfare 8, (2012).

Gill, T.D. The Temporal Dimension of Self-Defence: Anticipation, Pre-Emption, Prevention and Immediacy, 11 J. Conflict & Sec. L. 361, (2006).

Green, James A. *The 'Ratione Temporis' Elements of Self-Defence*, 2 J. Use of Force & Int'l L. 97 (2015).

Green, James A. *Collective Self-Defence in International Law* (Cambridge Univ. Press 2024).

Greenberg, Andy. *The Untold Story of NotPetya — The Most Devastating Cyberattack in History*, *Wired* (Aug. 22, 2018), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world

HM Gov't, *A Strong Britain in an Age of Uncertainty: The National Security Strategy* , (Cm. 7953, 2010), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf.

Hargrove, John Lawrence. The Nicaragua Judgment and the Future of the Law of Force and Self-Defense, 81 Am. J. Int'l L. 135 (1987).

Hollis, Duncan B. *Why States Need an International Law for Information Operations*, 11 Lewis & Clark L. Rev. 1023 (2007), https://ssrn.com/abstract=1083889.

Hollis, Duncan B. *Could Deploying Stuxnet Be a War Crime?*, *Opinio Juris* (Jan. 25, 2011), https://opiniojuris.org/2011/01/25/could-deploying-stuxnet-be-a-war-crime/

Shou-Ching Hsiao & Da-Yu Kao, *The Static Analysis of WannaCry Ransomware*, in Proceedings of the 2018 20th International Conference on Advanced Communications Technology (ICACT), 153 (IEEE 2018)

Herzog, Stephen. *Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses*, 4 J. Strat. Sec. 49 (2011).

Heller, Kevin Jon. The "Last Window of Opportunity" Test Is Unlawful and Dangerous, Opinio Juris (June 24, 2025), https://opiniojuris.org/2025/06/24/the-last-window-of-opportunity-test-is-unlawful-and-dangerous/.

Hollis, Duncan B. *An e-SOS for Cyberspace*, 52 Harv. Int'l L.J. 373 (2011).

Hoisington, Matthew. Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense, 32 B. C. INT'l & COMP. L. REV. 439 (Spring 2009).

Hughes**,** Rex B. *NATO and Cyber Defence: Mission Accomplished*, 33 Atlantisch Perspectief 4, (2009).

Hathaway, Oona A. Crootof Rebecca, Levitz Philip & Nix Haley, The Law of Cyber-Attack, 100 Cal. L. Rev. 817 (2012).

Int'l Law Comm'n, Draft Articles on Responsibility of States for Internationally Wrongful Acts with Commentaries, 2001, 2(2) Y.B. Int'l L. Comm'n 26, U.N. Doc. A/56/10.

Int'l Law Comm'n, Draft Articles on the Law of Treaties with Commentaries, U.N. Doc. A/CN.4/SER.A/1966/Add.1 (1966).

International Committee of the Red Cross**,** *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, U.N. Doc. 31IC/11/5.1.2 (2011).

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). *Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case*. Mar. 18, 2016. https://us-cert.cisa.gov/sites/default/files/documents/ICS-Cyber-Attack-Ukraine-Defense-Use-Case-S508C.pdf.

International Committee of the Red Cross, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, 32nd Int'l Conf. of the Red Cross & Red Crescent, Geneva, Switz., Dec. 8–10, 2015, Doc. 32IC/15/11 (2015)

Island of Palmas Case (Neth. v. U.S.), 2 R.I.A.A. 838 (Perm. Ct. Arb. 1928).

Joint Chiefs of Staff, *Joint Doctrine for Information Operations*, Joint Publication 3-13, (Oct. 9, 1998).

Jensen, Eric Talbot. *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense*, 38 Stan. J. Int'l L. 207 (2002).

Jinks, Derek. State Responsibility for the Acts of Private Armed Groups, 4 Chi. J. Int'l L. 83 (2003).

Jenkins, Ryan *Is Stuxnet Physical? Does It Matter?*, 12 J. Mil. Ethics 68 (2013).

RNA: Stuxnet a Product of US and Israel, Jpost.com Staff, *Jerusalem Post* (Apr. 16, 2011), https://www.jpost.com/breaking-news/irna-stuxnet-a-product-of-us-and-israel (lastly visited March 21 2025)

Katarzyna Chałubińska-Jentkiewicz, Filip Radoniewicz & Tadeusz Zieliński, eds., Cybersecurity in Poland: Legal Aspects (Springer 2022).

