



IMSIS
International Master
Security, Intelligence
& Strategic Studies



**Erasmus
Mundus**

Maintaining Peace and Security in Cyberspace:
Multilateral Approach of the United Nations on Advancing
Responsible State Behaviour in Cyberspace

July 2022

2337760 (UoG)

20109407 (DCU)

56399812 (CU)

Presented in partial fulfilment of the requirements for the Degree of
International Master in Security, Intelligence and Strategic Studies

Word Count: 23,960

Supervisor: Dr James Gallen

Date of Submission: 29 July 2022



**UNIVERSITY
OF TRENTO**



CHARLES UNIVERSITY

Abstract

The international community has concerned about the malicious development of Information and Communication Technology (ICT) that threatens international peace and security. This issue emerged since the same technology that supports our daily activities could also be used to conduct military hostilities. Such cases of DDoS attacks in Estonia and Stuxnet in Iran could provide a full illustration. Apart from the scholarly attention to this emerging issue, the research that particularly assesses the United Nations as the organization to preserve the current state of international peace and security is still lacking. Henceforth, this research will focus on evaluating how the UN has reacted to the malicious development of ICT in the context of international security and whether it has effectively established a new regime to regulate States in this hostile activity.

This research will benefit from detailed and critical examination using a documentary and archival analysis as well as critical discourse analysis. To elaborate on numerous notions and measures taken by the UN and provide a noteworthy discussion, this research will borrow transdisciplinary approaches ranging from international politics to international law. Through evaluation, this research found that the UN has put a concerted effort to tackle this issue by establishing the annually

provisional agenda in its General Assembly, forming specially designated bodies (UN GGE), and adopting an inclusive measure called OEWG (Open-Ended Working Group). Despite the success of GGE in acknowledging international law applicability in cyberspace and renouncing 11 norms that guided state behaviour in cyberspace, the norm-making process in this sector is still surrounded by the politicization of powerful States. As a result, the UN is halted from reaching a consensus on several important topics (i.e., international humanitarian law). Apart from this challenging process, the UN's established measures still present an accomplishment. However, in the end, the UN has not established a new regime to regulate cyberspace; instead, it chose to be guided by a soft law and existing international law. Consequently, the road to reaching a binding treaty is still considered a long journey, although it still has a possibility. As a result, to keep the UN process trustworthy, this research recommends that the UN take further effort to clarify the ambiguity in the current measures of ICT in the context of international security, such as publishing declarations related to the peaceful use of ICT.

Keywords: United Nations, ICT, Cybersecurity, International Law, Norm-Making Process, Soft Law, Use of Force, Customary International Law, International Peace and Security

Acknowledgement

I would like to thank my supervisor, Dr James Gallen, who has fully supported me toward the finalization of this dissertation. His guidance and encouragement are substantial to the completion of this study.

I also would like to convey my sincere gratitude to God, my family, and friends who constantly remind me that everything is possible, including finishing my study.

I also thank the IMSISS, which give me a chance to enhance my knowledge and see the world from many differing perspectives.

Finally, and thankfully, we have reached this final stage of the study. There are so many lessons I can learn from these precious two years. And I hope this research will complement the evolution of International Security Studies.

Table of Contents

Abstract	i
Acknowledgement	iii
Table of Contents	iv
Chapter 1: Introduction	1
1.1 Background	1
1.2 Research Question	10
1.3 Chapter Overview	10
Chapter 2: Literature Review	12
2.1 Cyber Power	12
2.1.1 Powerplays in Global Internet Governance	16
2.2 Cyber Operations	22
2.2.1 Cyber Penetration Attack	24
2.2.2 Denial of Service Attack	27
2.3 Applicability of International Law in Cyberspace	28
2.3.1 Use of Force, Self-Defense, and Armed Attack.	28
2.3.2 Non-Intervention	37
2.3.3 Sovereignty	43

2.4 Conclusion	46
Chapter 3: Methodology	48
3.1 Research Design	48
3.2. Data Collection and Selection Process	49
3.3 Data Analysis	51
3.4 Methodological Reflection	52
Chapter 4: Findings	55
4.1 United Nations General Assembly (UNGA)	56
4.1.1 The notion in the UNGA Resolution 1998-2009	57
4.1.2 The notion in the UNGA Resolution 2010-2016	61
4.1.3 The notion in the UNGA Resolution 2017-2021	65
4.1.3.1 US Sponsored Resolution	66
4.1.3.2 Russia Sponsored Resolution	68
4.2 United Nations Group of Governmental Experts (UN GGE)	73
4.2.1 Result of the 1st UN GGE 2004-2005	74
4.2.2 Result of the 2nd UN GGE 2009-2010	74
4.2.3 Result of the 3rd UN GGE 2012-2013	79
4.2.4 Result of the 4th UN GGE 2014-2015	83
4.2.5 Result of the 5th UN GGE 2016-2017	85

4.2.6 Result of the 6th UN GGE 2019-2021	86
4.2.7 Conclusion	89
4.3 United Nations Open-Ended Working Group (UN OEWG)	90
4.3.1 Primary Result of the UN OEWG	90
Chapter 5: Discussion	93
5.1 Power Dynamics in the UN Platform for Cyber Security	94
5.2 Dual use of ICT: Framework Clarity	98
5.3 Soft vs. Hard Law in Regulating International Cyber Security	102
5.4 Conclusion	105
Chapter 6: Summary and Conclusion	107
Reference List	111

Chapter 1: Introduction

1.1 Background

More than half a century has passed since the international community established the maintenance of lasting peace and security through the restriction of future war. After the devastating events of World War II, which impacted approximately half of the world's population, the United Nations was founded with the specific mission of ensuring and maintaining worldwide peace and security. As a result, the United Nations has accomplished its mission by developing and approving norms and international law that make it illegal for states to wage war against one another; the United Nations Charter is one such renowned document that remains in force to this day and is considered an instrument of international law.

While international law's applicability in the physical world, such as land, sea, air, and outer space, is unquestionable, its applicability in the virtual world, cyberspace, is still debatable. There are yet international laws that specifically regulate the prohibition of cyberspace for nonpeaceful purposes. On the other hand, the four other physical domains mentioned have been supplemented with internationally recognized norms and specific internationally binding laws. For example, Outer Space Treaty governed the prohibition of the use of outer space

for nonpeaceful purposes. Furthermore, it also reaffirmed outer space as the province of mankind; thus, it will be accessible for every country to explore.

Nonetheless, the position of cyberspace as the new realm is still disputable. Despite this, the extent to which our communities rely on this emerging sector continues to grow. The use of computer networks and the internet is tied to nearly every aspect of our life, including our finances, health care, and other substantial activities. The fact that we are becoming increasingly reliant on this newly digitalized environment makes us more susceptible to the threat to peace and security posed by information and communication technology (ICT).

There have been many discussions concerning the potential for ICT to be exploited for malicious actions; states can also use this motivation to launch an attack on adversaries. Today, contemporary warfare does not rely on complex military technologies like air strikes or nuclear bombings. Instead, it has found a more convenient approach to disrupt and destroy an object by simply utilizing malware or botnets. Cyber warfare thus becomes a strategic substitute for, rather than an operational complement to, conventional military force (Libicki, 2011)

The lack of international legislation controlling cyberspace facilitates its utilization. Such cyberspace-based attacks are simpler, more specific, and more effective. Instead of spending several billions of dollars on constructing highly advanced military weapons, many nations

are concentrating on improving their cyber capabilities for offensive or defensive purposes. States with limited military and financial resources view the emergence of cyberspace as an opportunity. It is to suggest that smaller States may contribute just as much as more powerful States to their cyber capabilities since it does not require vast manpower and modern artillery compared to merely a few people with a high level of expertise in ICT and a sophisticated computer network. Many argue that even weak states and other political actors are encouraged to acquire cyber capabilities, which increasingly threaten the United States and other advanced industrial countries (Nye, 2010).

It is believed, however, that this idea might allow further hostilities and have a more damaging consequence, such as an attack on the state's critical infrastructure. Due to this growing concern, several States have lately accused other countries of conducting cyber operations with disastrous effects on their internal governing functions. Defense Secretary Leon Panetta claimed, "a cyber-attack perpetrated by nation-states or violent extremist groups could be as destructive as the terrorist attack on 9/11. Such a destructive cyber-terrorist attack could virtually paralyze the nation." (US DoD, 2012, cited in Lindsay, 2013). In addition, the former President of the United States, Barack Obama, expressed his concern about the possibility that an opponent may take advantage of the vulnerabilities in the United States' computer systems rather than match the United States military superiority (White House, 2009).

Attacking the US traffic management system, banking, and financial industries, or even the power supplies using cyber-means is simpler than striking a bomb in the US. This suggests that the effects of cyberweapons could be comparable to those of conventional weapons. Finally, it is to underline that the use of cyberspace for nonpeaceful purposes is a critical issue that needs to be addressed to avoid further catastrophes that have an impact not only on the well-being of humanity but also on the current state of peace and security.

To provide a clear picture of how the exploitation of cyber capabilities might be detrimental to the current state of peace and security, we will look at two well-known cyber operations worth highlighting: Stuxnet in Iran and DDoS attacks in Estonia.

Stuxnet in Iran

Iran has been a subject of international condemnation due to its nuclear development program. Iran's uranium enrichment program is believed to have reached a point where it is no longer intended for the electrical power grid but as a deterrent weapon. As a result of this threat, Iran's Natanz nuclear facility reported in 2010 that its nuclear centrifuges were attacked by a specific malware that only matches its Siemens computer program: SIMATIC (Lindsay, 2013, p.380). This created an operation malfunctioning and led to the two years postponement of its

nuclear program. According to reports, sophisticated malware known as Stuxnet was responsible for destroying Iran's nuclear program.

Stuxnet is described as “the most technologically sophisticated malicious program developed for a targeted attack to date” and as a “precision, military-grade cyber missile” (Lindsay, 2013, p.366). Its development was suspected as a joint program between US-Israeli intelligence under a covert operation called the “Olympus Game” (Gibney, 2016). Moreover, the former head of the CIA, Michael Hayden (2012), affirmed that Stuxnet was the first cyber-attack that could create object damage and physical destruction. Stuxnet is considered the cyber equivalent of dropping the atomic bomb without human injuries (Clayton, 2011). The analysis of this incident may lead us to conclude that, first, the use of a cyber weapon in the attack was very effective and precise. Second, it does not result in any human fatalities. Third, the adversaries were unaware of when the attack would occur, giving rise to the term “silent warfare.” When seen from this angle, it is possible to conclude that cyber weapons will become an increasingly popular option in the future.

DDoS Attack in Estonia

After the relocation of a Soviet-era monument in Tallinn in April 2007, Estonia was exposed to a cyber-attack operation. The most well-known attacks were distributed denial of service (DDoS) attacks, which

caused degraded or lost service on numerous commercial and government systems. Some attacks targeted more vital targets, such as online banking and DNS, while others targeted less vital services, such as websites and e-mail (Haataja, 2017, p.160). The disruptions are reported to have seriously impaired the daily operation of various organizations, including banks, government departments, and small businesses (Tikk *et.al.*, 2010, p.16). Some estimates quantify the economic impact of the attacks at between 27 to 40 million United States (US) dollars (Haataja, 2017, p.161).

The cyber-attacks were related to the broader political confrontation between Russia and Estonia. Estonia initially blamed Russia as some of the attacks were traced to Russian Internet Protocol (IP) addresses (Haataja, 2017, p.161). A state-sponsored information operation seems to be the most likely explanation for this event. In this state, Estonian government requested formal investigative assistance from the Russian government to locate the perpetrators, which did not result in any favourable reaction. Investigations into those other attacks have been stalled because Russian officials have refused to cooperate. Several times, the Russian government has asserted that it had nothing to do with the 2007 cyberattack on Estonia. Nonetheless, it is astonishing that the Russian government has not presented evidence of efforts to resolve the issue. The Russian government's lack of cooperation with the Estonian investigation suggests that it is uninterested in locating the

criminals and is thus covering them. As a direct consequence, attackers were free to launch attacks against Estonian networks without worrying about facing punishment from the Estonian government.

The above-mentioned cyber operation cases illustrate how entities and governments influenced nation-states' alleged cyberspace activities to achieve a political objective in addition to their military mission. Cyberattacks provide a devastating method of targeting countries and groups with precision and accuracy while concealing one's identity. Cyber aggression is just as harmful as employing a physical weapon, but it is more sophisticated in allowing for confusion while remaining below the level of armed attack. This fact makes modern societies more vulnerable. A state's critical infrastructure, which is essential to the nation's security and wellbeing, may be the target of an attack launched by another state. Some attacks are significantly more dangerous than others due to the critical objects they target. The following case studies cannot be definitively attributed or linked to a particular nation-state based on any evidence presented up to this point. This resulted in the fundamental difficulty of cyber operations that endorsed anonymity.

With the knowledge of the potential destruction of cyber operations, the current global security and peace could be jeopardized. Therefore, when it comes to threats to the stability of peace and security, it will become an issue that needs to be discussed to avoid a further

catastrophe. Despite the fact that numerous cyber cases have been brought to the attention of the United Nations, the significance of establishing a regime to regulate cyberspace and limit its capabilities as a weapon has yet to be established. Although there are regulations governing international affairs in general, there are very few that govern cyberspace; the establishment of the International Telecommunication Union (ITU) could aid in comprehending the technicalities of cyberspace as a sphere to accelerate global communication. However, there was no mention of the prohibition of cyberspace for non-peaceful purposes.

The UN Security Council (UNSC) is the only UN body with the authority to take a legally binding decision, and whose primary responsibility is to maintain international peace and security, is still hesitant to discuss this agenda in its chamber. Therefore, the broader forum, such as the General Assembly (UNGA), is largely utilized to make recommendations and bring this issue to the UNSC's notice. Since 1998, when the Russian Federation proposed a draft resolution on the subject to the First Committee of the UN General Assembly (UNGA), a thematic discussion on the advent of ICT in the field of international security has been a matter of concern at the UN.

It is evident that international law can only be enacted by states, and the United Nations has been the sole organization able to facilitate this process. Amid uncertainty regarding which law applies in cyberspace, numerous scholars have interpreted current international

law, such as the United Nations Charter and Geneva Convention, as well as the customary international law of responsibility of States for internationally wrongful acts applied to cyberspace. It does not imply, however, that adherence to international law norms is a simple undertaking. According to Delerue (2020), there are substantial concerns surrounding the interpretation and application of specific regulations. On the one hand, given cyberspace's unique characteristics, interpreting international law's application to cyber operations may require a certain level of adaptation. On the other hand, international law subjects, particularly States, may have different if not divergent interpretations of certain specific norms of international law (Delerue, 2020, p.2).

Due to this fact, the effectiveness of the United Nations in its mission to preserve the current state of peace and security in cyberspace is questioned. Consequently, this study aims to determine whether the United Nations has effectively tackled the most recent developments of ICT in the context of international security. In addition, it seeks to conduct a critical analysis of the notions and measures adopted by the United Nations to assess the behaviour of states in cyberspaces as well as to identify the issues that remain unacknowledged under the current framework. As a result, this research aims to provide insights into how the United Nations can establish a more safe, secure, and reliable framework for cyberspace.

1.2 Research Question

After all, cyberspace represents a new realm for human activity. Consequently, the international community should recognize cyberspace similarly to land, sea, air, and outer space. The cyber operation could be both substitute and complementary to those existing domains. However, due to the uniqueness of its characteristics, this space requires its own set of international regulations that can address them particularly. For these reasons, examining the United Nations' response to this developing situation is crucial. Finally, this research aims to answer **how the UN has reacted to the malicious development of ICT that threatened international peace and security**. Furthermore, the study will evaluate **whether the UN has effectively established the new regime in creating a safe, peaceful, and secure cyberspace**.

1.3 Chapter Overview

This research will be based on six chapters. The first chapter will discuss the background information which was the reason of this research took place. It is evident that cyberspace has created new challenges for international peace and security and, thus, is essential to be a subject of further study. The second chapter will elaborate on a

broad discussion regarding literature on cyberspace, derived from the use of power in cyberspace, strategy of cyber operations, and applicability of international law in cyberspace. The third chapter will discuss the methodology used to present this research which is based on document and archival analysis as well as critical discourse analysis. The fourth chapter will examine the findings derived from the UN's adopted notions and measures from 1998-2021. The fifth chapter will discuss about the correlation of findings in chapter 4 with the concept and literature presented in chapter 2. Furthermore, this chapter is essential to capture the complexity of establishing a cyber-security-related regime. And finally, this research will be concluded in Chapter 6.

Chapter 2: Literature Review

This chapter will provide extensive research on the existing literature on the topic of international politics in cyberspace. Although the literature on this field is enormous, this chapter will mainly discuss three main thematic topics: cyber power and governance, cyber operations, and the applicability of international law in cyberspace. Furthermore, this chapter is essential in drawing the trends and gaps that emerge from extensive research. Therefore, it will contribute to the finding and discussion parts of this research.

2.1 Cyber Power

Since the early 21st century, it has been argued that cyberspace will become a sphere of power projection to express influence (soft power) and force (hard power). Cyber power, according to Nye (2010, p. 3), is the ability to achieve desired outcomes by utilizing the electronically networked information resources of the cyber domain. In addition, Stevens and Kavanagh (2021, p.2) define cyber power as the capacity to utilize or threaten to use other cyberspace resources to achieve strategic objectives contrary to the interests of others. Countries that choose this path are referred to as cyber power countries, in which they may build military capabilities as a component of their national cyber power for use against an adversary.

