Department of Political Science

MA in International Relations

Major in Global Studies

Double Degree Program with MGIMO University

Chair of Geopolitical Scenarios and Political Risk

Perspective trends of international cooperation in the field of cybersecurity

Supervisor

Prof. Gen. S.A. Carlo Magrassi
Prof. Elena Zinovieva

Candidate

Arianna Manili
634812

Co-Supervisor

Prof. Pietro Falletta

Academic year 2018/2019

Acknowledgements

Multilateralism and International Security have been fueling my curiosity for many years and now those two interests have been merged and framed in this thesis. My experiences abroad and my studies at home have enabled me to work on the topic of cybersecurity from a cooperative and comparative perspective, auspicating for a future where technology will only bear the function of bettering human life. Disserting on this topic has been a hard task, but my intention of showing all the sides of the story has motivated me to bringing into analysis all the different perspectives which characterize cyber international relations.

First of all, I would like to warmly thank my supervisors Professor Gen. Carlo Magrassi from LUISS University and Prof. Elena Zinovieva from MGIMO University for giving me the chance to implement and further expand my knowledge on the topic. Also, I would like to sincerely thank Doctor Simone Pasquazzi for providing essential support throughout the drafting process. Finally, Professor Pietro Falletta for having co-supervised this work.

I would like as well to thank the inspiring people I met throughout my University years all around the world. In particular, Ambassador Zappia, Dr. Ragnoni and Dr. Lobefaro, from the Permanent Mission of Italy to the United Nations, and Min. Cutillo, Cons. Bazzani, Dr. Di Nicola and Dr. Latini, from the Ministry of Foreign Affairs and International Cooperation, for letting me in the world of Italian and International diplomacy and multilateralism. Their priceless words and teachings will definitely guide me as a lighthouses in future experiences.

A lifetime would not be enough for thanking my family, Mum, Dad and Ale, for relentlessly supporting me at home and all around the world. They have constantly worked for gifting me the best future I could ever have and those three heartedly lines will never express enough gratitude to them.

I thank all my friends for having been there even when I was miles and miles away. I thank those friends who shared experiences with me and supported me in difficulties at home and abroad. I thank those friends that no matter the distance and the not-very-frequent visiting trips have always been solid rocks to me.

I thank Russia for letting me down many times and teaching me to never give up, even with -25° outside.

“The Internet is the first thing that humanity has built that humanity doesn’t understand, the largest experiment in anarchy that we have ever had.”

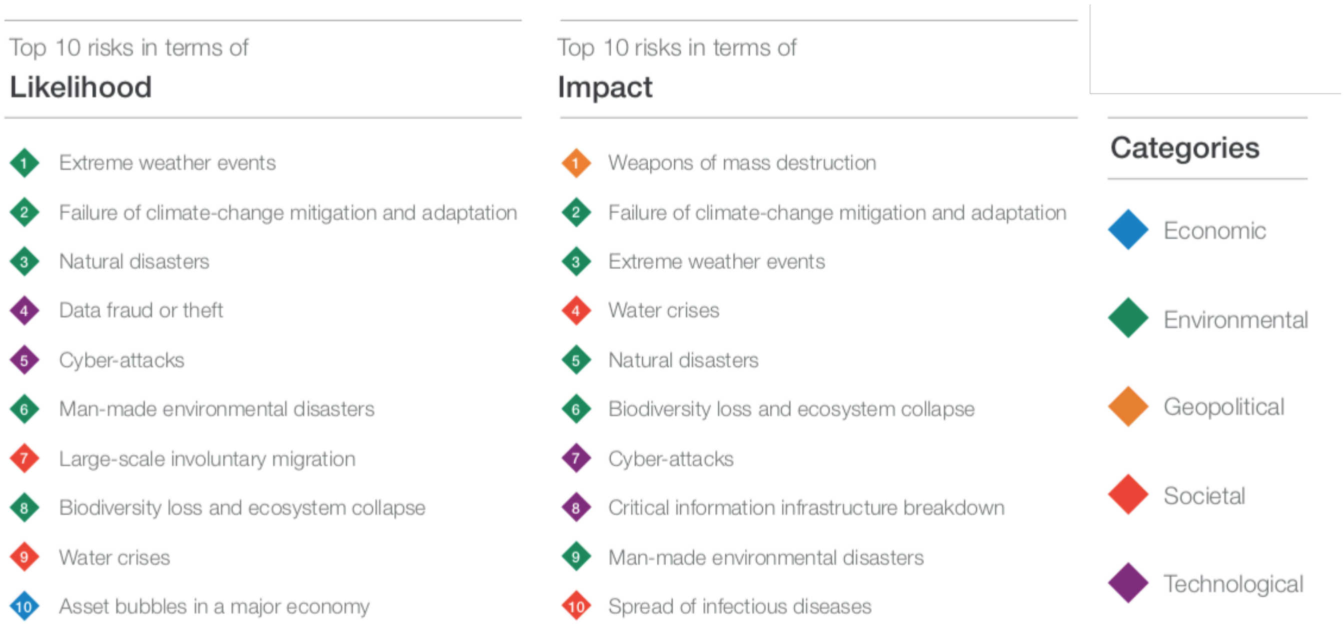
Eric Schmidt,
Google CEO from 2001 to 2011, said this in a 1997 programmers conference
in San Francisco, USA.

Table of contents

Introduction

The 21st century has been experiencing a rising number of new cyber threats that governments cannot face on their own by means of traditional tools. Technology has played one of the most important role in reshaping social interactions and progress over few generations, determining as well important implications for security. As displayed in the image below, according to the assessment of the World Economic Forum, cyber-attacks are among the five most likely dangers that may occur this year and among the ten risks in terms of impact, along with data fraud or theft and critical information infrastructure breakdown.[1]

Figure 1: The Global Risks Landscape 2019[2]



	Top 10 risks in terms of Likelihood		Top 10 risks in terms of Impact
1	Extreme weather events	1	Weapons of mass destruction
2	Failure of climate-change mitigation and adaptation	2	Failure of climate-change mitigation and adaptation
3	Natural disasters	3	Extreme weather events
4	Data fraud or theft	4	Water crises
5	Cyber-attacks	5	Natural disasters
6	Man-made environmental disasters	6	Biodiversity loss and ecosystem collapse
7	Large-scale involuntary migration	7	Cyber-attacks
8	Biodiversity loss and ecosystem collapse	8	Critical information infrastructure breakdown
9	Water crises	9	Man-made environmental disasters
10	Asset bubbles in a major economy	10	Spread of infectious diseases

Categories

- ◆ Economic
- ◆ Environmental
- ◆ Geopolitical
- ◆ Societal
- ◆ Technological

Cyber operations are constantly happening, either people realize it or not, and affect directly or indirectly our everyday life, causing huge negative impact and monetary damages. Massive thefts of intellectual property, large disruption of critical infrastructure, degrading national security capabilities are only some of the examples of events frequently discussed by media, policy-makers and cyber insiders. Shared awareness on the fact that the "attack surface" for cyber operations is incrementing because of the positive trend of technological diffusions and improvement brings the understanding that there are no safe neighbourhoods where we can be devoid of cyber threats. As a

[1] World Economic Forum, The Global Risks Report 2019, 14th Edition, Geneva, 2019. Available at: http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

[2] World Economic Forum, The Global Risks Report 2019 14th Edition, Geneva, 2019.

matter of fact, no single area is completely bereft of technology and those Countries who are highly reliant on technology appear to be the most vulnerable.

In the light of this uncertain scenario, this work takes into consideration which are the threats that arises in the cyber domain and how those affect the current scheme of relations between States. We came to an age where high-impact and low-profile cyber incidents are becoming the "new normal". Therefore, Countries have come to intensify the efforts for reducing the risk of cyberconflicts throughout different processes, such as relying on confidence-building measures or deterring behaviour at State level. Despite Countries' commitment to stabilize the overall dimension of cyber-international relations, we are currently experiencing a severe deterioration of conditions for security which do not only harm specific environments but also individuals' everyday lives. Moreover, there is a thriving sense of unease about the escalatory potential of cyberconflict that is mainly fuelled by the awareness that more States are equipping themselves with technology to achieve strategic goals.

Overall, these events advance questions on the capacity of States to pursue the goal of cooperation in cyberspace. Therefore, the relevancy of this work stands on the intent to provide an explanation for the shortcomings of cooperation in the field by demonstrating both with theory and practice that there are hurdlers originating from the technical aspects of cybersecurity and barriers deriving from the different perceptions States have developed on the matter. Inevitably, those two aspects strongly influence Countries' foreign policy and generate consequence at the international, regional and bilateral levels. In conclusion, the work aims to answering the following question: *in which way the technical difficulties arising from cyberspace and the different perceptions of States that define their national strategies shape the current and future patterns of cooperation in the field of cybersecurity*?

Methodology and Literature Review

The research encompasses a comprehensive and extensive literature:

1. *Literature on the theories of International Relations: Realism, Liberalism and Constructivism.*

The theories of International Relations constitute the starting point of the research as they provide the tools for analyzing the reasons behind States' behavior. The choice fell particularly on Realism and Liberalism, which represent classical theories of IR and provide two different keys for interpreting the current interactions in cyberspace. The environment in which States operate, as described by John

Mearsheimer (1994)[3], is anarchic and seems, at first sight and in conjunction with the security dilemma, to be applicable to the setting in which cyber interactions takes place. Realism has been employed as well for providing a general framework of analysis involving the objects of actors, power and structure, which is applied within the process of understanding the features of cyberspace. For what concerns Liberalism, this theory becomes a useful device for recognizing the plethora of actors performing in cyberspace and for understanding whether in the field of cybersecurity the collective security principle, in its traditional formulation, could be applied. I decided to employ as well the Constructivist theory as a supportive tool to understand the reasons for which Countries have different perceptions on the same matter. Based on the arguments of Alexander Wendt delivered in "Social Theory of International Politics" (1999), the work argues that, contrary to the Realist theory, Countries' behavior is based on ideas and culture, and not on natural instincts, while material constraints become secondary. Therefore, because Countries have dissimilar cultures and backgrounds, they as well develop different perceptions of threats and security.

2. *Literature on cybersecurity.*

In order to provide an assessment of the features of cybersecurity, I tried to collect literature that could explain how the new cyber domain practices have changed the standards promoted by classical theories. The foundation to such critical approach consisted in Martin Libicki's article "Cyberspace Is Not a Warfighting Domain" (2012), which argues that there are some relevant intrinsic differences that cyberspace has in comparison to the other domains. On the basis of Singer and Friedman's (2014)[4] researches, I explain the basic principles that characterize the cyber domain: the terms of physicality, temporality, permeation, fluidity, participation, attribution, accountability are put under scrutiny. I refer, as well, to the principle of power diffusion promoted by Joseph Nye in "The Future of Power" (2011) and to the cybersecurity dilemma elaborated by Ben Buchanan in his book "The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations" (2017). Finally, Nye's article "Deterrence and Dissuasion in Cyberspace" (2017) and Libicki's "Expectations of Cyber Deterrence" (2018) have provided the tools for understanding the relation between offense and defense as applied to the case of cyberspace. Additional clarification of specific features of cyber operations and instruments is provided in the Information Security Glossary, which is mainly conceived accordingly to the definitions offered by the Tallinn Manual.

3. *Official Documents on national strategies of Russia, China, the United States and Italy.*

[3] Mearsheimer, JJ, The False Promise of International Institutions, The MIT Press, International Security, 19(3), p. 5–49, 1994.

[4] Singer, P. W., & Friedman, A., Cybersecurity and cyberwar: What everyone needs to know. Oxford: Oxford University Press, 2014.

The analysis of national strategies heavily relies on government official sources, as they represent the recognized positions of States on the matter of cybersecurity. Those types of documentation are instructive as they evidently depict a specific point of view and the official discourse that shapes each State foreign policy. In particular the documents taken into account are the following: National Security Strategy published (September 2000), Foreign Policy Concept of the Russian Federation (November 2016) and Official document of the Russian Federation on the Doctrine of Information Security (December 2016) for Russia; National Cybersecurity Strategy (2016) and Cybersecurity Law (2017) for China; 2018 National Defense Strategy of the United States of America, Presidential Executive Order "Cybersecurity for the Nation" (2017) and Task Force on Cyber Deterrence (2017) for the United States of America; 2017 Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica and 2018 Relazione Sulla Politica Dell'Informazione by the Presidency of the Council of Ministers for Italy.

4. *Document review of International and Regional organizations.*

A substantive part of this work is built on official documents and reports issued by international and regional organizations and institutions. For what concerns data, I mainly relied on the 2018 Annual Progress Report published by the International Telecommunication Union and the 2018 Annual Progress Report by the World Economic Forum. For what concern the analysis of the main trends of cooperation, I critically engaged with both official records of entities such as the United Nations, the European Union, the North Atlantic Treaty Organization and the Shanghai Cooperation Organization, as well as commentaries by experts published on Center For Security Studies (CSS) ETH Zürich, Berkeley Journal of International Law, Georgetown Journal of International Law, Russian International Affairs Council (RIAC) and Valdai Discussion Club, among others.

The structure of this work is aimed at exploring the ways in which States, as the main subjects of the analysis, adopt strategies to tackle the threats to cybersecurity and at identifying the achievements and shortcomings of cooperation in the field.

Specifically, the *goals* of the research are:

- to study the shortcomings of classical IR theories in their application to the cyber domain;
- to analyse the main features of cyberspace and related definitions;
- to research on the national strategies adopted by Russia, China and the United States, as well as by Italy in the EU-NATO framework;
- to understand the current trends of cooperation by means of comparing experiences at the international, regional and bilateral level;

- to provide recommendations to researchers and policy makers that could offer valuable and plausible solution for tackling the threats and the risks originating from cyberattacks and for creating a global security regime dedicated to cyberspace.

The *object* of this research is to evaluate the accomplishments and the low performances of cooperation in the cyberspace framework.

The *subject* of this research consists in comparing the different national strategies' and plan for cybersecurity of Russia, China, the United States and Italy, and their intention of cooperation in the field.

The *relevancy* of this research is given by the fact that cyber strategies have come of age and can produce detrimental impacts. Major powers currently employ cyber strategies to gain a position of advantage relatively to their rivals, while small States and non-State actors attempt to use cyber operations to punch above their weight to maximize their potential goals.[5] The double employment of cyber tools is evident as it offers incredible instruments for human development while, at the same time, it threatens the lives of private citizens. Therefore, the topic is consistent with one of major trend in the ongoing security debate.

The *practical importance* of this work is to understand how national perceptions and technological features are shaping the current pattern of cooperation in cybersecurity. Therefore, the conclusions of this research are instructive in order to forecast perspective trends of cooperation in the field.

The main objective of this work is to convey an exploratory research to investigate the main aspects of a relatively-new researched topic and expand the scientific understanding on the matter of cyber security and international cooperation. In order to accomplish such aim, a descriptive and comparative approach to investigate the features of cyber-international relations and the possible perspective scenarios on the future cyber order has been performed. The investigation consists in the application of mixed methods of analysis which mainly includes comparative, qualitative and descriptive research. A deductive approach is used throughout the whole text and is applied for testing the most diffused theories of International Relations on issues related to the cyber domain. In particular, the Realist, Liberal and Constructivist theories will be presented and then reconsidered on the basis of the characteristics presented by the fifth domain. Secondly, the design is comparative as it sets the tone for confronting the cyber postures of three selected Countries – the United States, the Russian Federation and People's Republic of China – by means of studying their official national strategies. Those three Countries have been selected under the principle of being the most active and

[5] Valeriano B., Jensen, B., & Maness R., Cyber Strategy: The Evolving Character of Power and Coercion, New York: Oxford University Press, 2018, p.1-2.

prepared in the field of cyberwarfare[6], and because they represent as well models of behavior for several other Countries. Finally, qualitative methods of analysis of official documents are exploited in order to understand concepts, postures and opinions and to gather in-depth insights on topics which are complex and require further research.

The *hypothesis* of the research is the following: the current status of cooperation in the field of cybersecurity is determined by mistrust and misperceptions of States' intentions.
To investigate on this hypothesis, the work is divided into three main parts: Part One – Theory and Methodology of the research; Part Two – Major Cyber Rivals: towards cooperation or self-help?; Part Three – Perspective trends of cyber collaboration.

The first part of the work is committed to setting the conceptual framework of the analysis which is based on the understanding of the three main theories of International Relations, namely Realism, Liberalism and Constructivism. In practice, the author intends to develop the discussion on the themes of Security Dilemma and Collective Security by applying them on the matter of cybersecurity. What emerges by this first theoretical enquiry is that both paradigms are in some terms modified. In particular, the terms of physicality, temporality, permeation, fluidity, participation, attribution, accountability are put under scrutiny. Physicality is changing because of the unmarked boundaries of the cyber domain and temporality is modified both in the case of issuing an attack and detecting the same attack, which may take a diluted and countless amount of time. Permeation is increasingly evident due to the transcending character of technology, which involves each and other aspect of everyday life. The difficulties related to the process of detection of cyber-attacks raises problems of attribution of the operation, further complicating the terms required for implementing accountability standards. The concept of power becomes fluid and affects the structure of the international system applied to the cyber domain. Finally, participation is substantially enlarged thanks to the increasing availability of cyber tools worldwide. The Constructivist theory serves as a tool for understanding the different perceptions States have of the adversaries and how this influence their behaviour on the international stage.

In the second chapter, the work aims to provide a more practical approach to the question by putting under investigation the main strategies adopted by a set of selected Countries, which are protagonists in the discussion of current relations in the cyberspace. Indeed, in the course of a

[6] Cyber Warfare Infographics, Valdai Discussion Club, 27.08.2019, available at: http://valdaiclub.com/multimedia/infographics/cyber-warfare/

comparative analysis of the national strategies of the Russian Federation, People's Republic of China, the United States, some consideration are expressed with regards to the main divergent and colliding postures and technicalities that makes cybersecurity something difficult to agree upon. What emerges is that cooperation in the cyber domain develops at a slow peace not only because it is a rather new field of study but mainly because there are some technical and relational aspects that need to be addressed and overcome before the instrument of international law may be called to regulate international relations in the cyber domain.

The third part of this work is dedicated more specifically to the current status of cyber collaboration and its future trends. An assessment of the current role of International Institutions in guaranteeing a more secure Internet worldwide is provided. The duality in their scope of action is based on what follows. On one side, they are asked to regulate the use of cyber tools to guarantee a certain level of cybersecurity worldwide. On the other side, however, they are demanded to guarantee the benefits of a worldwide open access of the Internet to be respected. Such double perspective has been at the centre of discussion in several fora, such as the International Telecommunication Union (ITU) and the United Nations (UN). A further question, which is frequently addressed in international debates is the future shape of global governance on the matter of cyber collaboration and whether a cybersecurity treaty should be conceived. Among the examples of cooperation, a general display on how the public-private partnership's role is contributing to the betterment of security conditions for companies and individuals is provided. Three further cases of cooperation are addressed: the International ICT-security at the United Nations, the Tallinn Manual and the EU-NATO partnership with a country-focus on Italy. For what concern the United Nations efforts in setting the international agenda, the mandates of the Groups of Governmental Experts (UN GGEs) on Developments in the Field of Information and Telecommunications in the Context of International Security and the Open-Ended Working Group (OEWG) are discussed and compared, raising questions on their complementarity.

With regards to the example of the Tallinn Manual, the work intends to disclose the ways in which the known international laws regulating the most classical conflicts could be applied to the context of cyber operations and cyber warfare, trying to bridge the gap between old international laws and new technologies in the most comprehensive and authoritative way. Because the Manual represents an academic research, and not a piece of international law, the Tallinn Manual has been questioned in its role and significance.

A further section of the work focuses on the topic of regional cooperation by exploring the actions undertaken by the European Union – in coordination with NATO – in the field of cybersecurity and the specific features concerning the current status of affairs with regards to the strategic plan implemented by the Italian government, both at European and North-Atlantic level. The description of the Italian national strategy will serve as a demonstration of how every single Country can amplify its cyber expertise and resiliency from participating in regional initiatives aimed at developing effective mechanisms to achieve cyber readiness, while pursuing its double goal of protecting individuals and state infrastructure.

Finally, a critical investigation will be carried on the chances of cooperation and governance at an international level over the domain, by presenting and studying the possible future scenarios formulated by the researcher Jason Healey, which are Status Quo, Domain, Balkanization, Cybergeddon and Paradise.

The conclusion will summarize the main findings of the enquiry, acknowledging that this is a complex and not exhaustive research on the topic, designed to supplement with further material the already existing literature. Being a rather new topic, many researchers will dedicate in the future their effort to organize and better understand such complex reality within the International Relations field. Finally, some recommendations will be advanced with regards to the necessary steps to undertake in the short-term, that, in the long-term, could turn into the regimentation of cyberspace.

An Information Security Glossary

In this section of my work, I would like to create a non-exhaustive but relevant short list of terms which are recurrent throughout the text, that can facilitate the reader's understanding of the work. Those definitions are taken from the Tallinn Manual 2.0 on the International Law Applicable to Cyber operations, 2017, Oxford University Press.

- **Active Cyber Defense**: "The taking of proactive defensive measures outside the defended cyber infrastructure".[7]
- **Cloud Computing**: "A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (such as networks, servers, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing allows for efficient pooling of computer resources and the ability to scale resource to demand".[8]
- **Computer Emergency Response Team (CERT)**: "A team that provides initial emergency response aid and triage services to the victims or potential victims of 'cyber operations' […] or cyber crimes, usually in a manner that involves coordination between private sector and government entities. These teams also maintain situational awareness about malicious cyber activities and new developments in the design and use of 'malware' […], providing defenders of computer networks with advice on how to address security threats and vulnerabilities associated with those activities and malware".[9]
- **Computer Network**: "An infrastructure of interconnected devices or nodes that enables the exchange of data. The data exchange medium may be wired (e.g., Ethernet over twisted pair, fibre-optic, etc.), wireless (e.g., Wi-Fi, Bluetooth), or a combination of the two".[10]
- **Critical Infrastructure**: "Physical or virtual systems and assets of a State that are so vital that their incapacitation or destruction may debilitate a State's security, economy, public health or safety, or the environment".[11]
- **Cyber Infrastructure**: "The communications, storage, and computing devices upon which information systems are built and operate".[12]

[7] Schmitt, M., Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press, 2017.

[8] Ibidem.

[9] Ibidem.

[10] Ibidem.

[11] Ibidem.

[12] Ibidem.

- **Cyber Operation**: “The employment of cyber capabilities to achieve objectives in or through cyberspace”.[13]
- **Cyberspace**: “The environment formed by physical and non-physical components to store, modify, and exchange data using computer networks”.[14]
- **Data**: “The basic element that can be processed or produced by a computer to convey information. The fundamental digital data measurement is a byte”.[15]
- **Denial of Service (DoS)**: “The non-availability of computer system resources to their users. A denial of service can result from a ‘cyber operation’”.[16]
- **Firewall**: “A defensive technology designed to keep the bad guys out. Firewalls can be hardware or software-based”.[17]
- **Hacktivist**: “A private citizen who on his or her own initiative engages in hacking for, inter alia, ideological, political, religious, or patriotic reasons”.[18]
- **IP**: “A protocol for addressing hosts and routing datagrams (i.e., packets) from a source host to the destination host across one or more IP networks”.[19]
- **Malware**: “‘Software’ (see below) that may be stored and executed in other soft-ware, firmware, or hardware that is designed adversely to affect the performance of a computer system. Examples of malware include Trojan horses, ‘rootkits’, ‘viruses’ and ‘worms’”.[20]
- **Passive Cyber Defence**: “The taking of measures for detecting and mitigating cyber intrusions and the effects of cyber operations that does not involve launching a preventive, pre-emptive, or counter-operation against the source. Examples of passive cyber defence measures are firewalls, patches, anti-virus software, and digital forensics tools”.[21]
- **Software**: “The non-physical components of a computer system and cyber infrastructure. These components encompass programs, including operating systems, applications, and related configuration and run-time data”.[22]

[13] Ibidem.
[14] Ibidem.
[15] Ibidem.
[16] Ibidem.
[17] https://www.cybintsolutions.com/16-cyber-security-terms-that-you-should-know/
[18] Ibidem.
[19] Ibidem.
[20] Ibidem.
[21] Ibidem.
[22] Ibidem.

- **Virus**: “A type of ‘malware’ […] with self-replicating capability that attaches itself to an application program or other executable system component and leaves no obvious signs of its presence”.[23]

[23] Ibidem.

Part One – Theory and methodology of the research

1.1 Classical theories of International Relations

1.1.1 Realism and the Security Dilemma

To better appreciate the context in which Countries are dealing with issues concerning the threats to cybersecurity, a first look should be given to the different lenses according to which scholars and researchers investigate and interpret States' perceptions and interactions. In particular, this first section of the work will concentrate on the ways in which the interplay between States takes place, on which terms and by which tools. By engaging with theory, it will be assessed and defined the possible ways in which States operate in the field of cybersecurity, whether they intend to adopt a cooperative approach and the possible difficulties in its realization. The key source to study States' behavior within the international system is the study of International Relations (IR) and its theories.

The aim of IR theory is to study the interactions between States in terms of power and, therefore, to analyze a variety of aspects related to the conditions of war and peace. Scholars have developed and studied several theories in order to organize a coherent study on the subject offering different levels of analysis and considering different actors in the international arena. Therefore, the object of the study in the field of IR touches several domains and not strictly the military one. This means that the cultural, the economic, the political and many others aspects are taken into account as variables of behavior.

Among the different paradigms offered by the planet of IR theories, Realism, Liberalism and Constructivism as main approaches, have been selected as the most studied and pertinent to the topic of this thesis. In the first section Realism will be presented, while the next two sections will cover the theory of Liberalism and Constructivism. There are several reasons according to which Realism is relevant to the analysis of this topic. First of all, because cybersecurity is a security issue that very often seems to apply to a realist approach, especially when it comes to discuss the controversies arising from the security dilemma and the mistrust between States. Secondly, it is so because when analyzing the strategies of States, realist reasoning seems to prevail over the one of cooperation. Nevertheless, the topic of cybersecurity is still very much ongoing in its study process and, thus, it is actually difficult to cluster it into a single box. Additionally, because there is much uncertainty over the topic of cybersecurity, theories of the field are not complete and scholars always try to call attention to the objective difficulties of studying this new topic.

Realism is the ultimate paradigm for understanding and handling inter-State relations and, despite presenting different declinations of this theory, places the concept of power at the core of the theory. Realism, according to John Mearsheimer, is based upon four main assumptions: first, the most important actors in the international system are States; second, the State is a unitary actor; third, the State is a rational actor; fourth, security is the ultimate goal of international relations.[24]

The first assumption establishes as a unit of analysis the State, bringing the focus on a State-centric approach. The Westphalian State recognized by Realist scholars is built upon the principles of national sovereignty and political independence.[25] Those elements constitute the principle of national security, along with the idea of the "preservation of the State's territorial integrity and the physical safety of its inhabitants"[26]. The principle of non-intervention is of paramount importance, however can be, in very specific circumstances, effete for reasons of humanitarian intervention, conceived as coercive intervention in the internal affairs of a State to prevent large-scale human rights violations, such as genocide or ethnic cleansing.

In the absence of a designated global government, the International System (IS) is characterized by anarchy, and international security can only be achieved through the balance of power among States. Such anarchy is characterized by States acting in their own interest of self-help: as independent political units, they are concerned with their own survival, to defend their national sovereignty, and with national interest. Therefore, an important form of self-defense is retaliation. Secondly, despite the internal differences a Country may have, it will speak univocally in is foreign policy posture. Thus, the separation between foreign and internal policy is fundamental. Thirdly, the State is a rational actor and, throughout the decisional process of foreign policy, it rationally defines national interests through a cost-benefit evaluation in order to maximize the benefits. Fourthly, given that the ultimate aim of a State is to maximize national interest in a condition of anarchy, the international agenda is dominated by issues of security.

Conflict can be either present or possible and consequently force is the tool for resolving controversies or for preventing the violation of national sovereignty. Therefore, the concept of power is central to the realist doctrine, as politics always embodies the fight for power – also referred as *power politics* – and is based on power relations.[27]

The concept of power, albeit central in the study of IR, has been long under discussion. Despite different definitions offered by several scholars on the matter, there are mainly two ways

[24] Mearsheimer, JJ, The False Promise of International Institutions, The MIT Press, International Security, 19(3), p. 5–49, 1994.

[25] Mearsheimer, JJ, The False Promise of International Institutions, The MIT Press, International Security, 19(3), p. 5–49, 1994.

[26] Walt, S.M. (1991) The Renaissance of Security Studies. International Studies Quarterly 35 (2), 211–39.