Kajtár, Gábor. *The Caroline as the 'Joker' of the Law of Self-Defence – A Ghost Ship's Message for the 21st Century*, 21 Austrian Rev. Int'l & Eur. L. 3 (2016).

Da-Yu Kao & Shou-Ching Hsiao, *The Dynamic Analysis of WannaCry Ransomware*, in Proc. Int'l Conf. on Advanced Communications Technology (ICACT), 159 (2018).

Kesan, Jay P. & Carol M. Hayes, Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace, 25 HARV. J. L. & TECH. 429 (Spring 2012).

Kessler, Oliver. & Wouter Werner, Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare, 26 Leiden J. Int'l L. 793 (2013).

Kulesza, Joanna. *Due Diligence in International Law* (Brill Nijhoff 2016).

Kowalski, Michał. Armed Attack, Non-State Actors and a Quest for the Attribution Standard, 30 Pol. Y.B. Int'l L. 101 (2010), https://ssrn.com/abstract=2173000.

Kittichaisaree, Kriangsak. Public International Law of Cyberspace, Law, Governance and Technology Series 32, Springer, (2017).

Lau, Felix W. Stuart H. Rubin, Michael H. Smith & Ljiljana Trajkovic, *Distributed Denial of Service Attacks*, in Proc. IEEE Int'l Conf. on Systems, Man & Cybernetics, SMC 2000 (Vol. 3) 2275 (Oct. 2000).

Michael W. Lewis, Elongated Imminence and Operational Realites, Opinio Juirs, (Jan. 29, 2013), https://opiniojuris.org/2013/01/29/elongated-imminence-and-operational-realities/

Li, Johannes Xingan. *Cyber Crime and Legal Countermeasures: A Historical Analysis*, Int'l J. Crim. Just. Sci., July–Dec. 2017.

Lipson, Howard F. *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues*, CMU/SEI Special Report No. 2002-SR-009 (Nov. 1, 2002).

Liivoja, Rain. Maarja Naagel & Ann Väljataga, *Autonomous Cyber Capabilities under International Law*, 16, (NATO Cooperative Cyber Defence Centre of Excellence 2019), https://ccdcoe.org/library/publications/autonomous-cyber-capabilities-under-international-law/.

Lin, Herbert S. *Attribution of Malicious Cyber Incidents: From Soup to Nuts*, 70 J. Int'l Aff. 75, (2016)

Lin, Herbert S. Offensive Cyber Operations and the Use of Force, 4 J. NAT'l SEC. L. & POL'y 63 (2010).

L*egality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, 1996 I.C.J. 226, (July 8).

Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136, (July 9).

Lucas, George. *Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare* 45 (Oxford Univ. Press 2016).

McGhee, James E. Cyber Redux: The Schmitt Analysis, Tallinn Manual and US Cyber Policy, 2 J.L. & CYBER WARFARE 64 (Spring 2013).

Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Merits, Judgment, 1986 I.C.J. 14, (June 27).

Military Action in Iraq Without Security Council Authorization Would Be Illegal, 34 Ottawa L. Rev. 1, 2 (2002-03).

Myers, Steven Lee. *Estonia Removes Soviet-Era War Memorial After a Night of Violence*, N.Y. Times (Apr. 27, 2007), https://www.nytimes.com/2007/04/27/world/europe/27iht-estonia.4.5477141.html

Marsh, Sarah. *US Joins UK in Blaming Russia for NotPetya Cyber-Attack*, *The Guardian* (Feb. 15, 2018), https://www.theguardian.com/technology/2018/feb/15/uk-blames-russia-notpetya-cyber-attack-ukraine

Madubuike-Ekwe, Joseph N. Cyberattack and the Use of Force in International Law, 12 Beijing L. Rev. 631 (June 2021).

NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit, NATO Cooperative Cyber Defence Centre of Excellence (July 21, 2016), https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/.

Nagan, Winston P. & Craig Hammer, *The Changing Character of Sovereignty in International Law and International Relations*, 43 Colum. J. Transnat'l L. 141, (2004).

Nakashima, Ellen. *The NSA Has Linked the WannaCry Computer Worm to North Korea*, Wash. Post (June 14, 2017), https://www.washingtonpost.com/world/national-security/the-nsa-has-linked-the-wannacry-computer-worm-to-north-korea/2017/06/14/101395a2-508e-11e7-be25-3a519335381c_story.html

Nguyen, Reese. *Navigating Jus Ad Bellum in the Age of Cyber Warfare*, 101 Cal. L. Rev. 1079 (2013).