Cyberspace is not a natural field that lives within us: it is an artificial field. Since the development of cyberspace, the rule of exercising power has evolved. Cyberspace has become an accessible domain for everyone, it thus creates a power diffusion among actors in international relations. To illustrate, a powerful country such as the United States find itself sharing the stage with new actors and having more trouble controlling its borders in the domain of cyberspace (Nye, 2010, p.5-7). Due to the low cost of entrance, anonymity, and asymmetries in susceptibility, smaller actors are able to exercise more hard and soft power in cyberspace than in many more traditional domains of international politics (Nye, 2010, p.3). As a result, cyberspace became a more preferred domain because it is simpler and requires less sophisticated military equipment compared to other fields.

Due to increasing accessibility, cyberspace has emerged as the new battlefield. Since the end of the Cold War, the US has made significant investments in it. Furthermore, Russia and China also make a concerted effort to adapt and take control of this emerging domain. In addition, another smaller state, such as Estonia, is developing its cyber capabilities due to its experience with the 2007 DDoS attack.

Nye (2010) believes that the fundamental principle of exercising power is the same in all domains: establishing control and asserting influence. To understand power relations in cyberspace, Nye further explains the three faces of power in cyberspace. The first manifestation

of power is coercion, in which one entity forces another to act against their will. Such action can be illustrated with a DDoS attack in Estonia, which targeted most technological functions, including government websites, that hinder the country from operating against its will. The second face is the ability to shape or control the agenda. For example, the US has played a significant role in developing and establishing standards and norms in cyberspace through the establishment of ICANN and their involvement in the UN GGE. The last face of power involves shaping other initial preferences so that some strategies are not even considered. For example, authoritarian countries such as Russia and China practice control in cyberspace. They restrict access to any website that contains information deemed as a threat to state security or otherwise harmful to their citizens. From these faces of power, we may conclude that cyber power can be exercised through coercive, influencing, and manipulative measures.

Apart from Nye's faces of power, other prominent scholars, Stevens and Kavanagh (2021), also synthesize the concept of the forms of power concerning cyberspace strategy. They categorize this power as a compulsory, institutional, structural, and productive power. *Compulsory Power* exists in the relationship between actors that facilitate the direct control by one actor over another (Stevens&Kavanagh, 2021). An example of this form of power is the deployment of the Stuxnet malware that attacked the Iranian nuclear

operations by targeting the centrifuges. It was a direct and coercive action to control the undesirable outcome of Iran producing its nuclear weapons.

The second form of power is *Institutional Power* which is derived from the soft power approach embedded through institution forms such as international organizations, standardization regimes, and even the internet itself (Stevens&Kavanagh, 2021). The institutional approach aims to create indirect control by designing the architecture and rules of institutions in ways that are possible for their interest over others (Stevens&Kavanagh, 2021). To illustrate, the United States has used the institution of cyberspace to project its values by bringing and advocating their democratic norms to be universally agreed upon in an international forum. More totalitarian states like China and Russia openly oppose these norms. To counteract this movement, China and Russia use a similar method by engaging with like-minded countries to contest US values in cyberspace, such as the establishment of the Shanghai Cooperation Organization.

The third form of power is *Structural Power* which can be obtained through domination in the recent form of inter-relations. For example, the internet and cyberspace have now been dominated by US private firms, such as Cisco, IBM, Google, Intel, Apple, and Microsoft, which strongly favour the US policy. To counteract this dominance, China has advanced its technology and expanded its market through products such as

Huawei, ZTE, and Xiaomi, as well as through introducing its technology to emerging countries.

The fourth form of power, *Productive Power*, is often perceived as a smart power that can be obtained through constituting universal knowledge (Stevens&Kavanagh, 2021). For instance, the western media has been employed to narrate the news favourably from a western perspective. To restrict this type of influence, Russia disseminated fake news and disinformation to undermine the dominant viewpoint. Moreover, authoritarian regimes such as Russia and China limit and control citizens' access to information.

To summarize, the scholars view that cyberspace could be the ideal domain for States to project their power. The problem that emerges from this trend is that the power diffusion among states is getting narrow since not only big players could enter the arena, but smaller states could also play a significant role. Therefore, bigger states are struggling to ensure their power projection through three faces of power and four forms of power, which, when used ideally, could create tremendous cyber power.

2.1.1 Powerplays in Global Internet Governance

Power projection in cyberspace has created a chance for smaller actors to engage. Both Nye (2010) and Steven & Kavanagh (2021) agreed that States are no longer the only significant actors in

cyberspace. Few actors, like private firms, civil society, or even individuals, gain momentum to get involved. Cyberspace aimed to be governed with the multi-stakeholder model, which not only involve States as a policy maker. International Telecommunication Union (2012) expressed that internet governance is the development and application by government, private sectors, and civil societies in their respective rules of shared principles, norms, rules, decision making, procedures, and programs that shape the evolution of the internet. However, although the ideal model of multi-stakeholders internet governance has been established, Carr (2015) critiques that the legitimacy and accountability of such rule makers and rule takers were put in question. She affirmed that there is still a power mechanism reinforced through the current cyber governance dynamics.

To evaluate the role of power in global internet governance, it is crucial to identify the initial player on the field. Since the end of the Cold War, the United States has allocated a greater portion of the peace dividend to the development of information technology. Regarding a doctrine from the former US Vice President, Albert Arnold Gore (2000), information technology is a resource or source of power – by one which could be generated through human endeavour rather than extracted from nature. This notion marks the shift in US' preference for military technology. Instead of highly investing in expensive and sophisticated military technology, the US policy opts to maximize its potential in the

new domain: cyberspace. By participating in this new arena, the US believes it will be able to sustain its hegemonic status by establishing a productive and effective power. Furthermore, the US also started its campaign earlier by controlling the narratives, setting the agenda, and defining the terms of references (of cyberspace) in order to minimize (or delegitimize) dissent (Carr, 2015, p.642). In order to reach these goals, the US tries to manufacture the consensus by promoting its norms and values in cyberspace so that the opposite of this value leaves little room for alternative views.

The US also led multi-stakeholders cyber governance by establishing the Internet Corporation for Assigned Names and Numbers (ICANN). In the beginning, ICANN was created to facilitate assigning names and domains of the internet. However, in the end, it became a policy-making body that was heavily influenced by US policy. Carr (2015, p.648) views that ICANN is not able to facilitate an impartial view of the players in cyberspace; it only privileged the interest of actors that were instrumental in its establishment, which is the US and its allies whose agenda aligned. This issue, therefore, raises a notion of broader states' involvement in internet governance.

The US may promote the limitation of the state's involvement in internet governance simply because its norms and values have already taken root in the multi-stakeholders system that it established. The ICANN and the US private companies already dominate universal

cyberspace, and their stance is closely related to the US policy: hence they will always support the US objectives.

To oppose internet governance that solely relied on the US and the ICANN, the UN established the Internet Governance Forum (IGF) in 2005. This came as a result of an intergovernmental discussion at the World Summit of Information Society (WSIS) held in Tunisia. The reason member states need to initiate the intergovernmental forum is because internet governance includes more than internet naming and addressing; it also includes other significant public policy issues such as, *inter alia*, critical internet resources, the security and safety of the internet, and developmental aspect and issues pertaining the use of the internet (ITU, 2005). The 2005 summit was surrounded by governments fighting over ICANN's domain name governance which is firmly controlled by the US. China, for example, viewed that the UN's role in international internet management should be allowed in full scope; meanwhile, some EU member states endorsed replacing ICANN with an intergovernmental group (Maurer, 2011, p.46). Despite the establishment of the IGF to replace ICANN, many issues are still untouched by its mandate. For example, the IGF mandate pertaining to cyber security is only helping to find solutions to the issues arising from the use and misuse of the internet, of particular concern to everyday users (ITU, 2005). It is to imply that IGF is only governing the use of internet in the regular use and in its peaceful state. Nevertheless, the outcome document of the summit does

not mention the protection of critical information infrastructure, and it does not refer to the resolutions on the criminal misuse of information technologies (Maurer, 2011, p.46). This evidently shows the lack of UN involvement in the governance of ICT when used for harmful purposes.

Discussion related to internet governance became more polarized when the ITU convened the World Conference on International Telecommunication (WCIT) 2012, held in Dubai. This conference intended to review and revise the 1988 International Telecommunication Treaty (ITR), which includes a relatively technical treaty establishing the principles for global telecommunication infrastructure. However, the United States voted against the passage of a "binding" global treaty to act as a review and update on how international interconnection and interoperability of information communication services work (Carr, 2015, p. 653). The WCIT-12 galvanized and polarized these differences of approach: on the one hand, the Western democracies and their allies led by the US held the status quo of a light-handed and multi-stakeholder approach regarding internet governance should be maintained, including non-state actors that have so far played a key part in internet evolution; and on the other, the more restrictive regimes of the freedoms of expression and access, led by China, Russia, and some Arab states, advocated heavier regulation, with a greater role for state intervention in both internet and traffic content (Housen-Couriel, 2012, p.87-88). The end result of this conference was a sharp division between those

countries that signed the ITR's 2012 revisions and those that refused to do so, remaining only bound by the 1988 version of the ITRs (Housen-Couriel, 2012, p.88). By rejecting the revisions, these countries expressed their opposition to what they saw as a concerted effort by non-Western countries to establish an interventionist and anti-democratic regulatory model of internet governance. They concluded that a United Nations takeover of the internet could provide more authoritarian regimes with a potential victory in their quest to control the internet.

To fight the US objective, other smaller, new developing countries, as well as countries who simply oppose US cyber supremacy (Russia and China), highlight the importance of government engagement in internet regulation due to their views about sovereignty. Surprisingly, the European Union, whose its objective is mostly aligned with the US, has recently introduced its cybersecurity strategy, which campaigned for technological sovereignty (European Community, 2020). In addition, smaller and developing states recognize the significance of discussing internet governance in a multilateral forum since they have the opportunity to participate in and contribute to the formulation of globally binding principles. On the other side, authoritarian states like Russia and China saw it as an opportunity to challenge US norms, such as internet freedom, on the basis of their own territorial sovereignty.

In conclusion, power plays an important role in the cyberspace domain. Maintaining the status quo is the only way for the United States, which pioneered the concept of cyber superiority, to continue to govern. Many of the proposed multi-stakeholder approaches to control cyberspace are tied to the US national internet. In addition, efforts to incorporate additional actors in governance, such as private companies, also benefit the US agenda. Existing cyber governance frameworks with several stakeholders lack openness and accountability. In spite of the fact that this form of government encourages individualism and participation in civil society, it does not contribute in practice. At the end of the day, the United States maintains control over cyber governance.

2.2 Cyber Operations

There are many debates among scholars on whether States can utilize cyberspace to launch a military attack. For decades, a military attack is always associated with kinetic weapons and physical destruction. However, the emergence of information technology has brought discussions on whether military attacks nowadays could simply be employed in cyberspace. In addressing this issue, Clarke & Knake (2010), discussed the possibility of cyber war and its next threat to national security. Furthermore, they affirmed that in military activities, utilization of cyberspace has become more common. Countries such as

the US, Russia, and China which are notably known as the top three military power in the world have already established their own cyber military command. According to them, these military and intelligence organizations are preparing the cyber battlefield with things called “logic bombs” and “trapdoors,” placing virtual explosives in other countries in peacetime (Clarke&Knake, 2010, p.12). In essence, cyber operations have been the choice of military activities by larger countries. Hence, it is important to understand how cyber operations are employed and what can be constituted as a cyber-attack.

To date, there are many terms associated with cyber operations, such as cyber-attack and cyber warfare. Many scholars attempted to expand its definition of it. For example, military practitioners tend to opt for terms such as cyber warfare due to their associated professional tasks. As opposed to this, many international law commentators tend to use the terms cyber-attack. For them, it is essential first to define what constituted a cyber-attack in relation to the international law principles governing the resort of force: *jus ad bellum*. Nguyen (2013, p.1085) captured the overwhelmed explanation of cyber-attacks until today. In order to narrow the definition to be reviewed under the subject of international law, she argued that there are problems in defining cyber operations according to the subject level that it analyzed, whether it analyzed cyber as an instrument to employ an attack or cyber as an object to be attacked. She, thus, defines cyber-attacks as hostile acts

using computers or related networks or systems to cause a disruption or destruction of a political or national security objective (Nguyen, 2013, p.1089).

The next part of this chapter will give a more comprehensive discussion regarding cyber operations strategy. It aims to explore certain cyber operations as well as their methods and motives.

2.2.1 Cyber Penetration Attack

Cyber penetration attacks are used to break into a computer system, access its resources, and then deliver the payload that was intended for them. The term 'payload' describes the actions that can be executed once the vulnerability has been exploited (Nguyen, 2013, p.1092). Cyber penetration attacks are launched by taking advantage of system vulnerabilities. If an attacker is successful in directly penetrating a system by, for example, gaining access to it locally by exploiting security flaws in a local area network or remotely by connecting to it through an unencrypted wireless network, then the attacker will be able to directly access and modify files in order to accomplish a wide variety of their objectives.

The objective of this method is to intrude into the specific system and gain access and command to it according to its mission. Cyber penetration works by employing malicious software 'malware' that is specifically designed to damage, disrupt, steal, or in general, inflict some

negative or illegitimate action on data, hosts, or networks (Nguyen, 2013, p.1094). A popular method that is commonly used on this method such as inserting a virus into the USB stick or hard disk as well as tricking the user into clicking or downloading specific websites that contain malware, such as email phishing. The advantage of this method lies in the malware's code, which is designed so that user activation is no longer required to activate the mission. Instead, once the malware has gained access to the target system, it replicates and automatically weakens or shuts down the entire system.

Examples of operations using a cyber penetration attack happen in the Israeli airstrikes case in Syria as well as the popular Stuxnet cases. In September 2007, the Israeli Air Force was able to penetrate Syrian territory and destroy a facility suspected to hold a collaborative nuclear program between Syria and North Korea (Clarke&Knake, 2010, p.29). As much as this occurrence draws public attention to Israel's military capabilities, the primary discussion focuses on how Israel was able to intercept the most modern air defense system that Damascus had purchased from Moscow (Clarke&Knake, 2010, p.36). Reportedly, the air defense surveillance system failed to alert when an Israeli jet fighter entered Syrian territory at that time. One apparent conclusion that can be drawn from this incident is that the Israeli military was able to hack Syria's air defense system, thereby concealing their strike operation.

A few years later, Israeli and American were suspected of infiltrating Iran for the same reason: to prevent the country from acquiring nuclear weapons. However, the tactics of covert action employed at this time were entirely based on non-kinetic weapons. Iran's nuclear centrifuges program was destroyed with the help of Stuxnet, a well-known and sophisticated malware designed specifically for Siemens' software used in the Natanz nuclear facility (Lindsay, 2013, p.382). Thus, Iran's nuclear program was postponed for almost two years which allowed for further negotiation facilitated by the UN. It is, however, suggested that Stuxnet was inserted through the USB stick by one of the operators, thus facilitating its malware to replicate and destroy the centrifuges (Fildes, 2010).

The same pattern can be drawn from these two scenarios regarding how cyber capabilities were used to compromise an adversary's critical object. Although, in the first scenario, cyber capabilities were used to manoeuvre the attack while the attack itself was carried out with kinetic weapons (i.e., a missile launched by a jet fighter), the appearance of hacking a system remains critical to the success of this action. In comparison, the second case demonstrated that full-fledged cyber operations could achieve the same result: the ultimate goal of this action was to shut down other states' nuclear reactors that had been used for non-peaceful purposes. Based on these two incidents, it is possible to conclude that cyber capabilities can be

used as a weapon that is just as lethal as a conventional kinetic weapon, if not more efficient. Regardless of the method used to implement this strategy, cyber capabilities used as an instrument have been shown to achieve those military and political goals. These examples show how cyber capabilities were used as a means, instrument, and weapon of attack.

2.2.2 Denial of Service Attack

A denial of service (DoS) attack is also one of the prominent methods in employing a cyber-attack. In contrast to a cyber penetration attack, a denial of service (DoS) attack seeks to disrupt a computer system so that it would not be able to function normally. A denial-of-service attack is executed by bombarding a particular target with a large number of fake requests for service (Clarke&Knake, 2010, p.57). This causes the target's resources to become depleted, which prevents other users from making use of those resources. In addition to the standard Denial of Service attack, a distributed request coming from a variety of unique sources is a more effective way to interfere with the operation of an entire network or website; it is often called Distributed Denial of Service attack (DDoS). The Distributed Denial of Service attack is carried out by commanding multiple infected computers, or botnets, to perform the same action, which is to make a service request to a particular website or network provider (Nguyen, 2013, p.1097). As a

result of too many commands and requests, those networks or websites were unable to respond, at the same time, resulting in a processing halt.

In 2007, Estonian DDoS attacks were a famous example of this technique. The 2007 Estonian DDoS attack occurred after the removal of a Soviet Red Army statue in Tallinn, which is alleged to have prompted a Russian hacker to overload a crucial Estonian website with requests for access. The DDoS attack was carried out by creating thousands of computer systems, known as "zombie computers," that were tasked with flooding a website such that it could not run at its typical speed and frequently failed to perform its primary job (Clarke&Knake, 2010, p. 59). A similar tactic was also applied in Georgia, causing harm to people's access to information and necessities such as the internet banking system. However, the damage inflicted by this strategy is restricted to the disruption of daily live operations; it does not necessarily involve physical destruction or damage.

2.3 Applicability of International Law in Cyberspace

2.3.1 Use of Force, Self-Defense, and Armed Attack.

Whether cyber operations or cyberattacks could constitute a use of force, trigger the right to self-defense, or even qualify as an armed attack has been a central topic of discussion among international legal experts. Due to the lack of specific international law in cyberspace, the

existing principles of international law have been used to guide the conduct of states in cyberspace. In this instance, the UN Charter, as a widely accepted standard, became the definitive guide for interpreting cyber-attack. In addition to being legally binding for all UN member states, it is also becoming customary international law, which shall be followed regardless of UN membership.