[27] Mazzei F., Marchetti R., Petito F., Manuale di Politica Internazionale, Egea, 2010, p. 33-35.

according to which it is possible to provide an accurate and comprehensive description of it. Appreciating the definition of Kenneth Waltz of power as *influence*, we must consider it both the capacity of A to influence B through a differentiated range of tools or the relation based on the power that one actor is able to exert on another over a specific domain. Moreover, power can be either "hard", usually coercive and represented by the application of military or economic force, or "soft", usually non-coercive and applied through the means of appeal and attraction.[28]

One of the most important debate in this frame deals with the following question: *is international anarchy pushing States to maximize security or power?* The answer to this question have originated two opposite views. On one side, there is defensive realism, supported by Kenneth Waltz and Joseph Grieco, according to which States are defensive actors and, thus, consider survival as the ultimate aim of their actions. On the other side, we find offensive realism, argued by John Mearsheimer, which claims that States are power maximizer and pursue the ultimate aim of occupying an hegemonic position within the international system.[29]

Anyways, such competitive behavior among States increase the possibilities of fueling the security dilemma, concept which is central to the theory of defensive realism. Such condition can be verified when the military forces that are deployed by a State to augment its security can also be used for attacking a potential adversary. Consequently, the opponent has less capacity to defend itself and feels less secure. It is so because there is a lack of knowledge about the adversary type, namely whether it is a security-seeking State or a greedy State. Such status of uncertainty pushes States to arms races in order to be sure to be able to defend themselves and, thus, influences pressure for competition and augmenting mistrust, while eroding any chance of cooperation.

In practice, there are three steps that characterize this interaction among States. Firstly, to respond to a State's acquisition of new military capabilities, the adversary could respond by building up its own forces with the aim of increasing its security. At this point, because they both feel more insecure, the first State could perceive its opponent as a greedy State and this can call for more competitive policies. Moreover, because a State assess that its adversary is greedy, then cooperation becomes more risky, making competitive policies more attractive. Those interactions lead to a continuing negative spiral of deteriorating political relations, with possibly no end until reaching the status of war.[30]

Given this framework, for Realists, it appears that the space reserved for international cooperation remains quite limited. Specifically, there should be three conditions to be met according

[28] Mazzei F., Marchetti R., Petito F., Manuale di Politica Internazionale, Egea, 2010, p. 33-35.
[29] Collins, A., Contemporary Security Studies. Oxford: Oxford University Press, 2015, p. 19-20.
[30] Collins, A., Contemporary Security Studies. Oxford: Oxford University Press, 2015, pp. 21-23.

to which an international organization could actually govern the world in an impartial way. First of all, it should have sufficient power to deter any kind of aggression. Secondly, it should be based on a shared concept of collective security and of international law. Finally, it should pursue a genuine interest in subordinating its very own political interest to general well-being and international security.

However, because those conditions in practice are hardly met, the effectiveness of international mechanisms of justice is strongly questioned. In conclusion, the Realist path toward security is composed by the following steps: the increase of its own military arsenal, the creation of alliances through diplomacy and, finally, the negotiations aimed at the establishment of arms control treaties in order to consolidate an advantageous position.[31]

1.1.2 Liberalism and Collective Security

While Realist family theories provide a more pessimistic approach towards cooperation, Liberalism tends to offer a much more positive view about improving cooperation in the field of international politics. Indeed, the presentation of Liberalism offers an overview on the possible basis of building up cooperation in the cyber domain.

Generally, Liberalism describes international politics as evolving, becoming more imbued with interdependence, cooperation, peace and security. In this framework, emphasis is not given only to the State itself, on the anarchy of the international system and on the principle of self-help, but on individuals, on institutions and on the activities of Intergovernmental Organizations (IGOs), Non-Governmental Organizations (NGOs), major private economic entities and international regimes.

Such approach is defined as multi-centric, and it is so even within the border of a State that daily deals with its pluralist soul. Indeed, contrary to the Realist idea for which decisions concerning foreign policy are rational, for Liberals those decisions are the result of clashes, negotiations, compromises, alliances between the different actors involved in the decision-making process.

This family of theories depicts States' behavior as mainly the result of the perceptions, preferences and decisions of the elites, which are often related to the nature of each States' political system. Therefore, the character of international politics can change depending on the nature of its members, their objectives and their decisions on what to do and how to interact. While the Realist conceptualization of the rational coincides with the maximization of national interests in the short-term period, Liberals believe that States act rationally by looking at the well-being of the community

[31] Mazzei F., Marchetti R., Petito F., Manuale di Politica Internazionale, Egea, 2010, pp. 49-50.

in a long-term perspective. Therefore, the rationality of the Liberals places emphasis on collaboration rather than on conflict.[32]

Liberalism is a theory that strongly supports democracy, the principle of private property and free enterprise, widespread international interactions and cooperation. The expected benefits that come with the diffusion of those principles include greater cooperation and less conflict, given a highly interconnected globe which sees cooperation in several domains outpacing reasons for and achievements far from war.

One of the most important application of Liberal theories on the theme of international security is the concept of collective security, which is traditionally discussed by the scholar Inis L. Claude. This concept consist in the formation of a big alliance of the major international actors in order to jointly counteract the aggression of one State to another. It is possible to realize collective security on the general principles of the indivisibility of peace and of diffused reciprocity. The fundamental assumption is that conflict can be avoided due to the underlying harmony of interest among states which enables reconciliation. The principle of collective security is put into place with the aim of guaranteeing a more stable world for the whole international community. Collective Security is made of three elements: 1. identification of an agreed procedure (usually a treaty) for regulating the decisions of the international community; 2. renunciation of war as an instrument of policy, with the exception of self-defense; 3. formation of an international alliance against the aggressor. The main idea behind this three rules, is to render the aggression fruitless in order to punish violations and deter future wars.[33]

Liberal scholars are, indeed, offering a different solution to the problem arising from the security dilemma, and therefore believe that it is not through self-help or balance of power that such dilemma is resolved but through cooperation and collective efforts. Finally, in order to make sure that collective security is successful, two prerequisites are required: first, that all members respect the commitment to jointly oppose the possible aggressor, and secondly, that there must be a significant number of members to agree in identifying the aggressor.[34]

1.1.3 Constructivism and the role of ideas in shaping States' behavior

[32] Mazzei F., Marchetti R., Petito F., Manuale di Politica Internazionale, Egea, 2010, p. 72-73.

[33] Claude Jr. I., Collective Security as an Approach to Peace in: Classic Readings and Contemporary Debates in International Relations ed. Donald M. Goldstein, Phil Williams, & Jay M. Shafritz. Belmont CA: Thomson Wadsworth, 2006, pp. 289–302.

[34] Ibidem, p. 80

As it will be later discussed when analyzing the different national strategies of the States taken into consideration, the role of perceptions is conceived as one of the main factor shaping States' behavior. Constructivism is the theory of International Relations which understands the importance of ideas and structures in world politics, especially with regards to the issue of security. Alexander Wendt, one of the main founder of such theory, argues against the rationalist assumption of both Realist and Liberal theories which minimizes the importance of values and norms, claiming that decision-makers are not free agents who take decision in a pure rational manner according to the constraints they meet, but rather actors who come from social settings that influence their way of perceiving what is important, what choice has to be made, how the world should be. Contrary to the Realist idea that the interests of a State are inherently given, Wendt suggests that those are shaped by the interplay between States; therefore, the motives are not static but they change accordingly to States' interactions.

For what concern the environment in which States play their game, the concept of structure is differently addressed by the theories. While more traditional theories, and *in primis* Realism, believe that the environment in which Countries act is always determined by anarchy, Constructivism argues that the environment structure is based on material forces, interests and ideas.[35] In particular, Wendt emphasizes the value of ideas, which shape the belief and the meaning an object can assume. In the case of security, he argues that the object of threat does not exist *per se*, but is the result of our perceptions. Indeed, it can be considered threatful due to someone's education, knowledge or experienced events, but cannot be perceived as such by others.

Constructivists concludes that ideas are important to the determination of structures' construction, and those will exert influence on States' agents and decision-makers' strategies. Nevertheless, ideas are not more important than power or interest, but they are at the basis of their determination. Finally, for Wendt, whatever structure is actually possible in the international system is the result of what Countries make of it.[36] Structures are created and shaped accordingly to States' representation of *Self* and *Other*, therefore they come into realization as self-fulfilling prophecies, because they are determined by States' belief that an event will occur and they adapt their behavior to it.[37]

This theory enables to understand the concept of security as a construction, exploring its origins and characteristics and the reason for which threats are perceived differently by States due to their background experiences. As a consequence, every single actor will decide to apply a process of

[35] Wendt A., Social theory of international politics, Cambridge University Press, Cambridge, UK, 1999, p. 139.

[36] Wendt A., Anarchy is what States Make of it: The Social Construction of Power Politics, International Organization, Vol. 46, No. 2, 1992, pp. 391-425, The MIT Press.

[37] Wendt A., Social theory of international politics, Cambridge University Press, Cambridge, UK, 1999, p. 309.

securitization to a certain object. According to the theory of the Copenhagen school, the term of securitization is used to designate the process of bringing an issue from a politicized or even non-politicized stage into the security domain.[38] The characteristics of this process, like the authors, the mechanisms, the motivations and the reasons of this construction bring the theory to perceive even security as a construction.[39]

1.2 Defining the cyber domain

Before proceeding with the thesis' attempt to apply IR theories to the cyber domain, it is of paramount importance to provide a sufficient definition of the object, despite the difficulty and uncertainty surrounding the matter, for the following reasons. First of all, because the Internet and its related technology are in a continuous process of expansion. This happens both physically, by connecting more and more people, but also virtually and in terms of capacity and ability.

According to Singer and Friedman (2014), at the time of the writing of their book "Cybersecurity and Cyberwarfare", there can be found at least twelve definition of what cyberspace is.[40] Despite many of those are rejected, for the purpose of this thesis, more general and reliable definitions have been chosen.

As an example, according to Myriam Dunn Caveltry, "Cyberspace connotes the fusion of all communication networks, databases, and sources of information into a vast, tangled, and diverse blanket of electronic interchange".[41] Another general definition is provided by the Tallinn Manual 2.0[42], which defines cyberspace as "the environment formed by physical and non-physical components to store, modify, and exchange data using computer networks".[43]

Likewise, the International Relations' scholar Joseph Nye provides an integrated definition of the traits of cyberspace both under the technical and the relational points of view. He, indeed, embraces the definition of cyberspace as "an operational domain framed by use of electronics to [...]

[38] Dunn Cavelty Myriam, Cyber-Security and Threat Politics, op. cit., p. 25.

[39] Adler Emanuel, "Imagined (security) communities: Cognitive regions in international relations.", op. cit., pp. 249-277.

[40] Singer, P. W., & Friedman, A., Cybersecurity and cyberwar: What everyone needs to know. Oxford: Oxford University Press, 2014, p. 13.

[41] Collins, A., Contemporary Security Studies. Oxford: Oxford University Press, 2015, p. 401.

[42] The Tallinn Manual 2.0 is a comprehensive academic work for policy advisors and legal experts that offers an assessment of legal, technical and strategic cyber-scenarios: a broad explanation of this object will be provided in chapter three.

[43] Schmitt, M., Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press, 2017, p. 564.

exploit information via interconnected systems and their associated infrastructure".[44] At the same time he illustrates cyberspace as "a new and important domain of power", where "even large countries with impressive hard power, such as the United States, find themselves sharing the stage with new actors and having more trouble controlling their borders in the domain of cyberspace".[45] Therefore, Nye reads cyberspace through the lenses of power and affirms that it "will not replace geographical space and will not abolish state sovereignty, but the diffusion of power in cyberspace will coexist and greatly complicate what it means to be a sovereign state or a powerful country".[46]

Embracing the conceptualization of cyberspace as a domain of power, the United States' Pentagon defined it as the fifth warfighting domain, after the ones of land, sea, air and space.[47] However, calling cyberspace as a warfighting domain have raised issues of unclarity and confusion. Indeed, Martin Libicki have questioned such definition because of the intrinsic differences that cyberspace has in comparison to the other domains. Libicki argues, indeed, that appreciating the cyber domain as fully equivalent to the others raises conceptual inconsistencies.[48]

According to the scholars committed to the redaction of the Tallinn Manual, there are two main issues that differentiate the "classical" warfighting domains and the cyber domain. First of all, the main difference lays on the fact that the cyber domain is entirely manmade and, as an artificial creation, it is a pure on-going technological development with continuous and significant impacts on the whole globe. Because it is not merely a physical space and does not have geographical borders, it detains the characteristic of being boundless. Moreover, it plays major roles in each other domains, allowing them a technological infrastructure while at the same time complicating its assessment.

The second main characteristic is anonymity, the ability to execute operation in any dimension holding, most of the time, no price or risk to the perpetrators. Such scenario creates both an issue of retaliation and of legality, as the operation cannot be attributed to a specific individual, organization, or State entity. This unique characteristic has the most influential and decisive role in making the cyber threats, intangible but easily executed.[49]

[44] Nye, Joseph S., Cyber Power, Belfer Center for Science and International Affairs, Harvard Kennedy School, 2010. Retrieved from: https://projects.csail.mit.edu/ecir/wiki/images/d/da/Nye_Cyber_Powe1.pdf

[45] Nye, Joseph S., Cyber Power, Belfer Center for Science and International Affairs, Harvard Kennedy School, 2010.

[46] Nye, Joseph S., Cyber Power, Belfer Center for Science and International Affairs, Harvard Kennedy School, 2010.

[47] D. Allen, P., Gilbert, D. , "The Information Sphere Domain Increasing Understanding and Cooperation", Johns Hopkins University, Applied Physics Lab, Booz Allen Hamilton, 2018, p. 1. Retrieved from: https://ccdcoe.org/uploads/2018/10/09_GILBERT-InfoSphere.pdf

[48] Libicki M., Cyberspace Is Not a Warfighting Domain, A Journal of Law and Policy for the Information Society, v. 8, no. 2, Fall 2012, p. 325-340.

[49] Efrony, D., & Shany, Y., A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice. American Journal of International Law, 112(4), 2018, 583-657, p. 632. Retrieved from: https://www.cambridge.org/core/services/aop-cambridge-core/content/view/54FBA2B30081B53353B5D2F06F778C14/S0002930018000866a.pdf/rule_book_on_the_shelf_tallinn_manual_20_on_cyberoperations_and_subsequent_state_practice.pdf

Another interesting difference with the traditional group of domains consists in the role of governance in the new domain, which appears to be more global than anything else. While Countries compete with each other because of resource scarcity, as suggested particularly by the realist theory, digital resources are not "scarce" in the traditional sense. Because of this idea, the question of governance is built up differently, rather than on the classic problem of distribution.[50] In such domain, the principles of representation, power and legitimacy are risen but through the questions of interoperability and communication. According to Singer and Friedman (2014), some of the main issues arise over the technical standards for interoperability, distribution of IP numbers and the management of the Internet's naming system[51].

There are several different formal and informal international groups and organizations that take care of the growth process of the Internet and, among the other functions, are entitled to establish standards and assigning names and numbers meant to control over who can access the Internet and how. Examples of those are the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Society (ISOC) and the Internet Engineering Steering Group (IESG). With the growth of the Internet and the consequential requests for definition of identity, strong commercial and political interests have fueled conflicts creating winners and losers and have brought to the attention several controversies that defies traditional governance models.

Nevertheless, many criticism have been risen against those groups as solely representative of certain interests, mainly belonging to the United States as in the case of ICANN, due to the fact that governments usually have more chances to financially support its representative in those groups, unlike the representatives from civil society.[52] This is also the reason why cooperation in the field is much more complex and still very brand-new.

Finally, attention should be drawn on the definition of security in this domain. When speaking about security we may find several definitions, as the previous paragraphs suggested. One of those is provided by MIT Professor Choucri in her book "Cyberpolitics in International Relations" (2012), defines cybersecurity as "a State's ability to protect itself and its institutions against threats, espionage, sabotage, crime and fraud, identify theft, and other destructive e-interactions and e-transactions".[53]

[50] Singer, P. W., & Friedman, A., Cybersecurity and cyberwar: What everyone needs to know. Oxford: Oxford University Press, 2014, p. 26

[51] Singer, P. W., & Friedman, A., Cybersecurity and cyberwar: What everyone needs to know. Oxford: Oxford University Press, 2014, p. 27

[52] Ibidem, p. 30

[53] Ibidem, p. 39

In the field of cybersecurity, whenever there is a deviation in the behavior of the adversary from expectations, what is realized is a malfunction, which is to be differentiated from errors or accidents. Therefore, a cyber-problem becomes a cybersecurity issue when the adversary is seeking to gain something from that activity, whether to obtain private information, undermine the system, or prevent its legitimate use.[54]

Singer and Friedman (2014) explain that there are three clusters of canonical security goals in an information environment: confidentiality, which refers to keeping data private; integrity, which deals with making sure that there has not been an improper alteration or change of the systems and of data without any authorization; availability, which means being able to use the system in a safe way; and resilience. Despite those security elements seems to be only technical, they are as well organizational, legal, economic and social and they have some limits as well. In a way, we can tell there is no such thing as absolute security.[55]

However, the concept of security is as well embraced by several other scholars and national strategists with a broader and more inclusive approach which is provided, for example, by Russian official documents. According to those, in order to counter the current and future threats which are related to the technological domain either directly or indirectly, it is necessary to create a system of international information security. The denomination "international information security" is used to describe a wider problematic area, and not simply "cybersecurity". The Russian national interpretation of this concept unfolds on the idea that "international information security is a state of global information space in which the possibility of violating the rights of the individual, society and the rights of the state in the information sphere, as well as destructive and unlawful effects on elements of the national critical information infrastructure, are excluded".[56] From this definition it is clear that the issue of information security is not limited only to the protection of information systems and networks, as provided by the most common definitions of cybersecurity, but establishes as a priority of public policy, first and foremost, the protection of the interests of the individual and of the State in a more comprehensive and transversal understanding.[57]

Finally, as it is evident already in the differentiated definitions of cybersecurity and international information security, the question of terminology should be necessarily addressed. The

[54] Ibidem, p. 34

[55] Singer, P. W., & Friedman, A., Cybersecurity and cyberwar: What everyone needs to know. Oxford: Oxford University Press, 2014, p. 37

[56] Дмитрий Грибков, Референт аппарата Совета безопасности Российской Федерации, О формировании системы международной информационной безопасности, журнала «Международная жизнь», МИД РФ, 2015. https://interaffairs.ru/jauthor/material/1352

[57] Дмитрий Грибков, Референт аппарата Совета безопасности Российской Федерации, О формировании системы международной информационной безопасности, журнала «Международная жизнь», МИД РФ, 2015. https://interaffairs.ru/jauthor/material/1352

fifth domain is a rather new environment and has been approached in the last 30 years as an unexplored foreign land. Despite the application of already used vocabulary which is usually employed for other security issues, it does actually consist in a new discussion that requires a new framework and terminology. Such complexity is further enhanced when technical matters are considered with more broader concepts in which even the most basic terms can be loaded with meaning.

One of the highly discussed terms is the one of "attack" in cyberspace. It is true that this term has been used for many different actions from online protesting to stealing information or sabotaging. This condition increases constantly confusion in all cases. Furthermore, experts and non-experts in the field may take advantage of other's confusion on the topic, raising chances of noise and uncertainty. The real problem is that, because there is not sufficient clarity and knowledge on the matter, people tend to put under the umbrella of "cyberattacks" activities that are alike and non-alike, for the simple reason of involving Internet-related technology.

The issue of labeling cyberattacks is just one of the pixel composing the picture, and defining the terms involved in the fifth domain is just the starting point of a wider process of frameworking the issue, so that all the Nations, in their translated language, would be able to conceive the terms in the same way. This problematic is covering a big part of the questions arising out from cooperation in the cyber domain.[58]

1.3 The applicability of IR theory to the analysis of cybersecurity

1.3.1 Cyber Actors: uncertainty and the rising importance of non-State actors

In order to provide a sufficiently accurate analysis of the developing panorama of international relations that takes place within the cyber domain, it is of paramount importance to define the main key aspects of the enquiry. The methodology utilizes the same scheme of actors, power and structure, as previously done with the Realist, Liberal and Constructivist theories.

The first object of the analysis deals with actors and their characteristics. In the previous lines, we described the State as the main actor interacting in the international system, especially with regards to the theory of Realism. Additionally, Liberalism provided an enlarged view, which included

[58] Singer, P. W., & Friedman, A., Cybersecurity and cyberwar: What everyone needs to know. Oxford: Oxford University Press, 2014, p. 70-72.

other actors such as Intergovernmental Organizations (IGOs), Non-Governmental Organizations (NGOs) and other major private economic entities.

When thinking about cyber actors in the international arena, we must think of bigger numbers and hazy images. This is because every single individual in the planet can be a relevant international actor whenever has a computer, Internet access and possess a decent amount of knowledge on how to use the world wide web. If we consider that, in 2018, more than 57.8%[59] of world population had Internet access worldwide, we could consider as well that they could be all possible hackers, using the Internet for malicious purposes. Such expansion in numbers of possible malicious users raises issues also in terms of responsibility, as there is a significant difference when you hold an individual responsible, or a State or even more an entity of another kind.

Additionally to the constantly expanding numbers, there is also another problem that needs to be taken into consideration when it comes to identify who is the person behind a screen. This is generally defined as the attribution problem. Attributing network intrusions is the process of figuring out which actor is responsible for the digital break-in.[60] Several progress in technology in many cases have allowed understanding the origins of the intrusion. However, while it is possible to assess the geographical location of the computer, it is much more difficult to establish who acted maliciously behind it. This arises different questions. First of all, by the almost impossibility of discovering who is guilty, it is difficult to hold someone responsible before a tribunal. Such example raises the concern on how to enforce law and make people pay for their negative behavior. Secondly, such anonymity influences perceptions and therefore increases the overall level of fear for cyberattacks.

It does not take much imagination to understand how damaging these problems can be. This is, indeed, demonstrated by the poisoned relations between the United States and People's Republic of China. While it is true that the Chinese Government exerts a significant control over the population through the Internet and technological devices, it is easy also to believe that the Chinese Government is as well behind malicious activities launched by computers located in the Chinese territory. Nevertheless, other actors may take advantage of the situation and of these perceptions in order to pursue malicious activities through the use of computers geolocated in China, despite the actor being of any other nationality. Interestingly enough, this very same logic enables Chinese actors to deny their responsibility, arguing that some of the activities which are launched from China, in truth are perpetuated by others who intend to take advantage of the widespread suspicion towards China.

[59] International Telecommunication Union, ITU Annual Progress Report 2018, available at: https://www.itu.int/en/council/planning/Documents/Annual-report-2018.pdf

[60] Buchanan B., The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations, New York: Oxford University Press, 2017, p. 143

Essentially, there is a lot of finger-pointing but not much certainty.[61] Additionally to the question of attribution, it is of much difficulty to assess also the complicity of an actor with a specific government, which can cover the position of penetrator or sanctioner of the operation.

This framework of uncertainty is further supported by Nye (2011) formulation of the concept of power diffusion which envisages the process of shifting power from state to non-state actors in the technology realm, as one of the most dominating trends of the 21st century.[62] The fact that technology, while developing, have become increasingly accessible have enabled almost anyone to play the game, including – unfortunately – criminals and terrorists. This has caused the rise of new threats which hold global resonance and cannot be tackled through the sole use of military force but by States' commitment to cooperation. Therefore, Nye argues that Countries should reformulate the way in which they think about power: not power over others but power with others.[63] Because Countries' decisions can have serious consequences, the danger of misunderstanding the relations of power forces increases the development of fear and mistrusts by generating a self-fulfilling prophecy. An incorrect assessment of the true correlation of forces brings far from the focus on real problems, while countries would have much more to gain from cooperation than from competition.[64]

1.3.2 Cyber power: adding flexibility and fluidity to a traditional concept

According to the Realist Waltz, power is defined as the distribution of material capabilities, which can be of military, economic, or social nature. However, when it comes to analyze the cyber domain, it looks like this definition lacks in the recognition of new forms of power. Therefore, it would be more appropriate to understand the meaning of power within the cyber domain appreciating its significance of influence and more specifically, the influence on States' capabilities. As a matter of fact, the different techniques of cyber war are designed with the aim of limiting someone's autonomy and exerting control over someone's capabilities. What is more is that such weapons do not only increase a State's power, but can put it as well under the control of another actor, either a State or non-State actor. In this different context, control has not defined characteristics, it is

[61] Singer, P. W., & Friedman, A., Cybersecurity and cyberwar: What everyone needs to know. Oxford: Oxford University Press, 2014, p. 74

[62] Nye, Joseph S., The Future of Power, New York: Public Affairs, Vol.11-No. 8, 2011. https://www.files.ethz.ch/isn/154756/issuesinsights_vol11no08.pdf

[63] Ibidem, p. 6.

[64] Ibidem, p. 5.

technological and it is not merely State-centric or real.[65] Therefore, in order to adapt to a changing environment, a flexible theory of power must be applied to predict and understand new methods and techniques of control.

There are different approach to categorizing cyber power, as it can be conceived under multiple forms. First of all, the budget that one Country spends annually on the build-up process of a cyber arsenal. If it is so, we can classify Countries that have put financial effort and expertise into a strategy that develops both offense and defense cyber capabilities.

Table 1: Cyber Warfare: Countries with the strongest cyber forces[66]

Countries with the Strongest Cyber Forces		
Countries	Financing (mnl $ per year)	Personnel
United States of America	7,000	9,0000
China	1,500	20,000
United Kingdom	450	2,000
South Korea	400	700
Russia	300	1,000
Germany	250	1,000
France	220	800
North Korea	200	4,000
Israel	150	1,000

According to the researches of the Valdai Discussion Club (2019), the United States is the Country with the largest spending in financing cyber forces. China, while spending less on financing compared to the United States, has been employing the highest number in personnel. United Kingdom, South Korea and Russian Federation are placed respectively third, fourth and fifth in financing cyber forces worldwide.

An additional example is offered in the book "Cyber Strategy: the evolving character of power and coercion" by Brandon Valeriano, Benjamin Jensen and Ryan C. Maness. According to Valeriano et. al, an examination of States' cyber strategies and the way in which States exert their power over

[65] Kassab H.S. (2014) In Search of Cyber Stability: International Relations, Mutually Assured Destruction and the Age of Cyber Warfare. In: Kremer JF., Müller B. (eds) Cyberspace and International Relations. Springer, Berlin, Heidelberg, p. 63-64

[66] Cyber Warfare Infographics, Valdai Discussion Club, 27.08.2019, available at: http://valdaiclub.com/multimedia/infographics/cyber-warfare/

other States brings on a double categorization. On one side, they recognize that a State may have the power to produce negative repercussion on the population, like death. This is the case according to which cyber-attacks can be utilized as a tool to hamper the functioning of vital civil infrastructures for the population, such as the modification of the functioning of a central that produces energy, a hospital, the transit of trains and so on. However, their empirical studies brought them to the conclusion that until now cyber-attacks have resulted in limited coercive and signaling effects more than real and tangible outcomes on human's life, like people's death. Indeed, they demonstrated that all the cyber-attacks which we know never directly produced deaths[67].

On the contrary, Valeriano et al. demonstrated empirically that States have used their power through the use of cyber tools elaborating three different categories of cyber-attack: cyber disruption, espionage and degradation. Rival States use indirect cyber instruments to shape long-term competition more than to seek immediate concessions. Therefore, it seems like cyber operations complement rather than replace traditional statecrafts. In fact, cyberattacks have served as an additional foreign policy tool in the modern strategic competition recalling a much more fluid concept of power and influence.[68]

In the process of applying the traditional theories of International Relations to the topic of cyber security, we first have to recognize the differences between cyberattacks and traditional attacks. To begin with, the two categories requires the implementation of different tools to deliver the attack: instead of using kinetic force, digital means are the action's tools. Such first difference does actually matter because a cyberattack is not constrained by the usual physics of traditional attacks, as it can move at a very fast speed, within unlimited geography and pass beyond political boundaries.[69] The second important difference consists in the identification of the target. The main target of a cyberattack is always a computer and the information within and not necessarily something physical. A third and interesting point is based on considerations on the costs' side: while the price for delivering a physical attack implies as well the purchase of weapons and different materials, cyberattacks require much more investment on research and development.[70]

Finally, in all aforementioned cases and actions connected to it, we do encounter a good level of ambiguity. On one side, States may consider the utility of the cyber strategy applied as a way to infer power and influence over another actor in an optimized way that relies on tacit bargaining and

[67] Valeriano B., Jensen, B., & Maness R., Cyber Strategy: The Evolving Character of Power and Coercion, New York: Oxford University Press, 2018, p. 2

[68] Valeriano B., Jensen, B., & Maness R., Cyber Strategy: The Evolving Character of Power and Coercion, New York: Oxford University Press, 2018, p. 3.