NATO Cooperative Cyber Defence Centre of Excellence, *CCDCOE to Host the Tallinn Manual 3.0 Process* (Dec. 14, 2020), https://ccdcoe.org/news/2020/ccdcoe-to-host-the-tallinn-manual-3-0-process/.

Ottis, Rain. & Peeter Lorents, *Cyberspace: Definition and Implications*, in Proceedings of the 5th International Conference on Information Warfare and Security (Academic Publishing Ltd. 2010).

Oil Platforms (Iran v. U.S.), Judgment, 2003 I.C.J. 161 (Nov. 6).

Ochoa, Natalia. & Esther Salamanca-Aguado, *Exploring the Limits of International Law Relating to the Use of Force in Self-Defence,* 16 Eur. J. Int'l L. 499, (2005)

Ottis, Rain. *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective*, Cooperative Cyber Defence Centre of Excellence, (2008).

Owens, William A. Kenneth W. Dam & Herbert S. Lin, Technology, Policy, Law, And Ethics Regarding U.S. Acquisition And Use Of Cyberattack Capabilities, (Nat'l Acads. Press 2009).

Pantin, Nicholas T., Key Terrain: Application to the Layers of Cyberspace (Mar. 2011) (unpublished M.S. thesis, Naval Postgraduate School), https://calhoun.nps.edu/server/api/core/bitstreams/f3e5cfcd-de3b-40b0-bda1-ae3e9803308b/content

People's Republic of China, Chinese Position Paper on the Application of the Principle of Sovereignty in Cyberspace, U.N. Office for Disarmament Affairs (Dec. 2021), https://documents.unoda.org/wp-content/uploads/2021/12/Chinese-Position-Paper-on-the-Application-of-the-Principle-of-Sovereignty-ENG.pdf.

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts article 49 (Protocol I), June 8, 1977, 1125 U.N.T.S. 3.

Pobjie, Erin. *Prohibited Force: The Meaning of 'Use of Force' in International Law,* 93 (Cambridge Univ. Press 2024).

Peterson, Andrea. *Hackers Caused a Blackout for the First Time, Researchers Say*, Wash. Post (Jan. 5, 2016), https://www.washingtonpost.com/news/the-switch/wp/2016/01/05/hackers-caused-a-blackout-for-the-first-time-researchers-say/

Prosecutor v. Duško Tadić, Case No. IT-94-1-A, Appeals Chamber, Int'l Crim. Trib. for the Former Yugoslavia, (July 15, 1999).

Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea, James S. Brady Press Briefing Room (Dec. 19, 2017), https://trumpwhitehouse.archives.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/

Petkis, Stephen. Rethinking Proportionality in the Cyber Context, 47 GEO. J. INT'l L. 1431 (Summer 2016).

Pirker, Benedikt. *Territorial Sovereignty and Integrity and the Challenges of Cyberspace,* 189, (Katharina Ziolkowski ed., NATO Cooperative Cyber Defence Centre of Excellence 2013).

Park, Donghui. & Michael Walstrom, *Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks* (Oct. 11, 2017), Henry M. Jackson School of Int'l Studies, Univ. of Wash., https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/

RAND Corporation, *About RAND*, https://www.rand.org/about.html

Ruys, Tom. *The Meaning of "Force" and the Boundaries of the Jus ad Bellum: Are "Minimal" Uses of Force Excluded from UN Charter Article 2(4)?,* 108 Am. J. Int'l L., 174, (2014).

Russia's Strategy in Cyberspace, NATO StratCom COE 7, (June 2021).

Ruys, Tom. *The Intangible 'Armed Attack': Evolutions in Customary Practice Pertaining to the Right of States to Self-Defence and the Quest for a Definition of 'Armed Attack' under Article 51 UN Charter* (unpublished doctoral dissertation, Katholieke Universiteit Leuven 2009) (on file with Ghent Univ. Library).

Roscini, Marco. *World Wide Warfare – Jus ad Bellum and the Use of Cyber Force*, 14 Max Planck Y.B. U.N. L. 85, (2010).

Roscini, Marco. Cyber Operations and the Use of Force in International Law, Oxford University Press, (2014).

Rathmell, Andrew. *Controlling Computer Network Operations*, 26 Stud. Conflict & Terrorism 215 (2003).

Richardson, John. *Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield*, 29 J. Marshall J. Computer & Info. L. 1 (2011).

Michael, N. Schmitt. ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge Univ. Press 2013).

Michael, N. Schmitt. ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2d ed. 2017).