The law of prohibition of the use of forces is clearly enshrined in the Article 2(4) of the UN Charter (1945)

“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.”

The problem that emerges is that the UN Charter does not explain in detail what constituted a use of force. Furthermore, many scholars argue that activities in cyberspace are not forceful in nature (Schmitt&Vihul, 2017).

Due to many interpretations of how the use of force could be conducted, it is first necessary to revisit other articles in the UN Charter related to the applicability of the use of force. According to Article 51 of the UN Charter, the applicability of the use of force is only granted under two conditions: first, it could be operationalized under the right of self-defense, in which the State has experienced an armed attack from the other State; and second, when such an action is authorized by the

Security Council. The authorization of action that could be employed by the Security Council is further detailed in both Article 41 and Article 42. Article 41 mentioned that the Security Council may decide what measure that is not involving the use of 'armed' forces, such as complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations. While Article 42 suggested that if such a method employed in article 41 is not adequate, Security Council may use techniques that utilize land, sea, and air forces. To sum up, the UN Charter has successfully divided which actions constituted the armed forces and which ones that do not. In this sense, perhaps the principle of *lex specialis derogate lex generalis*; where specific rule will prevail over general rules could be applied. As a result, in reviewing back to article 2(4) the term use of force shall be interpreted as both the coercive measure which includes armed and non-armed methods.

After deconstructing the applicability of the use of force, it is necessary to evaluate the legal principles governing the use of force: *jus ad Bellum* as it pertains to cyber operations. According to *jus ad Bellum*, when certain conditions are met, the State can inherit the right to engage in self-defense through countermeasures. Nguyen (2013, p.1124-1125) presented her argument regarding the most appropriate method for determining whether a cyber operation or cyber-attack constitutes the use of force and an armed attack. First, she evaluates three prominent

jus ad Bellum approaches: the instrument-based approach, the target-based approach, and the effect or consequence-based approach (Nguyen, 2013, p.1117). She argues that despite presenting a useful analogy and insightful observation, each approach has significant theoretical and practical flaws (Nguyen, 2013, p.1124-1125). Therefore, she proposes her own approach based on intentional damage in the cyber-physical system (CPS).

The instrument-based approach is useful for determining whether cyberattacks could be classified under a subject of international law. However, this approach is outdated and implies that conventional or kinetic weapons are the only measures that could be classified under the use of force or an armed attack. In the meantime, a cyber operation dependent on the non-kinetic weapon is brought into question. The instrument-based approach looks to the principles of *ejusdem generis* (of the same kind, class, or nature) and *noscitur a sociis* (a word is known by the company it keeps) which conclude that a cyber-attack, by definition, cannot be a force or armed attack because the instrument used is not forceful in its nature (Nguyen, 2013, p.1079). As a result, although consequences derived from the non-kinetic weapons reach a threshold of a kinetic weapon, or it is to say that it could create the same devastating impact, it will not inherit the right of self-defense to the States. To illustrate, a cyber-attack that destroys electrical power grids and oil gas pipelines, disrupts emergency response communication

systems, and causes weapon systems, automobile safety, and medical devices to malfunction would not trigger UN scrutiny (Nguyen, 2013, 1119).

A second approach is a target-based approach which focuses on the status of the target of attack. Critical infrastructure may be widely used as a vulnerability target and thus needs to be protected under the international law of *jus ad bellum*. However, there is yet a consensus on what is listed under the subject of critical infrastructure. The problem of focusing only on the target of the attack will leave a very narrow interpretation of the right of self-defense. It is so dangerous that States could use this approach to justify an act of self-defense when only a small amount of disruption is employed to their critical infrastructure. According to Nguyen (2013, p.1121), if such an approach is used, then the employment of a DDoS attack in Estonia would qualify them to inherit the right of self-defense, although only little damage was done. If these justification methods were frequently used, international relations would be subject to an exaggerated accusation and legal justification.

The third approach that more comprehensively assesses the situation related to cyber-attack would be recognized as an effect-based or consequence-based approach. This approach was introduced by Michael Schmitt (2011) and also inserted into Tallinn Manual, which has been used widely in interpreting international law applied in cyberspace and thus endorsed by NATO accredited cyber defense hub (CCDOE).

This approach focused on the damage that resulted from an attack. According to Schmitt (2011, p.575), the threshold for the use of force must therefore lie somewhere along the continuum between economic and political coercion, and on the other hand, an act that cause physical harm on the other. However, it is necessary to note that such a coercive activity that includes economic and political character of coercion is not considered a use of forces based on the debate within UN member states in the proceeding of the UN General Assembly's Declaration on Friendly Relations (Schmitt, 211, p.569). Furthermore, he affirmed that cyber operations that directly result (or are likely to result) in physical harm to individuals or tangible objects equate to armed force, and therefore use of force (Schmitt, 2011, p.573). From this perspective, Schmitt attempts to present a clear distinction between what constituted the use of force and how the use of force reaches a threshold of armed attack.

Furthermore, Schmitt (2011, p.569-570) identified a number of factors that are likely to be used to determine when cyber operations constitute the use of force. These factors include severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, and responsibility. However, in the second edition of the Tallinn Manual, Schmitt (2017, p.335-337) revised these factors to exclude responsibility and include other two factors which are state involvement and military character. According to Schmitt's interpretation, cyber operations

conducted in Estonia DDoS attack could be categorized as use of force because it can satisfy those aforementioned factors. Moreover, it caused a large-scale disruption of the daily lives of Estonian for 22 days attack and severely damaged the inherently governmental function. Despite the fact that this attack constituted the use of force, Estonia would not inherit the right to self-defense because these attacks did not meet the threshold for an armed attack.

In contrast to Schmitt's perspective, Nguyen (2013, p.1078-1079) argued that Schmitt's interpretation can be easily manipulated to support the geostrategic objectives of the nation conducting the investigation. In addition, its application is inconsistent. In essence, Nguyen argued that an effect-based framework could vary from country to country based on the characteristics of the target nation. For instance, China, which has complete control over its cyberspace, could reduce the damage caused by a cyber-attack by simply shutting down all communication infrastructure, whereas the United States would require more bureaucracy and congressional approval. Therefore, based on this perspective, Nguyen offers her own approach to a cyber operation based on the actions and intents of attackers as well as on the defensive capabilities of the victim. This approach is called intentional damage to the cyber-physical system.

Based on this new approach, Nguyen (2013, p.1127) concluded that cyber-attack that do not threaten or result in physical effect should

not constitute force under *jus ad bellum* because such attacks are largely reversible. Hence Estonia DDoS attack would not be constituted as the illegal use of force from her point of view. On the contrary, she presented the idea that such an attack could reach a threshold of illegal use of force when the acts endanger not only life but also property, instilled fear, and threaten the nation's state sovereignty (Nguyen, 2013, 1125). Furthermore, she affirmed that an attack should be harmful to not only critical infrastructure but the cyber-physical system as a whole (CPS). Apart from that, she also indicated that a cyber-attack would be constituted as an armed attack when they are intended to cause an irreversible disruption or physical damage to the cyber-physical system (CPS) (Nguyen, 2013, p.1125).

Based on these four perspectives, I concluded that Nguyen's perspective, despite its attempt to form a new and more focused approach, lacked a clear definition and illustrative example of what cyber-attacks could be considered the use of force. Moreover, I believe it to be quite contradictory that she rejected the DDoS attack in Estonia as the illegal use of force while simultaneously including the threat to the state sovereignty and territorial integrity of a nation in her definition of illegal use of force. As a result, I conclude that Schmitt's approach, which is based on effect, damage, and consequence, is more reliable for assessing the level of force used in cyberattacks. In addition, it clearly

differentiates between what constitutes an act of use of force and what constitutes an armed attack.

To sum up, a cyber-attack or cyber operation is difficult to evaluate due to the multiple perspectives it offers. Therefore, I felt that justifying a cyberattack that reached the threshold of use of force or even armed attack would require an adequate understanding of the applicability of international law and could not be generalized; rather, it should be evaluated on a case-by-case basis. Although Schmitt's perspective on the consequence-based approach provided the most appropriate lens through which to examine cyber operations, Nguyen's perspective on emphasizing 'territorial integrity, state sovereignty, and political independence,' which is enshrined in article 2(4), is also essential when assessing cyber operation cases comprehensively. This is to say that I also wanted to point out that article 2(4) does not only discuss the use of force but also includes other important statements, such as "in the purpose of the United Nations," which many legal scholars failed to recognize. Thus, I reaffirmed unequivocally that cyber operations must be reviewed not only when they reach the threshold of use of force or armed attack, but also when they pose a threat to the fundamental purpose of the United Nations, which is maintaining international peace and security.

2.3.2 Non-Intervention

The terms "non-intervention" and "non-interference" are often used interchangeably to describe fundamental international principles that explain the prohibition of States from intervening in another State's exclusive right to govern. In essence, non-intervention principles prohibit direct or indirect intervention in which the state is permitted to freely decide, such as the choice of a political, economic, social, and cultural system and the formulation of foreign policy (Delerue, 2020, p.235). Furthermore, the principle of non-intervention is also endorsed under the UN Charter article 2(7), which emphasized the respect of a state's sovereignty to be free from interference from other states.

The principle of non-intervention is further elaborated under the ICJ case of Nicaragua. According to the ICJ, the principle of non-intervention shall forbid all States or groups of States to intervene directly or indirectly in the internal or external affairs of other States (ICJ, 1986). Summarizing the verdict of the Nicaragua case, Delerue (2020, p.238) defines three elements that constituted unlawful intervention. The first element is such action should be conducted by States. It is evident that the violation of international law could only be done by States or attributed to the States. Second, such action aimed to coerce another. And the third element is the action influences the ability of another to freely decide. A case of prohibited intervention would be exemplified by States or a group of States supporting a belligerent in an attempt to

overthrow the legitimate government of another State. Even if there is no use of force apparent, providing financial, training, weapons, intelligence, and logistical support to belligerents would constitute a violation of the principle of non-intervention (Delerue, 2020, p.237).

Several cyber operations were evaluated by Delerue (2020, p.239-244) in order to provide a clear illustration of how unlawful cyber operations violate the principle of non-interference. The first incident involves Sony Pictures Entertainment (SPE). In 2014, SPE was preparing to release the satire-comedy film 'The interview', which depicts the North Korean dictatorship in its plot. However, prior to the release of the film, SPE was subjected to a tactical network attack that delayed the distribution of this film. Although many have asserted that hackers backed by North Korea were responsible for this cyber operation, there is no evidence to support this claim. Consequently, based on Delerue's element, this form of intervention could not be justified as unlawful state intervention. In addition, despite the delay in the film's release, SPE was able to distribute this film globally. Consequently, no other elements of the intervention are violated, as the SPE is able to freely decide its own action. In conclusion, there is no violation of the non-intervention principle in this instance.

The second case to be assessed is the Stuxnet case. Stuxnet was known as the first cyber case that constituted the use of force. Despite causing the Natanz nuclear facility to halt its operation due to physical

damage, there is no clear evidence that this incident is attributed to an act of States. However, many reported that this case was a joint covert action of Israeli and US intelligence. Apart from this accusation, the US maintains its plausible deniability on the involvement of such action. In the end, the elements of the principle of intervention that proves the involvement of the state are not able to justify. In spite of the controversy that has surrounded the Stuxnet effect, the perpetrators of the attack have not been held accountable. This is due to the fact that Iran was thought to be developing nuclear technology for nonpeaceful purposes, which would put the safety and tranquillity of the world in jeopardy.

Another cyber operation worth mentioning is the case of the US 2016 & France 2017 Presidential elections. It is expected that both cases are employed by hackers related to the Russian intelligence services. Although both US and French authorities filed a complaint directed to the Russian government, the judicial proceeding failed to perform due to the Russian rejection of such a request. If only Russian involvement could be proven, this form of intervention could be justified as unlawful. To support this argument (Delerue, 2020, p.248) confirmed that a state's interference in the election process of another State constitutes a form of coercion by one State restricting the ability of another to freely decide its internal organization and government. In addition, if the foreign interference in the elections takes on a more intrusive dimension, for example, if the Russian Federation intelligence community hacked and

published stolen data, this would clearly constitute unlawful intervention, the same case with manipulation of voting machines in order to change the result of elections clearly constitutes an unlawful intervention (Delerue, 2020, p.249).

To sum up, from the above-mentioned cases, foreign meddling in the form of intervention in cyberspace faced one significant problem: attribution. It is to say, the problem of attribution of such an act to the States is often denied and lacks evidence. Although these cyber operations are clearly satisfied the element of coercion and hinder the ability of the States to freely decide, the evidence of the state's involvement is still necessary in order to proceed these cases under the subject of international law. Although the Tallinn Manual proposes to solve the attribution problem with the principle of due diligence, which emphasize that States must not allow their territory to be used in any way that could affect the rights of other States or produce serious adverse consequences for them (Schmitt, Vihul, 2017, p.30); the applicability of this method is still put in question. For instance, Russian authorities might refuse the United States request to carry out an appropriate investigation by referencing immunity as a justification.

The attributional issue may pose a challenge to Delerue's method for determining prohibited intervention. In order to demonstrate that the principle of non-intervention can be applied effectively to the complexities of contemporary international relations, particularly cyber

operations, Moulin (2020) attempted to present his own approach. In this state, Moulin attempted to shift the focus of the form of intervention from *domaine réservé* to *domaine privilège* and to redefine coercion as a deprivation of control (Moulin, 2020, p.1).

Domain réservé or reserved domain refers to the territory in which States can exercise their authority. In other words, *domaine réservé* refers to the area of States that are exempt from international obligations and regulations (Moulin, 2020, p.8). According to Moulin, the non-intervention principle's applicability in this domain is obsolete; it requires a specific modification to align with contemporary State practices. Therefore, a more contemporary approach that includes *domaine privilège* is required. The reason behind *domaine réservé* is no longer suitable to respond to the revolutionary of international law and states conduct is due to its shifting contours. Many subjects in international law have evolved while a reserved domain still sticks to the traditional areas of state government which fall into the scope of land, sea, air, and other physical territorial integrity. To give a clear example, *domaine réservé* does not regulate state affairs in economic areas although it is getting more relevant in the present day. Therefore, *domaine réservé* is so antiquated that it fails to regulate cyber operations directed solely against private actors, even if they are essential to the state's social and cultural system (Moulin, 2020, p.10).

To complement his thesis, Moulin modified the non-intervention principle to use *domaine privilège*. According to Moulin, *domaine privilège* presents clear-cut contours which remain unaffected by the development of international law and protect the fundamental interest of the state and its population (Moulin, 2020, p.11). *Domaine privilège* includes not only the elements necessary for the survival of the state but also essential for its independence, autonomy, and stability (Moulin, 2020, p.15). Therefore Moulin explains five characteristics of *domaine privilège* which help it to stay relevant in the applicability of the non-intervention principle: (1) it protects the political organization of the state, including the forms of government, the rule of law, personal, collective, and political freedoms, as well as the electoral process; (2) it encompasses internal and external security; (3) it incorporates major economic interest; (4) it embraces public services including health and social system; and (5) it extends to the preservation of states' environment. By applying this component of characteristic to ongoing cases of cyber operations, such as the hacking of Sony Pictures Entertainment or foreign interference in the election, it is possible that a violation of non-intervention could be justified. This is due to the fact that the case in question breaches the characteristic of *domaine privilège* that was mentioned earlier.

2.3.3 Sovereignty

The principle of sovereignty has been the most fundamental norm that regulates international relations. It is stated in the UN Charter Article 2(1) that all member states enjoy the basic principle of sovereign equality of member states. The principle of sovereignty is often associated with and cannot be separated from its territorial integrity. And this notion has also been emphasized in the UN Charter Article 2(4), where the territorial integrity of states shall be respected, and thus any use of force is prohibited. Another prominent definition of a state's sovereignty is also introduced by the Permanent Court of Arbitration in the case of the Island of Palma (1928), which refers to sovereignty in the relations between States signifies independence, and where 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.

To summarize, sovereignty and territorial integrity are two sides of the same coin. States enjoy their exclusive right to control and have the authority above their appointed territory. The problem with this territory-based approach is that it refers to the old interpretation which defines a state's territorial integrity to be limited only to its lands, internal waters, territorial seas, archipelagic water, and airspace above the areas (Delerue, 2020, p.203-204).

A state's claim over some territory often faces a dispute and debate under international law. We would not forget an attempt of states

to claim its archipelagic water under the UNCLOS negotiation. However, the land, sea, airspace, and outer space, which have been a subject of international law, are considered physical realms. Therefore, the question of whether sovereignty extends to the virtual sphere, cyberspace, has sparked a debate.

According to Tallinn Manual (Schmitt & Vihul 2017, p.11-19), the principle of sovereignty extends and applies to cyberspace. While cyberspace is a fictional territory, it is based on real and tangible infrastructures because computer networks and their components are located within the territorial sovereignty of States (Delerue, 2020, p.206). Furthermore, this principle is recognized under the UN GGE Report in 2013, where no States expressed disagreement or submitted any reservation (Delerue, 2020, p.207). On the basis of this approach, we might conclude that states have control over the physical infrastructures of computer networks that are located both within their areas of territorial sovereignty and in other locations over which they have jurisdiction.

