TALLINN UNIVERISTY OF TECHNOLOGY
School of Business and Governance
Department of Law

Priscila da Silva Leopoldino

INTERNATIONAL CYBER NORMS: THE UNITED NATIONS AS A NORMATIVE POWER

Bachelor’s thesis
Programme International Relations

Supervisor: Holger Mölder, Ph.D.

Tallinn 2020

I hereby declare that I have compiled the thesis independently
and all works, important standpoints and data by other authors
have been properly referenced and the same paper
has not been previously been presented for grading.
The document length is 10 108 words from the introduction to the end of summary.

Priscila da Silva Leopoldino ……………………………………
(signature, date)

Student code: 156096TASB

Student e-mail address: prisleopoldino@gmail.com

Supervisor: Hõlger Mölder:

The paper conforms to requirements in force

…………………………………………………………….
(signature, date)

Chairman of the Defence Committee:

Permitted to the defence

………………………………………
(name, signature, date)

TABLE OF CONTENTS

ABSTRACT

Considering technological developments within Information and Communications Technologies, the international community has recognized potential threats and risks in recent years emerging from the cyber domain. The subject of information security has been on the United Nations' agenda since 1998. In 2004 the United Nations established the first Group of Governmental Experts on developments in the field of Information and Telecommunications in the context of international security. The aim of this paper is to argue whether the United Nations, in the context of the Group of Governmental Experts, is a normative power in the cyber domain. To answer this question this study will test the Normative Power Europe theory coined by scholar Ian Manners through a normative discourse to assess the international role of the United Nations in shaping cyber norms and endorsing how things ought to be in the normative space.

Keywords: United Nations, United Nations Group of Governmental Experts, Cyber Norms, Normative Power, Normative Power Europe, Norm Diffusion, Cyberspace

LIST OF ABBREVIATIONS

GA – General Assembly

GGE – Group of Governmental Experts

ICTs – Information and Communications Technologies

NATO – North Atlantic Treaty Organization

NGO – Non-governmental organization

OEWG – Open-Ended Working Group

UN – United Nations

USA – United States of America

INTRODUCTION

The global interconnection of computer networks has the power to promote interaction between millions of individuals which, subsequently, forms a global network of individuals, institutions, companies, and governments. This interactivity between the technological and electronic means allows the establishment of diverse forms of relations such as: social; political; commercial; and professional. Nonetheless, this interactivity and increased exposure facilitate the emergence of cyber threats and paves the way for cybercriminals to pursue attacks against society, government agencies, and commercial institutions. The risks of potential infringement of critical data and moral damage are emergent.

In a globalized world, cyberspace constitutes a critical dimension on the functioning of the modern society. The necessity to exchange large amounts of information is inherently associated with security criteria as the data must be protected against non-authorized access and modifications. The lack of internationally recognized and binding laws and rules regulating cyberspace is deemed to constitute a global threat to society at large (Fidler 2018). The subject of information security has been on the United Nations' (hereinafter UN) agenda since 1998 upon Russian Federation's request and introduction of a draft resolution on the matter to the UN General Assembly (United Nations… 2015). In 2004, the UN established the United Nations Group of Governmental Experts on developments in the field of Information and Telecommunications in the context of international security (hereinafter UN GGE), a top bottom working group of experts with aim of strengthening the security of global information and telecommunications systems. Up to the present time, the UN GGE has held six working groups including a sixth group which was established in 2019 in the context of international security in the field of Information and Telecommunications. The role of the GGE is viewed as the main global arena in which to address discussions on international cybersecurity issues (Osula, Rõigas 2016, 13).

In essence, the concept of normative power means that an actor uses normative justification rather than physical force or material incentives form of engagement in the world politics (Manners 2009, 2). The basis of normative power steams from an understanding of its principles, actions and impact and it should be seen as legitimate in the principles being promoted (*Ibid.*). The normative justification must be consistent and coherent as well as have legitimate principles while being promoted in order to appear attractive or convincing toward the actors involved. The legitimacy of principles might arise from treaties or established international conventions, particularly if those are significant within the UN framework. The normative basis of the UN has been developed since its foundation and it's enshrined by the Charter of the UN which sets out four core purposes of the Organization: Maintaining world peace and security; develop friendly relations between nations; foster international cooperation among nation; and to serve as a forum to bring States together to meet the Organization's purposes and goal. Today, the UN is viewed a universal organization that can set standards and norms of behavior which are accepted on a global scale (Sills 2002). Thus, the UN's normative power exists not only on the Organization's wholeness but also in its individual programs, agencies, funds, and the international agreements *(Ibid.).*

The aim of this paper is to argue whether the UN, in the context of the GGE, is a normative power in the cyber domain. To answer this question this study will test the Normative Power Europe theory coined by scholar Ian Manners through a normative discourse to assess the international role of the UN GGE for shaping cyber norms and endorsing how things ought to be in the normative space. In order to contribute to this debate, the study will assess and answer the following questions: Firstly, what is the normative basis of the UN? Secondly, how does the UN exercise its normative power through the UN GGE? And lastly, how does the international community respond to the proliferation of cyber norms?

The first two questions will be answered through a thorough analysis of official UN and UN GGE documents to visualize and explain the normative basis of the Organization. The third question will be analysed and answered through a normative case study analysis focused on the United States of America (hereinafter USA), People's Republic of China, Russian Federation and Canada's position and diverse conceptions toward the UN GGE's promotion of cyber norms to understand the process of norm diffusion, and the challenges of adopting cyber norms on the national and international level perspectives. By answering those questions, the researcher aims to lay the normative foundation for the UN's determination to use its normative influence and instruments to shape cyber norms and to serve as a global arena in which to discuss issues related to international cybersecurity. The questions will also help to visualize the Organization's normative power, the instruments used to exercise this power, and the international community's response toward the UN's promotion of cyber norms.

The paper has the following structure. To understand the normative basis of the UN and to further develop the normative power discourse, the first chapter will provide a theoretical framework based on Normative Power Europe theory and Normative political theory to assess the UN's normative power in the context of the UN GGE. The second chapter will briefly lay out the concept of cyberspace, its core characteristics, and the development of cyber norms in the context of the Tallinn Manual and UN GGE. The third chapter will present a discussion of the UN's basis of normative power through an analysis of the UN Charter and UN GGE reports, followed by an overview of progress made in the GGE's framework. It will continue with a case study focused on four individual countries – the United States of America, China, Russia and Canada in order to understand how the emergence and proliferation of cyber norms from the UN GGE arena affect the international community to understand the process of norm diffusion through the lens of normative discourse analysis. The final chapter will make some concluding observations and summarize the study.

Research framework

This paper refers to qualitative research methods to better comprehend the phenomenon in the context of how it occurs and to analyze it from an integrative perspective to capture the phenomenon in the perception of the actors involved by considering all relevant points of view. Qualitative research methods collect various types of data to analyze and comprehend the dynamics of the phenomenon, starting from broad questions that will lighten up during the qualitative investigation. This research method can be driven through different paths such as a case study and documentary research.