Schmitt Michael N., *"Attack" as a Term of Art in International Law: The Cyber Operations Context*, in Proceedings of the 4th International Conference on Cyber Conflict (Christian Czosseck, Rain Ottis & Katharina Ziolkowski eds., NATO CCD COE 2012).

Michael N. Schmitt & Sean A. Fahey, *WannaCry and the International Law of Cyberspace*, Just Security (May 16, 2018), https://www.justsecurity.org/50038/wannacry-international-law-cyberspace/.

Steinberg, Sean. Adam Stepan & Kyle Neary, *The Hacking of Sony Pictures: A Columbia University Case Study*, SIPA Case Study No. 21-0023.1 (Columbia Univ. Sch. Int'l & Pub. Affairs Oct. 2021), https://www.sipa.columbia.edu/sites/default/files/2022-11/Sony%20-%20Written%20Case.pdf

Sanger, David E. *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES (June 1, 2012), https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

Sacks, Samm. China's Emerging Cyber Governance System, China Cyber Outlook, Center for Strategic & International Studies https://www.csis.org/programs/strategic-technologies-program/resources/china-cyber-outlook/chinas-emerging-cyber (last visited Aug. 2025).

Spafford, Eugene H. *The Internet Worm Program: An Analysis* (1988), https://spaf.cerias.purdue.edu/tech-reps/823.pdf.

Schmitt, Michael N. The Evolution of Cyber Jus ad Bellum Thresholds, *Articles of War* (July 28, 2022), https://lieber.westpoint.edu/evolution-cyber-jus-ad-bellum-thresholds/.

Schmitt, Michael N. *Classification of Cyber Conflict*, 89 Int'l L. Stud. 233 (2013)

Schmitt, Michael N. *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 Colum. J. Transnat'l L. 885 (1999), https://ssrn.com/abstract=1603800.

Schmitt, Michael N. *Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts*, in Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy 151 (Nat'l Research Council ed., Nat'l Acads. Press 2010).

Schmitt, Michael N. *Responding to Transnational Terrorism under the Jus ad Bellum: A Normative Framework*, 56 Naval L. Rev. 1 (2008)

Schmitt, Michael N. *Bellum Americanum: The U.S. View of Twenty-First Century War and Its Possible Implications for the Law of Armed Conflict*, 19 Mich. J. Int'l L. 1051 (1998).

Steinberg, Sean. Adam Stepan & Kyle Neary, *NotPetya: A Columbia University Case Study*, SIPA Case Study No. 21-022.1 (Columbia Univ. Sch. Int'l & Pub. Affairs, Oct. 2021)

Simmons, Noah. *A Brave New World: Applying International Law of War to Cyber-Attacks*, 4 J.L. & Cyber Warfare 42, (Winter 2014).

Schmitt, Michael N. & Liis Vihul, *Proxy Wars in Cyberspace: The Evolving International Law of Attribution*, 1 Fletcher Sec. Rev. 53, (2014).

Schmitt, Michael N. *Grey Zones in the International Law of Cyberspace*, 42 Yale J. Int'l L. Online (2017), https://ssrn.com/abstract=3180687.

Michael N. Schmitt & Liis Vihul, *Respect for Sovereignty in Cyberspace* (text originally titled *Sovereignty in Cyberspace: Lex Lata Vel Non?*), 95 Tex. L. Rev. 1639 (2017)

S.C. Res. 1368, U.N. Doc. S/RES/1368 (Sept. 12, 2001).

Smith, Brad. *The Need for a Digital Geneva Convention*, MICROSOFT ON THE ISSUES (Feb. 14, 2017), https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/.

Letter dated 7 October 2001 from the Permanent Representative of the United States of America to the United Nations addressed to the President of the Security Council, U.N. SCOR, U.N. Doc. S/2001/967 (Oct. 15, 2001)

Singer, P.W. *Stuxnet and Its Hidden Lessons on the Ethics of Cyberweapons*, 47 Case W. Res. J. Int'l L. 79, (2015).

Tsagourias, Nicholas, *The Legal Status of Cyberspace*, in Research Handbook on International Law and Cyberspace, 12 (Nicholas Tsagourias & Russell Buchan eds., 2d ed. 2021)

Tabansky Lior, *Basic Concepts in Cyber Warfare*. 3 Mil. & Strategic Aff. 75 (2011).

Tsagourias Nicholas, *Cyber Attacks, Self-Defence and the Problem of Attribution*, 17 J. Conflict & Sec. L. 229, (2012).

Titiriga, Remus. Cyber-Attacks and International Law of Armed Conflicts: A *Jus ad Bellum* Perspective, 8 J. Int'l Com. L. & Tech. 179 (2013).