While States have enjoyed their exclusive right under their jurisdiction, the problem occurs when states violate another state's territorial integrity? According to Tallinn Manual, violation of sovereignty can only be done by the States. It is to say such breach from an individual or organization which are not associated with the State could not qualify as a violation of the principle of sovereignty. Furthermore, Tallinn Manual expressed that violation of sovereignty could only be qualified by

assessing the threshold of harm that resulted from the breaching activities. In essence, such a cyber operation would only be unlawful only if there is physical harm and loss of functionality apparent, especially in relation to the inherently governmental functions (Schmitt & Vihul, 2017, p.20). This approach is concluded due to friction between States that justified some cyber operations such as stealing and collecting data are commonly used in espionage. Whereas the espionage act is not regulated under international law.

To oppose this view, Delerue (2020, p.211-212) concluded that even if (cyber) espionage is not *per se* regulated under international law, such an action still violates the state's sovereignty. And I agree with this perspective because the fact that there are no specific rules that interpret violation of sovereignty could only be justified if such damages or loss of functionality is apparent. For example, many states accuse other states of violating their territorial integrity when an unauthorized plane or ship enters their jurisdiction. In this stage, States are not afraid to launch a military intervention to stop an unpermitted vehicle from entering their territory. In other words, the trespassing of an unpermitted vehicle does not necessarily cause damage or interfere with the government functionality, but they are still unallowed and constituted as breaching of the state's territorial integrity. The same analogy should also be applied to a cyber operation that does not cause such damage or governance loss of functionality. As a result, any governmental acts, including cyber

operations, perpetrated on the territory of a foreign State without its consent constitute a violation of territorial sovereignty (Delerue, 2020, p.215). If a cyber operation penetrates the cyber infrastructures in the territory of a foreign State, this will irrefutably constitute a violation of territorial sovereignty (Delerue, 2020, p.214). Conversely, a cyber espionage operation that consists in spying on the data transiting via the territory of the spying State would not violate the territorial sovereignty of another State (Delerue, 2020, p.214). In conclusion, in order to be justified, a violation of the principle of sovereignty does not necessarily require the appearance of physical damage or loss of governmental functionality. This is due to the fact that state practices have evidently confirmed that action which intrudes on their territorial integrity would be constituted as an unlawful act.

2.4 Conclusion

From numerous pieces of literature addressing cyberspace and its use within the international security framework, there is yet specific research on how the UN specifically addresses the issue of cyber security. Some literature, particularly the international law related, touched upon the UN's role based on its UN Charter applicability; however, there is yet existing literature that reviews periodically the

notions and measures taken by the UN in order to create safe and secure cyberspace. As a result, the research will look upon this approach.

Chapter 3: Methodology

3.1 Research Design

This research will use qualitative methods, such as document and archival analysis, as well as critical discourse analysis (CDA) to complete the interpretation of the collected data. To keep the scope of the investigation manageable, this study is limited to the UN discussion in terms of emerging ICT in the context of international security ranging from 1998 and 2021. When the research size is narrowed, it is feasible to get an up-to-date view of the United Nations' strategy in its attempt to govern cyberspace in the context of international security. This research will elaborate on the discussion held at the UN General Assembly and its designated bodies, such as GGE and OEWG. The selection was made because other UN bodies are either unwilling or unqualified to address this subject in international security. For example, the UN Security Council continues to overlook the relevance of ICT development in the context of international security. At the same time, another UN subsidiary agency, the International Telecommunication Union (ITU), does not address the issue of the harmful use of ICT in hostilities.

In terms of applying critical discourse analysis (CDA), the primary focus of this study is located on the documents produced by the United Nations on the discussed topic of cyber security. CDA will be utilized to analyse the meaning in constructed context and assess the UN's change

of direction: the use of CDA in this course also includes critiquing the norm's formation process through contextual meaning. CDA is not only general commentary on discourse, it includes some form of systematic analysis in texts using a transdisciplinary approach; additionally, it is not just descriptive but also normative (Fairclough, 2010, p.56-57). Consequently, CDA enables researchers to demonstrate a connection between language and context because it could demonstrate the significance of language in social relations of power, and it could investigate how meaning is created in context (Bloor&Bloor, 2007, p.12). Therefore, language not only has visible consequences but also plays a significant part in the power dynamics that exist within global society and cyber governance settings. Criticizing the norm's creation process and its influence on society is a major part of the applicability of CDA in this course. Finally, this research will attempt to compare the report produced by the UN sequentially.

3.2. Data Collection and Selection Process

This research will collect the data through the documentary and archival selection process. It will use credible secondary sources based on the UN archives. According to Burnham et.al. (2004, p.11), using official materials that have been published by a government or international institution is more reliable because it includes material

circulated at the time or soon after the time of the event in question. Based on this, the UN archive on ICT security is supplemental for this research because they provide the closest interpretation of the event: these documents present the UN's primary representations in cyberspace governance.

To be specified, this research will use documents published in the archive of the UN Office of Disarmament for ICT Security. This archive has presented complete and sequential UN documents pertaining to the discussion of ICT security. These documents range from 1998-2021 since the establishment of this issue in the General Assembly. It will also touch upon the latest UN-cyber governance forum such as UN GGE and UN OEWG. Both UN GGE and UN OEWG offer the UN's overall objectives and proposals for enhancing cyberspace governance in the context of international security. Although these documents are not legally binding and just present a 'soft' law, all the proceedings taken within this forum are influential to the future of cyber governance. Hence, this selection process will help to answer the fundamental question in this research, which are the UN's actions pertaining to the emerging ICT security as well as its effort to provide a sufficient legal framework to maintain peace and security in cyberspace.

3.3 Data Analysis

Once the data have been fully gathered, the analysis will be conducted primarily by assessing the milestones of each document published related to international cyber governance. In this step, critical discourse analysis (CDA) will be utilized to assess the language and social construct developed by the outcome of the documents. In essence, the UN's position on the cyber-security debate will be determined by examining all language and phrases used in its official papers. It is believed that this method will also present varieties of discussions and distinct approaches of each member state which involved in the drafting of cyber security norms and standards.

CDA differs greatly from general discourse analysis because it emphasizes the critiques embedded in the research. Essentially, CDA includes systematic analysis in text, transdisciplinary analysis of relations between discourse and other elements of the social process, and addresses social wrongs in their discursive aspect and possible ways for righting or mitigating them (Fairclough, 2010, p.56-57). This research will present this line of analysis where the critiques derived from the finding of documents presented by the United Nations will be analyzed through transdisciplinary practices, such as international politics and international law. Furthermore, this research will put a "positive critique", such as how the UN should respond to the challenge

of its practices, to present the possible way to righting or mitigating social wrongs presented in the analysis.

In applying this method in this research, this study will focus on analyzing products (reports) that resulted from interactions within the UN member states regarding cyberspace governance. In order to provide a critical analysis based on this course, this research is supported by the theoretical framework presented in the previous literature review. Moreover, a comprehensive understanding of this topic would also benefit from using tertiary sources such as the Tallinn Manual, which elaborates on the norm creation process under the framework of UN GGE. In the end, this research will be able to investigate how ideologies are inserted into each language and discussion. And finally, this research will display the use of language as a power projection within the UN institutional debate.

3.4 Methodological Reflection

CDA has a wide range of analytical tools that investigate the relationships between language and power. It is also important to build awareness in the context of language and ideology. There are several advantages of using critical discourse analysis as a methodology. First, it is a powerful tool for social and political criticism. Second, it is not explicitly linked to any theory; it allows for a wide range of approaches to

be used in the research, thereby allowing for more theoretical flexibility (Fairclough, 2010, p.57). In essence, CDA is a method that offers flexibility in terms of assessing social reality. It is not only text or language analysis but also situational analysis, which includes another theoretical approach to establish its critiques.

CDA, in this sense, is a methodology that can be used to study the strategies conducted by the United Nations to manage the issue of cyber security. This methodology can help identify the underlying assumptions and ideologies guiding the UN's approach to cyberspace governance. More importantly, critical discourse analysis can also help uncover the power relations that shape the UN's cyberspace policymaking process. It allows for a detailed and nuanced analysis of the strategies and the discourses surrounding them. This can provide valuable insights into the effectiveness of the process and how different stakeholders perceive them (Fairclough, 2010, p.45). Applying this methodology can assist in developing context and strategies by providing a critical evaluation of the existing ones. Finally, this methodology help researcher raise their awareness of the role of discourse as a controlling force in society and gain a better understanding of how language is used to persuade and manipulate.

In summary, CDA strongly relies on interpretation, which leads to various researchers reaching different results about the same data. Furthermore, CDA can be seen as overly critical and may not be able to

capture the positive aspects of the strategies the UN has already put in place. It is possible to undertake such text assessment using CDA, but it would be not easy to do so using other approaches. Ultimately, every qualitative investigation has a few difficulties to be aware of; qualitative analysis is always subject to the researcher's prejudice and presumptions as an interpretation-based method. In order to avoid potential bias in the interpretation of this research, the findings will be cross-checked into prominent tertiary resources, such as the Tallinn Manual, which was broadly used to comprehend the applicability of international law in cyberspace.

Chapter 4: Findings

This part will examine the notions and measures taken by the UN to address the malicious development of ICT that threatened international peace and security. Ideally, the peace and security issue shall be discussed under the UN Security Council's authority. However, because of the lack of UNSC involvement, this finding will be based on the UN General Assembly's conduct and adopted resolution.

In order to be able to perform an in-depth investigation of the narratives and the actions that the UN has taken, it is essential to be aware of United Nations' direction toward the aforementioned issue. To present this objective, the first section will study the UN's response to this issue through the resolutions approved by the UN General Assembly from 1998-2021. The second section will delve further into the reports of UN GGE, a special group designated by the UNGA and founded in 2004 to provide recommendations on this particular topic. And the third section will assess the report of the newly formed UN OEWG as the latest cyber-related discussion forum. Finally, these findings will provide a better understanding of how the principal policy-making body at the United Nations responds to issues concerning ICT and its relation to international security.

4.1 United Nations General Assembly (UNGA)

The United Nations General Assembly (UNGA) is the principal policy-making body of the United Nations, where all the UN member states participate and vote equally. This body has functioned as the primary platform for discussing emerging challenges in international relations. Article 11 of the United Nations Charter stipulates that the General Assembly plays a crucial role in making recommendations or considering any issue related to maintaining international peace and security and may call the Security Council's attention to this matter. In addition, the First Committee of the UN General Assembly is entrusted to maintain discussions on disarmament, global issues, and threats to peace that affect the international community, as well as seeking solutions to the challenges in the international security regime.

The emerging issue of the development of ICT and its impact on international security has been on the UNGA agenda since 1998. The topic has become the attention since the Russian Federation first brought this notion. In this stance, the Russian Federation proposed a draft resolution titled "Development in the sphere of information and telecommunication in the context of international security" in the UNGA's First Committee. This draft was then adopted under the UNGA Resolution 53/70 without a vote. Since then, the UNGA has placed this topic on its annual agenda for discussion, and several intergovernmental

processes have been established to address the security of and use of ICTs in international security (UNODA).

4.1.1 The notion in the UNGA Resolution 1998-2009

The UNGA resolution 1998-2009 marked the first term of resolutions adopted before a further measure was established: the United Nations Group Governmental Expert (UNGGE). Its contents are still limited as it showed the UN's early undertaking on ICT in the context of international security. However, from those resolutions, we could draw several significant notions that have been continually addressed, which are:

Civilian and Military Use

Civilian and military application is the frequently used phrase in the UNGA Resolution adopted from 1998-2009. In essence, the UNGA agreed to recognize that scientific and technological developments in information and communication technology (ICT) could have both civilian and military use. This notion attempted to draw the attention of the UN that ICT could be used for military purposes despite its positive contribution to civilian lives. Therefore, the resolution further recommends how States should react to the development of ICT for the military and not use such capability for nonpeaceful purposes.

Maintenance of International Stability and Security

This notion stresses the importance of viewing that technology developed under the ICT framework could potentially be used for purposes inconsistent with the objectives of maintaining international stability and security (UNGA, 1998). In short, it views that ICT technology could serve nonpeaceful purposes. This is why states consider acknowledging existing and potential threats that could be pertinent to these circumstances. Moreover, since 2001, States have already called upon the possible measure to limit threats emerging in this field with the need to preserve the free flow of information (UNGA, 2001). As a result, since the early undertaking of this notion, States have agreed to discuss the possibility of unauthorized interference or misuse of the ICT system.

In adopting these resolutions, various adjustments were made to the vulnerability object, which must be secured from ICT misuse. In 1998, it declared that nonpeaceful purposes of ICT could harm state security. In 1999-2001, the object was expanded to encompass civilian and military security. Since 2002, the idea has evolved that the misuse of ICT might impair the integrity of states' infrastructure, affecting their civil and military security. In this changing rhetoric, member nations began to define the threat posed by ICT.

Involvement of Non-state Actors

The role of non-state actors such as terrorists and other criminal groups has been introduced since the beginning of the resolution adopted. The States view that the threat coming from the misuse of ICT would not only be utilized by States; this platform will also be used to continually facilitate non-state actors to launch an asymmetrical attack on the sovereignty of other States. In addition, there is a concern about the utilization of ICT to be used for financing and recruiting terrorist organizations. Recognition of this notion was affirmed in the resolution, such as mentioning the result of the Ministerial Conference on Terrorism.

International Cooperation

Since the early adoption of the resolution, the UN has encouraged the member states to facilitate multilateral efforts to address this issue. But the notion of international cooperation just clearly stated in 2000 when the member states agreed to view that international cooperation is essentially required in terms of disseminating the use of ICT and means that affect the interest of the international community. Furthermore, the early measure to bring international efforts together was taken by convening an international meeting of experts in Geneva in August 1999 on developments in the field of information and telecommunications in the context of global security, which was an initiative taken by the Secretariat and the United Nations Institute for Disarmament Research.

Further cooperation is also encouraged by engaging member states to advise developing international principles that would enhance the security of global information and telecommunications systems and help combat information terrorism and criminality (UNGA, 2001). The last part of international cooperation that was encouraged stipulated in the 2005 resolution, which invites all member states to make an effort at the national level to strengthen information security and promote international cooperation in this field (UN, 2005a)

Establishment of the UN GGE

Acknowledging the vast development of ICT, the UN member states agreed in UNGA Resolution 56/19 2001 to form the first group of governmental experts in 2004. Members of the group were appointed by Secretary-General on the basis of equitable geographical distribution and were given the mandate to assess present and potential threats to ICT security, identify cooperative responses, and report to the 60th UNGA session in 2005. Despite the effort to hold three consecutive experts' meetings, the group failed to reach a consensus due to different perspectives and given the complexity of the issues (UNGA, 2005b). Due to this failure to reach a consensus, the 2005 UNGA resolution agreed to form the second round GGE to be established in 2009 with a similar mandate and expected to report to the 65th UNGA in 2010. Given

the 5 years gap in reporting, the group was expected to evolve and find common ground on the issue.

4.1.2 The notion in the UNGA Resolution 2010-2016

The phrases used in the following resolution adopted during 2010-2017 had no significant changes from the previous resolution (1998-2009). It continuously adopts a similar approach to address the issue. However, several additional phrases and measures in the following resolution include:

Recognition of the subsequent work from UN GGE

Three of the UN GGEs formed from 2010-2016 showed significant milestones for cyber-security related governance. The 2010 GGE was able to produce a consensus report under resolution 65/201. Since then, UNGA began to accept UN GGE's work as guidance for member states in addressing ICT in international security. Due to its success, the UN formed the 3rd UN GGE in 2012 with a revised mandate to include assessing norms, rules of responsible state behaviour, and confidence-building measures in information realms. The 4th UN GGE also followed to be formed in 2014 with the additional mandate of promoting a common understanding of the use of information and communication technologies in conflicts and how international law

applies to the use of information and communication technologies by States (UNGA, 2013).

All three GGEs successfully reached consensus reports which were affirmed through UNGA resolution adoptions. The latest UNGA resolution in 2015, however, used more assertive words to adhere to the GGE report. For example, the 2013 resolution used the word 'take into account' of the UN GGE reports meanwhile the 2015 resolution emphasized 'call on the member states to be guided' by the UN GGE report. With a successful round of GGEs, member states thus agreed to form the 5th round of it to be established in 2016. Further details on the report and narratives that presented by GGEs will be discussed in the second subsection of this chapter.

Applicability of International Law in Cyberspace

The 2013 and 2015 resolutions were monumental in emphasizing the applicability of international law, in particular United Nations Charter, to be essential in maintaining peace and security in cyberspace. It also reaffirmed that the result submitted by the UN GGE contained voluntary non-binding norms, rules, and principles of responsible behaviour of States in the use of ICT that would be significant to reduce risks to international peace and security (UNGA, 2015a). In addition, this resolution also touched upon the unique attribution characteristics of ICT

and address that norms related to it will be developed over times (UNGA, 2015a).

Despite acknowledgement from the UN, many legal practitioners also confirm the applicability of international law in cyberspace. Schmitt and Vihul (2014) identified that the inquiry's foundational premise is that the rules of international law governing cyber activities are identical to those applicable to other types of conduct. This notion is further detailed in their Tallinn Manual on the International Law Applicable to Cyber operations (2013; 2017). Moreover, Delerue (2011, p. 4) also reinstated that nothing prevents international law from applying to cyberspace and it does not constitute a new territory, area, or domain, conversely to land, air, seas, and outer space.

Respect for Human Rights and Fundamental Freedoms in the use of ICT

The notion of respect for human rights and fundamental freedoms in the use of ICT firstly appeared in the 2013 resolution. Since then, this notion is continually used in the following adopted resolution. However, there is no further explanation or elaborated clause presented in the upcoming UNGA resolution. Despite the lack of discussion within the UN, Schmitt and Vihul (2017, p.179) argued that it is widely accepted that international human rights that individuals enjoy 'offline' are also protected 'online'; however, under specific circumstances, States may limit exercise and enjoyment of certain rights. Further elaboration of how

human rights apply to cyberspace is necessary, but the UN seems to not be interested in discussing this theme in the realm of cyber-security.