Documentary research was employed in this paper aimed at acquiring a thorough understanding of the UN's development of its normative basis. Furthermore, it was intended to visualize how the Organization exercises its normative power through the UN GGE, and to analyze how this affects relations in the international sphere. In order to achieve this objective an analysis of the text data was employed by investigating material to find appropriate content for this research. The data gathered and analyzed was acquired from the UN Charter, UN GGE reports, and official documents from the actors involved. This approach was selected to answer the following question: What is the normative basis of the UN?

Furthermore, the Normative Power Europe theory coined by scholar Ian Manner (Manners, 2002) and Normative political theory were applied to this study to analyze the UN's normative power through the UN GGE. This concept aimed to provide the basis for understanding how the UN uses normative instruments to define what is considered “normal” in international relations. The following question was addressed: How does the UN exercise its normative power through the UN GGE?

A case study focused on UN GGE’s role in shaping cyber norms and influencing the USA, China, Russia and Canada was performed to further develop how the emergence of norms, in the cyber domain context, affects relations within the international community. A normative discourse analysis was used for conducting this study aimed at analyzing official documents, national statements, and related articles from the UN GGE, USA, China, Russia and Canada. This study case was expected to provide a descriptive analysis of the four countries’ positions, shared concepts, and diverse conceptions toward the UN GGE’s proliferation of cyber norms and its applicability to international level perspectives. The case study was aimed to assess and comprehend the following: How does the international community respond to the proliferation of cyber norms?

1. THEORETICAL FRAMEWORK

1.1. Normative power Europe

To analyse the UN's normative power in the cyber arena, the UN GGE will be examined through the lens of the "Normative Power Europe" concept coined by scholar Ian Manners (Manners, 2002). This study views normative power as the use of normative instruments by States, for shaping how things ought to be in the normative sphere. According to Manners, normative power is the "ability to shape conceptions of normal" (Manners 2002, 29). According to Normative Power Europe theory, an actor's normative power originates firstly from its normative basis through the implementation of treaties, declarations, policies, criteria and conditions. Secondly, it originates through norm diffusion in the international community. (Manners 2002)

The Normative Power Europe theory was included in this study in order to understand and visualize how the UN normalizes rules and principles on the international scene through the UN GGE via non-coercive means with the primary aim of defining what is considered "normal" in international relations. Thus, the aim of implementing this concept was to analyze the Organization's normative behaviour in the cyber domain, and to further develop and understand where the UN's normative power comes from. An analysis of the UN Charter, more specifically, focusing on the core principles and values of the Organization, will be carried out to explain the normative basis of the UN. Furthermore, a review of UN GGE's reports will be performed to further develop the UN's normative basis discourse in the cyber domain, by finding links between the Organization's core values and the normative discourse of the UN GGEs vis-à-vis the international sphere.

According to Manners, there are six factors shaping norm diffusion in the international sphere that constitute an actor's normative power: Contagion, informational, procedural, transference, overt, and cultural filter. Analyzing the factors that shape norm diffusion within the context of the UN toward the international community will serve to assess the UN's normative power and contribute to answering the question of whether the UN is a normative actor in the cyber domain. In light of this research, a case study focused on UN GGE role for shaping cyber norms and the international community's response to the proliferation of these norms will be performed to understand the process of norm diffusion. This case study will be focused on four members of the GGE's: USA, China, Russia and Canada. For the UN to act as a normative power, the norms promoted within the UN GGE framework must be socially diffused. The absence of coercive means in the process of norm diffusion is a significant aspect of normative power. The promotion and maintenance of international peace and stability is the core foundation for the establishment of the UN and constitute its normative basis.

1.2. Normative political theory

Normative theory provides a value-based vision of how the world ought to work or ought to be by proposing standards and goals that should be achieved or are desirable through a normative actor for ordering political communities. Since its origin in Ancient Greece, normative political theory encompasses the legitimacy of political authority, the binding forces and nature of political duties and the rights of those living under such authority (Bauböck 2008). In regard to the normative political theory founders, one can honour Aristotle and Plato as the originators through their reflections of practical philosophy based on the non-separation between politics and ethics – what "is" and what "ought" to be (Pietrzyk-Reeves 2017).

The work of John Rawl entitled "A Theory of Justice" published in 1971, served as a turning point for the development of normative theories and became recognized as a necessary research method in political science since values can be seen as the element of political structures and systems in order for actors to engage into the role of mediators in descriptive and prescriptive terms of politics (Bauböck 2008). Normative theory is solely concerned with normative principles and norms. Each State or political community can function on the basis of principles and common standards shared by its members and the normative theory articulates statements as to what principles, norms and standards a State ought to be based on or follow. In the political context, norms can be seen as standards of political action and social behaviour. Normative theory attempts to determine what principles and standards ought to be desirable and followed by a State. The normative theory can be used to address the way in which norms exist, function and evolve (Pietrzyk-Reeves 2017).

In the context of the GGE, one can assert the UN's position to be a normative actor in international relations through non-coercive means and by serving as a global forum to shape cyber norms, State behaviour, and setting standards for how norms ought to be in the cyberspace. The normative basis of the UN is enshrined in the core values of the Charter of the UN to maintain world peace and security, develop friendly relations between nations, foster international cooperation among nations, and to serve as a forum to bring States together. Thus, the UN's normative power exists not only on the Organization's wholeness but also in its individual programs, agencies, funds, and international agreements (Sills 2002).

This research finds that since the establishment of the first GGE in 2004, the UN has achieved two major accomplishments: firstly, the outlining of a global cybersecurity agenda, and secondly, the introduction of the discourse that international law applies to the cyber realm. The UN's founding basis of fostering international cooperation between nations and maintaining the world peace and security serves as a normative basis for influencing how actors ought to behave in the cyber domain and for strengthening the security of global information and telecommunications systems. Although the regulations accomplished by the GGEs at this moment are voluntary and non-legally binding, the process of norm diffusion from the UN GGE to the global level is a work in progress which involves a deeper acceptance of States and the normalization of norms and regulations enshrined by the GGEs.

2. CYBERSPACE AND CYBER NORMS

2.1. The concept of cyberspace

The Internet has stablished a new space for human interaction and socialization by providing means of communication and interaction which had never before been imagined. Given the heterogenous aspect of the virtual space in which it transcends national boundaries and government centralization, the Internet is not subject to the exclusive authority of any actor or state. The decentralized and borderless construction of the virtual domain allows for freedom of communication, socialization, and the free movement of ideas and information. Hence, the Internet has become essential to global economic, social, and political interactions.

The concept of "cyberspace" was popularized by William Gibson in his science fiction novel entitled *"Neuromancer"*. The book was published in 1984 and tells the story of a man who was projected into the network of information created by millions of connected computers. Cyberspace is a human and technological environment of expression, information, and economic transactions. It consists of people from all over the world, from different cultures, languages, ranging from diverse age groups and professions which in their turn, provide and require information. A global network of interconnected computers through a telecommunication infrastructure allows for the provision or requirement of information to be processed and digitally transmitted.

However, it is essential to highlight that Internet and cyberspace, technically, are not the same. The former constitutes a man-made artificial construction that identifies a virtual environment, without physical borders, in which Internet users interact through the technological infrastructure of the global network of computers (Leiner *et al*. 1997).