[69] Singer, P. W., & Friedman, A., Cybersecurity and cyberwar: What everyone needs to know. Oxford: Oxford University Press, 2014,pag 68-68

[70] Ibidem, p. 69

ambiguous signaling to help rival States to achieve a position of relative advantage in the long-term competition. On the other side, as in many other domains, like land, space, air and sea, even in cyber signaling it gets a big deal of problematic, because it may happen that only the initiator may perceive the actual engagement.

Power in cyberspace can as well be conceived as the States' capacity of cyber defense.[71] According to Libicki's formulation, a Country should pursue three main goals in order to seek cyber defense: robustness, system integrity and confidentiality. In particular, the goal of robustness, which includes as well the faculty of recoverability, is described as "the ability to extract as much military power from systems under stress as from systems free of stress".[72] Finally, when a government commits to cyber defense, it should work on elaborating and implementing a safe and organized information system architecture and appropriate policy operations, among which subsidizing research and development in computer network defense and allocating more resources to cyber-forensics and to threat intelligence.[73]

An empirical example that describes the cybersecurity capabilities as means of deterrence is offered by the 2018 Global Cybersecurity Index redacted by the International Telecommunication Union (ITU) which presents a classification of States which have a high, medium or low commitment to cybersecurity in the year 2018.[74] Such index is based on a research which verted on a set of five main pillars.[75]

Figure 2: Geographical cyber commitment around the world[76]

[71] Libicki, Martin C., Cyberdeterrence and cyberwar, RAND Corporation, 2009, p. 162.

[72] Ibidem, p. 162.

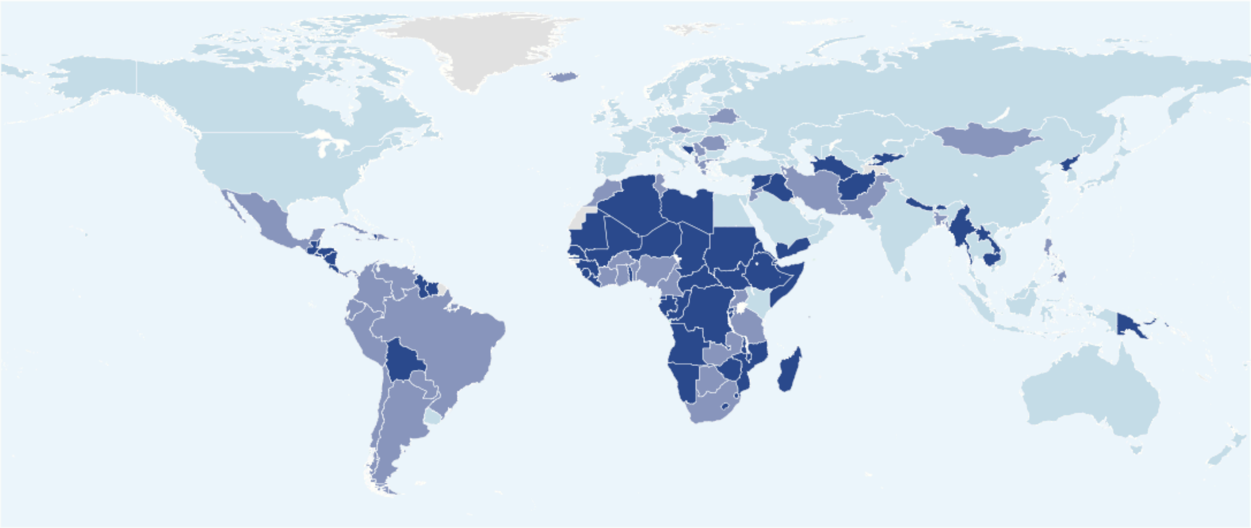
[73] Libicki, Martin C., Cyberdeterrence and cyberwar, RAND Corporation, 2009.

[74] International Telecommunication Union (ITU) report on the 2018 Global Cybersecurity Index (GCI), p. 8, available at the following link: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf

[75] The five pillars are: legal (cybercrime legislation, cybersecurity regulation, containing/curbing of spam legislation); technical measures (CERT/CIRT/CSIRT, standards implementation framework, standardization body, technical mechanism and capabilities deployed to address spam, use of cloud for cybersecurity purpose, child online protection mechanisms); organizational measures (national cybersecurity strategy, responsible agency, cybersecurity metrics); capacity building measures (public awareness campaigns, framework for the certification and accreditation of cybersecurity professionals, professional training courses in cybersecurity, educational programs or academic curricular in cybersecurity, cybersecurity R&D program, incentive mechanisms); cooperation measures (bilateral agreements, multilateral agreements, participation in international fora/association, public-private partnerships, inter-agency/intra-agency partnerships, best practices).

[76] This image is taken from the International Telecommunication Union (ITU) report on the 2018 Global Cybersecurity Index (GCI), p. 13.

Heat map showing geographical commitment around the world



The colours in the heat map above indicate differences in the level of commitment with high, medium, and low scores in a range of colours from light blue (peak commitment) to dark blue (low commitment).

Likewise, Libicki argues that the "appearance of robustness is almost as important as robustness itself, if the goal is for military power to act as a general deterrent".[77] Indeed, uncertainty does affect all forms of warfare, and in a particular way cyberwarfare.[78] Based on the elaborations of Mearsheimer, Libicki argues that Countries could be deterred from starting-off a cyberoperation if they are persuaded that the efforts would fail and, therefore, they would end up as losers.

1.3.3 The structure of the international system applied to the cyber domain

Having analyzed who could be the possible actors in an international cyber-system and having understood the infinite capacities that one Country has to exert its influence over another using cyber tools, we attempt now to provide an image on how the cyber world is shaping the relations between States. At first glance, it looks like the concept of anarchy promoted by Realist theory does well describe the current environment in which States act internationally. However, the first difference consist in the plethora of actors that takes part into to the international interplay of cyberspace. In fact, they are not merely States, as the Realist theory would suggest, but we do recognize a panorama

[77] Ibidem, p. 162.

[78] Libicki, Martin C., Expectations of Cyber Deterrence, Strategic Studies Quarterly, Winter 2018, The Air University Press, p. 51. https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-12_Issue-4/Libicki.pdf

of different actors that can actually exert some sort of influence on the international system as Liberalism and Constructivism prescribe. The Internet have revolutionized the way in which someone can be powerful: new tools have given the chance both to small States like Singapore, which have widely invested financially and technically in information security and can be considered as vanguard States in the sector, and non-State actors the possibility to play the game.

Despite this being true, a prominent scholar in the field of International Relations and security studies, Joseph Nye, stands against this idea, making sure that the most strategic and effective cyberattacks are those who combine sophisticated new weapons with vast economic, military and human resources, which are placed outside the cyber realm. According to Nye, the configuration of power that shapes the international system has something old, which is represented by more traditional concepts of power and capabilities, and something new, which deals with the development and implementation of new technologies.[79] Indeed, in a possible condition of arms race, big Countries like the United States or the Russian Federation still maintain the escalation dominance, by reserving the right to shift the conflict outside cyberspace where they retain evident advantages.

However the actual weight an actor can assume in the structure of the International System is as well determined by the perceptions that countries have of each other. As it is difficult to objectively assess both the capabilities and the intentions of the possible adversary or partner, States are building in cyberspace a specific structure of international relations which is mostly competitive. The competitive behavior that Countries are undertaking is determined by the perception that anarchy reigns in cyberspace due to the fact that there is an objective lack of diffused idea of collective security and of regimentation of the practices carried in cyberspace, which fuels the perception of mistrust among the participants. Therefore, the structure the international system is, as recognized by Constructivists, in an ongoing process where perceptions of the *Self* and the *Other* play important roles.[80] As long as there is mistrust, anarchy will be dominant and will be replaced only if there is an adjustment in perceptions and ideas that would bring Countries to behave differently.

1.4 The Offense-Defense Theory in the fifth domain

1.4.1 Threat assessment in cyberspace: offense over defense

[79] Nye, Joseph S., Cyber Power, Belfer Center for Science and International Affairs, Harvard Kennedy School, 2010.
[80] Wendt A., Social theory of international politics, Cambridge University Press, Cambridge, UK, 1999.

Countries deliver threat assessments with the objective of weighting the risks an entity may face. Herbert Lin, one of the leading figures in the field of cybersecurity, considers three main factors according to which such assessment should be delivered. Firstly, "the feasibility of adversaries being able to identify and exploit your vulnerabilities"; secondly, "the effect that would happen if they were able to take advantage of these vulnerabilities"; thirdly, "the likelihood that they will, in fact, be willing to do so".[81] Obviously, such process is extremely hard to be carried, given layers of uncertainty both looking at the personal and other's capabilities and likely intentions.

Very often, because of human and organizational inclination, in a condition of uncertainty while weighting risks, people tend to assume the worst-case scenario. Among the different elements of uncertainty, it is really hard to assess the capabilities and the weaponry of the adversary. While a war in the physic world is pursued under some specific law (e.g. the basic law of physics), by comparison cyberweapons are not bound to those laws. can be stored and classified in many different ways, which makes it even more hard to be assessed.[82] Following the process, even when a State is finally able to determine the fact that it has been targeted and by whom, it may still remain very difficult to figure out which is the adversary's actual intent, be it targeting your system, gather intelligence, steal information or shut down your operations. Unfortunately, in most of cyberspace cases, many of the abovementioned risks are undiscovered until after an attack takes place.

The context of competition in which States are found to act generally pushes them to increase their ability to defend themselves. Moreover, such inclination towards competition is reinforced by uncertainty due to information asymmetry on States intentions and motives, thus, security seems to be more achievable through balancing than through the stipulation of agreements. Such condition tends to be formed because States try to offsets others' power advantages and gain advantages of their own to protect themselves.

To better understand the situation, we must recall to the offense-defense theory by the structural realist Stephen Van Evera. In the book "Causes of War: Power and the Roots of Conflict", Van Evera proposed the Offense-Defense theory, which attempts to discern which are the factors that increase the likelihood of war. He formulates three main hypotheses: "1. War will be more common in periods when conquest is easy, or is believed to be easy, than in other periods. 2. States that have, or believe they have, large offensive opportunities or defensive vulnerabilities will initiate and fight more wars than other States. 3. Actual examples of true imbalances are rare and explain only a

[81] Singer, P. W., & Friedman, A., Cybersecurity and cyberwar: What everyone needs to know. Oxford: Oxford University Press, 2014, p. 148.

[82] Singer, P. W., & Friedman, A., Cybersecurity and cyberwar: What everyone needs to know. Oxford: Oxford University Press, 2014, p. 149

moderate amount of history. However, false perceptions of these factors are common and thus explain a great deal of history."[83]

The question of whether a new technology favor the offense or the defense posture is a critical issue when discussing cybersecurity. As it is widely shared that the future use of cyber weapons will be offensive, larger spending on cyber offense has been implemented worldwide. The basic idea beneath this approach is that it is much cheaper and easier to attack an information system instead of detecting it and find any possible solution to defend against it. Additionally, the attackers possess the initiative and the advantage to choose the time and the place of the attack.

While this reasoning may actually work with physical weapon, in the cyberspace there are few additional elements that kick in. First of all, there is an amount of "ground" that is well defined in the traditional scenario, while might be unlimited in the case of cyberspace, due to its virtual capacity. Secondly, there is uncertainty on the outcome of a cyberattack: the attacker can be able to successfully intrude himself in a system but the outcomes and the damages are very difficult to predict or assess. Therefore, in order to create balance in cyber warfare, it is important to develop a defensive mechanism against cyber offence, as in cyberspace States can only maximize their security by minimizing the probability of the cyber-attacks on their critical infrastructures. However, the path toward developing a substantive and effective defense meets several technical complexities.

In conclusion, the offense-defense balance in cyber warfare significantly resembles the one in conventional warfare, but not the one of nuclear kind, largely because the defensive side of the balance appears weak, which in turn provides superiority to the offense.[84] Thereby, in order to apply the Offense-Defense Theory, the critical point is to ascertain the balance between offense and defense, either perceived or real, which brings us back to the issue of assessment of the risks of a cyber-attack, being it the attribution problem, the lack of physicality, or the general uncertainty of the domain. In cyber warfare, given the advantages of mobility, surprise, penetration and precision that cyber weapons offer to an attacker and the underdeveloped defensive side of this warfare, the attacker will develop strong perception about its offensive advantage.[85]

1.4.2 Mutually Assured Destruction or Mutually Assured Stability?

[83] Van Evera S., Causes of War: Power and the Roots of Conflict, Ithaca, London, Cornell University Press, 1999.

[84] Shaheen S., Offense–Defense Balance in Cyber Warfare. In: Kremer JF., Müller B. (eds) Cyberspace and International Relations. Springer, Berlin, Heidelberg, 2014, p. 88.

[85] Shaheen S., Offense–Defense Balance in Cyber Warfare. In: Kremer JF., Müller B. (eds) Cyberspace and International Relations. Springer, Berlin, Heidelberg, 2014, p. 88.

Due to the subjectivity of threat perception and asymmetry of information, the actions undertaken by different actors, and particularly States, within the cyberspace may bear the risks of conflict escalation by undermining the stability of their relations. Essentially, the cybersecurity expert Ben Buchanan (2017) is applying cybersecurity issues to the classical security dilemma, raising some interesting peculiarities and deviations from the traditional approach.

First of all, intrusions are different from a classical weapon attack because the time and the action itself are faster and there is a higher chance of not being noticed while planning it. Moreover, considering that those intrusions can be quite harmful to States, such conditions pushes government to ensure against intrusions and thus, they work in order to develop stronger protections. While it might be easy to establish States' military defenses on land borders, in cyberspace it is even harder to establish States' frontiers.

Furthermore, States commonly believe that gaining information to detect threats more effectively can actually ensure their own network security, so they are highly likely to break into networks of other States. Despite the absence of offensive intentions in this attack, still they attack because the intrusions itself can lead to valuable information profit. On the side of the attacked, there will be a subjective perception of the attack: the State which suffer the intrusion will decide whether the attack had an offensive or defensive character, judging by limited and almost certainly insufficient amounts of data on the intentions of the opponent. Finally, even though States express their defensive intentions, still the opponents will perceive any serious intrusions with some degree of fear. Therefore, they have significant incentive in strongly responding, further animating the cybersecurity dilemma.[86]

Having acknowledged that the current status of affair in the cyberspace bring in so much risk into states relations, there is as well something that can be learned from past experiences, which raises the question on whether some kind of stability like the one settled during the Cold War can be applied on assuring cyber-stability. This idea has to be unfolded starting from a different point of view, which is the role of signaling. As demonstrated by Valeriano et al., while cyber degradation should only produce near-term concession in the digital domain, the utility of cyber operations is rather more utilized to signal rivals engaged in a long-term competition, with the opposite objective of managing escalation risks. Indeed, cyber strategies could be seen as well as ambiguous signaling that limits escalation, supporting the idea of mutually assured stability. There is no evidence that offensive dominance makes it more likely that powerful States will intervene to protect the status quo as

[86] Buchanan B., The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations, New York: Oxford University Press, 2017, p. 7

demonstrated by the fact that there has not been a major cyber escalation despite the several cyber-attacks that take place every day.

According to the idea that "talk is cheap", States use low-level cyber actions in order to put into practice signaling mechanism which are designed to limit future escalation and establish credibility. Therefore, it would be more appropriate to define the posture as a demonstration of credibility rather than of capabilities. Even if the signal is limited and temporary, the use of cyber tools offers a new opportunity for tacit bargaining between antagonists to probe intentions and manage escalation.

Likewise, Joseph Nye discusses the rather successful results of deterrence and dissuasion that have characterized cyberspace so far. Firstly, he offers a definition of deterrence as the process of "dissuading someone from doing something by making them believe that the costs to them will exceed expected benefit".[87] Nye argues that there are some means of deterrence and dissuasion that can be utilized to prevent cyberspace adverse actions: e.g. threat of punishment, denial by defense, entanglement and normative taboos.[88] Moreover, Nye is very attentive in specifying that still deterrence rests on perceptions and who is bearing those perceptions: much depends on how States perceive capability and credibility of others and of the deterrent instrument.

On the matter of perceptions Ben Buchanan (2017) offers an interesting argument that explains the reason for lowered risks of escalation. He claims the following: "because attribution is very difficult, States detecting a network intrusion are unable to determine who is responsible and whom to fear. A potentially destabilizing response against another State, as predicted by the cybersecurity dilemma, is therefore less likely"[89]. At this point, States have to deal with an enhanced attribution dilemma: one has to weigh the potential gains versus losses of pointing the finger at the group or person you think is behind a cyberattack.[90] In deciding this, your real-world goals then matter more than what actually took place in the cyber realm. Hence, the advantage of using cyber tools lays in the ability to deny responsibility and the real problem is that credibility is a critical factor in convincing an adversary that their actions will have important consequences.[91]

In conclusion, ambiguities of attribution and the diversity of adversaries do not make deterrence and dissuasion impossible in cyberspace, but punishment occupies a lower degree of the

[87] Nye J. S., Deterrence and Dissuasion in Cyberspace, International Security, 41, 2017, p. 45.

[88] Nye J. S., Deterrence and Dissuasion in Cyberspace, International Security, 41, 2017, p. 54.

[89] Buchanan B., The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations, New York: Oxford University Press, 2017, p. 143

[90] Singer, P. W., & Friedman, A., Cybersecurity and cyberwar: What everyone needs to know. Oxford: Oxford University Press, 2014, p. 76

[91] Valeriano B., Jensen, B., & Maness R., Cyber Strategy: The Evolving Character of Power and Coercion, New York: Oxford University Press, 2018, p. 15

strategic space than in the case of nuclear weapons. Uncertainty and attribution problems often slow and blunt its deterrent effects, but may as well prevent a State to act because of the unknown results of its actions. Additionally, limitations to act maliciously may have different effects on the different postures that States have.

We have been focusing on peacetime deterrence and dissuasion of cyberattacks, thus, there is little empirical evidence because no full-scale cyber war has occurred yet. It is therefore extremely difficult to assess whether *Mutually Assured Destruction* or *Mutually Assured Stability* has prevailed. However, it is important to rethink escalation and deterrence as they are applied differently in the cyber-world of International Relations.

1.5 Results of the applied analysis

The first chapter of this thesis is aimed at exploring the behavior of States in general terms by applying the classical theories of International Relations to the features of cyber space. After providing a comprehensive presentation of respectively the main traits of the Realist, Liberal and Constructivist theories, which have been selected because they discuss cooperation, conflict and security issues, the tools provided by the three theories have been applied to the cyber realm. By means of clarity and appropriateness, all the features composing the cyber realm have been displayed: the terms of physicality, temporality, permeation, fluidity, participation, attribution and accountability have been addressed as well as the ways in which those parameters assumes different connotation in the domain. The main findings originating from the analysis brings some main considerations which are presented as follows.

The first result deals with the issue of geography and sovereignty determination. While in the Realist theory the role of border determination assumes a fundamental meaning in assessing the traits of a Country’s sovereignty and national control over territory and resources, when we try apply those concepts to cyber, serious difficulties arise because there are very blurred borders due to the open character of the Internet. As a result, the uncertainty over territorial determination makes the governance of the network system a matter of discussion on whether it should imply a global governance or should apply the idea of national sovereignty. In this case, given determination a complex process, the option provided by the liberal theory of collective security appears to be a plausible solution to administer the Internet collectively as long as it remains open and global.

The second result is based on the assessment of the characteristics and the role that cyber actors detain. Even in this case, while the theory of Realism accepts Countries as main actors of the international system, the cyber realm has to deal with increased numbers and different typologies of participants. Indeed, the entities acting in cyberspace could be States as well as non-State actors such as International Organizations, individuals and private entities. This description resembles the assumption relative to the liberal theory which enlarge the pool of participants in the international relation scene. However, the problem that emerges with this expanded diversity is related to the miscellaneous intentions that the different entities have while acting in cyberspace, as not everyone share the same responsibility of collective security or have any consistent incentive for pursuing it.

The third result deals with the characteristics of power and embraces the problematics originating from the trend of power diffusion due to the fast development of technology. Assessing cyber power is challenging: the capabilities which were making a country militarily strong are questioned because power is modified and diffused.

Finally, the role of perceptions becomes fundamental in determining the limits of States' actions and makes threat assessment a challenging process. Uncertainty appears to have two conflicting consequences. On one side, it fuels competition pushing States to reinforce their offensive capabilities further enhancing the cybersecurity dilemma. On the other side, uncertainty may as well mitigate such dilemma due to the risk of an incorrect understanding of the real intentions or responsibilities of other States. By current times, it looks like the second option has been working as one of the major deterring force since no full-scale cyber war has occurred yet. The different results related to the issue of uncertainty demonstrates that countries feel like acting in a competitive environment only because of their ideas on anarchy governing the system. Following a constructivist approach, the idea of mistrust is what mostly shape their behavior and may bear the risk of setting up a conflict as a self-fulfilling prophecy.

The main conclusion to this analysis is that there is a need of rethinking the classical principles of International Relations when applying them to cyberspace, including the principle of deterrence and sovereignty, which by now do not find exhaustive applicability. Furthermore, because this topic is rather new to policymakers and scholars, for the future we may envisage additional discussion on the matter and probably a more organized discourse on the topic. It is undeniable that cyber-attacks are becoming the "new normal", therefore, we may expect to appreciate them as the new normal and build further research upon that.

Part two – Major Cyber Rivals: towards cooperation or self-help?

2.1 States' cyber postures: a selected analysis of national security strategies

In the second part of this thesis, after providing a broad analysis on the technical and theoretical issues concerning the fifth domain, States' postures will be taken into consideration. The choice fell particularly on three States: the Russian Federation, People's Republic of China and the United States for the following reasons. By first, according to researches carried by the Valdai Discussion Club, they are some of the most developed Countries in terms of usage of cyber-tools as well as their cyber component is well integrated in both domestic politics and in the country's foreign and security policies.[92] Secondly, they are, by more than 20 years, the most involved Countries when it comes to discuss cyberwarfare and cybersecurity.[93] They, indeed, have been at the center of several discussions on the topic, have been called responsible for several major intrusions and have put within their national security strategy their concern on cybersecurity issues.[94] Finally, because they advocate different views and different approaches to the topic, offering an interesting and widen outlook on the matter, as it will be later explained. Nevertheless, their order of examination is purely casual.

The main idea behind this chapter is to better understand the degree of cooperation between States in the field of cybersecurity by analyzing the postures of the mentioned main rival actors and their official strategies. In particular the Constructivist approach to security will be instructive to the analysis as strategies are the result of different ideas determined by the background of each State. By means of clarity, the definition stands as follows: "national cyber security strategy (NCSS) is a plan of actions designed to improve the security and resilience of national infrastructures and services. It is a high-level top-down approach to cyber security that establishes a range of national objectives and priorities that should be achieved in a specific timeframe".[95]

At the end of this analysis, some consideration will be drawn on the main divergent and colliding opinions and technicalities that make cybersecurity something difficult to agree upon. In

[92] Valdai Club, infographic: Cyber Warfare, 27.08.2019, available at: http://valdaiclub.com/multimedia/infographics/cyber-warfare/

[93] Nye, Joseph S., The Future of Power, New York: Public Affairs, Vol.11-No. 8, 2011. https://www.files.ethz.ch/isn/154756/issuesinsights_vol11no08.pdf

[94] Breene K., Who are the cyberwar superpowers?, World Economic Forum, May 2016: https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/

[95] Definition by ENISA; National Cyber Security Strategies, European Union Agency for Cybersecurity, ENISA, available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies https://www.enisa.europa.eu/topics/national-cyber-security-strategies

fact, it will be demonstrated that cooperation in the fifth domain develops at a slow peace not only because it is a rather new field of study but mainly because there are some technical and relational aspects that need to be first addressed and overcome before calling for the instrument of international law to regulate international relations in the cyber domain.

2.1.1 The Russian Information Security Strategy

Official documents and national interests

The latest operations of the Russian Federation in the fifth domain have pushed politicians, scholars and journalists to discuss frequently and vehemently about Russian intentions in the cyber sphere.[96] It has been clear by now, that Russian government have always considered cyber tools as a mean for reaching goals and objectives in the international arena. Unquestionably, Russian Federation recognizes the importance of this domain in its ambivalence, as a resource and as an additional stage where new threats are emerging. In this sense, official documentation of the Russian government supports the idea of an enhanced doctrine which is compliant with the current trend of modern hybrid wars and takes into consideration the impact of those on different security levels.[97]

As history tells, Russia, along with the United States and other European countries, has been one of the most relevant countries leading the rise of awareness concerning the impact of information attacks. This is, for example, demonstrated by the events that took place in 1998 under the roof of the United Nations Headquarters, when the delegation of the Russian Federation firstly introduced on the table of discussion of the First Committee on Disarmament and International Security the question of "Developments in the field of information and telecommunications in the context of international security".[98] Such first step has been a cardinal decision because for the first time information security threats could have been discussed officially within an international and widely recognized forum.

[96] Siim Alatalu, Irina Borogan, Elena Chernenko, Sven Herpig, Oscar Jonsson, Xymena Kurowska, Jarno Limnell, Patryk Pawlak, Piret Pernik, Thomas Reinhold, Anatoly Reshetnikov, Andrei Soldatov and Jean-Baptiste Jeangène Vilmer, Hacks, leaks and Disruptions: Russian cyber strategies, Chaillot Papers, European Union Institute for Security Studies, Paris, October 2018. Retrieved from: https://www.iss.europa.eu/content/hacks-leaks-and-disruptions-—-russian-cyber-strategies

[97] Directorate-General for External Policies – Policy Department, Russia's national security strategy and military doctrine and their implication for the EU, European Parliament, 2017. http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/578016/EXPO_IDA(2017)578016_EN.pdf.

[98] United Nations Resolution A/RES/53/70 approved by the General Assembly on the report of the First Committee (A/53/576) on 4 January 1999. Document retrieved at https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/760/03/PDF/N9976003.pdf?OpenElement

The Russian concern over these issues has been addressed since early times both at national and international level. Indeed, information security has been a topic present in the National Security Strategy published in September 2000, which includes, among other threats, the "manipulation of information disinformation, concealment or misrepresentation"[99]. Additionally, this document identifies as a major source of threat "the desire of some Countries to dominate and encroach on the interests of Russia in the global information space"[100].

The latest doctrine, which is expressed in the Foreign Policy Concept of the Russian Federation approved by the President of the Russian Federation Vladimir Putin on November 30, 2016, has redesigned and enlarged the previous concept of information security which was adopted in September 2000.

The analysis of this document shows important modification in the National Security doctrine, especially with regards to the topic of cybersecurity. Surely, this change has been determined by the rapid development that technology has experienced in the latest years, but mostly because of the increasingly malicious usage of cyber tools. Therefore, the official presidential decree identifies cybersecurity, privacy and information security as vital components to Russian national interests and poses itself as the basis for further foreign relations' developments on the matter and for information security improvements.[101]

Despite being a rather new document, it retains some core elements that are traditional to the view that Russia embraces about the order of the international system. Indeed, the document emphasizes the Country's status as one of the world leading power and its striving for pursuing an independent foreign policy. Therefore, information security, as a field where emerging threats are taking space, has to be defended both internally and externally as it consists in a direct threat to Russian national security.

For further clarification of this conceptualization, the official document of the Russian Federation on the Doctrine of Information Security approved by President Putin on December 5th, 2016 needs to be taken into account.[102] As defined by the official document, "the information security of the Russian Federation […] is the state of protection of the individual, society and the State against internal and external information threats, allowing to ensure the constitutional human and civil rights

[99] Russian presidential decree no. 1895, "Доктрина информационной безопасности Российской Федерации" [Doctrine of Russian Information Security], September 9, 2000, http://base.garant.ru/182535/

[100] Ibidem.

[101] Foreign Policy Concept of the Russian Federation (approved by President of the Russian Federation Vladimir Putin on November 30, 2016), retrieved from the official website of the Embassy of the Russian Federation to the United Kingdom and Northern Ireland: https://www.rusemb.org.uk/rp_insight/

[102] Doctrine of Information Security of the Russian Federation, "Доктрина информационной безопасности Российской Федерации", approved December 5th 2016 by Decree of the President Vladimir Putin. Retrieved from: http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163.

and freedoms, the decent quality and standard of living for citizens, the sovereignty, the territorial integrity and sustainable socio-economic development of the Russian Federation, as well as defense and security of the State".[103]

Moreover, the official paper stresses the importance of the information sphere in the implementation of the strategic national priorities of the country: "based on the analysis of major information threats and assessment of the state of information security, the Doctrine defines the strategic objectives and key areas of information security taking into account the strategic national priorities of the Russian Federation".[104]

Among the strategic national priorities in the information sphere, there is a set of specified objectives which can be considered both as matter of internal and external policies which includes "ensuring and protecting constitutional human and civil rights and freedoms with regard to the receipt and use of information; privacy in the use of information technologies, providing information support to democratic institutions and mechanisms of interaction between the State and civil society"[105], as well as the development of information technologies and the improvement of the production, research and scientific development performances.