Draft of International Code of Conduct for Information Security

In 2011, China, Russia, Tajikistan, and Uzbekistan submitted the draft of the international code of conduct (CoC) for information security to be circulated through the UNGA forum. This action aimed to establish international norms and rules guiding the behaviour of States in the information space at the earliest possible consensus (UNGA, 2011b). In summary, the CoC consisted of voluntary pledges of each State to comply with the UN Charter and its universally recognized norms as well as respect human rights and fundamental freedom and history, culture, and social system of all countries; not to use ICT for hostile activities which pose threats to international peace and security or proliferate information weapons; to combat criminal and terrorist activities using ICT; to ensure accessible ICT for every country and to prevent control of other ICT's resourceful States from threatening political, economic, and social security other countries; to bolster international cooperation in ICT within bilateral, regional, and multilateral platform; and to settle any dispute with a peaceful means and to refrain from the threat of use of force. The content of this draft of CoC was well noted by the member states, and it was acknowledged in both the UNGA resolution and UN

GGE report. However, there is no further action taken in the UNGA to adopt this resolution because several states had a reservation.

Because of this failed adoption, in 2015, the draft's content was updated to manage other member states' expectations. Some changes were introduced, especially in the use of 'the proliferation of information weapons' words. The 2015 report deleted that phrase and presented a more general point of view which only stated the prohibition of the use of ICT to carry out activities that counter the task of maintaining international peace and security (UNGA, 2015c). Moreover, this draft adds the norm of non-interference in the internal affairs of other States. Additionally, the new draft added the phrase of preventing other States from exploiting their 'dominant position' in ICT. It is estimated that this use of the phrase to limit Western dominance in their cyber infrastructure which was used universally. And in the end, this draft also emphasized the necessary protection of individuals in both offline and online environments; however, this shall be subject to certain restrictions, such as it should be in line with respect to the rights of the reputation of others and the protection of national security and public orders.

4.1.3 The notion in the UNGA Resolution 2017-2021

The year 2017 marks significant changes in how the member states view the importance of ICT technology in the context of international security. It also marks the decline of member states'

commitment to reaching a common understanding and consensus. It is evidenced by a failure of the 5th GGE to produce a consensus report. Additionally, for the first time since 1998, the UNGA failed to adopt a new resolution, therefore resulting in a weakened of the multilateral effort that has been built for more than a decade.

As a result of backsliding, in 2018, member states tried to discuss this subject more comprehensively. Starting from 2018-2020, there were two resolutions presented and adopted to address the question of ICT development in the context of international security: this marked the polarization of the UN. The first resolution, submitted and sponsored by Russia, was titled "Developments in the field of information and telecommunications in the context of international security", while the second resolution, submitted and sponsored by the US, was titled "Advancing responsible State behaviour in cyberspace in the context of international security." For the first time since 1998, the UNGA debated the role of ICT in international security with differing viewpoints. As a result, the following chapter will briefly analyze the changes in narratives and measures offered by each resolution.

4.1.3.1 US Sponsored Resolution

Overall, the resolution sponsored by the US (A/RES/73/266 in 2018, A/RES/74/28 in 2019, and A/RES/75/32 in 2020) had no significant changes in the contents compared to the previously adopted

resolution prior to 2017. It still borrowed the same narratives and approaches, although the adopted agenda was titled differently. The contents, however, added phrases such as confirming the dual use of ICT, which can be used for both legitimate and malicious purposes, and stressing the importance of utilization of ICT for peaceful purposes to prevent a conflict. Additionally, it also further confirmed the importance of confidence-building measures as well as capacity-building, which would promote a peaceful state in cyberspace. Moreover, it invited multi-stakeholders participation, such as private sectors, academia, and civil society, in discussing the issue of cyber-security. In the end, it requested the Secretary-General to establish the 6th round of UN GGE with a broadened mandate. For instance, the previous mandate had only encouraged the member states to promote understanding. However, in this renewed mandate, the UNGGE was also expected to implement effective measures.

As a result, in order to restore the consensus-based, this resolution also implements the new working method to employ a special session of UNGGE which includes two-day informal consultative meetings with all UN Member states under the open-ended framework presented by the Russian Federation. Finally, the 2019 and 2020 US-sponsored resolutions, also agreed to welcome the commencement of the work of the Open-Ended Working Group (UNGA, 2019a) and affirmed that the future framework for addressing this topic under the

UNGA platform would be considered based on the outcome from UN GGE and UN OEWG submitted in 2021 (UNGA, 2020a).

4.1.3.2 Russia Sponsored Resolution

Russian-sponsored resolutions (A/RES/73/27 in 2018, A/RES/74/29 in 2019, and A/RES/75/240 in 2020) presented different phrases, words, and sentences. Despite similar narratives which were brought compared to the US-sponsored, such as affirmation on the dual-use technology, it also presented several narratives and measures which are more detailed and distinct from the previous resolution.

Bridging the Divide

Russia-sponsored resolution firstly affirmed the urgency to bridge the development of the technological divide between member states. It recognized that some States might require assistance in their efforts to bridge the divide in the security of ICTs and their use (UNGA, 2018b). Hence, this resolution empowered the importance of capacity building which will bolster international cooperation and build confidence-building between States. In the end, this notion is believed to promote ICT to be used for peaceful purposes and would prevent conflict arising from its use.

Future Conflicts

In this resolution, member states agreed to address that ICT has been developed by member states for military purposes, and it is feared that it would be utilized in a future conflict. The agreed phrases in the resolution stated that “(the UN) expressing concern that a number of States are developing ICT capabilities for military purposes and that the use of ICTs in a future conflict between States is becoming more likely.” Furthermore, this resolution also touched on the embedding of harmful hidden functions which could be used by ICT to disrupt the supply chain of products and services, which would eventually damage national security (UNGA, 2018b).

International norms and principles

This resolution elaborates in detail which international norms and general principles of law that apply to cyberspace. By reinstating the commitment to adhere the international law and, in particular, the UN Charter, the 2018 resolution identified the importance to hold the principles of sovereign equality, settlement of international disputes by peaceful means, prohibition of the 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, respect for human rights and fundamental freedoms, and non-intervention in the internal affairs of other States (UNGA, 2018b).

In addition, the resolution also reaffirmed the applicability of sovereignty and non-interference principles. To illustrate, the resolution stated jurisdiction over ICT infrastructure within States, which implied that principles of territorial integrity apply to cyberspace. Furthermore, the resolution also emphasizes non-interference principles, especially related to the dissemination of false or distorted news and defamatory campaign or hostile propaganda for the purpose of intervening or interfering with other internal affairs of States (UNGA, 2018b).

Responsible State Behaviour

The problem of attribution has been a central discussion within the debate on the issue of cyber-security. Its norm and application are subject to further development as mentioned in the resolution that "... given the unique attributes of such technologies, additional norms can be developed over time" (UNGA, 2018b). As a result, Paragraph 1 of the 2018 resolution specifically addressed how States should conduct their responsible behaviour when such an attack using ICT is attributed to them. According to this paragraph, States first should not knowingly allow their territory to be used for internationally wrongful acts using ICT, including the use of proxy by non-state actors to conduct such actions; intentionally damaging critical infrastructure, or otherwise impairing the use and operation of critical infrastructure to provide services to the public; and supporting activity which harms the information system of the

authorized emergency response teams (UNGA, 2018b). These would summarize the obligation of States in the realms of cyber security.

Furthermore, States should present a fully cooperative behaviour in terms of conducting internationally wrongful acts attributable to them. In this respect, the attributed states would not be considered an aggressor without complete proof and evidence. Consequently, States shall collect all relevant information regarding attacks attributed to them, respond to the assistance request coming from a country whose critical infrastructure is subject to attack emanating from their country, as well perform appropriate mitigation to investigate an attack launched from their territory.

Establishment of Open-Ended Working Group

A failure to reach a consensus report in 2016-2017 UN GGE led to the forming of the UN Open-Ended Working Group, a more inclusive forum to discuss the issue of ICT in the context of international security. In the 2018 resolution, member states agreed to convene the Open-Ended Working Group by 2019. This group was mandated to further develop the rules, norms, and principles of responsible behaviour of States and the ways for their implementation (UNGA, 2018). Furthermore, this group aimed to be a framework to continue developing norms and principles related to ICT security. In addition to its mandate, this committee was tasked with bringing revisions, if necessary, to the

previously specified norms and principles and/or elaborating on additional rules of responsible behaviour. (UNGA, 2018). Besides its similar mandate to the UN GGE, this group was also expected to conduct intersessional consultative meetings with a broad participating party in a multi-stakeholder approach, which will include business, NGOs, and academia to discuss the issue of ICT in the purpose related to international security.

The urgent role of UN OEWG was continuously addressed in the following resolution of 2019 and 2020. The 2019 resolution further explained that the UN OEWG would operate simultaneously with the UN GGE, and their results will complement each other to address ICT in the context of international security. In addition, the 2020 resolution emphasized the importance of UN OEWG's democratic, inclusive, and transparent negotiation process (UNGA, 2020b). In response, the UN adopted Resolution 76/19 in 2021, establishing a mandate to continue convening the UN OEWG from 2021 to 2025 as the inclusive forum to examine the evolution of ICT in international security, with no mention of establishing the subsequent GGE. This decision marked the end of a divided perspective in the UNGA and the beginning of an endeavour to develop a shared understanding among member states. In the end, it was expected that the UN OEWG would operate under a consensus-based and results-oriented framework, submitting its final report to the 80th session of the UNGA assembly in 2025.

4.2 United Nations Group of Governmental Experts (UN GGE)

Article 22 of the United Nations Charter states that the General Assembly may establish subsidiary organs as it deems necessary for the execution of its duties. To address the complexity and development of ICT in the context of international security, the United Nations Group of Governmental Experts (UN GGE) was established in accordance with a resolution of the UNGA that outlines its functions and mandates. In total, six GGEs were constituted between 2004 and 2021, with four of them producing a comprehensive report that influenced the UN's response to cyber-security issue.

The work of the UNGGE is particularly illustrative. Most notably, it demonstrates the different positions defended by States on the norms-making process and their preference for non-binding norms, mainly norms of behaviour and confidence-building measures (Delerue, 2021, p.5). The UN GGE report in 2013 and 2015 marked a significant milestone for the UN governance of cyber security because they reinstated the applicability of international law, particularly the UN Charter, to cyberspace. However, departing from its conclusion, the 2017 meeting faced significant challenges as some States contested the applicability of entire branches of international law to cyberspace, such as the law of armed conflict, self-defense, and countermeasures (Delerue, 2021, p.5). The next subsection will briefly discuss the result and notions which were brought to each UN GGE.

4.2.1 Result of the 1st UN GGE 2004-2005

The first UN GGE was created under the UNGA Resolutions 56/19 in 2001. According to its mandate, the UN GGE was tasked to conduct a study on the concepts of strengthening the security of global information and telecommunication system. This group was aimed to be established by the Secretary-General based on equitable geographical distribution and with the help of Member States in a position to render such assistance. In the end, the group was encouraged to submit a report on the outcome of the study at the sixtieth session of UNGA in 2005. However, it failed to produce a report. It was presented in the UNSG report that, although the Group had a comprehensive-in-depth exchange of views, it failed to reach a consensus '*given the complexity of issues involved*' (UNGA,2005b). Therefore, the UNGA Resolution 60/45 (2005) aimed to form another UN GGE in 2009 with a similar mandate and to submit its report on the 65th session of UNGA in 2010.

4.2.2 Result of the 2nd UN GGE 2009-2010

In the hopes of achieving a feasible outcome, the UN agreed to convene the second UN GGE. Given the 5-year gap between the 1st and 2nd UN GGE, it was anticipated that the group would gain a broader perspective and achieve a consensus in discussing the complexity of issues involved in the development of ICT in the context of international security. The 2nd UN GGE marked an important milestone because, for

the first time, Member States agreed to develop a common understanding. Consequently, certain topics highlighted in the report of the 2nd UN GGE will be expanded upon as follows:

Threats to Critical Infrastructure

The first topic that was addressed in the 2010 GGE report was the potential use of ICT in threatening critical infrastructures. Because of the complex interconnectivity of telecommunications and the Internet, any ICT device can be the source or target of increasingly sophisticated misuse (UNGA, 2010b). It is affirmed in the report that the growing use of information and communications technologies (ICTs) in critical infrastructure creates new vulnerabilities and opportunities for disruption (UNGA, 2010b). In this sense, critical infrastructures are seen as objects where States are vulnerable. Although the report barely explains a further classification of critical infrastructures, however, it mentioned the possibility of ICT causing disruptive activities that target individuals, businesses, national infrastructure, and Governments alike (UNGA, 2010b). This perspective assumes that any infrastructure that serves the world community is susceptible to cyber activities. In the end, the group members agreed to mention that the threat emanating from this (cyber) action may cause substantial damage to economies and national and international security (UNGA, 2010b)

Dual use of ICT

ICT is believed to be used for both civilian and military activities. In the 2010 report, this notion is further affirmed according to a paragraph elaborating that the same ICT technology that supports robust e-commerce can also be used to threaten international peace and security (UNGA, 2010b). Frequently, the private sector owns the ICT infrastructures in whole or in part. This was especially problematic when civilian infrastructure was utilized for hostile cyber operations. A state could deploy cyber operations launched from private or civilian infrastructure as proxies to conduct hostile activities against adversaries. Finally, State might simply conceal its intentions and avoid international responsibilities by employing this strategy.

Attribution Problem

It was previously stated that the dual-use nature of ICT enables it to be easily camouflaged. As a result, identifying the perpetrators has been a prominent topic of discussion in the 2010 report. According to the research, ICTs are ubiquitous and widely available, therefore, it may be difficult to attribute the threats they pose. Typically, the perpetrators can only be inferred from the target, the effect, or other circumstantial evidence (UNGA, 2010b). However, they could launch an operation from nearly anywhere. As a result, these traits promote the disruptive use of ICTs.

According to the report, the threat posed by ICTs could emerge from various actors, such as criminal and terrorist organizations, as well as States themselves (UNGA, 2010b). As a result, there was a growing fear that states would utilize individuals or other organized groups as their proxies when initiating an attack against an adversary. In this 2010 report, the attribution problem remained unresolved due to this scenario. Uncertainty surrounding attribution and the absence of a shared understanding increase the likelihood of instability and misunderstanding (UNGA, 2010b).

Increased Cyber Capabilities for Harmful Action

The 2010 report noted an increase in reports that states are developing ICTs as military and intelligence tools, as well as for political goals (UNGA, 2010b). In addition, it was revealed that there are limited indications of terrorist attempts to compromise or impair ICT infrastructure in order to perform ICT-based operations, although such attempts could intensify in the future (UNGA, 2010b). Criminals and hackers are the originators of numerous dangerous tools and techniques; as a result, the sophistication and volume of criminal activities enhance the likelihood of detrimental actions (UNGA, 2010b). In addition, states evaluated the likelihood of supply chain disruptions resulting from the improper use of ICT. It is further underlined in the study that, “the inclusion of malicious hidden functions in ICTs can undermine

confidence in products and services, erode trust in commerce, and affect national security” (UNGA, 2010b). Finally, states agreed that misuse of ICT entails dangers and hazards that will be reviewed at future UN GGEs to limit and mitigate the risk of ICT for nonpeaceful purposes.

Cooperation Among Like-Minded Partners

According to the 2010 report, there is no other method to achieve robust ICT security except strong stakeholder cooperation. It is stated in the paragraph that, “collaboration among States, and between States, the private sector and civil society is important and measures to improve information security require broad international cooperation to be effective” (UNGA, 2010b). In addition, the report recommended that the most effective way to limit the threat of ICT security is to share best practices, manage incidents, build confidence, reduce risk, and increase transparency and stability (UNGA, 2010b). These steps are believed to aid States in the event of an ICT-related incident. In addition to that, the report also mentioned the vital importance of capacity-building measures in order to achieve success in ensuring global ICT security (UNGA, 2010b). The varying capabilities of each state in addressing ICT security threats could weaken the global ICT security system; consequently, there is an urgent need for capacity building to assist less-developed countries in enhancing their ICT security, including the protection of their critical infrastructures.

4.2.3 Result of the 3rd UN GGE 2012-2013

Due to the accomplishments of the 2nd UN GGE, the 3rd UN GGE was entrusted with conducting an in-depth investigation to develop a more workable method for promoting a safe, resilient, and open ICT environment. In 2013, the group had successfully established a consensus on producing a final report. Several topics that attract the attention of the member states will be discussed in the following sections:

Purposes that are inconsistent with international peace and security

ICT is known to serve as dual-use technology, which can be used for both legitimate and malicious purposes. Or in other words, the ICT could be used for both peaceful and nonpeaceful purposes. In the 2013 report, states agreed to firmly declare that “ICT can also be used for purposes that are inconsistent with international peace and security” (UNGA, 2013b). Hence, it emphasized that the use of ICT for peaceful purposes has become the interest of all States.

The report also elaborates on the possibility of ICT being used for disruptive activities. Furthermore, it also mentioned the potential development of sophisticated malicious tools and techniques of ICT technology, such as botnets, which explain how cyber operation is conducted and how the result of it could increase an unintended escalation among states. In addition, it also recognized the role of a terrorist organization and its utilization of ICT to communicate, collect

information, recruits, organize, plan and coordinate attacks, promote their ideas and actions, and solicit funding (UNGA, 2013b).