Etymologically, cyberspace constitutes a compound word and the origin of "cyber" is derived from the Greek word "kybernetes" which translates to ruler, governor, and pilot. The word "cyber" also denotes "cyborg", a term which describes a machine-human synthesis created by connecting complex devices to the human body. Cyberspace is conceptualized as a virtual place-metaphor to understand and describe the function of information and communications technologies (Fourkas 2012, 1).

In view of the cyberspace link with the technological infrastructure that composes the Internet, the former inherits the following core characteristics of the latter: it has a global reach, which can be accessed from anywhere in the world; it is present in several countries; it is interactive in that the user has the capacity to actively engage in cyberspace; it is open to the public and access to it is free (with the exception of a few authoritarian States); it is decentralized in that there is no a single central authority; it is heterogeneous in that millions of individuals are able to connect and engage through several means and devices; and lastly, it provides economic and political interaction between users.

2.2. The development of international cyber norms

In light of technological developments, the global dependence of governmental institutions, states, individuals, and international organizations on Internet systems enables new types of crimes such as cyber terrorism, hacking, cyber espionage, and cyber warfare to purposefully damage others. In spring of 2007 Estonia fell victim to a cyber-attack that lasted for twenty-two days and negatively affected the country's banking systems and digital-based public transportation which caused the systems to be disrupted. The problematic outcomes of cyber-attacks for non-state and state actors has become a major part of the international political agenda.

In the past decade, international experts have raised the question about how to deal with the emergence of irregular forms of warfare and the applicability of international law under cyber operation affairs. The most recent examples include the Tallinn Manual on cyber warfare and cyber operations prepared by the North Atlantic Treaty Organization (hereinafter, NATO), and the UN GGEs in the field of Information and Telecommunications in the context of international security. In this subchapter, the researcher discusses the Tallinn Manuals to show how experts deliberate with the construct of legal definitions and norms that can be used in the cyber domain in contrast to the GGE format that serves as an inclusive arena to deliberate on topics related to the application of international law, standards of responsible State behavior, and ways to implement regulations in norms in the cyberspace.

In 2013 NATO published a legal resource entitled "Tallinn Manual on the International Law Applicable to Cyber Warfare" authored by experts in military affairs, security law and conflict, led by the NATO Cooperative Cyber Defence Centre of Excellence located in Estonia. The first edition of the manual was aimed to examine the extent to which international law applies to cyber warfare with the emphasis on cyber-to-cyber operations in terms of the conditions in which a State may resort to war. The results of this process produced a non-binding legal resource applicable to existing law to cyber warfare with a list of possible themes that could theoretically be relevant for the assessment of cyberwars (Schmitt, *et al.* 2013).

An updated version of the Tallinn manual “Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations” was published in 2017 as an expanded version of the original 2013 edition. Tallinn Manual 2.0 addresses a wide spectrum of international law applicable to cyber affairs ranging from the law of armed conflict and peacetime legal systems, concealing international law norms and regimes that regulate procedures in the cyber domain (The NATO Cooperative… s.a.). The aim of the manual is to process a legal, strategic, technical and operational assessment of cyber scenarios in and out of armed conflict to serve as a guide for policy advisors and cyber commands on international law applicable to cyber operations.

The Tallinn manuals represent a prominent attempt by international experts to provide a guideline to facilitate the regulation of international law in cyber operations. This approach characterizes an attempt to adapt and expand existing law to new type of warfare and operations in the cyber realm instead of creating a new legal paradigm. The Tallinn Manual lays out a regulatory scheme for general norms and principles and their interaction with telecommunication law, human rights law, diplomatic law, and space law (Efrony, Shany 2018).

The expert-driven approach employed in the drawing up of the Tallinn Manuals appears to have received limited support at the international level since it is difficult to assess whether nations accept the rules outlined in the Manuals and wish them to become legal articulations of international law in cyberoperations (Efrony, Shany 2018). The autonomy of states, in regard to how they approach and promote legal certainty of the regulation of the cyberspace, puts into question the acceptance and degree to which the Tallinn Manuals ought to be universally recognized as a guideline or basis for formulating the applicability of legal norms to the cyber realm.

In contrast to the Tallinn Manuals, the UN GGE serves as a forum where interested UN members can send an official request for a seat on a GGE of particular interest. The composition of the Group will be formed based on the States’ political and geographical balance as well as their interest in the topic. Once the countries are identified, they are expected to nominate an expert to represent them in the GGE. These experts are often governmental officials including professionals from information security, diplomacy, and more technical background. Each GGE is guided by a skillful and strong Chair and shaped by the mandate in the General Assembly (hereinafter, GA) which defines its agenda and work plan. The first and second GGE was chaired by the Russian Federation in 2005 and 2010, the third by Australia in 2013, the fourth by Brazil in 2015, and the fifth by Germany in 2016. The sixth GGE established in 2019 is chaired by Brazil and it is expected to report back to the GA by 2021. The procedures of how the GGE members are selected allows for the inclusion and rotation of interested member states to share their views and perceptions based on the GGE's agenda and plans.

In December 2018, the UN GA established the Open-Ended Working Group (hereinafter, OEWG) to develop norms, rules, and principles of responsible behavior of states, and to deliberate on means for their acceptance and implementation through the establishment of institutional dialogues with wide participation under the auspices of the UN. The OEWG participation is open and allows all UN member states to express their desire to participate. The Group is also tasked with holding meetings with interested actors, academia, interested business and non-governmental organizations. The OEWG's work started in June 2019 and six substantive issues are included for discussion: Existing and potential threats; international law; rules, norms and principles; regular institutional dialogue; confidence building measures; and capacity building (Geneva Internet Platform… s.a.).

The GGE functions as a global arena where interested member states may hold open discussions about stability in cyberspace and the applicability of rules, norms and principles in the cyber domain in order to strengthen common understanding and to further advance and implement a legal framework endorsed by the UN GGE on the international level. In contrast, the Tallinn Manuals serve as a legal rule book to which states may or may not resort when faced with the dilemma, in the context of cyber operations, of trusting the ready-made international law framework in the midst of normative uncertainty in cyberspace.

3. THE UNITED NATIONS AS A NORMATIVE POWER

3.1. Developments in the United Nations Group of Governmental Experts

Since its establishment in 2004 by the UN General Assembly, the GGE framework has turned to the main global arena to address discussions on international cybersecurity issues (Osula, Rõigas 2016, 13). In the context of cyber norms, the Group serves as a platform for member states to deliberate on their national positions about developments in the field of ICTs.

The GGEs are composed on "the basis of equitable geographical distribution" (Lewis, Vignard, s.a). The five permanent members of the Security Council are granted a seat on all GGE sessions, and the remaining seats are distributed by UN regional grouping. States are eligible to officially send a request for seats on a session upon their interests. Members of the GGE, will be selected based on their geographical and political balances, as well as on demonstrated interest in the Group's topic. (*Ibid.*) Once potential members are identified, the UN Secretary-General has the task of structuring the GGE composition. The selected countries are requested to nominate an expert to partake in the GGE. To promote frank discussion within the GGEs, the meetings are held in a closed-door format and there are no publicly available summaries of the meetings. Therefore, only the member states which were granted a seat in a specific session will partake in the activities of the Group. The reports created by the GGE are the primary outcome of the Group, and the decisions in the final report are made by consensus.