Through the years, Russian behavior in the fifth domain has been largely discussed and criticized, raising the number of adversaries that the Country had been facing and a major interstate competitiveness in different fields, which are nevertheless connected to the use of tools in the cyberspace.[106]

The very first divergence that Russian Federation meets with Western Countries is disposed on a semantic level. The Russian definitions of cyberwarfare, its employment for strategic use, and other subjects concerning the cybersecurity sphere are different from the ones used in Western Countries. In the Russian language, the terms *cyber* or *cyberwarfare* are not used, with the exception of when referring, indeed, to Western Countries. The most equivalent Russian terms[107], such as "information warfare", as employed by Russian military theorists, retain a broader concept that includes computer network operations, electronic warfare and information operations.[108] Such

[103] Ibidem.

[104] Ibidem.

[105] Ibidem.

[106] Directorate-General for External Policies – Policy Department, Russia's national security strategy and military doctrine and their implication for the EU, European Parliament, 2017. http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/578016/EXPO_IDA(2017)578016_EN.pdf.

[107] In Russian, *кибер* (cyber) and *кибервойна* (cyberwarfare) are terms which are used only when it comes to talks concerning the West. Conversely, Russian experts usually use the term *информационная война* (information warfare) which gives a broader concept on the elements that composes cybersecurity.

[108] Michael Connell and Sarah Vogler, Russia's Approach to Cyber Warfare, CAN Analysis and Solutions, March 2017. https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf.

instruments are basically employed as part of a whole of governmental effort, along with more traditional weapons, in order to purse national interests. More specifically, offensive cyber usage is related to a significant supporting role in helping the State to achieve information dominance in all the stages of a conflict.

Russia's cyber capabilities are advanced and Moscow has demonstrated being able to employ both offensive and defensive cyber capabilities in neighboring and non-neighboring States. The 2007 cyberattacks to Estonia, 2008 cyberattacks to Georgia and 2016 United States elections' manipulation are some of the accusation presented against the Russian Federation, criticizing the fact that cyber tools are increasingly used for military means and for destabilizing political and social situation in various regions across the world, undermining sovereignty and violating the territorial integrity of States.[109]

Conversely, Russian government has responded to those accusations of interference by depicting the growing information pressure which is coming from the outside on the population of the Russian Federation, in particular over young people, and is eroding Russian traditional spirit and moral values. The perceived threat, which refers to the "cultural security" sphere, goes along with terrorist activities and computer crimes, which in conclusion converge in the basket of *national security threats*.

Additionally, as widely expressed in the 2016 Foreign Policy Concept, Russian government criticizes the absence of an effective international legal framework which is regulating inter-state relations in the information space, as well as mechanisms and procedures for their application.[110] However, the document expresses Russian acknowledgement on the complexity of the environment where to achieve strategic stability and equitable strategic partnership.[111] It is worth underlying that Russian government values both technological and humanitarian aspects on information security. The Doctrine enunciated in the official document also states that strategic deterrence and prevention of military conflicts is one of the main aim related to the enhancement of information security.

International Initiatives

[109] Valeriano B., Jensen, B., & Maness R., Cyber Strategy: The Evolving Character of Power and Coercion, New York: Oxford University Press, 2018, p. 110-112.

[110] Foreign Policy Concept of the Russian Federation (approved by President of the Russian Federation Vladimir Putin on November 30, 2016), retrieved from the official website of the Ministry of Foreign Affairs of the Russian Federation.

[111] Ibidem.

As already mentioned, Russia has been concerned about the misuse of information tools for political, military and criminal purposes for more than twenty years. Such fear has pushed the Country to be active at the international and regional level with the aim of enhancing cyber regulation for a safer use of technology for all humankind.

Russian international commitment to information and communication technology (ICT) security with the aim of preventing conflicts and a cyber-arms race between States is as old as the first resolution submitted by Moscow in 1998 to the United Nations. This document, which has been adopted by acclamation, expressed the concern over the malicious use of new technologies, in particular stressing the prevention of misuse of those tools for criminal or terrorist purposes.[112] Russian Federation promoted such new and compelling issue to the international forum of the United Nations and suggested that some important points and considerations should have been added, given the rising threats the technological world was advancing. Those further points were referring to the fact that the cyberspace could be used for military purposes and that the international community should start establishing some principles that could regulate such dangers. However, no document with biding effects had been adopted but the fact that such topic was finally discussed at the United Nations represented a possible path towards cooperation for the creation of a safer cyber and non-cyber environment. [113]

A further step was undertaken with the launch of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) in 2004. Under Moscow's point of view, this constituted a more promising international effort aimed at the adoption of rules of behavior in the field of cyberspace.[114] Beneath such project, Moscow recognized the principle according to which, because it was not realistically possible anymore to avoid the militarization of cyber utilities, the efforts would have been aimed at regulating the use of cyber tools.

Important results were achieved by Russian diplomats with the drafting of two important reports in 2013 and 2015. The report adopted in 2013 by the UN GGE group underlines that "international law, and in particular the Charter of the United Nations, is applicable" in cyberspace and that "state sovereignty and international norms and principles that flow from sovereignty apply

[112] Elena Chernenko in Hacks, leaks and Disruptions: Russian cyber strategies, Chaillot Papers, European Union Institute for Security Studies, Paris, October 2018, pag 43. Retrieved from: https://www.iss.europa.eu/content/hacks-leaks-and-disruptions-—-russian-cyber-strategies

[113] "Creation of a Global Culture of Cybersecurity and Taking Stock of National Efforts to Protect Critical Information Infrastructures", Resolution adopted by the General Assembly on 21 December 2009, http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/64/211

[114] Elena Chernenko in Hacks, leaks and Disruptions: Russian cyber strategies, Chaillot Papers, European Union Institute for Security Studies, Paris, October 2018, p. 44.

to state conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory".[115]

The report subsequently adopted in 2015 has been considered an important achievement of Russian diplomacy as it finally provided foundation to an internationally recognized governmental cyber code of conduct.[116] Specifically, the document includes a set of depoliticized norms among which the strong condemnation of internationally wrongful cyberattacks and the proliferation of malicious technologies with their hidden functions.[117]

Despite the important achievements that the United Nations Group of Governmental Experts have reached from its creation until nowadays, Moscow has looked as well to smaller pictures for more concrete and substantial actions through the usage of its diplomatic resources. Therefore, Russia have accompanied its multilateral cyber diplomacy with efforts both at regional and bilateral levels.

One of the most relevant results of this posture is recalled in the 2011 proposal advanced to the international community by Russia, China, Tajikistan and Uzbekistan as members of the Shanghai Cooperation Organization (SCO) for an international code of conduct for information security.[118] In 2015, a revised form of the Code was submitted to the UN General Assembly, stressing the urgent call for international consensus on digital norms.[119] Such document fully represents the development of the Russian foreign policy strategic thinking with regards to the cyber domain. Here, for example, the issue of terminology is addressed along with the promotion of the term "international information security" (replacing "cybersecurity") with the aim of enlarging the focus also on preventing the misuse of information and communication technologies for political purposes. Additionally, further points were stressing the importance of State sovereignty and territoriality in the fifth domain, urging Countries to refrain from the usage of information technology tools to interfere with the internal

[115] UN General Assembly, Resolution A/68/98, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," June 24, 2013, http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98

[116] Elena Chernenko in Hacks, leaks and Disruptions: Russian cyber strategies, Chaillot Papers, European Union Institute for Security Studies, Paris, October 2018, p. 44.

[117] UN General Assembly, Resolution A/70/174, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," July 22, 2015, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

[118] UN General Assembly, "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", A/66/359, https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf

[119] U.N. General Assembly, "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," U.N. Doc. A/69/273 (2015), http://www.un.org/Docs/journal/asp/ws.asp?m=A/69/723.

affairs of other Countries. Furthermore, it provides a detailed set of instructions for preventing military conflicts and the use of ITC by terrorists and cybercriminals.[120]

In particular, the view that Moscow promoted has to be framed in the discussion on the effects of new technologies on the widespread popular uprisings that recently took place, specifically the Arab Springs and the Color Revolutions. Russian Federation is part as well of two other important regional groups: the Collective Security Treaty Organization (CSTO) and BRICS. In both cases, Russia has been supported in its initiatives for the establishment of working groups on cooperation in the ICT sphere.[121] Parallelly, Russia established a network of bilateral agreements which were aimed at confidence building and trust enhancement with Countries such as China, India, South Africa, Belarus and Cuba.[122]

Furthermore, in 2013 Moscow signed the first ever cyber bilateral agreement with Washington which focused on technical aspects of the cooperation but leaving aside the issue of content. In particular, it provided the establishment of Computer Emergency Response Teams (CERTs) with the aim of information exchange as well as a channel for communication of incidents between the national Nuclear Risk Reduction Centres.[123] However, with the eruption of the conflict in Ukraine in 2014, those intentions got frozen and no further plan has been concluded.

By now, there are two main boundaries that prevent Russia from moving forward both on a multilateral and on a bilateral level: a conceptual and a trust issue. The first problem that Russian Federation encounters when it comes to agree upon norms is the wording and the meanings behind specific terms. As already mentioned, most of the Western Countries do not share the concepts offered by Russian proposals. However, because of the increasing threats that cyberspace is placing, more and more Western Countries are starting to share similar language to the Russian version, calling as well for a push in regulation and the right of governments to be able to control information within their jurisdiction.

In 2018, this view was for the first time publicly endorsed by the United Nations Secretary General Antonio Guterres, who affirmed that global rules should be established in order to minimize the impact of electronic warfare on civilians, because "the next war will begin with a massive

[120] Elena Chernenko in Hacks, leaks and Disruptions: Russian cyber strategies, Chaillot Papers, European Union Institute for Security Studies, Paris, October 2018, p. 46.
[121] Elena Chernenko in Hacks, leaks and Disruptions: Russian cyber strategies, Chaillot Papers, European Union Institute for Security Studies, Paris, October 2018, p. 47.
[122] Ibidem.
[123] Ellen Nakashima, "U.S. and Russia Sign Pact to Create Communication Link on Cyber Security", Washington Post, June 17, 2013, https://www.washingtonpost.com/world/national-security/us-and-russia-sign-pact-to-create-communication-link-on-cyber-security/2013/06/17/ca57ea04-d788-11e2-9df4-895344c13c30_story.html.

cyberattack to destroy military capacity [...] and paralyze basic infrastructure such as the electric networks."[124]

In response to the call launched by UN SG Guterres, Russia have introduced a new resolution A/RES/73/27 for convening in 2019 an Open-Ended Working Group (OEWG) that is meant to act on a consensus basis with the scope of progressing on and implementing the norms and principles of responsible behavior of States in cyberspace, parallelly to the ingrained UN GGE formula. The Russian setup intends to avoid the creation of "club agreement" and, unlike the selected formula endorsed by UN GGE, to encourage an inclusive, open and democratic negotiation process, while fostering the norms-building capacity of every State willing to be part of it.[125] The key goal of this resolution is to protect the digital interests of all States disregarding their different levels of technological development, while emphasizing the idea that aiding some countries to develop their own technological national capabilities is actually a matter of international security. A code of 13 rules is submitted with the aim of establishing foundations for peaceful interactions among States in the cyber environment, so to prevent wars, confrontations and any other aggressive actions.[126] By the implementation of this setup, Russian Federation had been able to succeeded in in getting International Information Security topic to grow beyond the narrow scope of the UN GGE.

Secondly, Russia has to deal with the hostile counterpart, made mainly of NATO Countries, which express very low trust in Russian intentions. This is so because of two main reasons. First of all, because of the several accusations of Russian interference into other Countries' systems, with on top of all the 2016 United States elections meddling. Secondly, because of the historical connection between Russian intelligence services and cybercriminals. Especially during the Perestroika in the mid-80s, the combination between the birth of an amateur computer culture and high-levels of mathematics education and unemployed scientists contributed to the creation of a fertile ecosystem for the growth of cybercrime.[127] According to Valeriano et al. and Professor Mark Galeotti, cyber hacking groups have become part of Russia's cyber tool-kit, because of their characteristic of being less easily detected as responsible of cyber-attacks. From such perspective, cyber proxies are cost-

[124] "UN Chief Calls For Regulatory Scheme For Cyberwarfare," Radio Free Europe/Radio Liberty, February 19, 2018. Retrieved from: https://www.rferl.org/a/un-guterres-calls-for-cyberwarfare-rules/29049069.html

[125] Samuele De Tomas Colatin, A surprising turn of events: UN creates two working groups on cyberspace, NATO Cooperative Cyber Defence Centre of Excellence, available at: https://ccdcoe.org/incyder-articles/a-surprising-turn-of-events-un-creates-two-working-groups-on-cyberspace/

[126] Anastasia Tolstukhina, Two Cyber Resolutions Are Better Than None, Russian International Affairs Council (RIAC), 2019. Available at: https://russiancouncil.ru/en/analytics-and-comments/analytics/two-cyber-resolutions-are-better-than-none/

[127] Valeriano B., Jensen, B., & Maness R., Cyber Strategy: The Evolving Character of Power and Coercion, New York: Oxford University Press, 2018, p. 117.

effective and they provide an extra-degree of anonymity, further complicating the attribution issue.[128] However, Russian is not a sole player of such kind, as China, Iran, North Korea and many others are blamed for following the same behavior. Nevertheless, the current status of affairs makes it extremely hard to achieve any global consensus on the matter.

2.1.2 The Chinese International Cyber Agenda

Official documents and national interests

Currently, among scholars and politicians there is a diffused fear of an aggressive behavior pursued by China in the international cyber stage which have led to a blind vision of China's intention in the fifth domain.[129] The actual behavior of the Country is not solely meant to be of a State seeking to use cyber espionage to catch up to its economic adversaries, but has the ultimate goal of maintaining a relevant, or even dominant, position in the Asia Pacific region and most of all within China itself.[130]

People's Republic of China has been putting major efforts in the enhancement of a cyber strategy devoted to security, regulation and control, within and outside borders. Indeed, cutting-edge technology development is key to China's economic and security goals. However, the Chinese central government recognizes that the advancement in technology have moved ahead of the government's capacity to control or regulate it; therefore, has started the process of building an extensive and comprehensive governance regime for cyberspace and information and communications technology in order to reconstruct a policy and regulatory framework spanning from cybersecurity, to digital economy and to the overall online media content.[131]

This has resulted in the adoption and implementation of a comprehensive set of laws – the Cybersecurity Law – in 2017 which covers both the topic of security (security review, encryption, securing critical infrastructure, online data management, data flow) and of digital economy. This consists in a starting point for setting a matrix of interlocking strategies, laws, measures, regulations,

[128] Valeriano B., Jensen, B., & Maness R., Cyber Strategy: The Evolving Character of Power and Coercion, New York: Oxford University Press, 2018, p. 115-117.

[129] Ibidem, p. 144.

[130] Ibidem, p. 143.

[131] Elsa Kania, Samm Sacks, Paul Triolo, China's Strategic Thinking on Building Power in Cyberspace, Cybersecurity Initiative, New America, 2019. Retrieved from https://www.newamerica.org/cybersecurity-initiative/blog/chinas-strategic-thinking-building-power-cyberspace/.

and standards. Such strategy has been unfolded both nationally and internationally and is mainly aimed at the protection of the Chinese "network sovereignty"[132].[133]

There is a fundamental posture beneath China's strategy which is not solely applied to the cyberspace but to the whole Chinese international security system and deals with the concept of national sovereignty and the posture of Western Countries conceived as superior to the rest of the world.[134] Such view is, as well, shared by the Countries part of BRICS.

As expressed in the official document of the National Cybersecurity Strategy released in 2016 by the Cyberspace Administration of China (CAC), cyberspace consists in a new, but Chinese owned, territory for national sovereignty and therefore needs to be taken care of by exerting cyber-control.[135] The National Security Strategy introduces a community view of cybersecurity, based on the condition according to which China depends on the Internet as much as on the West.[136]

What emerges from the document is the strong Chinese belief that the development of the Internet has been unbalanced, resulting in the fact that technology and security are mostly controlled by others, namely Western Countries, reflecting the common desires of the absolute majority of countries worldwide, but not particular interests. According to the Chinese position, there are few Western Countries which make use of their information technology superiority, as well as their power over the international Internet core infrastructure and its resource allocation, to monopolize the agenda-setting process, rule-making power, and the international discourse.[137]

Such discourse explains that China suffers a significant imbalance in the distribution and allocation of resources such as root servers and other global Internet infrastructures resources. Chinese government, indeed, argues that the difference in Internet development capabilities between various Countries is deep, pushing wider the digital divide. So far, developing Countries have found themselves under the control of majorly developed Countries in terms of cybersecurity and

[132] As in the case of Russia, China as well utilizes in its own language specific terms over the topic of cyberspace. In particular, the wording "network sovereignty" is the translation from Chinese of 网络主权, *wangluo zhuquan*, and comprises a wider meaning of cyberspace involving the whole panorama of information technology and ICT.

[133] Elsa Kania, Samm Sacks, Paul Triolo, China's Strategic Thinking on Building Power in Cyberspace, Cybersecurity Initiative, New America, 2019. Retrieved from https://www.newamerica.org/cybersecurity-initiative/blog/chinas-strategic-thinking-building-power-cyberspace/

[134] Rogier Creemers, National Cyberspace Security Strategy, December 2017, translation from the official National Cybersecurity Strategy released by Cyberspace Administration of China (CAC) available at the following link http://www.cac.gov.cn/2016-12/27/c_1120195926.htm

[135] China publishes first National Cybersecurity Strategy, Report by United States Information Technology Office (USITO), available at: http://www.usito.org/news/china-publishes-first-national-cybersecurity-strategy

[136] Valeriano B., Jensen, B., & Maness R., Cyber Strategy: The Evolving Character of Power and Coercion, New York: Oxford University Press, 2018, p. 169.

[137] Rogier Creemers, National Cyberspace Security Strategy, December 2017, translation from the official National Cybersecurity Strategy released by Cyberspace Administration of China (CAC) available at the following link http://www.cac.gov.cn/2016-12/27/c_1120195926.htm

development, which have brought them in an advantageous position. In conclusion, the international respect for cyber sovereignty is a necessary requirement in order to oppose cyber hegemony and monopoly.[138]

Defending cyberspace sovereignty is fundamental as it is aimed at protecting national security and critical information infrastructure (CII). The ultimate scope includes, but it is not limited to, basic communication and broadcasting networks, energy, finance, transportation, education, scientific research, hydraulic systems, industrial manufacturing, healthcare, social welfare, public service, and critical information and Internet application systems for government agencies. Furthermore, in order to ensure the protection of CII, the cybersecurity review regime is meant to expand in the future.

Summing up the 2016 National Cybersecurity Strategy, it is possible to say that China is getting ready to address three main factors which are constantly under threat, namely political stability, economic progress and culture solidarity.[139] What the strategy document is mentioning is the fact that competition is expanding in the cyberspace and there are some Countries, especially smaller ones, which are aggravating a possible cyber arms race. Therefore, what emerges from the conceptualization of the cyber strategy, is that China is a rising power but detains hidden vulnerabilities.

Despite the current status of affairs brings experts to commonly address China as a "Cyber Dragon", the reality appears to be slightly different. By looking at the type of cyber operations that China had put into practice, Valeriano et al. demonstrate that the Country does not behave in an aggressive way by promoting cyber violence. On the contrary, such actions are aimed at defending the digital domain and State's interest targeting internal actors or to catch up in the technological sector where the State is not allowed to acquire technological knowledge in a legal way.[140] According to a study on the type of cyber actions pursued by China, it is clear that the Country fancies cyber espionage rather than cyber degradation, therefore, choosing to conduct covert operations to leverage sufficient deniability and ambiguously signaling in order to alter the long-term balance of power.

Given the awareness of Chinese vulnerabilities and their sense of insecurity in the cyber domain, they have taken the opportunity of using this new space to catch up to the West. The Chinese

[138] Lu Wei, Persisting in Respect for the Principle of Cyber Sovereignty, Promoting the Construction of a Community of Common Destiny in Cyberspace, translation of the document released by the vice-director of the Central Propaganda Department, the Director of the Office of the Central Leading Group for Cybersecurity and Informatization, and the Director of the Cyberspace Administration of China: https://chinacopyrightandmedia.wordpress.com/2016/03/02/persisting-in-respect-for-the-principle-of-cyber-sovereignty-promoting-the-construction-of-a-community-of-common-destiny-in-cyberspace/

[139] Valeriano B., Jensen, B., & Maness R., Cyber Strategy: The Evolving Character of Power and Coercion, New York: Oxford University Press, 2018, p. 149.

[140] Valeriano B., Jensen, B., & Maness R., Cyber Strategy: The Evolving Character of Power and Coercion, New York: Oxford University Press, 2018, p. 147.

Cyber doctrine can be summed up into three main tasks. The first deals with espionage. In this case, the aim of cyber intrusion is to identify the vulnerabilities of another Country and exfiltrate its data in order to obtain informational advantages. This approach relies strongly on the relationship between information and power, intending information in a globalized world as even more integrated with development.

The second task deals with targeting communications networks in order to constrain the adversary. This requires adaption, analysis and application of the information gained from the espionage process, reiterating it in a way that China can show to other Countries that it knows which are its vulnerabilities so to alter the balance of information between the two sides in favor of the attacker. Finally, the third task consists in using such information advantage as a force multiplier, even on different levels and domains such as economic or military one.[141]

In a very paradoxical way, the fifth domain consists for China both of a critical capability and a long-term vulnerability. While cyber capacities are evidently a strategic advantage for China, its usage as a tool for economic espionage could turn as a misfortune. Indeed, looking at such posture in the long-term, vulnerability could represent a bigger problem due to the fact that stealing intellectual properties from other Countries does not guarantee a robust economic growth in the future. Indeed, stealing mass amounts of information makes the country dependent on another country's innovation, expanding such trap of dependency even in the security sector.[142]

International Initiatives

At the 2015 World Internet Conference in Wuzhen, China's president Xi Jinping, focusing on the international dimensions of China's cyber strategy, expressed a set of four principles aimed at reforming the existing international Internet governance system: respect for cyber sovereignty, peace and security, openness and cooperation, and the process of building a good order.[143]

According to the Chinese President Xi Jinping, those concepts should be paired with five action proposals: "1. Accelerate the construction of a global network infrastructure, and stimulating interconnection and interactivity; 2. Build shared platforms for online cultural interaction, and

[141] Ibidem, p. 152-153

[142] Ibidem, p. 149.

[143] Lu Wei, Persisting in Respect for the Principle of Cyber Sovereignty, Promoting the Construction of a Community of Common Destiny in Cyberspace, translation of the document released by the vice-director of the Central Propaganda Department, the Director of the Office of the Central Leading Group for Cybersecurity and Informatization, and the Director of the Cyberspace Administration of China: https://chinacopyrightandmedia.wordpress.com/2016/03/02/persisting-in-respect-for-the-principle-of-cyber-sovereignty-promoting-the-construction-of-a-community-of-common-destiny-in-cyberspace/

stimulating exchange and mutual learning; 3. Promote innovation and development in the online economy, and stimulating common flourishing; 4. Guarantee cybersecurity and stimulate orderly development; 5. Build the Internet governance system, and stimulate fairness and justice”.[144]

Currently, the Chinese government is on the verge of further advancing another aspect of the aforementioned strategy, which consists in operationalizing the concept of cyber sovereignty at the international level, suggesting that China has been planning to push internationally for further cooperation on cyber issues.[145]

For what concerns its international behavior towards global governance in the fifth domain, China has been putting effort in the discussion on what constitutes an acceptable notion of State’s behavior among a group of government experts at the United Nations by strongly reaffirming that the United Nations should play a central role in the regulation of international cyber space behavior.[146]

China’s intentions consist in participating in the discussion on how to build a decent and working international Internet governance on an equal footing together with the rest of the world. Such position is not new and not limited to the fifth domain, but, as already explained, finds its origin in several Chinese policies and practices in world affairs, frequently expressed by its position of non-interference in other Countries’ sovereignty.

The Chinese government is one of the primary norm entrepreneur of the network sovereignty concept and has long sought international legitimization of the concept to validate both its domestic and international agenda. After years of Beijing promoting Internet sovereignty, the concept is now part of international debates, even though its legitimacy is still critically questioned. Essentially, network sovereignty is still in the norm emergence phase, being the content and language of this concept evolving over the past two decades and reflecting ongoing contestation among States’ digital policy prerogatives.[147]

Furthermore, such posture is shared by several Countries in the international panorama, and claims that massive cyber surveillance and penetration has undermined their security and social

[144] Elsa Kania, Samm Sacks, Paul Triolo, China’s Strategic Thinking on Building Power in Cyberspace, Cybersecurity Initiative, New America, 2019. Retrieved from https://www.newamerica.org/cybersecurity-initiative/blog/chinas-strategic-thinking-building-power-cyberspace/

[145] Ibidem.

[146] Segal A., Year in Review: Chinese Cyber Sovereignty in Action, Council on Foreign Relations, 2018. Retrieved from: https://www.cfr.org/blog/year-review-chinese-cyber-sovereignty-action

[147] Sarah Mckune, Shazeda Ahmed, The Contestation and Shaping of Cyber Norms Through China’s Internet Sovereignty Agenda, International Journal of Communication 12(2018), 3835–3855. Retrieved from: https://www.google.it/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwjKuqHLwcjkAhURtosKHVq9BBcQFjAAegQIAhAC&url=https%3A%2F%2Fijoc.org%2Findex.php%2Fijoc%2Farticle%2Fdownload%2F8540%2F2461&usg=AOvVaw3TqT55DKCoVsK9CKoxjI1f

stability. They, indeed, stand behind the cyber sovereignty legality.[148] Not surprisingly, network sovereignty has gained a significant traction alongside China's increasing global prominence and economic clout. Norm contestation is a natural result of rising powers' interest in challenging inadequate representation in international forums and normative content established by prior hegemons.

Surely, China has placed itself as a promoter of the critique towards the insufficient non-Western representation in Internet governance, the dangers of the United States as an almost "unchallenged cyber hegemon" and the inapplicability of "Western values" in the Internet sovereignty discourse. Hence, Beijing does not only intend to stop Countries like the United States to interfere with its domestic cyber policies, but it also proposes itself in order to set the tone on the modalities according to which the rest of the world should govern the Internet.

China has advocated in international forums the Internet sovereignty model as the polar opposite of "Internet freedom", which many governments link to the facts of the Arab Spring or the Color Revolutions.[149] In order to exert influence on this, China serves itself of the direct outreach to foreign governments, as well as massive investments in Internet technologies through transnational initiatives such as the Belt and Road initiative, extensive military-to-military cooperation, and growing participation in international institutions.[150]

For example, in 2015, Tanzania has been chosen as a pilot country for the China–Africa capacity-building process, so that China could foster collaboration around cyberspace governance. Since then, Tanzania has enacted a cyber-crime law and subsequent restrictions on Internet content and blogging activity parallelly to China's content controls. Among other Countries where China has been pursuing heavy investment campaigns, such as Nigeria, Egypt, Ethiopia and Sudan, it is possible to register a strong engagement in aggressive online content control. What seems to be true, is that China's model appeals to these Countries because it provides them with tools to take control of an open internet, as online platforms used for terrorism and political dissent threaten national stability.[151]

The main problem with the model that China offers to the world is that it crashes headlong into the foundational principles of the Internet in market-based democracies, such as online freedom,

[148] Lu Chuanying, China's Emerging Cyberspace Strategy, The Diplomat, 2016. Retrieved from: https://thediplomat.com/2016/05/chinas-emerging-cyberspace-strategy/

[149] Sarah Mckune, Shazeda Ahmed, The Contestation and Shaping of Cyber Norms Through China's Internet Sovereignty Agenda, International Journal of Communication 12(2018), 3835–3855. Retrieved from: https://www.google.it/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwjKuqHLwcjkAhURtosKHVq9BBcQFjAAegQIAhAC&url=https%3A%2F%2Fijoc.org%2Findex.php%2Fijoc%2Farticle%2Fdownload%2F8540%2F2461&usg=AOvVaw3TqT55DKCoVsK9CKoxjI1f

[150] Samm Sacks, Beijing Wants to Rewrite the Rules of the Internet, the Atlantic, 2018. Retrieved from: https://www.theatlantic.com/international/archive/2018/06/zte-huawei-china-trump-trade-cyber/563033/

[151] Ibidem.

privacy, free international markets, and broad international cooperation. Moreover, China's model may also reveal not to be effective in delivering on its goals: as an example, government-imposed content-control measures have proven to be poor tools in fighting online extremism. Additionally, filtering or removing online content has not been successful, making it ineffective and cost-prohibitive.[152]

After the fifth UN GGE standoff in 2017, China has not fully abandoned the international mission but has contemporarily diverted into an environment of more likeminded Countries with which, through regional tools, have better chances of agreement and cooperation. In that sense, the Shanghai Cooperation Organization has been crucial to the incubation and strengthening of the network sovereignty concept and norm advancement.