Tikk, Eneken. Kadri Kaska & Liis Vihul, *International Cyber Incidents: Legal Considerations*, Cooperative Cyber Defence Centre of Excellence, (2010).

Tsagourias, Nicholas. & Michael Farrell, *Cyber Attribution: Technical and Legal Approaches and Challenges*, 31 Eur. J. Int'l L**.** 941 (2020).

Tsagourias, Nicholas. *Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace*, Univ. of Sheffield Legal Rsch. Pap. No. 159652 (Apr. 17, 2019)

U.S. Dep't of Def., *Department of Defense Dictionary of Military and Associated Terms*, Joint Pub. 1-02 (Nov. 8, 2010).

United Nations Charter

United Nations, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/70/174 (July 22, 2015).

United Nations, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/68/98 (June 24, 2013) https://dig.watch/wp-content/uploads/A_68_98_E.pdf

U.N. Gen. Assembly, Definition of Aggression, G.A. Res. 3314 (XXIX), U.N. Doc. A/RES/3314 (XXIX) (Dec. 14, 1974).

U.N. General Assembly, *Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from the Threat or Use of Force in International Relations*, U.N. Doc. A/RES/42/22 (Nov. 18, 1987).

U.N. Gen. Assembly, Declaration on Principles of International Law Concerning Friendly Relations and Cooperation Among States in Accordance with the Charter of the United Nations, G.A. Res. 2625 (XXV), U.N. Doc. A/RES/2625 (Oct. 24, 1970).

U.N. Secretary-General, Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, U.N. Doc. A/76/135 (July 14, 2021).

U.N. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Report of the Group of Governmental Experts, para 1–3, U.N. Doc. A/68/98 (June 24, 2013).

Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States, submitted by participating governmental experts in the GGE established pursuant to G.A. Res. 73/266, U.N. GAOR, 76th Sess., U.N. Doc. A/76/136 (2021).

U.N. News, *U.N. aviation council finds Russia responsible for downing of Malaysia Airlines flight*, May 13, 2025, https://news.un.org/en/story/2025/05/1163161.

United Kingdom, Application of International Law to States' Conduct in Cyberspace: UK Statement (Nov. 25, 2021), https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement.

UK GGE National Statement (2021), United Kingdom of Great Britain and Northern Ireland, Application of International Law to States' Conduct in Cyberspace: UK Statement,

U.N. Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (Nov. 25, 2021), https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement.

UK Attorney General Speech (2018), Jeremy Wright, Cyber and International Law in the 21st Century, Speech at Chatham House (May 15, 2018), https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

U.S., The National Security Strategy of the United States of America (Sept. 2002), https://2009-2017.state.gov/documents/organization/63562.pdf.

Vienna Convention on the Law of Treaties, May 23, 1969, 1155 U.N.T.S. 331.

Väljataga, Ann. Back to Square One? The Fifth UN GGE Fails to Submit a Conclusive Report at the UN General Assembly, September 1 ,2017, retrieved from: https://ccdcoe.org/back-square-one-fifth-un-gge-fails-submit-conclusive-report-un-generalassembly.html

Vostoupal, Jakub. *Stuxnet vs WannaCry and Albania: Cyber-Attribution on Trial*, 54 Comput. L. & Sec. Rev. 106008 (2024)

Ward Mark, *A Decade on from the ILOVEYOU Bug*, BBC News (May 4, 2010), https://www.bbc.com/news/10095957

Waxman Matthew C., *Cyber Attacks as "Force" Under UN Charter Article 2(4)*, 87 Int'l L. Stud., (2011).

Waxman Matthew C., *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 Yale J. Int'l L. 421 (2011), https://scholarship.law.columbia.edu/faculty_scholarship/1653.

War Would Be Illegal, *The Guardian* (London), Mar. 7, 2003, https://www.theguardian.com/politics/2003/mar/07/highereducation.iraq.

Weber, Amalie M. *The Council of Europe's Convention on Cybercrime*, 18 Berkeley Tech. L.J. 425, (2003).

Wolff, Josephine. *How the NotPetya Attack Is Reshaping Cyber Insurance*, Brookings (Dec. 1, 2021), https://www.brookings.edu/articles/how-the-notpetya-attack-is-reshaping-cyber-insurance/

Yannakogeorgos, Panayotis A. & Eneken Tikk, *Stuxnet as Cyber-Enabled Sanctions Enforcement*, in 2016 Int'l Conf. on Cyber Conflict (CyCon U.S.) 1 (IEEE 2016).