The first UN GGE in the context of international security in the field of telecommunications and information, held between 2004 and 2005, could not agree on a consensus and did not release any final report (UN document A/60/202). Instead, the Group released a brief report on procedural matters. The second GGE held between 2009 and 2010 proved to be more productive than its predecessor and released a consensus report. The GGE urged for cooperation among Nations, the private sector and civil society to increase cybersecurity capabilities, and the elaboration of a common understanding of terms and definitions within the information security field (UN document A/65/201). The third Group meeting held during 2012–2013, the GGE arrived at a consensus final report and reached comprehensive conclusions regarding the relationship between international law and cyberspace. The Group introduced two key facts: firstly, the agreement that international law, in particular the Charter of the UN, is applicable to cyberspace, secondly, the recognition that State sovereignty and international norms and principles apply to State conduct in cyberspace (UN document A/68/98). The report also acknowledged the vital role of the UN in promoting cyber dialogues among Nations.

In the 2014–2015 GGE's consensus report, a set of voluntary, non-binding norms, rules and principles of responsible State behavior in cyberspace were outlined to promote "an open, secure, stable, accessible and peaceful ICT environment" (UN document A/70/174). Furthermore, it reaffirmed the application of international law to cyberspace following principles of the UN Charter, and other international law: sovereign equality, respect for human rights and fundamental freedoms, law of war principles – including necessity, proportionality, humanity and distinction. (UN document A/70/174).

The fifth GGE working group, which lasted between 2016 and 2017, was unable to provide a final report due to the lack of consensus among its members. According to a statement by the U.S Deputy Coordinator for cyber issues, the lack of consensus was caused by "insufficient language" on how international law applies to a Nation's response and countermeasures to cyber-incidents. Additionally, the U.S. pointed out that a few member states were unwilling to seriously engage with and affirm the applicability of international rules and laws in cyberspace. (Markoff 2017)

In October 2018, a resolution on cybersecurity issues was proposed by the USA and adopted by the UN General Assembly in the following month, with 139 states in favor to 11 against. The resolution emphasized the final reports of the UN GGEs (2010, 2013, and 2015) and demanded the establishment of a new Group in 2019, delegated to further study norms, cyber capacity and confidence-building measures. Furthermore, it outlined that the final report must contain national submissions on the application of international law to cyberspace. The new GGE is expected to report to the UN's General Assembly in Autumn 2021. (United… 2018)

In December 2018 a second work group mandated by the UN entitled "Open-Ended Working Group" was established in parallel with the UN GGE which involves all interested UN member states, academia, businesses and non-governmental organizations (hereinafter NGO) to further change or develop norms, principles and rules of responsible State behavior in the field of ICTs in the context of international security enshrined by the UN General Assembly (hereinafter, UN GA) on December 5th 2018 (General Assembly… 2018). The OEWG mandate began on 2019 and is expected to report back to the UN GA by July 2020.

The composition of the OEWG is open and allows all UN member states to express their desire to participate. Additionally, the working group organizes meetings with NGOs, academia and organizations where the interested parties can apply to attend. The OEWG agenda consists of six issues for discussion according to paragraph 5 of the UN GA Resolution A/RES/73/27 (General Assembly… 2019):

1. Existing and potential threats
2. International Law
3. Rules, norms and principles
4. Regular institutional dialogue
5. Confidence building measures
6. Capacity building

Joint cooperation of the UN GGE and OEWG provides a forum for member States and interested parties to support rules, norms, and principles in cyberspace, advance openness and stability in cyberspace as well as strengthen a common understanding as enshrined by the UN GA. The strategy framework established by past GGE reports allows member States to promote, further advance, and implement the framework endorsed by the UN GGE.

3.2. The United Nations' normative basis

In response to the tragic events of World War II, The UN was founded in October 1945 with the primary objective of preventing and resolving international conflicts, and to promote and maintain peace and security through cooperation with the international community. Today the UN is the world's largest intergovernmental organization and is comprised of 193 members states. The normative basis of the UN has been developed since its foundation and it's based on the Charter of the UN. The values enshrined in the Charter set out four core purposes of the Organization: Maintaining world peace and security; developing friendly relations between nations; fostering international cooperation among nations to solve economic, social, cultural, or humanitarian conflicts; and serving as a forum for bringing States together to meet the Organization's purposes and goals (UN Charter 1945).

To maintain international peace and security the UN takes collective measures aimed at the prevention and resolution of threats to peace through peaceful means and in conformance with the principles of international law and justice. The development of friendly relations among nations helps the UN to strengthen international peace based on the principles of equal rights and the self-determination of peoples. International cooperation at the UN level serves as an instrument to solve economic, social, cultural, and humanitarian conflicts as well as to promote respect for fundamental freedoms and human rights. In order to achieve its core values on the international scene, the UN serves as an arena for harmonizing the acts of States vis-à-vis the Organization's values and goals. (UN Charter 1945)

In light of the technological developments within Information and Communications Technologies (hereinafter, ICTs), the international community have recognized potential threats and risks in recent years emerging from the cyber domain. The actual and potential threats posed by malicious activities in cyberspace are deemed to be a great concern and one of the most serious challenges of the twenty-first century. According to the Cyber Operations Tracker by the organization entitled "Council of Foreign Relations", there have been over 280 cyber-attacks sponsored by 22 countries since 2005, including 63 attacks in 2018 alone (Council… s.a.). In view of the implications of these developments for international security, in 2004, the UN established the UN GGE on developments in the field of Information and Telecommunications in the context of international security, with the primary aim of strengthening the security of global information and telecommunications systems. The normative basis of the UN GGE framework stems from the UN's core values: Maintaining world peace and security; fostering international cooperation among nations; and ultimately serving as a forum for bringing States together to meet the UN's purposes and goals.

The reports of the GGEs are the primary outcome of the Group's work. Although the reports are not legally binding, they serve as a valuable influence in the field of global cybersecurity. Since its establishment in 2004, the Group has held six working groups, out of which only three GGEs reached consensus on the final report among members states during the GGEs held in 2009–2010, 2012–2013, and 2014–2015. A sixth working group was established in 2019 and is expected to end by 2021.

During the 2009–2010 sessions the Group provided a report that included recommendations for further dialogue among Nations to reduce risk and secure critical international and national infrastructure, confidence-building and risk-reduction measures, the exchange of information on national legislation and strategy, and the elaboration of a common understanding of terms and definitions within the information security field (UN document A/65/201). The 2012–2013 report included the agreement that international law, in particular the UN Charter, applies the cyberspace along with the recognition that State sovereignty and international norms and principles apply to State's conduct in cyberspace (UN document A/68/98). In the 2014–2015 Group's report, the discussion continued towards the applicability of international law to the use of ICTs, and the emergence of norms, rules and principles of responsible State behavior in cyberspace. It also emphasized the importance of international cooperation and assistance in cybersecurity. (UN document A/70/174)

Based on the founding principles and values of the UN Charter, one can observe that the UN clearly has a normative basis vis-à-vis the international community. Through the Organization's principles of maintaining world peace and security, fostering international cooperation among nations, serving as a forum for bringing States together to meet the UN's purposes and goals, the UN GGE arena was established with the aim of strengthening the security of global information and telecommunications systems. Since 2004, the GGE has achieved two major accomplishments: firstly, outlining the global cybersecurity agenda and, secondly, introducing the discourse that international law applies to cyberspace.