The SCO founded in 2001 is currently composed by China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan, Uzbekistan, India and Pakistan. Its main focus pertains to the topic of security, by "combating terrorism, separatism, and extremism" – the "three evils" – and on the creation of "a democratic, fair and rational new international political and economic order"[153] At the regional level, among SCO members, the concept of network sovereignty enjoyed the prominence, coherence, and environmental conditions which were initially absent on the wider international stage.

Hereby, the SCO has served as a first staging ground in the norms elaboration and diffusion processes, uniting with the concept of "information security" lodged by Russia. An important step was undertaken in 2009 with the adoption of the Agreement on Cooperation in the Field of International Information Security, elaborating main threats and areas of cooperation.[154] Additionally to that, a SCO's operational unit – the Regional Anti-Terrorist Structure – has been established and pursues, among other functions, Anti-Cyber-terror Exercises.

Finally, the SCO has served as a platform to disseminate Member States' shared digital norms to the international community. SCO's Member States twice submitted at the United Nations General Assembly for debate an International Code of Conduct for Information Security, once in 2011 and again in 2015, with the aim of creating consensus around the two concepts of network sovereignty and information security.[155]

[152] Samm Sacks, Beijing Wants to Rewrite the Rules of the Internet, the Atlantic, 2018. Retrieved from: https://www.theatlantic.com/international/archive/2018/06/zte-huawei-china-trump-trade-cyber/563033/

[153] Shanghai Declaration on the Establishment of the SCO, Shanghai Cooperation Organization, 2001, paragraph 2. Retrieved from: http://eng.sectsco.org/load/193054/

[154] Sarah Mckune, Shazeda Ahmed, The Contestation and Shaping of Cyber Norms Through China's Internet Sovereignty Agenda, International Journal of Communication 12(2018), 3835–3855. Retrieved from: https://www.google.it/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwjKuqHLwcjkAhURtosKHVq9BBcQFjAAegQIAhAC&url=https%3A%2F%2Fijoc.org%2Findex.php%2Fijoc%2Farticle%2Fdownload%2F8540%2F2461&usg=AOvVaw3TqT55DKCoVsK9CKoxjI1f

[155] Ibidem.

Internet governance, national defense, and internal influence reflect the regime priorities of China's network sovereignty agenda, which however shows some contradictions. For example, China advocates the principles of non-interference in States' internal affairs and asserts the importance of equitable Internet governance, international law and international organizations in the process of norms formation in the fifth domain. Yet, China has itself relied heavily on extra-territorial digital intrusions in order to achieve its goals. It is claimed that China has rejected consistently the application of human rights principles to its domestic information controls and other digital authoritarian practices, branding such practices with a double-standard approach. Those accusations brings on the question whether an Internet sovereignty norm advances international law and non-interference or simply serves as a license to control and repress with impunity.

Notwithstanding this debate, it appears that thanks to China's rhetorical and economic support, the principle of Internet sovereignty has reached the status of emergence as a norm. The prospects for diffusion among a wider international constituency can be consolidated by the decline of Western normative leadership within the international arena and the Chinese growing financial and political power. Nevertheless, Internet sovereignty still lacks the criteria of legality that would strengthen its acceptance as a legal norm and finds contestation from several opponents.

2.1.3 The American Cyber Strategy

Official documents and national interests

Cyberspace was born in the 1960s in the United States. The Internet was called ARPANET and was used by a small number of users. Only thirty years later, Internet has become the most powerful tool for networking and connecting, mostly made in USA. Internet history has been shaped on top of the ideas of interconnectedness and globalization and, by providing an open source of networks, the United States have enjoyed a privileged position of such open source. However, because the Internet has become increasingly global, the United States have mostly lost the total control on it. This hypothesis is confirmed by the constant attacks that users are making to other computers and systems with, among different aims, espionages and disruptions.[156]

Substantially, the idea behind an open Internet has proven to be a double-edged sword: on one side, it allowed boundless connectivity especially in the interest of commerce and economic growth,

[156] Live FireEye Cyber Threat Map, available at: https://www.fireeye.com/cyber-map/threat-map.html

while on the other side, it facilitated extensively espionage and counter espionage.[157] However, despite the Internet has become a global good, plenty of Countries still contest the advantages that the United States enjoy over such powerful tool. As an example, the majority of IP addresses and cables are located on the American soil, and this is arguably going against the principle of an open and worldwide accessible source.

The position that the United States cover within the international system, by being the most economically, military and technologically developed Country in the world, makes it a highly appealing target for attacks. Moreover, because the United States are heavily reliant on technology and connectivity, they have become more attractive as cyber target. By their experience, they have recognized the emergence of both information warfare and cyber warfare, and took actions against them.

The approach that the United States have been embracing acknowledges an ongoing strategic environment which is "characterized by challenges to the free and open international order and the emergence of long-term, strategic competition between nations."[158]

Principally, the key challenge to the security of the Country consists in the posture adopted by China and Russia towards the entire international system. According to the 2018 US National Defense Strategy, China is claimed of leveraging military modernization, influence operations, and predatory economics to coerce neighboring Countries in order to rearrange the Indo-Pacific region to their advantage. At the same time, Russia is taking advantage of its veto power to exert influence and authority over its periphery in terms of economic, governmental and diplomatic operations in order to reshape the international system to its favor.[159]

Finally, the document claims that the current strategic environment suffers from the weakening of the post-World War II international order with the consequence of the fall of the constructed free and open international system aimed at safeguarding people and their liberty from aggression and coercion. Such responsibility of disruption is even shared by rogue regimes like the ones of North Korea and Iran, which contribute to the destabilization of their region by exerting coercion and increasing the chances of a threatening environment.

Given such complex status of affairs, the United States Department of Defense, along with the President of the United States Donald J. Trump, has set some objectives among which the

[157] Valeriano B., Jensen, B., & Maness R., Cyber Strategy: The Evolving Character of Power and Coercion, New York: Oxford University Press, 2018, p. 190.

[158] Mattis Jim, Summary of the 2018 National Defense Strategy of the United States of America, Department of Defense of the United States of America, available at: https://apps.dtic.mil/dtic/tr/fulltext/u2/1045785.pdf

[159] Mattis Jim, Summary of the 2018 National Defense Strategy of the United States of America, Department of Defense of the United States of America, available at: https://apps.dtic.mil/dtic/tr/fulltext/u2/1045785.pdf

prioritization of investments in resilience, reconstitution, and operations to assure the development of their own cyberspace capabilities and the continued integration of those into the full spectrum of military operations.[160] By now, the United States confirmed itself as the most equipped Country in the world with the strongest cyber force, financing cyber operations with $7,000 million per year and employing circa 9,000 people as its cyber personnel.[161]

By means of the analysis of further official papers, it is possible to acknowledge the meaning of technology to the United States as a developing tool and as an instrument for maintaining its leading role within the International Community. Technological innovation is of fundamental importance as overtime the United States have created extensive dependencies on information technologies. However, this dependency has increased the level of security vulnerabilities in many domain among which the economic and the military ones.[162]

On May 11th, 2017, the Office of the Press Secretary of the White House had released a Presidential Executive Order, addressing the issues of strengthening the cybersecurity of Federal Networks and of critical infrastructure. In section n. 3 of the document "Cybersecurity for the Nation", the United States' President expresses the need of promoting an open, reliable and secure Internet that fosters efficiency and innovation, by upholding national privacy. In order to achieve this, the President emphasizes the longing of protection of national data through deterrence.[163]

Deterrence is a central posture in the American counter-intrusion policy, mainly expressed in the Cyber Deterrence Task Force. The Task Force on Cyber Deterrence scrutinizes the requirements for deterrence of the full range of potential cyberattacks against the United States and its allies and partners. Moreover, it performs the task of identifying critical capabilities which are necessary to support deterrence actions, warfighting and hindering the escalation against highly cyber-capable adversaries.[164]

Such interest in cyber deterrence has been growing, especially due to the fact that the United States have experienced a number of cyberattacks and very costly cyber intrusions. Examples are

[160] Ibidem.

[161] Cyber Warfare Infographics, Valdai Discussion Club, 27.08.2019, available at: http://valdaiclub.com/multimedia/infographics/cyber-warfare/

[162] Remarks as delivered by the Honorable James R Clapper Director of National Intelligence. Senate Select Committee on Intelligence – IC's Worldwide Threat Assessment Opening Statement, Tuesday Feb 9, 2016. Retrieved from: https://www.dni.gov/files/documents/2016-02-09SASC_open_threat_hearing_transcript.pdf

[163] President Trump, The White House – Office of the Press Secretary, Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, May 11, 2017. Retrieved from: https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

[164] Final Report of the Defense Science Board (DSB) Task Force on Cyber Deterrence, Office of the Secretary of Defense, February 2017. Retrieved from: https://www.acq.osd.mil/dsb/reports/2010s/dsb-cyberdeterrencereport_02-28-17_final.pdf

provided by the alleged Russian interference in the 2016 Presidential elections and the Chinese theft of intellectual properties from American companies. Additionally, the sense of fear is constantly increasing because future intrusions and attacks will be of different type, as adversary capabilities will be continuing to quickly grow.

According to Task Force publications, United States faces three types of cyber deterrence challenges: the first comes from major powers like China and Russia, the second comes from regional powers like Iran and North Korea and, finally, the third one involves a range of States and non-state actors. More specifically, Russia and China have significant and growing abilities that could harm the United States network system via cyberattacks and also contrast United States military responses to any of such attacks.[165] Facing this, the United States have already developed enhanced capabilities that would reduce the pervasive cyber vulnerabilities of the American critical infrastructure. However, the government still feels its strategic position very threatened.

As far as Countries like Iran and North Korea are concerned, the United States government, taking into account their growing potential to conduct catastrophic attacks on United States critical infrastructure, is working also hand in hand with the private sector to defend and boost the security of the American cyber domain. Not of less importance, the non-State actors which have the capacity of pursuing persistent cyber-attacks against the United States are part of this urgent priority of assuming a cyber deterrence posture.[166]

Each of those examples are stressing the frequency with which cyber intrusions occur on a daily basis in both the United States and globally, including the ones that are conducted by nations as part of their espionage programs. Moreover, such attacks are considered risky due to their effects in disrupting the flow of electricity, money, communications, fuel and water and, thus, harming civil society – what is technically defined as the damage of "critical infrastructure".

International Initiatives

According to the United States Administration office, there are five major priorities on the topic of cybersecurity that should be pursued: the protection of the country's critical infrastructure from cyber threats; the improvement of the ability to identify and report cyber incidents in order to be able to respond in a timely manner; the engagement with international partners to promote internet

[165] Final Report of the Defense Science Board (DSB) Task Force on Cyber Deterrence, Office of the Secretary of Defense, February 2017. Retrieved from: https://www.acq.osd.mil/dsb/reports/2010s/dsb-cyberdeterrencereport_02-28-17_final.pdf

[166] Final Report of the Defense Science Board (DSB) Task Force on Cyber Deterrence, Office of the Secretary of Defense, February 2017.

freedom on one side and secure cyberspace on the other; the securement of federal networks; and finally, the development of a deeper partnership with the private sector.[167]

The United States government has expressed several times its own belief in international engagement and cooperation on this matter. Following the establishment of the fifth domain, the United States have promptly called cyberspace as militarized, exactly as air, land, sea and space, recognizing the threat and possible confrontation in such new domain. Moreover, because cyberspace can host both national and international threats, by crossing international boundaries, the US calls upon the importance of the engagement with different partners.

In particular, such posture consists of participating in the development of international norms of behavior in cyberspace, the promotion of collaboration in cybercrime investigation though the modernization of the Mutual Legal Assistance Treaty[168] and the international cybersecurity capacity building program. Most of all, the United States have presented itself as a leading Country able to guide towards the process of forging criteria for a solid international cyber governance. Nevertheless, its efforts have already been put into practice through NATO operations in order to enhance cybersecurity measures in the view of the core task of collective defense.[169]

The approach that has been adopted by the United States government perceives cybersecurity as any other issue of foreign affairs, which directly impact the life of American people. According to Simran Maker[170], cybersecurity should be among the top priorities in the agenda like any other issue concerning security on a broader scale.

To combat adversaries, more should be done in order to collaborate with traditional allies that can be cyber allies as well. Only by working with international partners, cyber norms can be created and carried out in a meaningful way. The only way to pursue this is through the commitment of the International Community to cyber cooperation, and the United States strongly believe that this rhetoric should be met with appropriate investments and resources.[171] Cyber defense can be improved and offense can be upgraded. The best way through which the United States can improve their cybersecurity is by including the amelioration of its relationship with those who are adversaries in cyberspace.

[167] Obama B., Publication on Foreign Policy Cyber Security, the White House, retrieved from https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity

[168] MLATs are bilateral agreements that allow generally the exchange of evidence and information in criminal and related matters.

[169] NATO, “Cyber Defence”, 2017, February 17, NATO Official Website. Retrieved from: http://www.nato.int/cps/en/natohq/topics_78170.htm

[170] He is part of the National Committee on American Foreign Policy.

[171] Simnar R. Maker, New frontier in defense: cyberspace and U.S. Foreign Policy, A national committee on American Foreign Policy Report, May 2017. Retrieved from https://www.ncafp.org/2016/wp-content/uploads/2017/05/Cyberspace-and-US-Foreign-Policy-Report-May-17.pdf

The United States have been showing interest for a global cyber governance by occupying a leading role in the United Nations, by being part of the UN GGE process and proposing resolutions and possible path for cybersecurity commitment.[172] There are some specific principles that the United States have brought to the attention of the United Nations' Members, which have been set since Obama's presidency and have been largely shared in the diplomatic forum. First, international law principles do apply in cyberspace, therefore cyberspace should not be conceived as a "law-free" zone where anyone can conduct hostile activities without rules or restraint.[173] As technology have already changed the way in which international law is applied, the United States government calls for the articulation and building consensus around how it should be applied and reassessed, whenever is needed, its additional understanding. Such global consensus-building process should be aimed at the promotion of stability in this and other areas, because of the pervasive characteristic of technology in human life. Second, for what concern the *jus ad bellum* (law of going to war) and the *jus in bello* (law in conducting war), the American representatives have expressed what follows. Cyber activities may in certain circumstances constitute the use of force within the meaning of Article 2(4) of the UN Charter[174] and customary international law, especially in cases in which the effects are similar to the ones produced by kinetic weapons. Additionally, United States recognizes that State's national right of self-defense, as in Article 51 of the UN Charter, may be triggered by computer network activities that correspond to an armed attack or imminent threat thereof. Finally, *jus in bello* rules apply to computer network attacks in the context of an armed conflict in order to regulate the use of cyber tools in hostilities; the principles of necessity and proportionality would limit the employment of force in the case of self-defense, and would regulate what may constitute a lawful response under the circumstances.[175] Third, the United States are calling for States' responsibilities for the activities that are undertaken through "proxy actors" – namely those who acts on State's instruction or under its direction or control.[176]

Along with those more general principles of international law, the United States have been promoting a set of four voluntary and non-binding norms that responsible state behavior should comply with in peacetime. "First, a State should not conduct or knowingly support cyber-enabled theft of intellectual property, trade secrets, or other confidential business information with the intent

[172] Further information on role and structure of UN GGEs are displayed at paragraph 3.3 of this thesis.

[173] Hongju Koh, Harold, International Law in Cyberspace, Yale university, 2012. Faculty Scholarship Series, 4854. Retrieved from: https://digitalcommons.law.yale.edu/fss_papers/4854

[174] Charter of the United Nations, San Francisco, 1945, Art. 2, paragraph 4.

[175] Hongju Koh, Harold, International Law in Cyberspace, Yale university, 2012. Faculty Scholarship Series, 4854. Retrieved from: https://digitalcommons.law.yale.edu/fss_papers/4854

[176] Hongju Koh, Harold, International Law in Cyberspace, Yale university, 2012. Faculty Scholarship Series, 4854. Retrieved from: https://digitalcommons.law.yale.edu/fss_papers/4854

of providing competitive advantages to its companies or commercial sectors. Second, a State should not conduct or knowingly support online activity that intentionally damages critical infrastructure or otherwise impairs the use of critical infrastructure to provide service to the public. Third, a State should not conduct or knowingly support activity intended to prevent national computer security incident response teams (CSIRTs) from responding to cyber incidents. A State also should not use CSIRTs to enable online activity that is intended to do harm. Fourth, a State should cooperate, in a manner consistent with its domestic and international obligations, with requests for assistance from other States in investigating cybercrimes, collecting electronic evidence, and mitigating malicious cyber activity emanating from its territory."[177]

Despite being voluntary and non-binding norms with the aim of supplementing international law, such proposal advanced in the 2015 UN GGE report have fallen into disagreement and discussions, especially with regards to the latest events of intrusions and interference.

Nevertheless, the United States had promoted a similar approach within the North Atlantic Organization Treaty environment being supported by other Countries which share more similar views on the matter. The acknowledgement of the necessity of strengthening cyber capabilities to defend against cyber-attacks firstly occurred at the 2002 Prague summit and then became an increasingly important topic within the NATO agenda, making cyber defense a core part of the collective defense principle and declaring that a cyber-attack could lead to the invocation of the collective defense clause – Article 5 – of NATO's founding treaty. Furthermore, in 2016, Allies recognized cyberspace as a domain of military operations, and further pledged to enhance the cyber defenses of their national networks and infrastructure as a matter of priority.[178]

There are three main tasks for the Alliance that are laid out in the NATO's Strategic Concept: collective defense, crisis management and cooperative security.[179] In order to carry on those, NATO has been putting efforts into achieving the military end of operating in cyberspace, by relying not only on military means or stakeholders. Examples are the creation of the Cyberspace Operations Centre, which serves as a provider for cyberspace situational awareness, centralized planning for the cyberspace aspects of Alliance operations and missions, and coordination for cyberspace operational concerns, or the NATO Cooperative Cyber Defense Center of Excellence, which retains the

[177] Remarks on International Law and Stability in Cyberspace; Legal Adviser Brian J. Egan; Berkeley Law School, California, 2016. Retrieved from: https://2009-2017.state.gov/s/l/releases/remarks/264303.htm

[178] Brent L., NATO's role in cyberspace, NATO Review, 2019. Available at: https://www.nato.int/docu/review/2019/Also-in-2019/natos-role-in-cyberspace-alliance-defence/EN/index.htm

[179] "Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation", Adopted by Heads of State and Government in Lisbon, NATO, 2010. Retrieved from: https://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf

responsibility for identifying and coordinating education and training solutions in the field of cyber defense operations for all NATO bodies across the Alliance.[180]

Finally, in the view of improving cyber defense capabilities even outside the military sphere, NATO has encouraged the adoption of the Cyber Defense Pledge to exchange information and best practices as well as leveraging innovative practices from academia and private sector. To fully achieve this goal, NATO has been conjointly working with several other partners among which the European Union, as established by the Joint Declaration on NATO-EU Cooperation of 2016.

2.2 Drawing conclusions on the analyzed States' strategies: common or divergent paths?

By the analysis of the official documents of the national cyber strategies of the States that have been taken into account, it is possible to acknowledge that in the international panorama there is a full recognition of the threats and the dangers that the cyber domain presents. However, despite the common threat and contrary to the assumptions of the liberal theory, no shared collective security arrangement has been adopted yet. At the same time, Countries have the feeling of operating in an anarchic system, as the realist theory suggests. Nevertheless, the sense of fear is produced by the perception that they have of the *Self* and of the *Other*, which brings them into developing different national strategies, based on a subjective understanding of the other's intentions. In practice, the constructivist approach is instructive in this case to explain the reasons for which Countries offer diversified conceptualization on the matter of cybersecurity, with consequential actions at the international and regional level.

In practice, there are two main obstacles that arise from perceptions and subjective ideas and make cooperation difficult to be implemented. The first issue is the widespread lack of trust among States at the level of cyberspace. This is inevitably determined by the fact that there is an acquiescence on the use of cyber tools between States but there is no clarity or transparency on that. Because of the difficulties related to the issue of attribution, it is difficult to hold someone responsible and therefore, due to lack of information, Countries are simply not trusting each other. Aware of that, in order to cut off the distrust among each other, NATO Countries have decided to share information in order to set the path towards the same objective and increase the overall level of trust.

The second issue deals with language and terminology. Despite some may advocate this as irrelevant, it is in fact very much relevant for the following reason. Such problematic subsist not only

[180] Brent L., NATO's role in cyberspace, NATO Review, 2019. Available at: https://www.nato.int/docu/review/2019/Also-in-2019/natos-role-in-cyberspace-alliance-defence/EN/index.htm

because there is an actual difficulty with different languages, which anyway could be overcome by translators, but the real problem lays on the basis that what may seem to be the correct translation of a certain term, in another language has a very much different meaning. This is widely demonstrated by Russian and English versions of cyber and information warfare, as they are used dissimilarly and with different meanings.

It is evident that the national strategies are emerging from a rhetoric which is characterized by fear and accusation, especially towards the Country that, most of all, had the chance of setting the rules of the games in the fifth domain due to mainly historical and technical reasons. For example, the posture that China and Russia, among many others, have adopted towards the United States is based on the accusation of imposing its structure and control over the Internet, therefore they strongly call for inclusion and participation in the decision making process of Internet regimentation and advocate a fully recognized position in influencing the cyber global governance scenario. Such rhetoric is very much embraced nowadays, in a world in which the so-called Westphalian order is constantly challenged, where emerging countries now exert an increasing pressure in the classical scenario of international relations.

The only way of pursuing the establishment of a cyber regime is by accepting the constructivist idea that the structure of the system in an ongoing process, and not necessarily a static and anarchic system, which can change following the ideas that the States develop and embrace. Mediating perceptions and combining ideas are possible solutions for moving closer States' different postures and for guiding them toward a commonly shared normative system, which require time and appropriate tools.

Despite this being a rather new topic, there are previous experiences in other fields that could actually provide an example of *modus operandi* for future performances. The conclusion is that what Countries need to make is a step forward the simple adoption of United Nations General Assembly resolutions, because they do not possess a binding mandate, by committing to those initiatives that can concretely set the ground for actions that could regulate transnational interaction, reducing mistrust and increase commonly shared views and values. At the regional or local level, such pattern seems to be more able to flourish due to the fact that groups of countries shares similar backgrounds, ideas and perceptions. Indeed, Russia, China and the United States have committed already to such regional process, as demonstrated by the Shanghai Cooperation Organization[181] and the NATO

[181] Sarah Mckune, Shazeda Ahmed, The Contestation and Shaping of Cyber Norms Through China's Internet Sovereignty Agenda, International Journal of Communication 12(2018), 3835–3855. Retrieved from: https://www.google.it/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwjKuqHLwcjkAhURtosKHVq9BBcQFjAAegQIAhAC&url=https%3A%2F%2Fijoc.org%2Findex.php%2Fijoc%2Farticle%2Fdownload%2F8540%2F2461&usg=AOvVaw3TqT55DKCoVsK9CKoxjI1f

Centers of Excellence. Therefore, it is evident that as long as the strong discrepancies in ideas and in perspectives are not resolved, it will be hard to establish the concept of collective security in the field of cyberspace.

Part Three – Perspective trends of cyber collaboration

3.1 A World Wide Governance for a World Wide Web: assessing the current role of International Institutions in guaranteeing a more secure Internet

After providing an analysis of the national strategies of the major States in the field of cyber, the current section deals in particular with the status of global governance and Institutions and their role in regulating cyber relations. Some general mention has been already provided with regards to United Nations Group of Government Experts and several regional initiatives. The first question to be answered deals with the role that International Institutions may cover in such field: on one side, they should be asked to regulate the use of cyber tools to guarantee a certain level of cybersecurity worldwide; on the other side, however, they should guarantee the benefits of a worldwide open access of the Internet to be respected.

Such debate is everything but new, and was vigorously discussed in December 2012 when governments came to renegotiate the International Telecommunication Regulations and to decide whether the International Telecommunication Union (ITU) would have been the natural continuation of telecommunication international regimentation with the development of the Internet. Countries like Russia, China and Sudan, motivated by the concern of rising threats to cybersecurity, were pushing for the inclusion of the Internet international regulation within ITU's responsibilities, and therefore allowing Countries to directly manage how the Internet would have been structured. The main aim corresponded to provide support in managing the Internet in its continued mission, in order to build "confidence and security in the use of international communications technologies."[182]

However, such proposal of change has been under sustained discussion because, as claimed by Countries like the United States and its NATO allies, it would have changed the nature of Internet governance and therefore hand over sweeping powers to governments. The main fear would have been that some Countries would have controlled not only the access within their own borders but would have also controlled the access of users from other Countries. In the end, such dispute terminated in not mentioning the word "Internet" and just sticking to regulating traditional telecommunications. Consequently, the proposal to have the ITU reformed in order to include cybersecurity issues had basically failed, not meeting half of world government agreement.

[182] Singer, P. W., & Friedman, A., Cybersecurity and cyberwar: What everyone needs to know. Oxford: Oxford University Press, 2014, p. 183.

In a historical moment in which international institutions are posed under scrutiny and strongly subjected to criticism, the question of what roles the old international organizations should play when it comes to a new feature, as in the case of the Internet, is very difficult to assess and probably will remain under discussion for the years to come. In fact, the world has been dividing into very different visions of the Internet and its governance. To put it in simple terms, one bloc craves for regaining sovereignty over their national bits of the Internet. On the other side, an alternative vision is provided by those Countries that perceive the very openness of the Internet as a key to its success, regardless of their geographical location in the world.[183] As a result, the interplay between this two visions is what makes the issues and problems of cybersecurity crucial. The most appropriate pathway would be to set grounds in the awareness that there is a legitimate need for action, but being mindful by abuses and manipulation that can be hidden beneath the discussion on security.

Another question which is discussed by the international community on the issue of cybersecurity and cooperation deals with the chance of creating a cyberspace treaty. As for the case of international institutions regimentation, not everyone is pushing equally hard for such treaty. This would be the case of establishing a treaty that basically would apply the law of armed conflict to the fifth domain. However, some governments, especially those Countries which possess the biggest cyber capabilities, express their reticence for mainly two reasons. The first consist in the fear among the more advanced cyber powers of having less area of maneuver, while others can catch up with technology and bypass the new laws. For example, the treaty could ban cyberweapon but nonstate patriotic hacker could still act maliciously. The second issue deals with the differences in conceptualization of the matters related to cybersecurity which are giving birth to different priorities that leading States have in cyberspace. As shown in the comparison made in the second chapter of the divergent national strategies and given the current status of affairs, coming into common terms in the short term and with small ground for agreement seems to be hardly obtainable.

Additionally to this, some advocate the possibility of using the 1967 Outer Space Treaty[184] as a model for a cybersecurity treaty, because both the outer space and the cyber space share a direct

[183] Singer, P. W., & Friedman, A., Cybersecurity and cyberwar: What everyone needs to know. Oxford: Oxford University Press, 2014, p. 184.

[184] The Outer Space Treaty, which entered into force in 1967, provides the basic framework on international space law, including the following principles: the exploration and use of outer space shall be carried out for the benefit and in the interests of all countries and shall be the province of all mankind; outer space shall be free for exploration and use by all States; outer space is not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means; States shall not place nuclear weapons or other weapons of mass destruction in orbit or on celestial bodies or station them in outer space in any other manner; the Moon and other celestial bodies shall be used exclusively for peaceful purposes; astronauts shall be regarded as the envoys of mankind; States shall be responsible for national space activities whether carried out by governmental or non-governmental entities; States shall be liable for damage caused by their space objects; and States shall avoid harmful contamination of space and celestial bodies.

link with fast developing technology and the fact that no Country can claim to own it. Theoretically, an equivalent cyber treaty would similarly ban any nation from using weapons in this new global zone. In practice, despite some relevant similarities between the outer space and the cyber space, the latter possesses some peculiarities which are unique and which contribute to increase the difficulties by establishing a sort of arms control regime.