Confirming international law applies in cyberspace

The 2013 resolution reaffirmed that international law, particularly the United Nations Charter, is applicable and essential for maintaining peace and stability and developing an open, safe, peaceful, and accessible ICT environment (UNGA, 2013b). In addition, principles established from existing international law, such as State Sovereignty and Internationally Wrongful Acts, would be crucial in determining how States should conduct their activities in cyberspace. However, the report noted that further research is required to determine how such norms will relate to state behaviour and in their use of ICT (UNGA, 2013b). Despite the absence of clarity over the applicability of international norms, this report outlined how states can behave responsibly with regard to ICT security.

“States must meet their international obligations regarding internationally wrongful acts attributable to them. States must not use proxies to commit internationally wrongful acts. States should seek to ensure that their territories are not used by non-State actors for unlawful use of ICTs.” (UNGA, 2013b)

Essentially, this paragraph was written to address the attribution issues raised in the prior report. In order to tackle the increasing use of ICT for malevolent objectives, the group concluded that specific norms in regard to unique attribution could be developed over time (UNGA, 2013b).

International cooperation: confidence-building and capacity-building measures

Besides adopting similar measures as enshrined in the previous 2010 report, the 2013 report emphasized the importance of conducting confidence-building measure as well as capacity-building as an effective way to build global resilience on ICT. In order to increase predictability and reduce misperception between States, the report recommended some actions: voluntarily exchange views and information in regards to national strategies and policies, best practices, decision-making processes, relevant national organizations and measure to improve international cooperation; creation of bilateral, regional, and multilateral consultative frameworks for confidence-building; enhanced sharing of information among States on ICT security incidents; enhanced information and communication between national Computer Emergency Response Team (CERT); and enhanced mechanism for law enforcement cooperation to reduce incident that could otherwise be misinterpreted as hostile State action (UNGA, 2013b).

On the other side, the report suggested capacity-building efforts to mitigate the possible implications of ICT security threats. According to the report, member states have varying capacities for ICT security, which might heighten vulnerability in a globalized society. As a result, assistance in an effort to improve the security of critical ICT infrastructure; develop technical skills and appropriate legislation, strategies, and regulatory frameworks, is essential to build resilience in ICT security (UNGA, 2013b).

Promoting Dialogue and Common Understanding

The report suggested that the United Nations should take the lead in facilitating dialogue among the Member States in order to build a shared understanding of the use of ICT for peaceful purposes. Given the rate of ICT development and the magnitude of the threat, the Group believes it is necessary to strengthen shared understandings and expand practical cooperation. In this regard, the Group advises regular institutional engagement under the auspices of the United Nations, as well as regular dialogue through bilateral, regional, and multilateral forums and other international organizations. (UNGA, 2013b). In the 2013 report, the phrase promoting shared understanding appears repeatedly. It is utilized to encourage member states to adopt the same approach when discussing which international norms and principles are applicable in cyberspace.

4.2.4 Result of the 4th UN GGE 2014-2015

The 4th UN GGE was able to produce a consensus report. It, however, still borrowed the same approach in comparison to the previous report, where it reiterates the importance of confidence-building and capacity-building measures as ways to limit and minimize disruptive results emanating from ICT. Nevertheless, a different outcome was presented in this report, as it further detailed the applicability of norms and rules in cyberspace.

Norms, rules, and principles of the responsible behaviour of the State

This report discusses a number of norms and principles with the aim of promoting responsible State behaviour in cyberspace. It is essential to be applied amid the growing malicious development of ICT to be used by States. In detail, these norms guide how States should respond under the circumstances if an attack utilizing an ICT occurs. In essence, these norms are designed to avoid the potential international catastrophe that could result from the misuse of ICT.

According to the report, there are several responsibilities which encouraged. First, States should not conduct or knowingly allow their territory to be used for internationally wrongful acts using ICT. It includes the act in which States are supporting ICT activity contrary to its obligation under international law that intentionally damages critical

infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public as well as the activity which could harm the information system of the authorized emergency response team (UNGA, 2015b). Second, States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats as well as respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts and conduct appropriate mitigation of it (UNGA, 2015b). To summarize, these norms prohibit States to conduct malicious acts using ICT activities and encourage cooperation when there is an attack attributed to their territory.

Although the set of norms and principles are explained, the report continuously affirmed that it has a non-binding nature. According to the 2015 report, norms do not seek to limit or prohibit action that is otherwise consistent with international law. Instead, norms reflect the expectations of the international community, set standards for responsible State behaviour, and allow the international community to assess the activities and intentions of States (UNGA, 2015b).

How international law applies to the use of ICT

It has been confirmed in the 2013 report that international law applies, particularly the UN Charter, applies to cyberspace. In the 2015

report, the group identified several essential principles. First, the States agreed to bring principles of sovereignty as well as norms that flow from its applicability, such as jurisdiction and non-intervention apply to cyberspace. Second, the States acknowledge the inherent right of states to adopt actions compatible with international law and the UN Charter, although the applicability of this principle is subject to further review. In essence, States have yet to agree on when this principle applies. In addition to this, States took notice of the pre-existing legal concepts that are pertinent to international law, such as the principles of humanity, necessity, proportionality, and distinction. Finally, States affirmed that in applying this principle, States shall adhere to the settlement of the dispute by peaceful means and refrain from the use of force against the territorial integrity of other States (UNGA, 2015b).

4.2.5 Result of the 5th UN GGE 2016-2017

The 5th UN GGE failed to adopt a report by consensus. Several publications (Korzak, 2017; Sukumar, 2017; Valjataga, 2017) indicate that a consensus could not be established on several elements of international law, such as countermeasures and the right to self-defense. Although the group acknowledged in previous reports (2013, 2015) that international law, particularly the UN Charter, applies to cyberspace, it appears that the States have not yet reached a consensus on its implementation. The 2015 report does indeed acknowledge the inherent

right referred to in Article 51 of the UN Charter. However, in the same paragraph, it also mentioned that its applicability is subject to further study.

Upon further discussion of this principle at the 5th UN GGE, numerous states rejected its applicability. China, Cuba, and Russia opposed the notion that article 51 applies to cyber operations (Valjataga, 2017). In an explanation of its GGE position, Cuba declared that it opposed the equivalence [made] between the malicious use of ICTs and the concept of 'armed attack' (Sukumar, 2017). It is feared that applying the self-defense principle in cyberspace would create a legal basis for the emergence of hostile cyber operations of unprecedented intensity and impact, or, as the Cuban delegate put it, "legitimizing cyber war" (Valjataga, 2017). This notion establishes the drawback for future cyber security discussions. Consequently, from 2017 to 2019, the UN was divided into two opposing viewpoints. This could be clearly assessed from double resolutions that were adopted by UNGA from 2018-2019 and presented under the same provisional agenda.

4.2.6 Result of the 6th UN GGE 2019-2021

After 5 years attempted to promote common understanding, especially in the issue of how international law applies in cyberspace, the 6th Un GGE was able to present its consensus report. The issue of the inherited right of States to take measures consistent with

international law and as recognized in the UN Charter is still subject to further study. In summary, there are no new norms introduced in this phase. Instead, it reinstated 11 norms that were previously agreed upon by the States to be future guidance on how States should act responsibly in cyberspace. Furthermore, it still encouraged the confidence-building and capacity-building measures as an effective way to tackle hostile cyber operations between States.

Responsible State Behaviour

According to the 2021 report, the GGE agreed to suggest 11 norms that could assist States to become responsible in its action in cyberspace, these norms are summarized as follows:

- (1) adhering to the purpose of the United Nations in maintaining international peace and security;
- (2) providing all relevant information in regard to malicious cyber activities;
- (3) preventing the use of their territory from misuse of ICT;
- (4) being cooperative in prosecuting terrorist and criminal use of ICTs;
- (5) respecting human rights and freedom of expression in the digital sphere;
- (6) not conducting any operation that could damage the critical infrastructure of other States;

- (7) ensuring an effort to protect their critical infrastructure;
- (8) being responsive to the request of assistance or mitigation pertaining to malicious ICT activities attributed to their territory;
- (9) ensuring the safety and reliability of the supply chain through ICT;
- (10) taking an active measure to report ICT vulnerabilities;
- (11) affirming its commitment to not harm or use an emergency response team.

An attempt to define international law applies to cyberspace

Several international legal principles such as sovereignty, non-intervention, and international obligation under internationally wrongful acts are reaffirmed in this report. Despite its repetitive phrases, this report also presents new detailed information regarding how States should seek solutions by peaceful means and avoid the use of force. In paragraph 71(a), States agreed that, in responding to any international dispute, they would adhere to the methods encouraged in Article 33 of the UN Charter, which encouraged states to seek solutions through peaceful means such as negotiation, investigation, mediation, conciliation, arbitration, judicial settlement, or any other arrangements that resort to regional agency. In addition, paragraph 71(d) also reinstated the prohibition of the use of forces in their utilization of ICT. This part refrains States from conducting any action that could violate the territorial integrity and political independence of other States. And

finally, paragraph 71(f) stated that international humanitarian law only applies to the situation of armed conflict with reference to principles of humanity, necessity, proportionality, and distinction. In the end, the only outstanding question regarding the application of international law was whether self-defense and countermeasures were permissible within the context of ICT. However, paragraph 71(e) reinstated that the applicability of this principle is subject to further study. It is to say that States opt to leave this interpretation with ambiguity.

4.2.7 Conclusion

The establishment of six rounds of the UN GGE is essential to building norms related to cyber security. Many of the adhered rules originated from the report of this group. Moreover, its recommendation has been further affirmed in the UNGA resolution. However, many member states look at the importance of their involvement in the discussion of this issue; the idea where cyber security was to be held on the Open-Ended method introduced by resolutions 73/27 and 74/29 thus became a favourable option. As a result, the next chapter will review the result of the Open-Ended Working Group.

4.3 United Nations Open-Ended Working Group (UN OEWG)

UN OEWG was established pursuant to UNGA Resolution 73/27. This forum promotes inclusivity and broader participation of all UN member states in addressing the issue of ICT in the context of international security. Furthermore, UN OEWG attempted to replace the UN GGE that has been ongoing for decades yet is still unable to reach a consensus among member States on the applicability of specific international law and principles, namely self-defense and countermeasure. It is expected that, by inviting the broader participation of all member states, compared to only few-chosen exclusive states, the UN would finally be able to create a new regime or sufficient framework to address the issue of malicious development of ICT in the context of international security.

4.3.1 Primary Result of the UN OEWG

UN OEWG submitted its first consensus-based report in 2021 which circulated under Resolution A/75/816. According to its report, States reached the following conclusions and recommendations, which include concrete actions and cooperative measures to address ICT threats and promote an open, secure, stable, accessible, and peaceful ICT environment. Its content is not relatively new; it adopted and developed the notion which was brought in the UN GGE as well as concerns mentioned in the UNGA. Several issues and measures are

repetitively mentioned in this report. The UN OEWG discussed existing and potential threats in the sphere of information security and possible cooperative measures to address them; further development of rules, norms, and principles of responsible behaviour of States; how international law applies to the use of ICTs by States; confidence-building measures; capacity-building; and the possibility of establishing a regular institutional dialogue with broad participation under the auspices of the United Nations (UNGA, 2021c).

Despite its repeated notions, there are few additional agendas or expanded topics mentioned in this report. First, States concluded that there are potentially devastating security, economic, social, and humanitarian consequences of malicious ICT activities on critical infrastructure (CI) and critical information infrastructure (CII) supporting essential services to the public (UNGA, 2021c). Second, States elaborated on which infrastructures that designated as critical. This report further affirmed that critical infrastructure may include medical facilities, financial services, energy, water, transportation, and sanitation (UNGA, 2021c). Third, States agreed to continue to discuss this challenging issue within the democratic and inclusive framework, in which it endorses the continuation of UN OEWG until 2025. Fourth, States suggested that there was a need for additional neutral and objective efforts to build capacity in the areas of international law, national legislation, and policy (UNGA, 2021c). Fifth, States brought in

mind the possibility of additional legally binding obligations. And finally, States agreed that this forum has benefited from the expertise, knowledge and experience shared by representatives from inter-governmental organizations, regional organizations, civil society, the private sector, academia, and the technical community (UNGA, 2021c).

These recently added agendas marked a significant milestone introduced by the United Nations. Even though there is a great deal of work that needs to be done in the future, particularly regarding resolving the divergent point of view of member states pertaining to the applicability of international humanitarian law in cyberspace, the UN OEWG raises a glimpse of hope for the establishment of a future framework of ICT security.

Chapter 5: Discussion

This chapter will present noteworthy discussions based on the correlation between the findings of Chapter 4 and the concepts or literature of Chapter 2. The first section will explore the relational power that has formed in the United Nations framework over the last quarter-century of cyber security norm-setting. Several states, including Russia, China, and the United States, have differing perspectives on international cyber security, resulting in the polarization of the United Nations in tackling this issue. The second section will examine the dual use of ICT that can be applied to cyber operations. This section will argue that current international law in armed conflicts is sufficient to clarify the dual use of technology. In addition, this section would compare similar dual-use technologies that have been successfully restricted via legally binding documents. The final section will examine the emergence of soft law vs hard law regarding the State's preferred approach to cyber security. Evidently, any international norms and laws making tend to be politicized. Nonetheless, this section will elaborate on the States' inconsistent position that, while they do not wish to be bound by specific cyber-related treaties, they instead reiterate their commitment through customary international law and general principles of law, which are, in fact, binding in nature.

5.1 Power Dynamics in the UN Platform for Cyber Security

It is pertinent that the discussion of ICT in the context of international security at the UN forum has been impacted by the interests of numerous powerful states. Russia introduced the discussion of this context in 1998, and since then, it has been a UNGA's provisional agenda for about 25 years. The use of power in this UN dialogue lies in soft power: to influence others rather than force (compulsive power). As a result, the form of power that is closely related to this debate is institutional power, wherein the UN serves as the global institution through which power is embedded. The objective of institutional power, according to Stevens & Kavanagh (2021), is to achieve control by constructing a framework or architecture of norms within the organization that, in some ways, might place their national interest. This viewpoint is exemplified by the competition between powerful nations, such as the United States and its allies, Russia, and China, in creating a suitable framework to govern how states should conduct in cyberspace.

Almost all UN efforts to create an open, peaceful, safe, and reliable cyberspace are intertwined with competition between powerful countries. Since the inaugural meeting of the UN GGE in 2005, which was led by the representative of the Russian Federation, Andrey Krutskikh, disagreements have arisen during the discussion. For instance, the UK and the US opposed the establishment of a new multilateral instrument such as an international convention (Meyer, 2020,

p. 289). Comparatively, more authoritarian states, such as Russia and China, have sought for total control of information technology through international codes of conduct.

After a successful consensus report established in 2010, Russia and China aimed to follow up on this issue by circulating their draft of the International Code of Conduct (CoC) for Information Security (UNGA, 2011b). On this occasion, the CoC contents were established in favour of their national interest and political stance. To illustrate, the first paragraph of the CoC's pledges delivered the necessity to comply with the UN Charter; however, this paragraph also inserted the need to respect the history, culture, and social system of all countries. This sentence explicitly embeds Russia-China's interest, which is related to their authoritarian system that applies control in information spheres. While China and Russia emphasize the rights of states to protect their 'cyberspace' and 'information and media spheres', Western states fear that such rights will be used to justify surveillance, censorship, and repression in authoritarian states (Schia&Tikk, 2020, p.360). This matter of ideology and political stance continues to revolve around a debate on cyber security. In the end, the persistent polarization of states prevents the creation of a framework for cyber security that is free and neutral to the interests of powerful States.

Moreover, it is pertinent that Russia and China continue to limit US cyber supremacy. To illustrate, paragraph 4 of the 2011 draft of CoC

asserted the necessity to prevent States from using their resources to interfere with other countries' domestic policies. In addition, the 2015 amendment to this clause expressly prohibited other states from leveraging their dominant position in ICT. From this vantage point, we may assume that Russia and China are concerned about the United States cyber dominance, which controls the worldwide internet infrastructure. In order to combat the United States cyber superiority, these nations campaigned for independent control of information and communication technology. In the end, because the text of both CoCs in 2011 and 2015 explicitly opposed the US stance, this CoC failed to receive a majority vote and was thus never adopted under the UNGA.

Afterwards, the polarization between the US and China-Russia is extended through the period 2017-2020. It is illustrated by the failure of the 5th UN GGE to generate a consensus report in 2017. Despite the fact that resolutions establishing GGEs have previously achieved consensus status, the General Assembly's First Committee session in 2018 was confronted with two opposing resolutions outlining various future routes for UN engagement on cyber security (Meyer, 2020, p. 292). For the first time in the history of the United Nations, member states adopted two resolutions on the same issue during one session at the initiative of the Russian Federation and the United States (Krutskikh&Streltsov, 2020, p.260). The resolution (73/266), adopted at the initiative of the United States, proposes the creation of a GGE based

on its achievements in the field of ICT in the context of international security, whereas the Resolution (73/27) adopted on the initiative of the Russian Federation provides for the creation of an Open-Ended Working Group (UN OEWG) oriented as a priority for the further development of norms, rules, and principles of responsible behaviour of states in the field of ICT (Krutskikh&Strelsov, 2020, p.260).

There is somehow an overlap within the mandate and task of both designated bodies; however, the UN OEWG successfully won the heart and minds of other member states, which acknowledged the importance of inclusivity in directly engaging in the debate of cyber security in comparison to only being represented by a few member states in the UN GGE. As James Lewis has noted, 'Over time, the GGE process has evolved into a proxy for negotiations between States, and there have been suggestions that it might be time to move these discussions to a more regular diplomatic process' (UNIDIR, 2016, cited in Meyer, 2020). As a result, the UN OEWG that parallels the UN GGE has been dubbed the cyber-UNGA (Krutskikh&Strelsov, 2020, p. 264). Finally, the UN OEWG has been trusted to be the sole platform to continue the discussion of cyber security because it promotes the value of democracy and inclusivity. At the same time, the UN GGE was finalized in 2021 with no further mandates and establishment. This event marks the triumph of Russia and China's approach to establishing a more inclusive framework for cyber security. These countries successfully influenced a larger

member of the UN by its agenda-setting and power narration to frame the necessity of inclusivity in discussing the topic of cyber-security.