3.3. The United Nations' exercise of normative power

According to Ian Manners, to accept the normative basis of an actor does not make it a normative power. Hence, the scholar raises the following question: *"Where does the Normative Power come from?"* To answer this question, Manners suggests that normative power – in the context of the European Union – originates from different factors shaping norm diffusion in international relations. The diffusion of norms represents a combination of "power by example (symbolic normative power)" and "power by relations (substantive normative power)". (Manners 2002, 35)

There are six factors that shape norm diffusion (Manners 2002, 35):

1. Contagion - unintentional diffusion by EU
2. Informational - strategic and declaratory communications by EU
3. Procedural - institutionalisation of relationship by EU
4. Transference - exchange of benefits by EU and third parties
5. Overt - physical presence of EU in third states and organisations

6. Cultural Filter - cultural diffusion and political learning in third states and organisations

Contagion diffusion of norms results from “the unintentional diffusion of ideas” from the normative agent to other pollical actors (*Ibid.*). Examples of this are to be found in Joe Sills’ – former Vice-President of the UN Association of the United States of America, and UN’s Spokesman for the Secretary-General – essay of how the UN is a universal organization that can set standards and norms of behavior which are accepted on a global scale (Sills 2002). The UN’s specialized agencies The World Health Organization, World Bank Group, and the UN Educational, Scientific and Cultural Organization play major roles in the establishment of standards and norms for the world community.

Informational diffusion of norms is considered as “symbolic normative power” (*Ibid.*) observed by declaratory communications, and new policy initiatives by the normative actor. One example of declaratory communication is the UN Secretary-General António Guterres’ appeal on the creation of cyber norms, at the opening ceremony of the Munich Security Conference by stating that:
“[…] it’s high time to have a serious discussion about the international legal framework in which cyberwars take place and I think it would be essential to use what is the competence of the First Committee of the General Assembly of the United Nations to do it, and to do it sooner rather than later.” (United Nations… 2018).

Additionally, in the past six years, the UN GGE has set initiatives to the applicability of international law to cyberspace, and in particular the Charter of the UN, as well as sovereign equality, respect for human rights and fundamental freedoms, and principles of international humanitarian law – including necessity, proportionality, humanity and distinction.

Procedural diffusion involves both “symbolic” and “substantial” normative power (Manners 2002, 35) and comprises institutionalization between the normative actor and a third party. For instance, intergovernmental cooperation of UN GGEs by serving as a global arena for cyber dialogues, and a basis for the equitable geographical distribution of seats in the GGE sessions based on a State’s demonstrated interests and political views, constitutes a procedural diffusion of norms within the UN GGE context.

Transference diffusion occurs when the normative actor "exchanges goods, trade, aid or technical assistance with third parties through substantive or financial means" (*Ibid.*). One example of a specialized agency that provides aid assistance is the United Nations Children's Fund that provides support for children in over 190 countries and territories through the defense of their rights and support to fulfil their potential. It also provides inclusive initiatives aimed at gender equality, environment and climate change, social inclusion, education and the prevention of child mortality.

Overt diffusion takes place as the result of physical presence in third countries and international organizations. The extensive number of funds, programs, and specialized agencies developed from the UN system allows the UN to assert its presence in hundreds of nations through research and statistical work, by providing advice and assistance to its member states, through the negotiation and implementation of binding and non-binding international instruments, and by facilitating the creation of networks for cooperation between organizations and nations.

The final factor, cultural filter diffusion of norms, intermediates the impact of political learning and international norms in third states and organizations, leading to the construction of knowledge, diffusion or rejection of norms (*Ibid.*). One example of this cultural filter of norm diffusion is the 2012–2013 UN GGE report in which a consensus was reached that international law, and in particular the UN Charter, applies to cyberspace and is essential "to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment" (UN document A/68/98). Although the report is non-legally binding, an agreement on the application of international law was reached between the following fifteen countries: Argentina, Australia, Belarus, Canada, China, Egypt, Estonia, France, Germany, India, Indonesia, Japan, Russian Federation, United Kingdom, and USA (Geneva… s.a.).

Although cyber norms which emerged from the UN GGEs resolutions during the past six years are non-legally binding and have not yet been fully diffused to the international community at large, it has served as a step toward institutionalizing cyber norms. The process of norm diffusion in the context of the UN GGE vis-à-vis the international sphere is a work in progress which involves a deeper acceptance of States. Considering the USA proposal of a resolution in October 2018 demanding the establishment of a new GGE in 2019, with 139 states in favor to 11 against, and being adopted by the UN General Assembly in November 2018, one can observe that the discussion of the implementation of norms in cyberspace is a vital debate in international relations (United… 2018). The new GGE will be delegated to further study norms, with an emphasis on the final reports of past GGEs (2010, 2013, and 2015), and to outline on the final report expected to be delivered in Autumn 2021.

In the past fifteen years, since the establishment of the first GGE on developments in the field of Information and Telecommunications in the context of international security, the UN has increasingly been exercising normative power based on the Organization's values and principles enshrined in the UN Charter, and further outlined in the GGE reports as it seeks to shape international norms according its own values and purposes. There are three principles which lead the UN to work toward the establishment of the UN GGE: firstly, maintaining world peace and security; secondly, fostering international cooperation among Nations; and lastly, serving as a forum for bringing States together to meet the UN's purposes and goals. Those three principles are firmly rooted in the UN Charter and constitute the normative basis of the Organization. Thus, the establishment of the GGE has served, and still serves as a normative instrument that the UN uses to influence international relations on a global perspective.

The endorsement of norms and the application of the rule of law to cyberspace constitutes the normative essence of the UN to influence how things ought to be in the normative space. Thus, one can conclude that the UN has the normative basis and instruments to shape international relations as well as the normative power "to shape conceptions of normal" (Manners 2002, 29) and to influence the diffusion of cyber norms at a global level. The UN GGE serves as a mechanism to expand and establish an international multilateral framework in the cyber domain through normative discourse and non-binding norms. Today, the UN has held six Working Groups and established the Open-Ended Working Group in December 2018 to continue developing norms, rules and principles of responsible State behavior and to deliberate on ways to implement the possibility of regular institutional dialogue at the international level under the UN's auspices.

3.4. Case study: The United States, Russia, China and Canada's response to cyber norms

To analyze the diffusion of norms from the UN GGE to the international community, a case study focused on the USA, China, Russia, and Canada was carried out to understand the four Nations' positions and diverse conceptions towards norms developed during the GGE's work. A normative discourse analysis was used for conducting this study through the analysis of official documents, national statements, and related articles which served as the primary material of this study strategy. Furthermore, a review of the UN GGE reports was performed to outline the norms that emerged from this arena. This case study aims to answer the following question: How does the international community respond to the proliferation of cyber norms?