According to the article of Erica D. Borghard and Shawn W. Lonergan, there are four reasons that justify why there is no arms control regime in the field of cyberspace yet. First of all, there is a consistent difficulty in assessing and measuring the relative strength of States in cyberspace. While for conventional weapons, their armament can be approximately counted for every and each State, there is much more uncertainty with respect to cyber technology, both because virtual weapons, by definition, cannot be destroyed, and because cyber weapons are usually used for targeted systems. Therefore, it would be easier to deliver a qualitative rather than an quantitative assessment of States' capabilities.[185]

Secondly, and as a consequence of what stated above, there is uncertainty in respect of the military effects of cyber technology, due to the rapid and unpredictable pace technological development goes at. In contrast with the slow timeline that nuclear innovation requires, at a tactical level attack, vectors and offensive capabilities are continuously evolving shortening the timeline for arms control agreements adjustments or other means development. "In cyberspace, the open-ended promise of innovation coupled with quickly changing tradecraft that can emerge with little to no warning challenges the creation of any agreement. A cyber arms control agreement runs the risk of being outdated or restrictive in some unanticipated way before the ink has even had time to dry."[186]

A third issue relates to the challenges of monitoring compliance and detect cheating once cyber arms control agreements are established. This is related to the fact that government would be required to agree upon opening up their own networks to be inspected or to observe a third party penetrating its network without being able to ascertain whether it is a procedure of compliance or intrusion from an enemy.

Finally, enforcement appears challenging as well for two main reasons: attribution and proportionality principles. In the case of a violation, States would have to agree upon the attribution

Source: Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, United Nations Office for Outer Space Affairs, 1967, available at: http://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introouterspacetreaty.html

[185] Borghard E. D., Lonergan S. W., Why Are There No Cyber Arms Control Agreements?, Council on Foreign Relations, January 16, 2018. Retrieved from: https://www.cfr.org/blog/why-are-there-no-cyber-arms-control-agreements

[186] Ibidem.

that would justify a reciprocal response. However, despite attribution capabilities have been improving over time, not all the Countries hold the same attribution capabilities or possess enough confidence in those to justify such action. Such example becomes particularly relevant when a State is able to detect a violation and is asked to convince other parties that a violation occurred. Second, enforcing an arms control agreement requires a proportionate responses to an observed violation and this might be problematic for several reasons. The time factor appears to be troubling because time lag occurs between the attack and the detection and thus the deterrent effect of a response is likely to be diluted by time. Furthermore, resource and access constraints may limit the capabilities that a State has in the specific moment of responding, increasing the chances of not being sufficiently effective. Finally, even crafting an effective response that relies on physical elements of power may be challenging to understand if the attack only provoked virtual damage.[187]

This pessimism regarding the feasibility of cyber arms control agreements does not imply that there are no avenues for cooperation between cyber adversaries. A starting point would be, whatever the tools of cooperation chosen, to establish a basic bloc of key rules and values that all responsible parties can and should agree to. This can be delivered by starting from mutual interests, so that the Internet runs smoothly and that cybercrime is controlled.[188] Furthermore, the so-called grey zones should be addressed, by discussing how the existing laws of armed conflicts should be updated for cyberspace and how to resolve the crux of cybersecurity debate on how to separate civilian space and military targets in the domain.

The issue when discussing the possibility of creating a treaty on the basis of strong disagreement, implies that there are also very few chances that such treaty would be actually respected in the future. What would be of much more convenience is starting shaping Countries behavior in the domain so that certain norms are actually followed even if no treaty has been signed yet. When there is a certain behavior that becomes a commonplace, because it is followed by the majority, the expectations of States will be built upon those practices.

As in the case of Cold War, the example of establishing something similar to the principle of the “red lines” might shape behavior in the case of espionage. Therefore, even in the absence of formal treaties, the starting point of a broader and more solid cooperation in the field among States would consists in establishing a concept of greater responsibility for the activities that emanate from a network. However, based on the principle of reciprocity, if one Country do not follow such norm

[187] Ibidem.

[188] Singer, P. W., & Friedman, A., Cybersecurity and cyberwar: What everyone needs to know. Oxford: Oxford University Press, 2014, p. 187

of behavior, the other networks in the system no longer owe it the same type of reciprocal exchanges that allow it to access the Internet smoothly. To put it into simple worlds, if you violate the norm, you also lose the privileges that come with it.[189]

What is appealing in this strategy is that, historically, even the actors that are initially loathe to sign onto any formal treaties or agreements become increasingly engaged with the norms over time. As the rules spread and non-signatories cannot do anything but engage in the process, Countries start to internalize the logic of cooperation, i.e., they begin to act like rules are there, even if there are no formal rules agreed upon.[190]

3.2 The Public-Private Partnership in the field of Cyber Security

States have the duty of guaranteeing security for their citizens, however they meet specific limits in cyberspace. The first limit consists in the issue of territoriality. In fact, whenever an issue appear to be linked to the physical side of the Internet, it is much more easy for a State to exert control over it. For example, even technically sophisticated organizations can actually be seized through their physical and financial assets even when they serve themselves with cyber tools. However, the fact that the Internet is made as well of non-physical and trans-boundaries subjects makes it much more difficult to be controlled by one single State. Another difficulty that a government usually meets deals with is the fact that private actors control most of the cyberspace infrastructure.

Furthermore, the dependence that Countries have on private networks includes the traffic of the most critical national infrastructure. As a result, while many Countries have focused on controlling the getaways between their own Country and the global Internet, it come about to be far more challenging to discern civilian, from military and government issues. Such status of affair makes governments highly reliant on private industry for almost every component of their information infrastructure, and even in the case of sharing responsibilities in securing the global Internet.

The challenge for governments is to understand how to foster information security without trying to dismantle the Internet's architecture and undermining the very benefits of cyberspace. States certainly shouldn't ignore their roles or responsibilities to their citizens, but they must also recognize the structural limitations of their power. Governments have valid concerns, but they no longer have direct control over most of the key sectors, as they are largely held in private hands.

[189] Singer, P. W., & Friedman, A., Cybersecurity and cyberwar: What everyone needs to know. Oxford: Oxford University Press, 2014, p. 192

[190] Singer, P. W., & Friedman, A., Cybersecurity and cyberwar: What everyone needs to know. Oxford: Oxford University Press, 2014, p. 193

The real question for governments is therefore how to better coordinate defense not only with other Countries' governments, but with private actors, as cybersecurity requires a public-private approach. A multi-stakeholder model that is the preferable approach to deal with issues related to cyber security, where State-based actors work with corporations and individuals to develop functional patterns of international governance.[191]

An interesting effort has been advanced by the tech industry related to the proposal of cyber norms in order to start stepping in as a norm-developer actor, which has been until now a mere governmental role. The main proposals have been advanced by Microsoft, Google and other tech representatives for setting the terms of digital security.

In particular, the Microsoft's proposal for a Digital Geneva Convention, firstly advanced in 2017, fascinated the digital policy community on the matter of requiring governance to avoid cyber intrusions targeting the private sector or critical infrastructure or stealing intellectual property.[192] With the aim of providing a secure and stable Internet, tech companies would be asked to engage with governments in order to establish reasonable policy arrangements that would become legal obligations, with corresponding enforcement mechanisms. According to the proposal, there are six major principles summarized as follows. First, application of the *ius ad bellum* principle in cyberspace; second, assisting private sector efforts to detect, contain and respond to and recover from attacks; third, report vulnerabilities to vendors; fourth, exercise restraint in developing cyber weapons with a strong disarmament focus; fifth, to commit to non-proliferation activities to cyberweapons; sixth, limit offensive operation to avoid mass events.[193]

Further examples are the Cybersecurity Tech Accord agreed by 34 tech companies, including Facebook, LinkedIn, Arm, ABB, Telefonica, Cisco, and Dell among others, committed to protect and empower all customers everywhere from malicious attacks by cybercriminal enterprises and States, and to improve the security, stability and resilience of cyberspace; and the 2018 Charter of Trust for a Secure Digital World jointly supported by leading global technology companies such as Siemens, IBM, Deutsche Telecom, Airbus.[194]

[191] Brown, C., Eckersley, R., Valeriano, B., & Maness, R., International Relations Theory and Cyber Security: Threats, Conflicts, and Ethics in an Emergent Domain. In The Oxford Handbook of International Political Theory, Oxford University Press, 2018.

[192] A Digital Geneva Convention to protect cyberspace. Microsoft Policy Papers, available at: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH

[193] Stephanie Borg Psaila, New cyber norms to protect cyberspace, GIP Digital Watch observatory, 2018. Retrieved from: https://dig.watch/trends/cyber-norms

[194] Ibidem.

3.3 Setting the international agenda: the UNIDIR 2019 Cyber Stability Conference and International ICT-security at the United Nations

What has been done within the walls of the United Nation Headquarters probably represents the biggest and most comprehensive international effort in the field of cybersecurity. The topic of cybersecurity is comprised in the actions of the United Nations Institute for Disarmament Research (UNIDIR), supported by the discussion in the rooms of the Security Council and General Assembly. This work belongs to the Security and Technology Program of UNIDIR in support of the work sponsored by governments within the United Nations framework.

The UNIDIR's Annual Cyber Stability Conference was held in June 2019. The key issues brought to attention at the conference were covering some major areas of cyber debate, in particular "the impact of the global digital technology development on States, economies, industries and security ecosystems, the risks of mounting cyber threats and the potential costs of failure to agree on effective international cybersecurity cooperation mechanisms – and the incentives for States to engage with the multilateral processes on cybersecurity policy norms, including UN GGE and OEWG on cybersecurity."[195]

Through the lens of these propositions, participants discussed the mandates of the two groups of GGE and OEWG, how both processes could produce complementary outcomes, and how capacity-building measures development could contribute to the strengthening of global cybersecurity. Such goals have been established in coherence with the United Nations Secretary-General's Agenda for Disarmament, launched in May 2018. The Agenda acknowledged that we currently suffer from the threats that cyberattacks represent due to an increasingly global interconnectivity and the fact that they can affect a wide number of system at the same time. Therefore, two points have been added to the implementation plan of the Agenda for what concern cybersecurity: one, "prevention and peaceful settlement of conflict stemming from malicious activity in cyberspace" and two, "foster a culture of accountability and adherence to emerging norms, rules and principles on responsible behavior in cyberspace".[196]

For what concerns the direct involvement of States in the United Nations process for cybersecurity, the Groups of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security were established by

[195] United Nations Institute for Disarmament Research, 2019 Cyber Stability Conference Summary Report, United Nations, New York, available at: http://unidir.org/programmes/security-and-technology/2019-cyber-stability-conference

[196] Securing our common future: An Agenda for Disarmament, Office for Disarmament Affairs, United Nations, New York, 2018. Retrieved from: https://s3.amazonaws.com/unoda-web/wp-content/uploads/2018/06/sg-disarmament-agenda-pubs-page.pdf#view=Fit

the 2004 United Nations resolution approved by consensus by the General Assembly.[197] Up to nowadays, six UN GGEs have been convened: in 2004/2005[198], 2009/2010[199], 2012/2013[200], 2014/2015[201], 2016/2017[202], and 2019/2021[203].

The composition of the United Nations GGE is based on the principle of equitable geographical distribution, with the inclusion of the five permanent members of the Security Council. For the years 2019-2021, the established UN GGE members are: Australia, Brazil, China, Estonia, France, Germany, India, Indonesia, Japan, Jordan, Kazakhstan, Kenya, Mauritius, Mexico, Morocco, Netherlands, Norway, Romania, Russian Federation, Singapore, South Africa, Switzerland, United Kingdom, the United States, and Uruguay. Ambassador Guilherme de Aguiar Patriota of Brazil covers the position as Chair of the GGE for the current term.[204]

Previously, the different sets of GGEs comprised a mixed group of experts on information security, some with diplomatic backgrounds and others with a more technical background. However, over the course of time, the composition of the experts changed and Countries decided to select experts with, arms control, or non-proliferation experience. Finally, the process of the United Nations GGE decision-making includes the adoption by consensus of the final Report which is drafted during the consultation and discussion sessions and submitted to the General Assembly.

The United Nations GGEs can be credited with two major achievements which have been scored through a long process of diplomatic engagement. The first accomplishment deals with being one of the first international platform which has been able to outline the global agenda based on a multilateral and multi-stakeholder approach. Indeed, since the Russian draft resolution proposal in 1998, the problem of cybersecurity has been brought to the most important international table of discussion and has been addressed to reach international cyber stability, raising awareness and setting the agenda on the topic. A second milestone reached by the United Nations GGE acknowledged and introduced the principle of applying international law to the digital space.[205] The group agreed that "International law, and in particular the Charter of the United Nations, is applicable and is essential

[197] United Nations, A/RES/59/61

[198] United Nations, A/RES/58/32

[199] United Nations, A/RES/60/45

[200] United Nations, A/RES/66/24

[201] United Nations, A/RES/68/243

[202] United Nations, A/RES/70/237

[203] United Nations, A/RES/73/266

[204] UN GGE and OEWG, GIP Digital Watch observatory, 2019. Retrieved from: https://dig.watch/processes/un-gge

[205] Mauer, T., Cybersecurity in a Complex Environment: Transatlantic Divergences and Diplomatic Achievements, VEREINTE NATIONEN – German Review on the United Nations, Vol. 64, 2/2016, pp. 51–55. https://dgvn.de/fileadmin/publications/PDFs/Zeitschrift_VN/VN_2016/Heft_2_2016/Maurer_Cyberraum_VN_2_16_engl_web.pdf

to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment."[206]

Alongside those major achievements, the UN GGE work has not been free from disputes and disagreements, which turned, for example, in the acceptance only on a voluntary basis of such applicability, letting the implementation of the norms on the political will of the various States and the internal coherence of their bureaucracy.[207] Furthermore, two main questions have been raised by the international community on the matter: the will for a broaden legitimacy of these agreements and the modalities of implementation for a more secure environment.

In December 2018, in order to answer – at least partially – those challenges, the UN General Assembly has also established the Open-Ended Working Group (OEWG) for the period 2019/2020.[208] In complementarity to the UN GGE scheme, this group offers an open composition that allows all United Nations Member States to participate, if desired. OEWG has started working in June 2019 and will proceed by developing its report on a consensual basis, which will supposedly be more difficult to achieve considering the large number of States taking part to it. The report is to be presented at the 75th United Nations session in autumn 2020.

This group has been set up with the aim of developing rules, norms, and principles of responsible behavior of States, discussing their implementation, and contributing to the establishment of a regular institutional dialogue with broader participation under the United Nations umbrella.[209] Among the initiatives of such group, there are some norms that differentiate from the earlier activities of the UN GGE, such as the fact that all charges against States regarding organizing and/or conducting illegal activities with the use of ICT need to be substantiated as well as the problem of attribution and of behavior for cyber-incidents. Further commitment deals with the necessity to assist Countries in bridging the ICT security gap.[210]

The creation of two separated groups have raised some controversies, while have tried as well to respond to some of the major criticism that the UN GGE had to dealt with overtime. The advantages related to the creation of the new OEWG deal with inclusivity and participation, in contrast to the limited number of GGEs members due to its composition standards. Moreover, the resolution related to the establishment of the OEWG already includes a set of norms which can be used and developed

[206] United Nations Doc. A/68/98, 24 June 2013, p. 8.

[207] Mauer, T., Cybersecurity in a Complex Environment: Transatlantic Divergences and Diplomatic Achievements, VEREINTE NATIONEN – German Review on the United Nations, Vol. 64, 2/2016, pp. 51–55. https://dgvn.de/fileadmin/publications/PDFs/Zeitschrift_VN/VN_2016/Heft_2_2016/Maurer_Cyberraum_VN_2_16_engl_web.pdf

[208] United Nations, A/RES/73/27.

[209] Ibidem.

[210] Additional information on the proposals of Russia for OEWG, please check the paragraph on Russia in the second part of this work.

along with their mechanism of implementation. Finally, the submission of the OEWG report is set one year before the one of UN GGE, therefore the time factor could play a substantial role. Nevertheless, there are as well some disadvantages related to OEWG, such as its open composition which brings more difficulty in maintaining the focus in the discussion and in reaching consensus. Along with that, Countries will meet ideological and technical discrepancies in definitions and principles, differences in technical, legal and diplomatic capacity and leadership and regional alignments.[211]

Most of all, some States have expressed their suspicion over the decision of creating two groups which work parallelly and with similar goals. Probably, one of the biggest challenge is to avoid polarization among the two groups in order to make sure that they work in a complementary way in the future, while avoiding overlapping missions. This is because the debate about how cyberspace should be regulated is characterized by a high politicization and States are actively sponsoring norms and legal interpretations that coincide with their strategic and ideological national preferences. Therefore, it looks like that for the time being, those different preferences cannot be reconciliated and this raise the risk for larger fragmentation in the regulation of cyberspace.[212]

3.4 The Tallinn Manual 2.0: an effort in understanding and applying international laws to cyber operations

The 2007 attack to the Estonian critical infrastructure marked for NATO Members the day for a new challenge to the collective defense ideology. Estonia, which at that time was a new alliance Member, was one of the most wired Nation as its citizens were used to conducting their everyday life mostly online, from online voting to banking and suffered one of the most severe Denial of Service attack. Apart from pointing the finger at the Russian government at that time, the Estonian Foreign Minister Urmas Paet called for assistance, fearing that the large-scale cyber-attack would have threatened the security of the Country and of the NATO alliance as a whole. Specifically, he argued

[211] Stadnik I., Discussing state behaviour in cyberspace: What should we expect?, Diplomacy.edu, 2019. Retrieved from: https://www.diplomacy.edu/blog/discussing-state-behaviour-cyberspace-what-should-we-expect

[212] Henriksen, A., The end of the road for the UN GGE process: The future regulation of cyberspace, Journal of Cybersecurity, 2019, 1–9. Retrieved from: https://academic.oup.com/cybersecurity/article/5/1/tyy009/5298865

that, under the Article 5[213] of the Treaty of the Alliance, NATO was obliged to intervene in defending the Country from an approaching status of cyberwar.[214]

However, at that time, while the Member Countries were actually worried about the future of cyber tools use, they didn't think that the Article 5 was actually applying on this specific case, since no deaths were registered and no property was actually damaged or destroyed. Simply speaking, it seemed there were no actual conditions for starting a war with Russia.

The case of Estonia have been instructive as it represented a constitutive case for which the discrepancy between old laws and the development of new technologies does not meet the necessity of instructing the correct behavior for defending a partner Country from external attacks. Therefore, NATO Countries found themselves unable to answer the question of whether what Estonian infrastructure suffered was actually to be considered as an act of war in the cyber domain.

Nowadays, the issue that frequently emerges when discussing the legal framework of cyberspace is that most of the laws that we currently observe are dated to the post World-War II 1945 United Nations Charter and to the 1949 Geneva Conventions. However, given the fast technological development that the world has been experiencing from that date, the concepts that were developed back then do not necessarily apply to the cyber domain. One of the most clear example is the definition of *aggression* which is described by the United Nations Charter as a "use of force against the territorial integrity […] of a State".[215] Such definition is clearly problematic because it assumes that aggressions may occur only in a physical world with demarcated borders, while cyberattacks do not imply physical force, do not take place in a specific geographic realm and do not necessary involve only State entities.[216]

In this context, the Tallinn Manual on the International Law Applicable to Cyber Warfare was born with the aim of reducing the "wild west" and the law gaps characterizing cyberspace and placing itself in the process of updating old codes or creating new ones which are currently going on. In 2009, the NATO Cooperative Cyber Defense Centre of Excellence commissioned twenty law professors to formally examine how the known international laws regulating war could be applied to the context of cyber operations and cyber warfare, trying to bridge the gap between old international laws and new technologies in the most comprehensive and authoritative way.[217]

[213] "The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all." Art. 5 of the North Atlantic Treaty, Washington D.C., 4 April 1949.

[214] Singer, P. W., & Friedman, A., Cybersecurity and cyberwar: What everyone needs to know. Oxford: Oxford University Press, 2014, p. 122.

[215] Charter of the United Nations, San Francisco, 1945, Article 2, Paragraph 4.

[216] Singer, P. W., & Friedman, A., Cybersecurity and cyberwar: What everyone needs to know. Oxford: Oxford University Press, 2014, p. 123.

[217] Ibidem.

The Group of Experts that were dedicated to the creation of such manual includes highly respected scholars and legal experts with large experience in the field of cyber issues and were aided, during their work, by information technology specialists. In particular, the group was leaded by Professor Michael N. Schmitt, chairman of the international law department at the United States Naval War College.[218] Moreover, three organization were participating to the drafting process through the presence of their observers: NATO representatives, of course, from its Allied Command Transformation, the International Committee of the Red Cross in the capacity of international humanitarian law guardian and the United States Cyber Command for an expert and mature perspective on the process.[219]

The format which is adopted for the work is a non-binding manual, divided into sections named after *black letter rules* and their steering commentaries. Basically, the work of the Group of Experts consisted in restarting the principles of international law in the context of the cyber domain. It is to be noted that every and each rule has been understood and agreed by all the authors based on the principle of consensus. Therefore, in each commentary we may find the different opinions that emerged during the redaction and the study of the work.[220]

In February 2017, the Tallinn Manual 2.0 was released, following the steps of the original manual and expanding the scope of the former version. The most relevant difference between the old and the new version of the manual lays on the object of the study. While the old Tallinn Manual focused on the most disruptive and destructive cyber operations that are addressed as qualified armed attacks and therefore allow States to respond in the name of self-defense, the Tallinn Manual 2.0 takes into consideration more general cyber operations that may occur. Indeed, in the last 10 years, States

[218] Other members of the Group of Experts included the following figures: Professor Wolff Heintschel von Heinegg (Viadrina European University), Air Commodore William H. Boothby (United Kingdom Royal Air Force), Professor Thomas C. Wingfield (George C. Marshall European Center for Security Studies), Bruno Demeyere (Catholic University of Leuven), Professor Eric Talbot Jensen (Brigham Young University), Professor Sean Watts (Creighton University), Dr. Louise Arimatsu (Chatham House), Captain Geneviève Bernatchez (Office of the judge advocate general of the Canadian Forces), Colonel Penny Cumming (Australian Defense Force), Professor Robin Geiss (University of Potsdam), Professor Terry D. Gill (University of Amsterdam, Netherlands Defense Academy, and Utrecht University), Professor Derek Jinks (University of Texas), Professor Jann Kleffner (Swedish National Defense College), Dr. Nils Melzer (Geneva Centre for Security Policy), and Brigadier General Kenneth Watkin (Canadian Forces). The technical advisors were Professor James Bret Michael (United States Naval Postgraduate School), Dr. Kenneth Geers and Dr. Rain Ottis (both from the NATO Cooperative Cyber Defense Centre of Excellence).

[219] Schmitt, Michael N (Gen. ed.) (2013). Tallinn Manual on the International Law Applicable to Cyber Warfare. New York, United States of America: Cambridge University Press.

[220] Schmitt, Michael N (Gen. ed.) (2013). Tallinn Manual on the International Law Applicable to Cyber Warfare. New York, United States of America: Cambridge University Press.

have been constantly challenged by malicious cyber activities, that however did not escalate to a conflict level.[221]

For sake of completeness, the content analysis of the Manual takes into consideration its latest version, the Tallinn Manual 2.0, which is divided into four sections. The first part covers general provisions of international law and cyberspace; the second part deals with specialized regimes of international law and cyberspace; the third part addresses international peace and security and cyber activities; finally, the fourth part recalls the instances already expressed in the original Tallinn Manual covering the modalities of application of international law to cyber armed conflicts.[222]

More specifically, in the first section, the following issues are tackled: sovereignty, due diligence, jurisdiction, international responsibility and, finally, cyber operations not *per se* regulated by international law. In the second section, the topic of international human rights law and other specialized regimes laws. In the third part, peaceful settlement of disputes and prohibition of intervention are discussed. In the last and fourth part, the Manual discuss the conditions for the use of force.[223] In the following lines, some of the aforementioned topics will be briefly covered in order to illustrate the major scholar achievements of the Group of Experts.

The first concept discussed in the Manual recalls that the sovereignty principle does apply to cyberspace and remarks the difference between internal and external sovereignty, stating that a "State must not conduct cyber operations that violate the sovereignty of another State".[224] Because sovereignty is a rule of international law, it is assumed by the Experts that its violation can be considered as an internationally wrongful act. However, such approach is not fully shared especially because States have not yet fully clarified their positions on the matter of sovereignty.[225]

Due diligence is the second topic addressed, which despite not being a substantive provision of international law, still consists in a standard which prescribe States to prevent their territory from being used to cause transboundary harm. However, it is not specified which standard and when it should be applied, denoting that such rules is still widely under discussion. Moreover, Experts

[221] Leetaru, Kalev, What Tallinn Manual 2.0 teaches us about the new cyber order, Forbes, 2017. Retrieved from: https://www.forbes.com/sites/kalevleetaru/2017/02/09/what-tallinn-manual-2-0-teaches-us-about-the-new-cyber-order/#1780f04d928b

[222] Schmitt, M., Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press, 2017.

[223] Jensen, E.T., The Tallinn Manual 2.0: Highlights and Insights, 48 Georgetown Journal of International Law, 735 (2017). Retrieved from: https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf

[224] Schmitt, M., Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press, 2017, rule 17, chapter 4, p. 94.

[225] Jensen, E.T., The Tallinn Manual 2.0: Highlights and Insights, 48 Georgetown Journal of International Law, 735 (2017). Retrieved from: https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf

affirmed that there should be a codified threshold that would trigger the rule, in order to avoid "serious adverse consequences", which, by the way, are not specified. Due diligence is frequently discussed even under the auspices of the UN GGE and have never particularly appealed States due to the fact that it places significant responsibility on them and encounter objective difficulties in dealing with proxy-pursued activities.[226]

Concerning the theme of jurisdiction, the Manual affirms that "[s]ubject to limitations set forth in international law, a State may exercise territorial and extraterritorial jurisdiction over cyber activities".[227] For both prescriptive and enforcement jurisdiction, States can exercise their jurisdiction in their own territory; nevertheless, they possess more limited capacities to exercise them extraterritorially. Undoubtedly, those jurisdictions are not exclusive, because States may often have concurrent jurisdictions emphasizing the need for international cooperation.[228]

There is a full agreement among the Experts on the fact that customary law of State responsibility should apply to cyber activities. Moreover, physical damage nor injury are required elements for a cyber act to be considered as an internationally wrongful act, and geography is not determinative in establishing State responsibility. The most complex legal question is linked to the issue of attribution to non-State actors, who could be working on behalf of States as proxies, therefore it is expected that the attribution standard will increase as a method for victim States to access broadly countermeasures. Finally, the question of attribution is excluded when it comes to consider cyber operations as cyber countermeasures, so they are not limited to "in-kind" response but still raise several issues on the matter, such as temporality or proportionality[229].

The Manual is as well noting that there are some actions which are not specifically regulated by international law, so that there is a category of unregulated cyber activities which should be addressed: the cyber operations not *per se* regulated by international law. In this category fall, for example, peacetime cyber espionage, which in practice does not meet a clear prohibition, nevertheless recognize that there might be ways according to which espionage is pursued in an unlawful manner.[230]

Important considerations are drawn on the topic of international human rights law, as part of the section on specialized regimes. Due to the lack of clarity of the international human rights law,

[226] Jensen, E.T., The Tallinn Manual 2.0: Highlights and Insights, 48 Georgetown Journal of International Law, 735 (2017). Retrieved from: https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf

[227] Schmitt, M., Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press, 2017, rule 8, chapter 3, p. 51.

[228] Jensen, E.T., The Tallinn Manual 2.0: Highlights and Insights, 48 Georgetown Journal of International Law, 735 (2017). Retrieved from: https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf

[229] Ibidem.

[230] Ibidem.

this section has been one of the most discussed. The most important point recalls the idea that, even if human rights apply to a cyber activity, this does not directly imply that the cyber activity has violated human rights. Therefore, the potential violation should be assessed in a separate and additional procedure. While the obligation to protect or ensure human rights is an affirmative obligation on States, there is part of the international community which contests the parameters of such obligation. This is also because, States take into account other important responsibilities such as national security and public order and ask for limitation when it comes to international human rights law application.[231]

Regarding the section dealing with International Peace and Security and Cyber Activities, the following rules are discussed. First of all, the principle of peaceful settlement of dispute is recognized, by application of the United Nations Charter paragraphs 2(3) and 33(1) – generally accepted as customary international law. Given the current status of affair according to which transnational cyberattacks do happen daily, this discussion appears very important and raises further question when also non-State actors are involved.[232]

Secondly, the Manual cover the principle of prohibition of intervention, which is dealing both with States and with the United Nations. The first related rule prescribes that "a State may not intervene, including by cyber-means, in the internal or external affairs of another State"[233] and applies only to the relations between States when coercive interference takes place. Nevertheless, Experts have been endorsing conflicting opinions on the circumstances of the real application of such rule. Concerning the United Nations, Experts have expressed the idea that the UN should not intervene with cyber-means in the domestic jurisdiction of a State.[234] Exclusion are applied with the enforcement of measures decided by the UN Security Council under Chapter VII of the United Nations.