5.2 Dual use of ICT: Framework Clarity

The dual-use nature of technology means that the same technology could be utilized for both civilian and military applications. The military use of ICT has previously been acknowledged in Chapter 2 of cyber operation: it elaborated on the case where ICT was used to create a devastating impact on global security. This notion has also been acknowledged since the establishment of the 1st UNGA resolution pertaining to this issue, which reinstated that ICT could have both civilian and military use. Because of the complex use of ICT, the UN faced difficulty in deciding whether the prohibition of ICT for cyber weapons is necessary. I argued that non-proliferation is not necessary; however, a framework to clarify its use is a necessity.

The problem with the proliferation of cyber weapons resides in its anonymity. It is harder to locate and attribute cyber perpetrators. Additionally, when such cyber activities are employed by State, it can easily use proxies to conceal its identity. Besides, cyber activities have been widely used to conduct espionage activity, which is not *pe ser regulated* under international law. If such a measure to limit the proliferation of cyber is taken, many States will present their objection.

Consequently, the UN frameworks have continuously discussed the issue of emerging threats that emanated from the use of ICT. In conclusion, the UN has already affirmed that ICT can be used for purposes which inconsistent with the maintenance of international peace and security or, on the other hand, for nonpeaceful purposes. Therefore, it is logical to assume that the use of ICT for military purposes shall be further guided, if not limited. However, restrictions on the use of ICT for non-peaceful purposes have not yet been specified in the legally enforceable instrument.

Although the rule to prohibit the use of cyber weapon for nonpeaceful purposes is still paucity. The rule regarding the international armed conflict is available to limit State's activity. At least, this is the approach presented by international legal scholars to fill the gap in cyber governance in the context of international security. Tallinn Manual is one of the legal instruments that could guide the applicability of international law in cyber activities, including cyber armed conflict. In terms of addressing the dual-use functionality, Tallinn Manual Rule 101 clarified that where the object or cyberinfrastructure is used for both civilian and military purposes, it is then considered a military object (Schmitt&Vihul, 2017, p.445). On the other hand, the objects that are ordinarily devoted exclusively to civilian use shall not be used for military purposes (Schmitt&Vihul, 2017, p.448). To sum up, when facing conduct of

hostilities, cyber infrastructure shall only serve one purpose, either military or civilian, and it cannot be used to serve a dual function.

This clarity on the framework of law in armed conflict may clarify the dual use of technology. Nevertheless, this approach has not been adopted in the current norms and rules of cyber-security as stipulated in the 2021 report of UN GGE and UN OEWG. Numbers of States are still hesitant to acknowledge the applicability of international humanitarian law to the case of cyber activities. It shows that many States are reluctant about the militarization of cyberspace.

Military use of technology not only applies in the ICT. For example, several technologies, such as nuclear and outer space technology, contain dual-use purposes. However, they have been equipped with more clarity in a specific framework. Nuclear technology has been regulated under the IAEA and affirmed to have dual use. If peaceful nuclear energy activities cannot be effectively controlled, the diversion of nuclear technologies and materials from peaceful uses to nuclear weapons or other nuclear explosive devices may bring devastating disaster to humanity (Ge, 2022, p. 30). In addition, space technology also has both military and civilian applications (Johnson-Freese, 2006). There is a rising concern that the dual-use nature of space technology challenges the proliferation of space weapons and raises serious concerns about its utilization (Pražák, 2021, 397). In essence, both of these technologies presented a threat to international

security because their disastrous military use may have catastrophic consequences for the worldwide community. The same narratives are also brought into the discussion of ICT. But on the contrary, both nuclear and outer space technology have been addressed and regulated under the international legally binding treaty. Numerous nations have expressed that the same concept needs to be implemented in ICT. Nonetheless, the UN has not reached a consensus on this matter.

Since the establishment of the IAEA in 1957, dozens of multilateral international conventions related to the use of nuclear energy, as well as a large number of bilateral or multilateral agreements on the uses of nuclear energy between countries and with international organizations, have been formed, constituting a relatively complete international nuclear legal framework, based on the principles of peace, safety, security, liability and cooperation, and providing a legal basis for the development of the peaceful uses of nuclear energy worldwide (Ge, 2020, p.35). On the other hand, the use of space technology has been limited to only serving a peaceful purpose, as stipulated in Article 4 para 2 of the Outer Space Treaty (UNOOSA, 1967) and Article 3 of the Moon Agreement (UNOOSA, 1979). These specific treaties have successfully proven to limit the harmful effect of dual-use technology. For the same reason, the legally binding documents to limit the dual use of ICT shall also be a topic of necessity. Nevertheless, many countries have presented their objection to this notion by clearly endorsing that the

current international legal framework has been adequate to limit the harmful purposes of the ICT. Consequently, the next section will discuss which law applies to international regulation of cyberspace.

5.3 Soft vs. Hard Law in Regulating International Cyber Security

The applicability of international law in cyberspace has continuously become a central discussion in the UN. Although the UN GGE report in 2013 and 2015 has reiterated that international law, particularly the UN Charter, and principles derived from it are applicable and essential to maintaining peace and security in cyberspace, the debate on the topic of self-defense and countermeasure, which actually elaborated under the UN Charter, is still persistent. This contradictory stance on applying the UN Charter as a norm to govern cyber activities arises from the different interpretations of the applicability of this customary law by each state. In this regard, it may be necessary to evaluate the objectivity of international law. Koskenniemi (1999; 2006) stated that international law must be normative so that it can prove its independence from the politicization of States. Nonetheless, the law should be concrete in order to be easily validated by State practices. In essence, international law should strike a balance between normativity and concreteness in order to be entirely objective. To show that international law exists, with some degree of reality, the modern lawyer

needs to show that the law is simultaneously normative and concrete – that it binds a State regardless of that State's behaviour, will or interest but that its content can nevertheless be verified by reference to actual State behaviour, will or interest. (Koskenniemi, 2006, p.17). To explain, if the customary law endorsed by the rule governing cyber operations is objectively understood, it will bind the States regardless of their preference, will, or interest. As a result, the principles derived from it, including self-defense and countermeasure, will not be a subject of further study because it applies entirely.

The binding nature of international law led States to be very cautious in associating themselves. According to Article 38 of the Statute of the ICJ, international law is formed from the treaty, customary law, and general principles of law (Schmitt&Vihul 2014, p.3). In this sense, UN Charter is recognized as the customary international law, and several principles derived from it, such as sovereignty, non-intervention, and prohibition of the use of force, are considered the general principles of law. By adopting this approach, there is no further reason as to why these principles are not applicable to cyber activities. On the contrary, the 25 years of negotiation between UN member states to set the rule of State's activities in cyberspace are still halted because of this issue. In consequence, to dissociate themselves from the binding rule and legal implication, States opted to adopt a soft law. The norms and resolutions presented under the UNGA framework are considered soft law. The

nature of soft law is not binding, consists of general norms and principles, not rules, and is not readily enforceable through binding dispute resolutions (Boyle, 1999, p.901-902).

It is pertinent that the UN member states are still reluctant to establish a legally binding document. Evidently, it could be assessed through the repetition of 'non-binding' words used in the 2015 GGE report, specifically in paragraphs 9, 10, and 27. Furthermore, the GGE report in 2021 affirmed that 11 norms established under this framework do not seek to limit or prohibit action that is otherwise consistent with international law (UNGA, 2015b). Instead, the norms only reflect the expectation of the international community, set standards for responsible state behaviour, and allow the international community to assess the activities and intentions of States (UNGA, 2015b). It is to say that the applicability of norms has no legal implication, which contrasts with the applicability of legally binding documents.

The result of the UN GGE and UN OEWG aimed to recommend rather than prohibit State behaviour in cyberspace. The substance of their report, however, demonstrated a rather inconsistent stance regarding norms vs law. On the one hand, States agreed not to be bound by internationally binding documents and only viewed the norms as a guide. On the other hand, it recognized that the general principles of international law, such as the UN Charter, which is binding in nature, are of central importance for the conduct of States in cyberspace. This was

reaffirmed through the GGE report, especially in paragraph 70 of 2021 report that addresses:

In this respect, the Group reaffirmed the commitments of States to the following principles of the Charter and other international law: sovereign equality; the settlement of international disputes by peaceful means in such a manner that international peace and security and justice are not endangered; refraining 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; respect for human rights and fundamental freedoms; and non-intervention in the internal affairs of other States (UNGA, 2021b).

From this vantage point, it is abundantly evident that states agreed to be bound by international law's general principles. However, it appears that other states have a different perspective on adopting it. The failure of GGE to capture the necessary element of international law and its applicability to cyberspace could be the result of some state representatives' lack of expertise in international law (Chung&Park, 2020, p.383). As a result, there is considerable ambiguity apparent in both the report of GGE and OEWG.

5.4 Conclusion

In conclusion, the UN GGE and UN OEWG presented a list of norms to regulate responsible state behaviour in cyberspace. In addition,

it validated the general rules of international law that govern the activity of states in cyberspace. Despite these double affirmations, States continue to refer that they chose not to be bound and preferred to be guided under the soft law, which is outlined in the norms of responsible state behaviour. It is due to the fact that soft law is generally developed and adopted relatively quickly compared to hard law, which is deemed to be more legitimate, precise, and detailed (Bosi, 2021). The discussion about the international regime of cyber security ends here with the conclusion of State's preference to adopt a soft law and be guided by existing international law. Finally, although the hard law, or in this sense, the cyber-specific internationally binding documents, has yet to emerge, in the upcoming term, there will be another notion from States to seek for more clarity. It is simply to put that detailed and specific cyber-security regulation for States will soon be an option for the cyber-security-related outcome.

Chapter 6: Summary and Conclusion

The malicious development of ICT has been a subject of concern within the international community. This is due to the fact that the same technology that is used to improve a community's quality of life could also be used to threaten the current state of peace and security. Multiple cyber operations have been launched to date, capturing the world's attention as they have proven to present the same devastating impact as conventional kinetic operations. Therefore, it has been anticipated that future hostilities will favour cyberspace-based attacks since it is easier, more precise, more effective, and less expensive. Despite the rapid development of ICT for harmful purposes, specific international legislation controlling cyberspace remains lacking, facilitating the advanced use of it by a State, non-State actors, or even the State using non-state actors as proxies. This pattern creates more complexity as the cyber operations endorse anonymity.

With the knowledge of the potential destruction of cyber operations, the current global security and peace could be jeopardized. Therefore, the United Nations, which is tasked with preserving peace and security, shall be able to adopt a strategy that restricts the use of ICT for potential catastrophe. Despite the absence of the UN Security Council in dealing with this issue, the UN General Assembly has taken the necessary steps and measures to resolve it for more than two

decades. However, the move made by the UN is not a simple undertaking. To discuss the evolution of this issue, the UN and its multilateral effort have conducted an annual provisional agenda in the UNGA since 1998. Furthermore, it established six subsequent special designated bodies, known as the UN Group of Governmental Experts (UN GGE) from 2004-2021, to investigate threats emanating from ICT and make recommendations to the Assembly. The outcome of this UN GGE is monumental in terms of developing norms for state behaviour in cyberspace. In 2013 and 2015, this group endorsed the applicability of international law, especially the UN Charter and principles derived from it, to be essential to maintain peace and security in cyberspace. In addition, its 2021 report acknowledged the 11 norms that guide the responsible behaviour of States in cyberspace, which could reduce harmful actions conducted by States. Nonetheless, these measures are not legally binding and thus have no legal ramifications.

Despite its success in developing normative guidance, the UN GGE faced significant challenges, most notably when it failed to produce a consensus report in 2017. Nevertheless, the same issue that occurred in 2017 has yet to be resolved. This was about states' differing perspectives on the applicability of international law in the realm of armed conflict, which regulated the inherent right of self-defense and countermeasure. Consequently, this issue continues to be a source of disagreement among member states, with no consensus on how to

resolve it. I would argue that it is quite contradictory for States to affirm that they acknowledge the UN Charter and the principles derived from it, such as sovereignty, non-intervention, prohibition of the use of force, and peaceful resolution of disputes, while simultaneously abandoning their commitment to the right of self-defense and countermeasures. As a result of the lack of consensus within the UN GGE, the UN has finally taken another step to address this issue by forming an Open-Ended Working Group that encourages all member states to participate in the norm-making process. The adopted measure was particularly interesting because, in the end, the UN chose the UN OEWG to be the sole platform for determining the future of cyber-security-related governance, effectively ending the role of the UN GGE, which had served the community for nearly two decades.

Finally, the last 24 years of the United Nations' attempt to regulate State behaviour in cyberspace have not been an easy journey. It faced numerous challenges and was surrounded by opposing views from powerful states. Furthermore, its norm-making process is surrounded by State politicization, favouring particular interests, will, and objectives of influential States. This is why the UN has yet to arrive at a consensus on the applicability of international humanitarian law in cyberspace. Despite this constraint, the UN ultimately agreed to be guided by soft law rather than be bound by hard law.

To summarize, the UN did not establish a new regime to create peaceful cyberspace; instead, it chose to adopt existing law and establish a normative measure to guide state behaviour in cyberspace. However, the process of developing a regulation that promotes the security and peaceful use of cyberspace does not end here. The UN OEWG is still mandated to work until 2025 and submit its report at the UNGA's 80th session. In addition, it is tasked with establishing neutral and objective efforts in interpreting the international law framework and, if necessary, revising the existing measure. Aside from that, several States have been developing a Plan of Action to achieve a more concrete outcome. However, all initiatives of the United Nations to regulate cyberspace should be presented under the UN-OEWG platform. In conclusion, the journey to establish a legally enforceable cyber-security regime is still long and complex. In light of the reluctance of many states to be bound by internationally legally binding treaties, perhaps the State could keep moving forward by endorsing the Declaration of the Peaceful Use of Cyberspace, which could serve as soft law and yet is still influential in affirming and clarifying the ambiguity of the rule that applies to cyberspace.

Reference List

- Bloor, Meriel and Bloor, Thomas. (2007). *The Practice of Critical Discourse Analysis*. London: Routledge.
- Bosi, Giulia. (2021). 'Overcoming the "Soft vs Hard Law" Debate in the Development of New Global Health Instruments', *OpinioJuris.org*
Available at: <https://opiniojuris.org/2021/11/30/overcoming-the-soft-vs-hard-law-debate-in-the-development-of-new-global-health-instruments/> (Accessed 17 July 2022)
- Bowcott, Owen. (2017). 'Dispute along cold war lines led to collapse of UN cyberwarfare talks', *The Guardian*, 23 August 2017.
Available at:
<https://www.theguardian.com/world/2017/aug/23/un-cyberwarfare-negotiations-collapsed-in-june-it-emerges>
(Accessed: 13 July 2022)
- Boyle, Alan E. (1999). 'Some Reflections on the Relationship of Treaties and Soft Law' *The International and Comparative Law Quarterly* 48(4), pp. 901-913. Cambridge University Press.
Available at: <https://www.jstor.org/stable/761739> (Accessed: 19 July 2022)
- Brown, Gary D. (2020). 'International law and cyber conflict' in in Kerttunen, M & Eneken Tikk (eds). *Routledge Handbook of International Cyber Security*. New York: Routledge, pp. 366-378.
- Burnham, Peter. Et.al. (2004) *Research Methods in Politics* (1st ed.) London: Palgrave Macmillan.
- Carr, Madelaine. (2015). 'Power plays in global internet governance' *Millenium: Journal of International Studies* 43(2). Available at: <https://doi.org/10.1177/0305829814562655> (Accessed 30 April 2022)

- Chung, Myung-Hyun & Park, Nohyoung. (2020). 'Exploring the general principles of international law in the cybersecurity context' in in Kerttunen, M & Eneken Tikk (eds). *Routledge Handbook of International Cyber Security*. New York: Routledge, pp. 379-388.
- Clarke, Richard A. and Knake, Robert. (2010). *Cyber War : The Next Threat to National Security and What To Do About It*. Toronto: HarperCollins Publishers.
- Delerue, Francois. (2020). *Cyber Operations and International Law*. Cambridge University Press. Available at: <https://doi-org.ezproxy.lib.gla.ac.uk/10.1017/9781108780605> (Accessed 24 April 2022)
- Fairclough, N., 2010. Critical discourse analysis as a method in social scientific research. *Methods of Critical Discourse Analysis*. Available at: <https://doi.org/10.4135/9780857028020.d8> (Accessed: 5 May 2022)
- Fildes, Jonathan. (2010). 'Stuxnet worm targeted high-value Iranian assets', *BBC News*, 23 September 2010. Available at: <https://www.bbc.com/news/technology-11388018> (Accessed 24 April 2022)
- Gartzke, Erik. 2013. 'The Myth of Cyberwar', *International Security*, Vol. 38, No. 2, pp. 41–73. Available at: doi:10.1162/ISEC_a_00136 (Accessed 24 April 2022)
- Ge, Deng. (2022). 'Nuclear Laws for Peaceful Uses of Energy' in IAEA. *Nuclear Law: The Global Debate*. The Hague: T.M.C Asser Press, pp.29-43. Available at: <https://doi.org/10.1007/978-94-6265-495-2> (Accessed 16 July 2022)
- Gibney, Alex (director). (2016). *Zero Days*. California: Participant Media [documentary movie] <http://www.zerodaysfilm.com/>