The case study discussed below involved the USA, China, Russia, and Canada's perceptions to developments in the GGE. Obstacles to the diffusion of norms at the international level stem from fundamental ideological views and attitudes towards basic freedoms and the openness of the Internet. In the West, cyberspace serves as a tool for spreading and securing the freedom of expression and human rights. However, the free flow of information in cyberspace may be viewed with less enthusiasm in other parts of the world. China and Russia serve as examples where an open cyberspace is considered as a threat to government structures (Henriksen 2019). Additionally, different priorities within the selected states may contribute to their ability to remain passive and uncertain about the adoption of a single strategic priority. In light of the diverse ideological views of the four States selected in this case study, it allowed the researcher to conduct a search of official documents and statements designed to identity the USA, China, Russia and Canada's response to the UN GGE's efforts to normalize rules and principles in cyberspace.

Since the 2012–2013 UN GGE final consensus reports, the application of international law, and in particular the Charter of the UN, in cyberspace "to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment" was agreed between fifteen member states – including the USA, China, Russia and Canada – and served as the main source for regulating state behaviour in cyberspace (UN document A/68/98). It was the first time that global powers had recognized and agreed upon the applicability of international law to State behavior in cyberspace. Furthermore, the report addressed the applicability of human rights and fundamental freedoms set out by the Universal Declaration of Human Rights, and of norms, rules and principles for responsible State behaviour by framing it as "voluntary, non-binding norms" (*Ibid.).* While consensus was reached on the application of international law, norms, rules and principles of responsible behaviour by States, the main problem arises as the GGE failed to provide a clear understanding or agreement on how these norms might apply to cyberspace (Osula, Rõigas 2016, 13).

The debate over the application of norms and international law to cyberspace was furthered during the 2015 GGE. It was aimed at continuing to study the potential threats in the field of information security, to promote a common understanding of norms, rules and principles of responsible State behaviour, and to address how international law applies to the use of information and communication technologies by Nations (UN document A/70/174). The 2015 GGE reached a consensus by participating countries including Russia, USA and China which was able to provide additional references to international law, by reaffirming that it applies to cyberspace following principles of the UN Charter.

The 2015 GGE report provided the first opening to the interested stakeholders in preserving cyberspace for peaceful commitments. However, the positive momentum achieved by the GGEs concealed several problems that manifested in unsettling ways. Firstly, the GGE had turned to become the only arena at the international level for deliberation of universal cybersecurity policy. The GGE was aimed at providing an expert study of a new topic with recommendations which would be taken by the UN GA for action. After the 2012–2015 GGE's that had produced meaningful reports, the wider body had not taken up actions in terms of launching actions for negotiation of multilateral agreement. Secondly, the Group failed to lead cyber powers to reach a general understanding of the concept of cyber operation regarding common security. Since 2011, Russia and China had expressed a concern that information content could characterize a threat to the security at the national level, whereas the Western concept was favorable toward a free flow of information content in the cyber domain. This diversion of concept and fundamental divisions between the USA, Russia and China has been managed through cooperative attitude, but the geopolitical environment had deteriorated in the following GGE.

In the past, China has argued that the application of international humanitarian law to cyberspace would serve as a catalyst to legitimise military activities in response to cyber conflicts (Sukumar, 2017). Also, some member states of the 2014–2015 GGE have stated that the application of the Charter of the UN, particularly the principles on the use of force, and the further application of international humanitarian law would cause the "militarization" of cyberspace (Sukumar, 2017). On the one hand, while the USA wished to further develop how principles of the law of war might constrain cyber conflict, Russia and China viewed USA's propositions as a way to find justifications in international law to exercise countermeasures by utilizing cyber or conventional means in response to a cyber incident (Grigsby 2017, 113). On the other hand, Russia and China wanted to focus their efforts on the prevention of cyber conflicts instead of setting legal rules and norms for conflicts which should not be allowed to occur.

Despite the fruitful emergence and proliferation of norms, the GGE process reached a roadblock in the sessions held between 2016 and 2017 as it failed to reach a consensus. The GGE mandate was to further deliver recommendations on how international law applies to cyberspace. Specifically, the USA wanted the report to provide a clear commendation on the applicability of international humanitarian law, the right to self-defense, and the use of countermeasures (Markoff 2017). Without naming China or Russia, Michele Markoff who led the USA delegation to the GGE, released a statement that some participants of the Group were unwilling to affirm the applicability of international legal rules by stating that "it is premature to make such a determination" and those States are inclined to "walk back" on the progress made in previous GGE consensus reports" (Markoff 2017). On the contrary, the Deputy Secretary of the Security Council of the Russian Federation, has officially stated that Russia and its partners expected that the 2016–2017 UN GGE, would draft a report focusing on rules of responsible State behavior in cyberspace, and the Federation points out that Western Countries blocked the GGE from reaching a consensus and to adopt an outcome (The Ministry… 2017).

The fundamental division toward the applicability of international law to cyberspace among major powers is due to the link between strategy and law which leads to a clash of State's strategic interests and ideological worldviews. The outcome of the deliberation would determine how states can use ICTs to further their foreign policy agenda and political goals. To the USA, the promotion of cyber norms is considered as a way to predict and deter cyber threats, and the reliance on international law in the cyberspace helps the nation to maintain their superior position as a dominant power in the cyber domain and to prevent other state actors to engage in hostile activities (Henriksen 2019, 4). The USA has been consistently against the creation of new legal instruments and advocate for the use of existing legal principles to regulate cyberspace. For China, and to some extent Russia, the unwillingness to affirm the applicability of international law in cyberspace is a way to counter the American dominance in the information age (*Ibid*). Therefore, China, Russia and USA are consistently seeking to promote legal interpretations in which they believe will be suitable for their strategic interests.

Despite the lack of consensus in previous GGE reports, Canada has identified best practices and implemented previously recognized non-binding and voluntary norms of responsible State behaviour endorsed by the UN GA based on the GGE report of 2015. Eleven norms were identified and the most prominent eight of these will be analyzed based on Canada's determination to implement them as follows.

The first norm endorsed by the UN GGE consists of the maintenance of international security, in which States are expected to cooperate in the development and application of measures to increase security and stability in the use of ICTs to prevent harmful threats to international peace and security. In 2010, Canada's government released a cybersecurity strategy to defend its nation against cyber threats. In 2018, a new cybersecurity strategy was published to strengthen the partnership at the national and international level to protect its citizens, to enhance the detection and ability to respond to emerging threats in cyberspace. Furthermore, Canada has supported and recognized the applicability of internal law in cyberspace as well as voluntary norms for responsible State behaviour to counter cyber threats based on the 2013 and 2015 UN GGE reports.

The second norm, related to the State's consideration to relevant information, challenges of attribution in the ICT environment, and the nature of the consequences in case of ICT incidents, has been supported by Canada to implement or enhance their Computer Security Incident Response Teams, which allows for information sharing on cyber-attacks across nations. Canada is working together with the judiciary system of foreign nations to increase the capability to perform cyber investigations. The third norm provides that States should not allow their territory to be used for wrongful acts using ICTs. Canada deems that States have full responsibility to ensure their territories are not used in a way that could potentially harm other States. The nation should work with international organizations such as the Council of Europe and The International Criminal Police Organization to promote legal frameworks for countries against cybercrimes to successfully investigate and prosecute cybercriminals in accordance with international human rights and norms.