Some final words should be spent on what the original version of the Tallinn Manual provided on the topic of the use of force. In general, a condition for the use of force verifies when a State, acting aggressively "through armed or coercive forces, threatens or violates the territorial integrity, the political independence or the practice of any other action incompatible with the purpose of the

[231] Ibidem.

[232] Jensen, E.T., The Tallinn Manual 2.0: Highlights and Insights, 48 Georgetown Journal of International Law, 735 (2017). Retrieved from: https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf

[233] Schmitt, M., Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press, 2017, rule 66, chapter 13, p. 312.

[234] Jensen, E.T., The Tallinn Manual 2.0: Highlights and Insights, 48 Georgetown Journal of International Law, 735 (2017). Retrieved from: https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf

United Nations against another State".[235] However, because cyberattacks are much more difficult to be perceived and assessed, scholars have met a significant challenge interpreting situations that have occurred in the digital domain and establishing whether the use of force has actually occurred. There are some examples, such in the case of espionage, which do actually lack of coercive characteristics, but by themselves do not directly violate the aforementioned non-intervention principle.[236]

In order to advance clarity on the matter, the Experts of the Manual have redacted a list of criteria which facilitate the comparison between cyber-attacks and effects caused by armed conflicts. The list includes the following benchmarks: a) Severity, according to which any cyber-operation resulting in damage, destruction, harm and death will be viewed as a case of use of force; b) Immediacy, for which the faster the effects of an attack surface, the fewer ways to defend itself a State has and, thus, the more severe are its damages; c) Directness as the causal connection of a cyber-attack; d) Invasiveness, based on the object of the operation, from military to civilian, will be considered as more intrusive; e) Measurability of effects, considered as the quantitative value of the caused damage; f) Military Character, as the nexus on the use of military forces; g) State Involvement in cyber operations; and finally, h) Presumptive Legality over norms and international treaties.[237]

Despite, by mistake, many refer to as a NATO Manual, the Tallinn Manual should be conceived as an independent academic research which, although being born on NATO necessities and experience, stand alone in its specificity. Indeed, the Manual in itself does not express countries opinion on the theme, but of experts international law in the cyber context. It is of outstanding consideration given the fact that it is considered one of the first and biggest effort in understanding and interpreting international law in the cyber domain, and, for sure, will influence States' views and approached in those matters in the future.

Because it represents academic research, and not a piece of international law, some criticism have questioned whether the Tallinn Manual is simply a "rule book on a shelf". The scholars Dan Efrony and Yuval Shany summarize governments and critics opinions in three main argument against the proposed rules and related interpretation of the Manual. The first finding shows that there is unclarity whether States have accepted or are ready to accept the Tallinn Rules, both following the latest actions pursued by States in the cyber domain and by an analysis of their official national strategies. Secondly, it is claimed that States often maintain silence with relations to their activities

[235] Francisco Rogério Moreira Campos, Bruno de Pinheiro Tavares, Tallinn Manual and the use of force, The Institute for Research on Internet & Society, 2016. Retrieved from: http://irisbh.com.br/en/tallinn-manual-and-the-use-of-force/

[236] Jensen, E.T., The Tallinn Manual 2.0: Highlights and Insights, 48 Georgetown Journal of International Law, 735 (2017). Retrieved from: https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf

[237] Francisco Rogério Moreira Campos, Bruno de Pinheiro Tavares, Tallinn Manual and the use of force, The Institute for Research on Internet & Society, 2016. Retrieved from: http://irisbh.com.br/en/tallinn-manual-and-the-use-of-force/

in cyberspace and, therefore, they show uneven interest in promoting legal certainty in cyberspace. The reason behind this behavior is due to the fear of States to rely more on transparency and therefore becoming more vulnerable to the eyes of other States. Thus, States tend to act in cyberspace, offensively or defensively, in a clandestine manner, raising ambiguity and adopting a selected approach on the application of international law. Finally, because States are not fully certain that the disposition provided by the Tallinn Manual do adequately protect their long-term interest, they are reluctant to pressure for their endorsement. However, such condition do not preclude that no international law regulation in cyberspace are desirable. As a matter of fact, the approach applied to the Tallinn Manual proves that there is a constantly growing need for coordinated response to cyberattacks, which however lawmakers are fearing to address.[238]

As many experts note, there are still many areas of disagreement and lack of clarity both among States and even among the Experts who took part in the writing process of the Tallinn Manuals. Undoubtedly, the cyber domain is still a rather new topic and an expanding law area that requires deeper insights and understanding to create new approaches to existing problems. However, until States clarify their position on where the law is headed, the Tallinn Manual 2.0 will be serving, for sure, as a starting point for forward moves with the law on cyber space.

3.5 The role of the Republic of Italy in the EU-NATO cybersecurity framework: an example of regional cooperation

This section of the thesis intends to provide an example of regional cooperation by exploring the actions undertaken by the European Union (EU) – also in coordination with NATO – in the field of cybersecurity and the specific features concerning the current status of affairs with regards to the strategic plans implemented by the Italian government, both at European and North-Atlantic level.

The European acknowledgement of the threats rising from cyberspace have brought to the establishment, in 2004, of the Greece-based EU Agency for Cybersecurity (ENISA) with the goal of representing a point of reference in such field. The Agency is set to backing Member States and to other EU institutions in the process of policy development and implementation of cybersecurity standards and in support of EU Members' coordination in case of large-scale attacks and crises.[239]

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

[239] The EU Cybersecurity Act brings a strong agency for cybersecurity and EU-wide rules on cybersecurity certification, European Commission, June 2019, retrieved from: https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-act-brings-strong-agency-cybersecurity-and-eu-wide-rules-cybersecurity

The adoption of the Cybersecurity Act in June 2019 is the latest achievement that involved the Agency and Member States in the field. This document introduces, for the first time, EU-wide rules for cybersecurity certification of specific categories of ICT products, processes and services. Also, the Act supports the enhancement of EU's cybersecurity preparedness and resilience through the intensification of information sharing among EU Members with the support of the network of Computer Security Incident Response Teams (CSIRTs) and pan-European cybersecurity exercises and trainings. Likewise, it functions to assist EU Member States in implementing the "Directive on the Security of Network and Information Systems" (NIS Directive)[240] which elucidate national authorities' reporting obligations in case of serious cybersecurity incidents.[241]

Policy development and implementation, operational cooperation, knowledge and information sharing, capacity-building measures are some of the main tasks attributed by Member States to the European Union, and they run parallelly with NATO's commitment to cybersecurity. Being the EU and NATO historic partners, they have committed to relaunching their strategic partnership with the stipulation of a Joint Declaration in 2016, aiming at mobilizing efficiently Members' resources to address cyber challenges and at enhancing the security of their citizens. "Cybersecurity and defense" is comprised among the seven different areas[242] of this strategic cooperation, and prescribes "active interaction at staff level […] on concepts and doctrines, existing and planned training and education courses, threat indicators, ad-hoc exchanges of threat alerts and assessments, cross-briefings, including on the cyber aspects of crisis management and regular meetings" [243].

The current status of EU-NATO affairs on the theme of cybersecurity is instructive in the effort of tackling the risks that emerge from cyberspace, especially in the field of cybercrime and digital market and it consists in a virtuous example of partnership in the field. Nevertheless, the mutual effort of the parties have met and will encounter obstacles in the process of cooperation.

[240] The NIS Directive, which entered into force in August 2016, is the first piece of EU-wide legislation on cybersecurity. It provides legal measures to boost the overall level of cybersecurity in the EU, which Member States have to adopt by May 2018, by ensuring: preparedness by requiring them to be appropriately equipped, e.g. via a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority; cooperation among all the Member States, by setting up a cooperation group and a CSIRT Network, in order to promote swift and effective operational cooperation on specific cybersecurity incidents and sharing information about risks, a culture of security across sectors which are vital for our economy and society which rely heavily on ICTs, requiring different sectors to comply with the security and notification requirements under the new Directive.

[241] EU Cybersecurity Act, ENISA And Cybersecurity Certification Framework, European Commission, June 2019, retrieved from: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60505

[242] The 42 proposals of the NATO-EU Joint Declaration of July 2016 are subdivided into the 7 following areas: 1. countering hybrid threats; 2. operational cooperation including maritime issues; 3. cyber security and defense; 4. defense capabilities; 5. defense industry and research; 6. parallel and coordinated exercises; 7. defense and security capacity building.

[243]EU-NATO cooperation – Factsheet, EU External Action, Bruxelles, June 2019. Available at : https://eeas.europa.eu/headquarters/headquarters-Homepage/28286/eu-nato-cooperation-factsheet_en

First and foremost, the concept of national sovereignty still plays an important role in shaping the national security strategies of Member States, due to the nature of both entities. Indeed, there are acknowledged imbalances which are determined by the different perceptions that Countries have of the threats originating in cyberspace, as for the case of Estonia which was subjected to one of the most damaging cyber-attack registered in history. Secondly, the two parties needs to deal with the implementation of cooperation procedures that concretely put into practice the material and the topics discussed during the meetings. Indeed, even if the ideas of facilitating the process of information sharing and the performance of joint exercises are remarkable, the EU-NATO partnership needs to be more operational and concrete. Finally, as already mentioned in the previous paragraph concerning the Tallinn Manual, the two parties should deal with the issue of agreeing on a shared set of definitions and on a common framework of applicability of international law to the field of cyberspace.[244] Clearly, if those considerations will not be addressed by the two counterparts, upgrading the effort for an increased cybersecurity will be much harder to achieve.

Being Italy founder of both the North Atlantic Treaty Organization[245] and the European Union[246], the Country represents an example of integration of different priorities which have been crucial in shaping its foreign policy. Italy endorses closer cooperation and complementarity between the two entities in their effort of promoting regional security by means of crisis management and peace-keeping operations.[247] Within the priorities set by this cooperation, Italy recognizes and supports the path towards the adaptation to new security threats including hybrid and cyber attacks.[248]

As reported by the 2018 National Security Document (Documento di Sicurezza Nazionale), from 2017 to 2018, there has been a steady increase of hostile actions mainly addressed to the detriment of the computer systems of central and local public administrations (72% of total attacks).[249] In particular, it has been registered a significant increase of attacks against networks of ministerial offices (24% of the hostile actions) and against IT infrastructures attributable to local authorities (39%

[244] Raik, K., Järvenpää, P., A New Era of EU-NATO Cooperation: How to Make the Best of a Marriage of Necessity, Report, International Centre for Defence and Security, May 2017, available at: https://icds.ee/wp-content/uploads/2018/ICDS_Report_A_New_Era_of_EU-NATO.pdf

[245] Official page of the Italian Ministry of Foreign Affairs on the role of Italy in NATO. http://www.esteri.it/mae/it/politica_estera/organizzazioni_internazionali/nato.html

[246] Official page of the Italian Ministry of Foreign Affairs on the role of Italy in the EU. http://www.esteri.it/mae/it/politica_europea/italia_in_ue

[247] Statement on the EU-NATO cooperation on the official website of the Italian Ministry of Foreign Affairs. http://www.esteri.it/mae/it/politica_estera/organizzazioni_internazionali/nato.html

[248] Statement on the EU-NATO cooperation on the official website of the Italian Ministry of Foreign Affairs. http://www.esteri.it/mae/it/politica_estera/organizzazioni_internazionali/nato.html

[249] Presidency of the Council of Ministers, Relazione Sulla Politica Dell'Informazione 2018, Relazione al Parlamento, p. 6 https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2019/02/Relazione-2018.pdf

of the total). In 2018, the detriment of private subjects, mostly related to the telecommunications sector, accounted for 6% of total attacks and transports for 6% (tripled compared to 2017), with particular focus on operators in the energy sector (11%) and their suppliers. The majority of hostile actors is represented by diversified groups of hacktivists which accounted for 66% of the total of cyber-operations perpetrators.[250]

Due to the constant increase of threats in the cyber realm, Italy has been developing a national cyber security framework to counter those attacks since 2007 with the adoption of the Law 124/2007 which reformed the entire Italian Intelligence Apparatus and raised concern on the risks soaring from practices in cyberspace. The Italian effort for cybersecurity has run parallelly to the European one, as demonstrated by the establishment, in 2012, of the Agenzia per l'Italia Digitale (AgID, Digital Italy Agency) and its related Agenda, in line with the European Digital Agenda. Such effort was aimed at pursuing higher levels of innovations and infrastructures through the process of digitalization.

In 2013, the formal establishment of the Italian institutional architecture dedicated to the protection of cyber security was achieved with the adoption of the "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale" (Directive on Cyber Security and National Computer Security) adopted by Decree of the President of the Council of Ministers (DPCM) Monti. The text prescribes the competent offices and the procedures to be followed in order to reduce vulnerabilities, respond promptly to attacks and restore system functionality in the occasion of a crisis.

This cybersecurity strategic doctrine is designed on two main documents adopted within the DPCM 2013 framework: the "Quadro Strategico Nazionale per la Sicurezza dello Spazio Cibernetico" (National Strategic Framework for Cyberspace Security) and the "Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica" (National Plan for Cyber Security and Computer Security) which comprise the operational framework and the strategic guidelines for national cybersecurity implementation, respectively.

Most recently, the latest improvement has been disposed by the adoption of "Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica" (National Plan for Cyber Defence and Computer Security) by the Comitato Interministeriale per la Sicurezza della Repubblica (CISR, Interministerial Committee for the Security of the Republic).[251] This mainly consists in an updated version of the 2013 document which displays the alignment of the Italian framework to the new

[250] Presidency of the Council of Ministers, Relazione Sulla Politica Dell'Informazione 2018, Relazione al Parlamento, p. 6 https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2019/02/Relazione-2018.pdf

[251] Presidency of the Council of Ministers, March 2017, Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica. https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/05/piano-nazionale-cyber-2017.pdf

European standards contained in the aforementioned 2018 European NIS Directive. In practice, the new action plan embraces the following goals:

- Review of the National Cyber Security Core;
- Contraction of the chain of command for the cyber-crisis management;
- Reduction of the complexity of the national architecture, through the suppression/consolidation of organs;
- Progressive unification of CERTs;
- Establishment of a national ICT evaluation and certification center;
- Foundation or venture capital fund;
- Establishment of a national research and development center for cybersecurity;
- Establishment of a national cryptography center.[252]

The body entitled to represent the national reference point for relations with the UN, NATO, the EU and other international organizations and States is the Nucleo Sicurezza Cibernetica (Cybersecurity Center), which covers the role of coordinator with all the actors involved under different forms in the field of cybersecurity.

Italy has been participating to international exercises both at civil and military levels, such as the Cyber Europe 2018, promoted by ENISA, or the Cyber Coalition, promoted by NATO. Moreover, December 31, 2018 marked the end of the Italian presidency of the SMART CYBER 5+5 exercise, which aim is to test the ability of the participants[253] to communicate and respond, in a collaborative way, to the threats originating in cyberspace to improve the collective capacity of cyber defense within a persistent federated framework.[254]

A further example of Italian commitment to strengthening cybersecurity multilaterally by means of cyber diplomacy is testified by its engagement in the drafting process of the “G7 Declaration on Responsible States Behavior in Cyberspace”. This document, also known as the “Lucca Declaration”, was adopted in 2017 during the G7 Foreign Affairs Summit and consists in an important acknowledgement of States’ commitment to address the major risks arising in cyberspace that undermine the political, economic and technological sectors. The document suggests the development and implementation of CBMs for conflict prevention, cooperation, and stability in cyberspace.[255]

[252] Presidency of the Council of Ministers, March 2017, Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica. https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/05/piano-nazionale-cyber-2017.pdf

[253] France, Italy, Malta, Spain, Portugal, Algeria, Libya, Mauritania, Morocco, Tunisia.

[254] Ministry of Defense, Italian Chairmanship of the 5+5 Defense Initiative. https://www.difesa.it/SMD_/Avvenimenti/Iniziativa_5plus5_Presidenza_Italia_2018/Pagine/default.aspx?lang=en

[255] G7, April 11 2017, G7 Declaration on Responsible States Behavior in Cyberspace, Lucca

Despite Italy ranks 25th in the ITU Global Ranking of the 2018 Global Cybersecurity Index[256], the variegated international exercise panorama and the complex framework for national cybersecurity the Country has developed throughout the years reveals the strong awareness of Italian authorities concerning the importance that these opportunities for cooperation have played and will play more in the future. One of the keys to success in protecting national digital assets and services is represented by a necessary process of integration and validation of capabilities in the field of cyber defense in an increasingly broader and more varied international context. Italy, for its part, is working on boosting the efficiency and effectiveness of the national strategic protection system, also with the support of partners and other entities, fully aware that further commitment and coordination is required for guaranteeing a resilient cyber structure.

The regional cooperation between the EU and NATO has always met several challenges due to the differences in the structure of each organization's membership. First of all, the regime of cooperation suffers intrinsically from the different natures of EU and NATO, as the former is merely a military alliance while the latter embraces a broader range of issues, while espousing security issues in a rather indirect way. Secondly, the cybersecurity ambitions and the organizational capacities of both NATO and the EU have been limited by the deliberate preference of national governments for sovereignty in the realms of foreign and defense policy. The third issue, which is arising from the result of the two previous conditions, consists in the limited capability that this cooperation can put into practice when working for a safer cyber-environment. Despite the engagement against cybercrime represents an outstanding example of the EU-NATO, it demonstrates as well that the partnership is limited to few subject matters and in the international resonance this affiliation may have on a global scale.

In order to be effective, this partnership should overcome these constraints by means of complementarity and coordination:

1. The meetings and the initiatives should not be occasional but rooted in a synergic process aimed at developing best-practices for cybersecurity. Indeed, the Countries being part of both entities should commit in developing solid foundations which enable well-established practices, such as the application of similar technological system on different sectors, respectively to the rationality of EU and NATO competences. Information sharing is key to cooperation success and has to be pursued along with broader joint programs on exercise, education and training.

[256] Report on the 2018 Global Cybersecurity Index (GCI),International Telecommunication Union, available at: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf

2. Moreover, those efforts should be backed by bilateral initiatives, such as a possible convergence of EU-USA interests relatively to security standards for cyber products and services, including joint procurements in less sensitive areas; more structured information sharing; continued development and elevation of international cybercrime law enforcement regimes; and consistent and practical data protection regulations.

The trends showing the global impact of cyber threats makes it feasible that partnerships on matters of law enforcement and cybersecurity in general will continue to grow. Given the complex international environment, regional and bilateral experiences could serve as a starting point for global action.

3. After establishing strong basis for collaboration, EU and NATO could further cooperate on cybersecurity policy by including forensics training to improve attribution, additional support to resilience and remediation practices, and greater coordination between the U.S. and EU judicial regimes when it comes to deliver justice to cybercriminals operations.

Only by doing this, they can demonstrate to be valid models for broader partnerships.

Italy, from its side, should stand as a promoter of such cooperation both because has demonstrated to possess qualities in the area of cyber diplomacy as seen in the case of the Lucca Declaration or by working alongside other international law enforcement agencies to increase transnational cooperation on cybersecurity, information sharing, border security, and surveillance. Nevertheless, Italy has also an immense opportunity of amplifying its cyber expertise from both EU and NATO partners that have developed effective mechanisms to achieve cyber readiness, while pursuing its double goal of protecting individuals and state infrastructure.

In conclusion, on the agenda of EU and NATO partners, including Italy of course, the following points should be prioritized:

- Enhancing civil-military cooperation;
- Aligning national and regional economic vision with national security preferences;
- Reorganizing competences so that duplication of efforts are avoided and priorities are concretely met;
- Agreeing on a shared set of definitions and on a common framework of applicability of international law to the field of cyberspace.
- Reinforcing law response procedures to ensure an adequate protection of citizens, businesses, and public institutions;

Only if those, and other goals, are going to be met in the future the countries in the region will be able to navigate the digital age in a safer way.

3.6 The future of cooperation in cyberspace: what lies ahead?

The cyber domain in its width offers a plethora of opportunity and challenges that will dominate several future discussions. Undoubtedly, cyberspace provides opportunities for innovation, trade, social advancement and generally contributes to the development of the whole humankind. In its almost uncontrolled development, however, technology have raised issues for policymakers in cybersecurity's vulnerability, ensuring privacy and protection of data. Moreover, cyber weapons have started being considered as a national security asset, increasing the overall sense of insecurity worldwide. It is now evident that cyberthreats are an everyday challenge that constantly increments in its frequency and capacity as both governmental and non-State actors have become increasingly sophisticated in their assets. Critical infrastructure, intellectual property, private data and sensitive national security information are further and further threatened by cyberattacks, raising competitivity and mistrust among States. Thus, this environment strongly contributes to amplifying the prospects of cyber-warfare between Countries.[257]

Given this uncomfortable environment, questions arise on how the conflict will unfold in this rather new domain. While in the long-term cooperation is strongly desirable, Jason Healey have tried to describe five potential mid-term cyber futures named as Status Quo, Domain, Balkanization, Cybergeddon[258] and Paradise.[259] Each possible scenario is mainly based on the analysis of three key factors: "how strongly the "geography" of cyberspace favors offense over defense; the intensity and kinds of cyber conflicts; and the intensity and kinds of cyber cooperation".[260]

What all those possibilities share, according to Healey, is the fact that the cyber domain will be absolutely not static in the future, but will be governed and transformed by developing technology. Moreover, because the current generations of digital natives has never lived in a world without the Internet, their experience with cyberspace in terms of security and collaboration will probably be different from the one of current experts in the field. Therefore, future generations might embrace cybersecurity diversely.[261]

[257] Rand Corporation, Challenges and Opportunities in Cyberspace, available at: https://www.rand.org/research/primers/cyber.html

[258] Cybergeddon refers to cataclysm resulting from a large-scale sabotage of all computerized networks, systems and activities. It combines cyberterrorism, cyberwarfare, cybercrime, and hacktivism into scenarios of wide-scale internet disruption or economic collapse. Definition from: Goodwin, Bill (2014-01-17). "Internet at risk of 'cybergeddon' says WEF". Computer Weekly.

[259] Healey J., The Five Futures of Cyber Conflict and Cooperation, Atlantic Council, available at https://www.atlanticcouncil.org/images/files/publication_pdfs/403/121311_ACUS_FiveCyberFutures.pdf

[260] Ibidem.

[261] Ibidem.

The Status Quo prediction described by Healey is characterized by stability notwithstanding discontent, difficulties and disruptions. No massive cyber war has occurred. In brief, the future of cyberspace conflict looks similar to the circumstances we are experiencing nowadays, where offense prevails over defense and the intensity of cooperation on response, standards and cybercrime remains limited.[262]

If the Conflict Domain is going to be realized in the mid-term future, cyber terror and cyber war will become reality, with full range conflicts encompassing all the domains of air, space, land and sea. Even if in this scenario offense will prevail over defense, defensive measures will be enhanced in order to respond to full range attacks. For what concerns cooperation, nations will behave accordingly to the norms and rules established and supervised by international bodies, as for the case of international law that regulates the other domains air, space, land and sea. All the rules, treaties, confidence-building measures and laws will be probably re-adapted or forged to the new status quo of the conflict.[263]

A different alternative is defined by the process of Internet Balkanization, where Countries instead of relying on a single open source of Internet, will be able to establish borders and create a compound of "small Internets", on the basis of the discourse elaborated mainly by Russia and China. Inevitably, the Internet would be transformed not representing anymore a global network but a fragmented one and, thus, would require agreements on the exchange of international traffic. This trend is everything but new, and have been already covered in this work by mentioning the Shanghai Cooperation Organization's latest commitment on the matter. An alternative format would see the United Nations taking the lead in regulating the scheme of agreements so that no Country is surmounted by others. Despite a Balkanized Internet could represent a solution to the problems of cyberspace, benefitting from a strongly regulated regime, States would meet as well severe limits on cross-border commerce and interaction, levelling the trade-off in an unprofitable way.[264]

The Paradise features a safer and more secure world thanks to both technological development and regulation. Only in this case, we could experience a superior defense rather than offense, so it would be arduous for actors to act maliciously. Despite history has demonstrated that it is actually possible to build technology which is aimed at securing the Internet, the chances that Paradise will fully occur are unlikely. Indeed, along with technology, what is needed is a cooperative and good behavior pursued by all actors, being they governments, companies, and individuals.[265]

[262] Ibidem.
[263] Ibidem.
[264] Ibidem.
[265] Ibidem.

Finally, Cybergeddon represents the worst-case scenario where we find a completely unruled cyber domain with an uncontrollable offense-over-defense scheme. In this scenario, with very little effort, hackers (being they individuals, organized-crime groups, or national militaries) could achieve large-scale effects, while the Internet would be not trusted as a safe place where to communicate or commerce. The level of cooperation among nations would be basically null and useless, completely overwhelmed by distrust and its realization would be the result of lack of responsibility and commitment by government and civil society.[266]

In the attempt to apply the analysis of national strategies, the United States and other NATO Countries would prefer the Paradise condition, as it would provide long-term stability and solid basis on which commerce and international interactions could be carried without too much worry. On the other side, despite countries like Russia or China would appreciate a certain level of stability provided by the conditions of the Paradise solution, they would much prefer a Balkanized Internet, in order to exert substantial control over the field making it strictly a national domain that enables Countries to blocking access to content, while transnational relations are strictly regulated by stipulated agreements.

While it is not very much clear what to expect in the future of cyberspace, experts and policymakers have as well raised the question of whether cyberspace need a hegemon. Clashing national and global interests are unavoidable in the cyber domain as no global government is responsible for resolving disputes. However, the United States have often posed themselves as guarantor of such public good amalgamating it with national interest. Covering the position of hegemon in the international system for decades, the US have tried to extend such control over the fifth domain as well. This has been so for an evident rationale: the United States, the biggest economy in the world, has strong economic reasons to secure and support a safe and reliable Internet. Furthermore, the Country retains an important military stake in cybersecurity given the scope and the complexity of communications among military forces and along the chain of command.[267]

All of those motifs are enough justification for noticing the United States to take the lead and other Countries to accept it, as international cybersecurity cooperation is difficult to sustain in a complete anarchic environment. This is the reason why the "Theory of Hegemonic Stability" have partially shaped the debate over the future cooperation in the cyber domain: in the case of clear hierarchic structure, a State with dominant capabilities can take the lead and sustain the cooperation by providing public goods and reducing the problems arising from collective action. Furthermore, the

[266] Ibidem.

[267] Rovner, Joshua and Tyler Moore, Does the Internet Need a Hegemon?, Journal of Global Security Studies, 2017. Published by Oxford University Press on behalf of the International Studies Association.

hegemon is supposed to provide help to coordinate action and deter challengers that could threaten the global order.

There are some concerns against this view. Firstly, the fear that hegemony could destabilize the status quo exerting its preponderance of power and increasing fear and suspicion among others should be recognized. Secondly, the status of leadership, although being functional in the first period of cooperation, might become less relevant and, if the leading Country is not ready to give up its position, could behave against the collective interest.[268] Additionally, contemporary observers raised doubts on the ability of the United States to play the role of a "good hegemon". This claim can be explained by the fact that not only the United States are currently experiencing a period of downfall of their leading role in the world order, but even because – cybersecurity wise – they have demonstrated not having the sufficient capabilities to protect their own critical system, as demonstrated by the latest alleged Russian intrusion in the American system during the period of the 2016 Presidential elections.[269]

We have registered a decline in the American influence but not a complete cancellation. Thus, what should we expect for the future? Probably, the United States could more safely pursue its interests without the fear of eroding cybersecurity. According to the investigation of Rovner and Moore (2017) based on empirical data, it appears that the government in Washington is intending to both increase its involvement in the process of building up an Internet governance in order to provide with help in codifying a set of rules for the domain, as well as to give up opportunities for espionage and sabotage by strengthening encryption, alerting technology firms to vulnerabilities in software and taking additional steps to make Internet communications inviolable.

There is a mission for the global community for the years to come and consists in assuring resilience to the cyber global infrastructure, which evidently will be more pervasive in our everyday life and in the practice of business and states activities. In this process of avoiding what Haley would call the Cybergeddon scenario, the commitment of governments covers a fundamental function. Notwithstanding the different ideologies that the Countries reasonably assume according to their strategies and interests, every and each State bears the responsibility of working for the goal of cyber resilience. It is undeniable that cybersecurity is a global good, and should be treated as such for the years to come. We have showed how countries perceive the threats originating from cyberspace, demonstrating that the majority of States understand this as a global concern that needs to be tackled.

[268] Ibidem.

[269] Valeriano B., Jensen, B., & Maness R., Cyber Strategy: The Evolving Character of Power and Coercion, New York: Oxford University Press, 2018, p. 200.