- Gold, Josh. (2021). 'Unexpectedly, All UN Countries Agreed on a Cybersecurity Report. So What?', *Council for Foreign Relations*, 18 March 2021. Available at: <https://www.cfr.org/blog/unexpectedly-all-un-countries-agreed-cybersecurity-report-so-what#:~:text=The%20success%20of%20the%20OEWG,its%20work%20in%20May%202021>. (Accessed: 13 July 2022)
- Green, James A (eds). 2015. *Cyber Warfare: A Multidisciplinary Analysis*. London: Routledge.
- Haataja, Samuli. 2017. 'The 2007 cyber attacks against Estonia and international law on the use of force: an informational approach', *Law, Innovation and Technology* 9(2), pp.159-189. Available at: <https://doi.org/10.1080/17579961.2017.1377914> (Accessed 22 April 2022)
- Housen-Couriel, Deborah. (2012). 'The "Dubai Clash" at WCIT-12: Freedom of Information, Access Rights, and Cyber Security' *Law and National Security*. Available at: <http://www.jstor.com/stable/resrep08957.9> (Accessed 19 July 2022)
- International Telecommunication Union (ITU). (2005). *World Summit of Information Society*. Available at: <https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html> (Accessed 19 July 2022)
- Johnson-Freese, Joan. (2006). 'A New US-Sino Space Relationship: Moving Toward Cooperation', *Astropolitics: The International Journal of Space Politics and Policy* 4(2), pp. 131-158. Available at: <https://doi.org/10.1080/14777620600910571> (Accessed 16 July 2022) *Astropolitics* 4 (2) (2006) 131–158

- Kaska, Kadri., Tikk, Eneken., Vihul, Liis. (2010). *International Cyber Incidents: Legal Consideration*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence. Available at: https://ccdcoe.org/uploads/2018/10/legalconsiderations_0.pdf (Accessed: 24 April 2022)
- Kerttunen, M & Eneken Tikk (eds). 2020. *Routledge Handbook of International Cyber Security*. New York: Routledge
- Korzak, Elaine. (2017). 'UN GGE on Cybersecurity: The End of an Era?', *The Diplomat*, 31 July 2017. Available at: <https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/> (Accessed: 13 July 2022)
- Koskenniemi, Martti. (1990). 'The Politics of International Law' *European Journal of International Law* 4. Available at: <http://ejil.org/pdfs/1/1/1144.pdf> (Accessed 20 July 2022)
- Koskenniemi, Martti. (2006). *From Apology to Utopia: The Structure of International Legal Argument*. Cambridge: Cambridge University Press. Available at: <https://doi.org/10.1017/CBO9780511493713.003> (Accessed 20 July 2022)
- Koskenniemi, Martti. (2009). 'The Politics of International Law – 20 Years Later', *European Journal of International Law* 20(1), pp. 7-19. Available at: <http://www.ejil.org/pdfs/20/1/1785.pdf> (Accessed 20 July 2022)
- Krutsikh, Andrei V & Streltsov, Anatoli A. (2020). 'International information security: problems and ways of solving them' in Kerttunen, M & Eneken Tikk (eds). *Routledge Handbook of International Cyber Security*. New York: Routledge, pp. 260-267

- Kuehl, D.T., 2009. 'From Cyberspace to Cyberpower: Defining the Problem' in Kramer, Franklin D., Starr, Stuart H., Wentz, Larry K (eds.) *Cyberpower and National Security*, pp.24–42. Available at:
<https://ndupress.ndu.edu/Media/News/Article/1216674/cyberpower-and-national-security/> (Accessed 30 April 2022)
- Libicki, Martin C. (2011). 'Cyberwar as a Confidence Game', *Strategic Studies Quarterly* 5(1), pp.132–47. Available at:
<http://www.jstor.org/stable/26270514>. (Accessed: 24 April 2022)
- Lichtman, Allan J. & French, Valerie. (1978). *Historians and the Living Past: The Theory and Practice of Historical Stud.* Arlington Heights.
- Lindsay, Jon R. (2013). 'Stuxnet and the Limits of Cyber Warfare', *Security Studies*, 22:3, pp.365-404. Available at:
<https://doi.org/10.1080/09636412.2013.816122> (Accessed 22 April 2022)
- Maurer, Tim. (2011). *Cyber Norm Emerging at the United Nations*. Belfer Center for Science and International Relations. Available at:
<https://www.belfercenter.org/sites/default/files/files/publication/maurer-cyber-norm-dp-2011-11-final.pdf> (Accessed: 26 May 2022)
- Meyer, Paul. (2020). 'Confidence-building measures in cyberspace: new application for an old concept' in Kerttunen, M & Eneken Tikk (eds). *Routledge Handbook of International Cyber Security*. New York: Routledge, pp. 297-311
- Moulin, Thibault. (2020). 'Reviving the Principle of Non-Intervention in Cyberspace: The Path Forward', *Journal of Conflict & Security*

- Law* 25(3), pp.423-447. Available at:
<https://doi.org/10.1093/jcsl/kraa011>(Accessed: 22 April 2022)
- Nguyen, Reese., (2013). 'Navigating jus ad Bellum in the age of cyber warfare'. *California Law Review* 101(4), pp. 1079-1129.
Available at: <https://www.jstor.org/stable/23784325> (Accessed: 23 March 2022)
- Nye, Joseph. (2010). *Cyber Power*. Belfer Center for Science and International Affairs. Available at:
<https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf> (Accessed: 24 April 2022)
- Pražák, Jakub. (2021). 'Dual-use conundrum: Towards the weaponization of outer space?', *Acta Astronautica Vol. 187*, pp. 397-405. Available at:
<https://doi.org/10.1016/j.actaastro.2020.12.051> (Accessed: 16 July 2022)
- Schia, Niels N & Tikk, Eneken (2020). 'The role of the UN Security Council in cybersecurity: international peace and security in the digital age' in in Kerttunen, M & Eneken Tikk (eds). *Routledge Handbook of International Cyber Security*. New York: Routledge, pp. 354-365
- Schmitt, Michael. (2011). 'Cyber Operations and the Jud Ad Bellum Revisited'. Available at:
<https://digitalcommons.law.villanova.edu/vlr/vol56/iss3/10>(Accessed: 22 April 2022)
- Schmitt, Michael N. & Liis Vihul (eds.) 2013. *Talin Manual on the International Law Applicable to Cyber Warfare* (1st ed). Cambridge: Cambridge University Press.

Schmitt, Michael N. & Liis Vihul (eds.). 2017. *Tallinn manual 2.0 on the International Law Applicable to Cyber Operations* (2nd ed). Cambridge: Cambridge University Press

Schmitt, Michael. (2021). 'The Sixth United Nations GGE and International Law in Cyberspace', *Just Security*, 10 June 2021. Available at: <https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/> (Accessed: 13 July 2022)

Stevens, T. & Kavanagh, C. (2021). 'Cyber Power in international relations'. *The Oxford Handbook of Cyber Security*, pp.65–81. Available at: 10.1093/oxfordhb/9780198800682.013.4 (Accessed: 26 April 2022)

Sukumar, Arun M. (2017). 'The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?', *Lawfare*, 4 July 2017. Available at: <https://www.lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well> (Accessed: 13 July 2022)

United Nations. (1945). *UN Charter*. Available at: <https://www.un.org/en/about-us/un-charter/full-text> (Accessed: 22 April 2022)

United Nations General Assembly (UNGA). (1998). A/RES/53/70: *Developments in the field of information and telecommunications in the context of international security* (4 December 1998). Available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/760/03/PDF/N9976003.pdf?OpenElement> (Accessed: 29 May 2022)

United Nations General Assembly (UNGA). (1999). A/RES/54/49: *Developments in the field of information and telecommunications in the context of international security* (1 December 1999).

Available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/777/13/PDF/N9977713.pdf?OpenElement> (Accessed: 29 May 2022)

United Nations General Assembly (UNGA). (2000). A/RES/55/28:
Developments in the field of information and telecommunications in the context of international security (20 November 2000).

Available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N00/561/07/PDF/N0056107.pdf?OpenElement> (Accessed 29 May 2022)

United Nations General Assembly (UNGA). (2001). A/RES/56/19:
Developments in the field of information and telecommunications in the context of international security (29 November 2001).

Available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N01/476/28/PDF/N0147628.pdf?OpenElement> (Accessed 29 May 2022)

United Nations General Assembly (UNGA). (2002). A/RES/57/53:
Developments in the field of information and telecommunications in the context of international security (22 November 2002).

Available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N02/541/45/PDF/N0254145.pdf?OpenElement> (Accessed 29 May 2022)

United Nations General Assembly (UNGA). (2003). A/RES/58/32:
Developments in the field of information and telecommunications in the context of international security (8 December 2003).

Available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N03/454/83/PDF/N0345483.pdf?OpenElement>. (Accessed 29 May 2022)

United Nations General Assembly (UNGA). (2004). A/RES/59/61:
Developments in the field of information and telecommunications

in the context of international security (3 December 2004).

Available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N04/479/92/PDF/N0447992.pdf?OpenElement>. (Accessed 29 May 2022)

United Nations General Assembly (UNGA). (2005a). A/RES/60/45:

Developments in the field of information and telecommunications in the context of international security (8 December 2006).

Available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N05/490/30/PDF/N0549030.pdf?OpenElement>. (Accessed 29 May 2022)

United Nations General Assembly (UNGA). (2005b). A/RES/60/202:

Report of the Secretary-General on Group of Governmental Experts on Developments in the Field of Information and Telecommunication in the Context of International Security (5 August 2005).

Available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N05/453/63/PDF/N0545363.pdf?OpenElement>. (Accessed 29 May 2022)

United Nations General Assembly (UNGA). (2006). A/RES/61/54:

Developments in the field of information and telecommunications in the context of international security (6 December 2006).

Available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N06/497/67/PDF/N0649767.pdf?OpenElement> (Accessed 29 May 2022)

United Nations General Assembly (UNGA). (2007). A/RES/62/17:

Developments in the field of information and telecommunications in the context of international security (5 December 2007).

Available at: <https://daccess-ods.un.org/tmp/3811022.6392746.html> (Accessed 29 May 2022)

- United Nations General Assembly (UNGA). (2008). A/RES/63/385:
*Developments in the field of information and telecommunications
in the context of international security* (2 December 2008).
Available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N08/473/01/PDF/N0847301.pdf?OpenElement>. (Accessed 29 May 2022)
- United Nations General Assembly (UNGA). (2009). A/RES/64/35:
*Developments in the field of information and telecommunications
in the context of international security* (2 December 2009).
Available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N09/463/33/PDF/N0946333.pdf?OpenElement> (Accessed 29 May 2022)
- United Nations General Assembly (UNGA). (2010a). A/RES/65/41:
*Developments in the field of information and telecommunications
in the context of international security* (8 December 2010).
Available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N10/515/00/PDF/N1051500.pdf?OpenElement> (Accessed 29 May 2022)
- United Nations General Assembly (UNGA). (2010b). A/RES/65/201:
*Report of the Group of Governmental Experts on Developments
in the Field of Information and Telecommunications in the
Context of International Security* (30 July 2010). Available at:
<https://documents-dds-ny.un.org/doc/UNDOC/GEN/N10/469/57/PDF/N1046957.pdf?OpenElement> (Accessed 29 May 2022)

United Nations General Assembly (UNGA). (2011a). A/RES/66/24:
*Developments in the field of information and telecommunications
in the context of international security* (2 December 2011).
Available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N11/460/26/PDF/N1146026.pdf?OpenElement> (Accessed 29 May 2022)

United Nations General Assembly (UNGA). (2011b) A/66/359: *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*.
Available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N11/496/56/PDF/N1149656.pdf?OpenElement> (Accessed 15 July 2022)

United Nations General Assembly (UNGA). (2012). A/RES/67/27:
*Developments in the field of information and telecommunications
in the context of international security* (3 December 2012).
Available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N12/480/22/PDF/N1248022.pdf?OpenElement> (Accessed 29 May 2022)

United Nations General Assembly (UNGA). (2013a). A/RES/68/243:
*Developments in the field of information and telecommunications
in the context of international security* (27 December 2013).
Available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/454/03/PDF/N1345403.pdf?OpenElement> (Accessed 29 May 2022)

United Nations General Assembly (UNGA). (2013b). A/RES/68/98:
*Report of the Group of Governmental Experts on Developments
in the Field of Information and Telecommunications in the
Context of International Security* (24 June 2013) Available at:

<https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/371/66/PDF/N1337166.pdf?OpenElement> (Accessed 29 May 2022)

United Nations General Assembly (UNGA). (2014). A/RES/69/28: *Developments in the field of information and telecommunications in the context of international security* (2 December 2014). Available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/662/40/PDF/N1466240.pdf?OpenElement> (Accessed 29 May 2022)

United Nations General Assembly (UNGA). (2015a). A/RES/70/237: *Developments in the field of information and telecommunications in the context of international security* (23 December 2015). Available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/457/57/PDF/N1545757.pdf?OpenElement> (Accessed 29 May 2022)

United Nations General Assembly (UNGA). (2015b). A/RES/70/174: *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (22 July 2015). Available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf?OpenElement> (Accessed 29 May 2022)

United Nations General Assembly (UNGA). (2015c). *Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*. Available at: https://digitallibrary.un.org/record/786846/files/A_69_723-EN.pdf (Accessed 15 July 2022)

United Nations General Assembly (UNGA). (2016). A/RES/71/28:
*Developments in the field of information and telecommunications
in the context of international security* (5 December 2016).
Available at: [https://documents-dds-
ny.un.org/doc/UNDOC/GEN/N16/399/50/PDF/N1639950.pdf?Op
enElement](https://documents-dds-ny.un.org/doc/UNDOC/GEN/N16/399/50/PDF/N1639950.pdf?OpenElement) (Accessed 29 May 2022)

United Nations General Assembly (UNGA). (2018a). A/RES/73/266:
*Advancing responsible State behaviour in cyberspace in the
context of international security* (22 December 2018). Available
at: [https://documents-dds-
ny.un.org/doc/UNDOC/GEN/N18/465/01/PDF/N1846501.pdf?Op
enElement](https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/465/01/PDF/N1846501.pdf?OpenElement) (Accessed 29 May 2022)

United Nations General Assembly (UNGA). (2018b). A/RES/73/27:
*Developments in the field of information and telecommunications
in the context of international security* (5 December 2018).
Available at: [https://documents-dds-
ny.un.org/doc/UNDOC/GEN/N18/418/04/PDF/N1841804.pdf?Op
enElement](https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/418/04/PDF/N1841804.pdf?OpenElement) (Accessed 29 May 2022)

United Nations General Assembly (UNGA). (2019a). A/RES/74/28:
*Advancing responsible State behaviour in cyberspace in the
context of international security* (12 December 2019). Available
at: [https://documents-dds-
ny.un.org/doc/UNDOC/GEN/N19/410/00/PDF/N1941000.pdf?Op
enElement](https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/410/00/PDF/N1941000.pdf?OpenElement) (Accessed 29 May 2022)

United Nations General Assembly (UNGA). (2019b). A/RES/74/29:
*Developments in the field of information and telecommunications
in the context of international security* (12 December 2019).
Available at: [https://documents-dds-](https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/410/00/PDF/N1941000.pdf?OpenElement)

ny.un.org/doc/UNDOC/GEN/N19/410/07/PDF/N1941007.pdf?OpenElement (Accessed 29 May 2022)

United Nations General Assembly (UNGA). (2020). A/RES/75/240: *Developments in the field of information and telecommunications in the context of international security* (31 December 2020). Available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/000/25/PDF/N2100025.pdf?OpenElement> (Accessed 29 May 2022)

United Nations General Assembly (UNGA). (2021a). A/RES/76/19: *Developments in the field of information and telecommunications in the context of international security, and advancing responsible State behaviour in the use of information and communications technologies* (6 December 2021). Available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/377/48/PDF/N2137748.pdf?OpenElement> (Accessed 29 May 2022)

United Nations General Assembly (UNGA). (2021b). A/RES/76/135: *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security* (14 July 2021). Available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/075/86/PDF/N2107586.pdf?OpenElement> (Accessed 29 May 2022)

United Nations General Assembly (UNGA). (2021c). *Final Substantive Report of Open-ended working group on developments in the field of information and telecommunications in the context of international security* (10 March 2021). Available at: <https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf> (Accessed 1 June 2022)

United Nations Office for Outer Space Affairs (UNOOSA). (1967).
Treaty on Principles Governing the Activities of States in the
Exploration and Use of Outer Space, including the Moon and
Other Celestial Bodies. Available at:
https://www.unoosa.org/pdf/gares/ARES_21_2222E.pdf
(Accessed 16 July 2022)

United Nations Office for Outer Space Affairs (UNOOSA). (1979).
[Agreement Governing the Activities of States on the Moon and
Other Celestial Bodies](#). Available at:
https://www.unoosa.org/pdf/gares/ARES_34_68E.pdf (Accessed
16 July 2022)

Väljataga, Ann. (2017). 'Back to Square One? The Fifth UN GGE Fails
to Submit a Conclusive Report at the UN General Assembly',
NATO CCDCOE, Available at: [https://ccdcoe.org/incyder-
articles/back-to-square-one-the-fifth-un-gge-fails-to-submit-a-
conclusive-report-at-the-un-general-assembly/](https://ccdcoe.org/incyder-articles/back-to-square-one-the-fifth-un-gge-fails-to-submit-a-conclusive-report-at-the-un-general-assembly/) (Accessed: 13
July 2022)

White House. (2009). 'Remarks by the President on Securing Our
Nation's Cyber Infrastructure, *The White House*, 29 May 2009.
Available at: [https://obamawhitehouse.archives.gov/the-press-
office/remarks-president-securing-our-nations-cyber-
infrastructure](https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure) (Accessed 17 March 2022)