The fourth norm consists of how a State should consider cooperation to exchange information, implement measures to address cyber threats, and how to prosecute cybercriminal. Since 2015, Canada has invested over 9 million dollars in cyber capacity building in the Americas (Canada's implementation… 2019) to encourage nations to develop their own cyber capacity building and cyber strategies. Additionally, in May 2019, Canada drafted a resolution on cybercrime with the support of Austria at the 28th session of the UN Commission on Crime Prevention and Criminal Justice to stress the significance of technical assistance in the cyber realm.

The fifth norm stipulates that States should respect Human Rights Council resolutions on the promotion, protection and enjoyment of human rights on the Internet while ensuring the secure use of ICTs as well as guaranteeing full respect of human rights and the freedom of expression enshrined by the GA. Canada's protection of human rights is founded on a framework of responsible and representative government, statute law, common law and independent judiciary and constitutional guarantees stemming from the Universal Declaration of Human Rights (Minister of Justice, 2019). Additionally, Canada believes that the security of ICTs must work together with respect for fundamental freedoms and human rights. The same rights that apply to people while "offline" must also be protected online.

The sixth norm states that a nation should not knowingly conduct or support ICT activity contrary to its obligations endorsed by international law that could potentially damage critical infrastructure. Based on Canada's 2017 Defence Strategy, it indicates that the nation will pursue an assertive posture in the cyber domain by stating that "cyber operations will be subject to all applicable domestic law, international law, and proven checks and balances such as rules of engagement, targeting and collateral damage assessments." (Connolly, Perry, 2017). The seventh norm consists of a State's ability to take suitable measures to protect its own critical infrastructure from cyber threats. Based on Canada's Cyber Security Strategy, a diverse set of measures have been taken to protect the nation's critical infrastructure from cyber threats through cyber education, awareness tools and cyber certification programs, and cyber capacity-building in foreign countries to enhance the knowledge of governments to detect and prevent cyber-attacks and by the development and implementation of information sharing internality (Public Safety Canada, 2018).

The eighth norm encompasses a State's ability to respond to requests of assistance from another State whose infrastructure has been compromised by malicious cyber-attacks. States should also respond to requests to moderate malicious ICT activities aimed at another nation's infrastructure originating from their territory. Canada is actively encouraging information sharing and assistance during cyber incidents as well as being a participant in the intergovernmental Organization for Security and Co-operation in Europe.

Although fundamental divisions between USA, China and Russia's visions of what needs to be regulated in the cyber domain have led to unresolved legal debate, the UN GGE has served and still serves as an arena for global discussions on norms, rules and principles for State behavior in cyberspace. Canada's positive reassertion of the best practices and lessons learned on the implementation of voluntary and non-binding norms endorsed by the UN GA laid out in GGE report of 2015, serves as an illustration of the UN's normative power in the context of the GGE to shape cyber norms and to endorse how things ought to be in the cyber domain.

This case study found that the UN's normative power to promote cyber norms aimed to the regulation of cyberspace is one of the most prominent frameworks that facilitate the cooperation between nations in an attempt to build lasting legal regulations in cyberspace. By testing the Normative Power Europe theory in the context of the UN through the lens of normative discourse, the researcher found out that the Organization's normative power originates from six factors outlined by Ian Manners (Manners 2002, 35): contagion, informational, procedural, transference, overt, and cultural filter which represents the diffusion of norms through a combination of symbolic normative power and substantive normative power. This case study illustrated how difficult it has become for States to liaise on legally binding norms in cyberspace. However, the non-legally binding cyber norms emerged from the UN GGE process has served as a step toward the institutionalization of cyber norms on the international level and it currently is a work in progress, after all, it usually takes considerable effort and time for Nations to reach common agreement on how to regulate and approach means of coercion and new technologies.

CONCLUSION

This research has examined the United Nations normative discourse vis-à-vis the international community, in the context of the United Nations Group of Governmental Experts, to address international cybersecurity discussions. In this final chapter, the results of the analysis will be presented. In the introduction, three research questions were provided, which have guided this investigation. The analysis of the Charter of the United Nations and consensus reports of the UN GGE sought to assess and explain what the normative basis of the United Nations is. By testing the Normative Power Europe theory in the context of the UN through the lens of normative discourse, the researcher found out that the Organization's normative power originates from six factors outlined by Ian Manners (Manners 2002, 35): contagion, informational, procedural, transference, overt, and cultural filter which represents the diffusion of norms through a combination of symbolic normative power and substantive normative power. In addition, an analysis of how norms are diffused from the UN GGE toward the international community was conducted to provide some insight into the United Nations' normative power in the cyber domain.

The research shows that, in the past fifteen years since the establishment of the first UN GGE on developments in the field of Information and Telecommunications in the context of international security, the United Nations has increasingly been exercising normative power. The Organization's founding principles of maintaining world peace and security, fostering international cooperation among nations, serving as a forum for bringing States together to meet the UN's purposes and goals, have served as a normative basis and are deeply rooted in the UN GGE framework, which sought to strengthen the security of global information and telecommunications systems. Since 2004, the GGE has achieved two major accomplishments: firstly, outlining the global cybersecurity agenda and, secondly, introducing the discourse that international law applies to cyberspace.

Although the cyber norms and rules that emerged and proliferated from the UN GGEs' resolutions are non-legally binding and have not yet been fully diffused into the international sphere, the GGE's work has served as a step toward institutionalizing norms. To date, the process of norm diffusion in the context of the UN GGE is a work in progress. In October 2018, the USA proposed the establishment of a new GGE in 2019, in which, 139 member states of the United Nations have voted in favour. Based on this result, one can observe that the discussion of norms and rules in cyberspace is a vital debate in the field of international relations. Furthermore, in December 2018 a second work group "Open-Ended Working Group" mandated by the United Nations General Assembly was established in parallel with the UN GGE which involves academia, business, non-governmental organizations and all interested UN member states to further debate and develop the norms and principles of responsible State behaviour in the context of international security endorsed by the General Assembly.

The case study developed in this paper which involved the USA, China, Russia and Canada's perceptions and responses to the developments in the GGE provided an analysis of the diffusion of norms into the international community. The study found that fundamental divisions among the USA, China and Russia led to unresolved legal debate where the viewpoints of the three nations seem to diverge. The link between strategy and international law applicably to the cyberspace led to a clash of State's strategic interests and ideological worldviews. In contrast to the unresolved debate, Canada has identified some best practices learned from past GGEs and has taken action to implement on the national level previously recognized voluntary norms of responsible State behavior, aiming to serve as an example to other Nations to follow the same path. Although fundamental dilemmas among the States under study were observed, the UN GGE has served and still serves as an inclusive forum for international deliberation on topics related to norms and rules in cyberspace.

Given the findings stated above, it is concluded that the United Nations, in the context of the UN GGE, is a normative power in the cyber domain and plays an important role in outlining the global cybersecurity agenda and shaping cyber norms, all and by introducing and promoting discourse on the applicability of norms, rules, and international law to cyberspace.

LIST OF REFERENCES

Assembly, U.G. (2005). Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. *UN document A/60/202.*

Assembly, U.G. (2010). Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. *UN document A/65/201.*

Assembly, U.G. (2013). Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. *UN document A/68/98.*

Assembly, U.G. (2015). Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. *UN document A/70/174.*

Bauböck, R. (2008). Normative political theory and empirical research. In: P. D. Donatella, Keating. M (Eds.), *Approaches and Methodologies in the Social Sciences: A Pluralist Perspective* (40-60). New York: Cambridge University Press.

Charter of the United Nations and Statute of the International Court of Justice. (1945). Retrieved from https://treaties.un.org/doc/publication/ctc/uncharter.pdf, 01 December 2018.

Council on Foreign Relations. (s.a.). Cyber Operations Tracker. Retrieved from https://www.cfr.org/interactive/cyber-operations, 01 December 2018.

Connolly, A. Perry, D. (2017). Canada to get 'assertive' with cyber missions, commits to major military spending boost. Retrieved from https://www.cgai.ca/inthemediajune72017h, 23 November 2019.

Efrony, D. Shany, Yuval. (2018). A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice. *American Journal of International Law,* 112 (4), (583-657).

Fidler, D. (2018). The UN Secretary-General's call for regulating cyberwar raises more questions than answers. Retrieved from https://www.cfr.org/blog/un-secretary-generals-call-regulating-cyberwar-raises-more-questions-answers, 11 November 2019.

Fourkas, V. (2012). What is cyberspace. Retrieved from http://www.academia.edu/download/32289373/400.pdf, 11 November 2019.

General Assembly. (2018). Resolution adopted by the General Assembly on 5 December 2018. *UN document A/RES/73/27.*

General Assembly. (2019). Open-Ended working group on developments in the field of information and telecommunications in the context of international security. *UN document A/AC.290/2019/1.*

Geneva Internet Platform Digital Watch Observatory. (s.a.). The UN GGE and OEWG. Retrieved from https://dig.watch/processes/un-gge#view-7541-3, 30 November 2019.

Grigsby, A. (2017). The End of Cyber Norms – *Survival: Global Politics and Strategy*, 59(6), pp. 109-122

Henriksen, A. (2019). The end of the road for the UN GGE process: The future regulation of cyberspace. *Journal of Cybersecurity,* 5(1).

Leiner, Barry., Cerf, Vinton., Clark., Kahn, E. (1997). Brief History of the Internet. Retrieved from https://www.internetsociety.org/internet/history-internet/brief-history-internet/, 11 November 2019.

Lewis, J., Vignard, K. (s.a.). Report of the International Security Cyber Issues Workshop Series. Retrieved from http://www.unidir.ch/files/publications/pdfs/report-of-the-international-security-cyber-issues-workshop-series-en-656.pdf, 1 November 2019.

Manners, I. (2002). Normative power Europe: a contradiction in terms? *JCMS: Journal of common market studies*, 40 (2), pp. 235-258.

Manners, I. (2009). The Concept of Normative Power in World Politics. Retrieved from https://pure.diis.dk/ws/files/68745/B09_maj_Concept_Normative_Power_World_Politics.pdf, 29 December 2019.

Markoff. G., M. (2017). Explanation of Position at the Conclusion of the 2016-2017 UN Group Of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security. Accessible: https://s3.amazonaws.com/ceipfiles/pdf/CyberNorms/Multilateral , 01 December 2018.

Minister of Justice. (2019). Canadian Human Rights Act. Retrieved from https://laws-lois.justice.gc.ca/eng/acts/h-6/, 23 November 2019.

Public Safety Canada. (2018). National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age. Retrieved from https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf, 23 November 2019.

The Ministry of Foreign Affairs of the Russian Federation. (2017). Statement by Deputy Secretary of the Security Council of the Russian Federation Oleg Khramov at the Cyber Security Summit (28 June 2017, Tel Aviv, the State of Israel). Retrieved from https://goo.gl/ES9Nmv, 02 December 2018.

Osula, A.M, Rõigas, H. (2016). International Cyber Norms: Legal, Policy & Industry Perspectives. Tallinn: NATO CCD COE Publications.

Pietrzyk-Reeves, D. (2017). Normative Political Theory. *Teoria Polityki,* 1, pp. 173-185.

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

Sills, J. (2002). The Role of the United Nations in Forming Global Norms. *Academic Council on the United Nations System.* No 2. Connecticut: Yale University.

Sukumar, M.A. (2017). The UN GGE Failed. Is International Law in Cyberspace Doomed As Well? Retrieved from https://www.lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well, 02 December 2019.

The NATO Cooperative Cyber Defence Centre of Excellence. (s.a.) Tallinn Manual 2.0: *The most comprehensive guide for policy advisors and legal experts on how existing International Law applies to cyber operations.* Retrieved from https://ccdcoe.org/research/tallinn-manual/, 27 December 2019.

Tikk, E., Kerttunen, M. (2017). The Alleged Demise of the UN GGE: An Autopsy and Eulogy. Retrieved from https://cpi.ee/wp-content/uploads/2017/12/2017-Tikk-Kerttunen-Demise-of-the-UN-GGE-2017-12-17-ET.pdf, 11 November 2019.

United Nations Office for Disarmament Affairs. (2015). Fact Sheet – Developments in the field of information and telecommunications in the context of international security. Retrieved from https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2015/07/Information-Security-Fact-Sheet-July2015.pdf, 11 November 2019.

United Nations. (2018). First Committee Approves 27 Texts, Including 2 Proposing New Groups to Develop Rules for States on Responsible Cyberspace Conduct. Retrieved from https://www.un.org/press/en/2018/gadis3619.doc.htm, 01 December 2019.

United Nations Secretary-General. Secretary-General's address at the Opening Ceremony of the Munich Security Conference [as delivered]. Retrieved from https://www.un.org/sg/en/content/sg/statement/2018-02-16/secretary-general%E2%80%99s-address-opening-ceremony-munich-security, 01 December 2019.

United Nations. (2019). Canada's implementation of the 2015 GGE norms. Retrieved from https://www.un.org/disarmament/wp-content/uploads/2019/11/canada-implementation-2015-gge-norms-nov-16-en.pdf, 23 November 2019.

APPENDICES

Appendix 1. Non-exclusive licence

A non-exclusive licence for granting public access to and reproducing the graduation thesis[1]:

I ……Priscila da Silva Leopoldino…………..(*author's name*)(*date of birth*……13/07/1993…)

1. Give Tallinn University of Technology a free of charge permission (non-exclusive licence) to use my creation

International Cyber Norms: The United Nations as a Normative Power,

(*title of the graduation thesis*)

Supervised by Holger Mölder,

(*name of the supervisor*)

1.1. to reproduce with the purpose of keeping and publishing electronically, including for the purpose of supplementing the digital collection of TUT library until the copyright expires;

1.2. to make available to the public through the web environment of Tallinn University of Technology, including through the digital collection of TUT library until the copyright expires.

2. I am aware that the author will also retain the rights provided in Section 1.

3. I confirm that by granting the non-exclusive licence no infringement is committed of the third persons' intellectual property rights or the rights arising from the personal data protection act and other legislation.

[1] *The non-exclusive licence is not valid during the access restriction period with the exception of the right of the university to reproduce the graduation thesis only for the purposes of preservation.*