No matter the strategies, Countries should share this sense of global responsibility and act by this terms in the following ways. First of all, acknowledging the fact that the knowledge around the world of cyber is still underdeveloped and limited to some few experts of the field, there should be massive investments in researching and training, both to deliver a far-reaching understanding of the characteristics and the threats originating from cyberspace and to be able to tackle the consequent perils. Only through this way it is actually possible to strengthening the cybersecurity of the systems and replace legacy systems that are – by demonstration – insufficiently secure.

Secondly, Countries should address what has become the common behavior in cyberspace and the necessity to avoid a completely unregulated future of cyber warfare. If the new normal has become the practice of cyber espionage and governments will never be prone to ban completely this kind of action, they should agree at least on establishing benchmarks of what is acceptable behavior and what is not. This means, first of all, coming to agreeing on the definitions of practices conducted in cyberspace. The acceptance of a shared terminology is really upon the effort and the sound judgement of States and is fundamental as it consists in the first step for establishing solid cooperation. Only after such achievement it is actually possible to elaborate a set of shared and agreed norms which can positively regulate the relations in the cyber sphere.

As presented throughout the work, this process of cooperation encounters a wide range of technical and strategic limitations which pose serious challenges to the feasibility of a possible treaty on cybersecurity. Thus, it is clear that such goal will require time, effort and, possibly, creativity. The experience of the Cold War has demonstrated that humankind can step further clashing interests and ideologies and proceed towards development. However, if policymakers can learn from this experience, they can as well elaborate different schemes of cooperation, being it hegemonic collectivity, multilateral cooperation or any other formula they may find as appropriate. Whatever the model, it is of paramount importance to channel the resources in a way to avoid overlapping functions and waste, especially because technological development runs much faster than law enforcement.

In conclusion, even if the Paradise condition is hardly meetable, everything should be done in order to avoid any chance of cybergeddon realization.

Conclusions

This thesis aims to identifying current challenges and perspective scenarios of international cooperation in the field of cybersecurity. Following the applied analysis of International Relations theories to the national strategies of Russian Federation, People's Republic of China and the United States, it can be concluded that despite there is a diffused awareness of the increasing trends of threatful scenarios in cyberspace, the international community has a long way ahead to establish a sufficient level of global governance to ensure resiliency and protection both at State and non-State level. The results that have emerged from the applied research showed that there are some important complexities that governments should address in order to be able to establish a resilient cybersecurity regime. Some of the deadlocks are strictly related to the nature of technology and its fast development, thus, they could be faced down with improvements in research and knowledge in the field. In addition to those aspects, some other complications stem from high levels of diffused uncertainty and different strategies and perceptions. Combining those altogether, Countries risk to incur in several dilemmas which, if not mitigated by established lawfully framework, could result – in the worst case scenario – in a large-scale sabotage of all computerized networks, systems and activities which combines cyberterrorism, cyberwarfare, cybercrime, and hacktivism into scenarios of wide-scale Internet disruption or economic collapse.

The main objective of the first chapter consisted in the investigation of the characteristics of the cyber domain through the analytical instruments offered by the Realist, Liberal, and Constructivist theories. In particular, the classical concepts of power, structure and actors have been confronted with the corresponding object of cyberspace, allowing the work to present some main findings. The first observation is related to the principles of geography and sovereignty determination, which are cardinal concepts to the realist theory for determining the characteristic of a State as the main actor of the international system. Due to the virtual nature of cyberspace and to the open character of the Internet, cyber participants have to deal with blurred borders and uncertain definitions of national sovereignty. Therefore, the ambiguity over territorial determination makes the governance of cyberspace and of network systems a matter of discussion regarding whether it should imply the establishment of global governance or should respect the idea of classical national sovereignty. However, given that cyberspace produces transnational threats, the option of collective security provided by the liberal theory sounds to be a plausible solution to collectively administer the Internet as long as it remains open and global. The second result is based on the assessment of the characteristics and the role that cyber actors assume in the fifth domain. In this field, we have acknowledged that the entities acting in cyberspace could be States as well as non-State actors, in recognition of the approach pursued by the liberal theories. Therefore, compared to other warfighting domains, cyberspace hosts increasing numbers of cyber-participants who have to deal with miscellaneous intentions and different perceptions of their responsibility on collective security, with the risk of fueling the conditions for instigating the cybersecurity dilemma. Finally, the third result deals with acknowledging the trend of power diffusion which the world has been experiencing due to the fast development and outreach of technology. Power is barely quantifiable when speaking about cyber: traditional capabilities are questioned because power is modified, diffused and difficult to be observed. Having large territories and substantial amount of resources became differently important when the technological skills are considered one of the most relevant tool for warfighting, both for States and non-State actors. Moreover, due to high levels of ambiguity with respect to capabilities and – consequently – to intentions, the role of perceptions becomes fundamental in determining the limits of States' actions and makes threat assessment a challenging process. Uncertainty produces as well two conflicting consequences. On one side, it fuels competition pushing States to reinforce their offensive capabilities further enhancing the cybersecurity dilemma. On the other side, uncertainty may as well mitigate such dilemma due to the risk of an incorrect understanding of the real intentions or responsibilities of other States. By current times, it looks like the second option has been working as one of the major deterring force since no full-scale cyber war has occurred yet. In conclusion, the Realist and Liberal theories encounters too many barriers to their applicability in cyberspace.

The analysis carried in the second chapter focused on the official documents of the national cyber strategies of the States have led to acknowledging that in the international panorama there is a full recognition of the threats and the dangers that the fifth domain advance. Nevertheless, the collective security initiative that has been embraced until now by the international community have provided unsatisfactory results. At the same time, Countries have the feeling of operating in an anarchic system, as the realist theory suggests. Nevertheless, the sense of fear is produced by the perception that they have of the *Self* and of the *Other*, which brings them into developing different national strategies, based on a subjective understanding of the other's intentions. In practice, the constructivist approach is instructive in this case to explain the reasons for which Countries offer diversified conceptualization on the matter of cybersecurity, with consequential actions at the international and regional levels. The analysis bring into consideration two main elements which hamper the achievement of cooperation in the field. The first issue is the widespread lack of trust among States at the level of cyberspace. This is inevitably determined by the fact that there is an acquiescence on the use of cyber tools between States, especially with regards to espionage practices, but there is no clarity or transparency on its purpose. The second issue deals with language and terminology. Such problematic subsist not only because there is a concrete difficulty with different languages, which anyway could be overcome by translators, but the real problem lays on the lack of agreement on the use of specific cyber terminology. The only way of pursuing the establishment of a cyber regime is by accepting the constructivist idea that the structure of the system in an ongoing process, and not necessarily a static and anarchic system, which can change following the ideas that the States develop and embrace. Mediating perceptions and combining ideas are possible solutions for moving closer States' different postures and for guiding them toward a commonly shared normative system, which require time and appropriate tools.

The examples displayed in the third chapter reveal how Countries have decided to tackle the issues arising in cyberspace by means of establishing cooperation at the international, regional level and bilateral level. Even in those examples, what emerged from the analysis is that despite the cooperative effort, States are still largely behaving accordingly to their ideas and perceptions. Therefore, all those examples of cooperation are showing that, especially at the international level, there are fundamental discrepancies that place the international community far from embracing a shared concept of collective security in the field of cyber. This is demonstrated by the fact that, throughout the years of activity of the UN GGEs, concerns have been raised in terms of inclusivity and participation, with the consequence of settling the OEWG as a more all-embracing and inclusive group. Moreover, Countries have met ideological and technical discrepancies in the adoption of definitions and principles, differences in technical, legal and diplomatic capacities and leaderships, due to regional alignments. From the constructivist point of view based on ideas, a regional example of cooperation is offered by the partnership between EU and NATO, which associate Countries with rather similar goals and interests, thus, reducing the conflictual approach which characterizes the international debate. This partnership, indeed, represents a good starting point for coordination, but encounters already challenges due to the structural differences of memberships and the fact that the joint work is still limited to few subject matters. Further models of cooperation have also been framed with examples of public-private partnerships and of an attempt, with the Tallinn Manual, to design a framework for international law applied to cyberspace which nevertheless is a product of a non-State sponsoring initiatives.

Based on the elaboration of collected results, it is clear that the current levels of cooperation in the field of cybersecurity are not reaching satisfactory standards both in technical and legal terms. Given that establishing transnational cyber security is definitely a hard task which will constantly occupy future discussions, it is of paramount importance that all cyber participants contributes to the cause with enhanced commitment. To better understand the implications of the results achieved throughout the analysis, we must emphasize the important role that governments occupy in this field, as main developer of resilience of a global public good and since no global cyber regime has been established yet.

There are four main tasks for the future to come that government should accomplish:

1. Governments should invest in enhancing training and research in order to build resilient systems not only for States' infrastructure but as well for private entities and individuals. Indeed, public-private partnerships could offer a good practice for defense systems' development which are inclusive and address all actors' necessities.
2. By the time defense systems get developed, Countries should commit to the process of information exchange in order to reduce the current levels of uncertainty, in an effort to overcome the problem of attribution. Those actions should be the result of the implementation of confidence-building measures among participants, having understood the effects of distributing the costs associated with overcoming technical hurdles.
3. Once good practices are established as the "new normal", further efforts of cooperation are required among States to develop consensus on a framework of norms that regulate the sharing of information, arrest, extradition, and prosecution of criminal acts in cyber space. Crimes committed in cyberspace often cross international borders; therefore, a global action is needed in tackling such misbehaviors.
4. Those practices, which will grow gradually and accordingly to technological progress, will contribute to the development of a cyber weapons non-proliferation regime. Despite being this a long-term and rather ambitious goal, it would have the effect of limiting the number of cyber threats to which a State must develop counter measures, while States are able to enjoy better defense systems thanks to their initial investments.

Thus far, governments need creativity in shaping the ways and the tools for pursuing such recommendations. Definitely, regional and bilateral cooperation could represent models from which to start this cooperative process, and which can later be applied at the international level. Nevertheless, this kind of selected approach raises the chances of polarization. This is the reason for which it is important that the international community continues to set year by year a global agenda on the matter, in order to provide general guidelines for cooperation and to pursue a common goal of open and safe Internet. Finally, States should rethink what leadership could provide and should perceive best practices of other States in a lucrative way rather that by increasing alienation and mistrust.

The contribution that this work is giving to the research on the matter of cybersecurity is to provide a comprehensive application of the most relevant theories of International Relations to the features of cybersecurity, by underlying and trying to fix the grey areas of theoretical investigation of the cyberspace. What emerged from this analysis is the need of rethinking the classical assumptions of International Relations when applying them to cyberspace, including the principles of deterrence and sovereignty, which by now do not find exhaustive applicability in the field of cyberspace. The Constructivist theory has been instructive for understanding States' perceptions and consequential behavior. Given its assumption on the international system as a process, by denying that it is static and anarchic, offers hopes for future cooperation when countries will start to share matching ideas and norms. Furthermore, because this topic is rather new to policymakers and researchers, future expectations envisage additional discussion on the matter and a reorganization of the approach to the topic. If it is true that cyber-attacks are becoming the "new normal", therefore, we may expect to appreciate them as the "new normal" and build research upon that.

For what concern the State's strategies and the patterns of cooperation in cybersecurity, this comparison have served to display the achievements of the global community as well as the conflicting arguments that Countries have been facing so far. As we are currently living in a moment of transition, the old standards that regulated the global order seem to not fully apply to ongoing and future security trends. Countries are evidently diverging on the methods for assuring cybersecurity worldwide and have decided to embrace regional or bilateral practices to achieve – at least – minimum standards of cybersecurity. Notwithstanding the different ideologies that Countries reasonably assume according to their strategies and interests, each State holds the responsibility of working hard for achieving the goal of cyber resilience. Scenarios of cooperation are plausible from the moment that cybersecurity is perceived as a global good, and if States are intending to avoid total anarchy in the domain they should actively commit to build up resilient networking systems through both technological development and law enforcement. While this is definitively a long-term perspective, in the short-term we should expect the effort of implementing confidence building measures and basic practices of information sharing in order to rebuilt trustworthy relations among the components of the international community.

Bibliography

Official documents of the Russian Federation

- Doctrine of Information Security of the Russian Federation, “Доктрина информационной безопасности Российской Федерации”, approved December 5th 2016 by Decree of the President Vladimir Putin. Retrieved from: http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163.
- Foreign Policy Concept of the Russian Federation (approved by President of the Russian Federation Vladimir Putin on November 30, 2016), retrieved from the official website of the Embassy of the Russian Federation to the United Kingdom and Northern Ireland: https://www.rusemb.org.uk/rp_insight/
- Russian presidential decree no. 1895, “Доктрина информационной безопасности Российской Федерации” [Doctrine of Russian Information Security], September 9, 2000, http://base.garant.ru/182535/
- Дмитрий Грибков, Референт аппарата Совета безопасности Российской Федерации, О формировании системы международной информационной безопасности, журнала «Международная жизнь», МИД РФ, 2015. https://interaffairs.ru/jauthor/material/1352

Official documents of People’s Republic of China

- Rogier Creemers, National Cyberspace Security Strategy, December 2017, translation from the official National Cybersecurity Strategy released by Cyberspace Administration of China (CAC) available at the following link http://www.cac.gov.cn/2016-12/27/c_1120195926.htm
- Lu Wei, Persisting in Respect for the Principle of Cyber Sovereignty, Promoting the Construction of a Community of Common Destiny in Cyberspace, translation of the document released by the vice-director of the Central Propaganda Department, the Director of the Office of the Central Leading Group for Cybersecurity and Informatization, and the Director of the Cyberspace Administration of China: https://chinacopyrightandmedia.wordpress.com/2016/03/02/persisting-in-respect-for-the-principle-of-cyber-sovereignty-promoting-the-construction-of-a-community-of-common-destiny-in-cyberspace/

Official document of the Republic of Italy

- Ministry of Defense, Italian Chairmanship of the 5+5 Defence Initiative. Retrieved from: https://www.difesa.it/SMD_/Avvenimenti/Iniziativa_5plus5_Presidenza_Italia_2018/Pagine/default.aspx?lang=en
- Official page of the Italian Ministry of Foreign Affairs on the role of Italy in NATO. Retrieved from: http://www.esteri.it/mae/it/politica_estera/organizzazioni_internazionali/nato.html
- Official page of the Italian Ministry of Foreign Affairs on the role of Italy in the EU. Retrieved from: http://www.esteri.it/mae/it/politica_europea/italia_in_ue
- Presidency of the Council of Ministers, March 2017, Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica. Retrieved from: https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/05/piano-nazionale-cyber-2017.pdf
- Presidency of the Council of Ministers, Relazione Sulla Politica Dell'Informazione 2018, Relazione al Parlamento. Retrived from: https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2019/02/Relazione-2018.pdf
- Statement on the EU-NATO cooperation on the official website of the Italian Ministry of Foreign Affairs. Retrieved from: http://www.esteri.it/mae/it/politica_estera/organizzazioni_internazionali/nato.html

Official documents of the United States

- China publishes first National Cybersecurity Strategy, Report by United States Information Technology Office (USITO), available at: http://www.usito.org/news/china-publishes-first-national-cybersecurity-strategy
- Final Report of the Defense Science Board (DSB) Task Force on Cyber Deterrence, Office of the Secretary of Defense, February 2017. Retrieved from: https://www.acq.osd.mil/dsb/reports/2010s/dsb-cyberdeterrencereport_02-28-17_final.pdf
- Mattis Jim, Summary of the 2018 National Defense Strategy of the United States of America, Department of Defense of the United States of America, available at: https://apps.dtic.mil/dtic/tr/fulltext/u2/1045785.pdf
- Obama B., Publication on Foreign Policy Cyber Security, the White House. Retrieved from: https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity

- President Trump, The White House – Office of the Press Secretary, Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, May 11, 2017. Retrieved from: https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/
- Remarks as delivered by the Honorable James R Clapper Director of National Intelligence. Senate Select Committee on Intelligence – IC's Worldwide Threat Assessment Opening Statement, Tuesday Feb 9, 2016. Retrieved from: https://www.dni.gov/files/documents/2016-02-09SASC_open_threat_hearing_transcript.pdf
- Remarks on International Law and Stability in Cyberspace; Legal Adviser Brian J. Egan; Berkeley Law School, California, 2016. Retrieved from: https://2009-2017.state.gov/s/l/releases/remarks/264303.htm

Official documents of International and Regional Organizations

- "Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation", Adopted by Heads of State and Government in Lisbon, NATO, 2010. Retrieved from: https://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf
- Brent L., NATO's role in cyberspace, NATO Review, 2019. Available at: https://www.nato.int/docu/review/2019/Also-in-2019/natos-role-in-cyberspace-alliance-defence/EN/index.htm
- Charter of the United Nations, San Francisco, 1945. Retrieved from: https://www.un.org/en/charter-united-nations/index.html
- EU Cybersecurity Act, ENISA And Cybersecurity Certification Framework, European Commission, June 2019. Retrieved from: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60505
- EU-NATO cooperation – Factsheet, EU External Action, Bruxelles, June 2019. https://eeas.europa.eu/headquarters/headquarters-Homepage/28286/eu-nato-cooperation-factsheet_en
- G7, April 11 2017, G7 Declaration on Responsible States Behavior in Cyberspace, Lucca. Retrieved from: https://www.mofa.go.jp/files/000246367.pdf
- ITU Annual Progress Report 2018, International Telecommunication Union, available at: https://www.itu.int/en/council/planning/Documents/Annual-report-2018.pdf
- National Cyber Security Strategies, European Union Agency for Cybersecurity, ENISA, available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies

- NATO, "Cyber Defence", 2017, February 17, NATO Official Website. Retrieved from: http://www.nato.int/cps/en/natohq/topics_78170.htm
- Report on the 2018 Global Cybersecurity Index (GCI),International Telecommunication Union, available at: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf
- Russia's national security strategy and military doctrine and their implication for the EU, Directorate-General for External Policies – Policy Department, European Parliament, 2017. Retrieved from: http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/578016/EXPO_IDA(2017)578016_EN.pdf.
- Securing our common future: An Agenda for Disarmament, Office for Disarmament Affairs, United Nations, New York, 2018. Retrieved from: https://s3.amazonaws.com/unoda-web/wp-content/uploads/2018/06/sg-disarmament-agenda-pubs-page.pdf#view=Fit
- Shanghai Declaration on the Establishment of the SCO, Shanghai Cooperation Organization, 2001. Retrieved from: http://eng.sectsco.org/load/193054/
- The EU Cybersecurity Act brings a strong agency for cybersecurity and EU-wide rules on cybersecurity certification, European Commission, June 2019, Retrieved from: https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-act-brings-strong-agency-cybersecurity-and-eu-wide-rules-cybersecurity
- The North Atlantic Treaty, Washington D.C., 4 April 1949. Retrieved from: https://www.nato.int/cps/en/natolive/official_texts_17120.htm
- The Shanghai Convention on Combating Terrorism, Separatism and Extremism, Shanghai Cooperation Organization, 2001. Retrieved from http://eng.sectsco.org/load/202907/
- Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, United Nations Office for Outer Space Affairs, 1967, available at: http://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introouterspacetreaty.html
- United Nations General Assembly Resolutions:
  - A/53/576, Role of science and technology in the context of security, disarmament and other related fields : report of the 1st Committee, UN General Assembly (53rd sess. : 1998-1999)., available at: https://digitallibrary.un.org/record/264457?ln=en,
  - A/66/359, Letter dated 2011/09/12 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, available at: https://digitallibrary.un.org/record/710973?ln=en

- A/68/98, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, : note / by the Secretary-General, 2013, available at: https://digitallibrary.un.org/record/753055?ln=en
- A/70/174, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security : note / by the Secretary-General, 2015, available at: https://digitallibrary.un.org/record/799853?ln=en
- A/RES/58/32, “Developments in the field of information and telecommunications in the context of international security”: resolution / adopted by the General Assembly, UN. General Assembly (58th sess. : 2003-2004), available at: https://digitallibrary.un.org/record/507790?ln=en
- A/RES/59/61, “Developments in the field of information and telecommunications in the context of international security”: resolution / adopted by the General Assembly, UN. General Assembly (59th sess. : 2004-2005), available at: https://digitallibrary.un.org/record/536240?ln=en
- A/RES/60/45, “Developments in the field of information and telecommunications in the context of international security”: resolution / adopted by the General Assembly, UN. General Assembly (60th sess. : 2005-2006), available at: https://digitallibrary.un.org/record/562444?ln=en
- A/RES/64/211, “Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures”: resolution / adopted by the General Assembly, UN. General Assembly (64th sess. : 2009-2010), available at: https://digitallibrary.un.org/record/673712?ln=en,
- A/RES/66/24, “Developments in the field of information and telecommunications in the context of international security”: resolution / adopted by the General Assembly, UN. General Assembly (66th sess. : 2011-2012), available at: https://digitallibrary.un.org/record/718518?ln=en
- A/RES/68/243, “Developments in the field of information and telecommunications in the context of international security”: resolution / adopted by the General Assembly, UN. General Assembly (68th sess. : 2013-2014), available at: https://digitallibrary.un.org/record/763298?ln=en
- A/RES/70/237, “Developments in the field of information and telecommunications in the context of international security”: resolution / adopted by the General Assembly", UN. General Assembly (70th sess. : 2015-2016), available at: https://digitallibrary.un.org/record/815989?ln=en

    - A/RES/73/266, “Advancing responsible State behaviour in cyberspace in the context of international security”: resolution / adopted by the General Assembly, UN. General Assembly (73rd sess. : 2018-2019), available at: https://digitallibrary.un.org/record/1658328?ln=en
    - A/RES/73/27, “Developments in the field of information and telecommunications in the context of international security”: resolution / adopted by the General Assembly, UN. General Assembly (73rd sess. : 2018-2019), available at: https://digitallibrary.un.org/record/1655670?ln=en
- United Nations Institute for Disarmament Research, 2019 Cyber Stability Conference Summary Report, United Nations, New York, available at: http://unidir.org/programmes/security-and-technology/2019-cyber-stability-conference
- World Economic Forum, The Global Risks Report 2019 14th Edition, Geneva, 2019. Available at: http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

Books and publications

- Brown, C., Eckersley, R., Valeriano, B., & Maness, R., International Relations Theory and Cyber Security: Threats, Conflicts, and Ethics in an Emergent Domain. In The Oxford Handbook of International Political Theory, Oxford University Press, 2018.
- Buchanan B., The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations, New York: Oxford University Press, 2017.
- Choucri N., Cyberpolitics in International Relations, MIT Press, 2012.
- Collins, A., Contemporary Security Studies. Oxford: Oxford University Press, 2015.
- Deibert R., Trajectories for Future Cybersecurity Research, in Gheciu A., Wohlforth W. C., The Oxford Handbook of International Security, New York: Oxford University Press, 2018.
- Dunn Caveltry M., Cyber-Security in Collins A., Contemporary Security Studies, New York: Oxford University Press, Fourth ed., 2016.
- Kassab H.S. (2014) In Search of Cyber Stability: International Relations, Mutually Assured Destruction and the Age of Cyber Warfare. In: Kremer JF., Müller B. (eds) Cyberspace and International Relations. Springer, Berlin, Heidelberg.
- Kremer JF., Müller B. (eds) Cyberspace and International Relations. Springer, Berlin, Heidelberg.
- Libicki, M. C., Cyberdeterrence and cyberwar, RAND Corporation, 2009.
- Mazzei F., Marchetti R., Petito F., Manuale di Politica Internazionale, Egea, 2010.

- Sanger D. E., The perfect weapon: war, sabotage, and fear in the cyber age, New York: Crown, 2018.
- Schmitt, M., Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press, 2017.
- Schmitt, M., Tallinn Manual on the International Law Applicable to Cyber Warfare. New York, United States of America: Cambridge University Press, 2013.
- Shaheen S., Offense–Defense Balance in Cyber Warfare. In: Kremer JF., Müller B. (eds) Cyberspace and International Relations. Springer, Berlin, Heidelberg, 2014.
- Singer, P. W., & Friedman, A., Cybersecurity and cyberwar: What everyone needs to know. Oxford: Oxford University Press, 2014.
- Valeriano B., Jensen, B., & Maness R., Cyber Strategy: The Evolving Character of Power and Coercion, New York: Oxford University Press, 2018.
- Van Evera S., Causes of War: Power and the Roots of Conflict, Ithaca, London, Cornell University Press, 1999.
- Wendt A., Social theory of international politics, Cambridge University Press, Cambridge, UK, 1999.

Articles and Journals

- "UN Chief Calls For Regulatory Scheme For Cyberwarfare," Radio Free Europe/Radio Liberty, February 19, 2018. Retrieved from: https://www.rferl.org/a/un-guterres-calls-for-cyberwarfare-rules/29049069.html
- A Digital Geneva Convention to protect cyberspace. Microsoft Policy Papers, available at: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH
- Anastasia Tolstukhina, Two Cyber Resolutions Are Better Than None, Russian International Affairs Council (RIAC), 2019. Available at: https://russiancouncil.ru/en/analytics-and-comments/analytics/two-cyber-resolutions-are-better-than-none/
- Borghard E. D., Lonergan S. W., Why Are There No Cyber Arms Control Agreements?, Council on Foreign Relations, January 16, 2018. Retrieved from: https://www.cfr.org/blog/why-are-there-no-cyber-arms-control-agreements
- Breene K., Who are the cyberwar superpowers?, World Economic Forum, May 2016. Retrieved from: https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/
- Brian J. Egan, International Law and Stability in Cyberspace, 35 Berkeley Journal of International Law. 169, 2017. Available at: http://scholarship.law.berkeley.edu/bjil/vol35/iss1/5

- Claude Jr. I., Collective Security as an Approach to Peace in: Classic Readings and Contemporary Debates in International Relations ed. Donald M. Goldstein, Phil Williams, & Jay M. Shafritz. Belmont CA: Thomson Wadsworth, 2006, pp. 289–302.
- Cyber Warfare Infographics, Valdai Discussion Club, 27.08.2019, available at: http://valdaiclub.com/multimedia/infographics/cyber-warfare/
- D. Allen, P., Gilbert, D. , "The Information Sphere Domain Increasing Understanding and Cooperation", Johns Hopkins University, Applied Physics Lab, Booz Allen Hamilton, 2018. Retrieved from: https://ccdcoe.org/uploads/2018/10/09_GILBERT-InfoSphere.pdf
- Dunn Cavelty M., The Normalizaiton of Cyber-International Relations, Center For Security Studies (CSS), ETH Zürich, 2015. Retrieved from: https://css.ethz.ch/en/services/digital-library/articles/article.html/189525/pdf
- Efrony, D., & Shany, Y., A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice. American Journal of International Law, 112(4), 2018, 583-657. Retrieved from: https://www.cambridge.org/core/services/aop-cambridge-core/content/view/54FBA2B30081B53353B5D2F06F778C14/S0002930018000866a.pdf/rule_book_on_the_shelf_tallinn_manual_20_on_cyberoperations_and_subsequent_state_practice.pdf
- Ellen Nakashima, "U.S. and Russia Sign Pact to Create Communication Link on Cyber Security", Washington Post, June 17, 2013. Retrieved from: https://www.washingtonpost.com/world/national-security/us-and-russia-sign-pact-to-create-communication-link-on-cyber-security/2013/06/17/ca57ea04-d788-11e2-9df4-895344c13c30_story.html.
- Elsa Kania, Samm Sacks, Paul Triolo, China's Strategic Thinking on Building Power in Cyberspace, Cybersecurity Initiative, New America, 2019. Retrieved from https://www.newamerica.org/cybersecurity-initiative/blog/chinas-strategic-thinking-building-power-cyberspace/
- Francisco Rogério Moreira Campos, Bruno de Pinheiro Tavares, Tallinn Manual and the use of force, The Institute for Research on Internet & Society, 2016. Retrieved from: http://irisbh.com.br/en/tallinn-manual-and-the-use-of-force/
- Goodwin, Bill (2014-01-17). "Internet at risk of 'cybergeddon' says WEF". Computer Weekly. Retrieved from: http://www.computerweekly.com/news/2240212690/Internet-at-risk-of-cybergeddon-says-WEF
- Healey J., The Five Futures of Cyber Conflict and Cooperation, Atlantic Council, available at: https://www.atlanticcouncil.org/images/files/publication_pdfs/403/121311_ACUS_FiveCyberFutures.pdf

- Henriksen, A., The end of the road for the UN GGE process: The future regulation of cyberspace, Journal of Cybersecurity, 2019, 1–9. Retrieved from: https://academic.oup.com/cybersecurity/article/5/1/tyy009/5298865
- Hongju Koh, Harold, International Law in Cyberspace, Yale university, 2012. Faculty Scholarship Series, 4854. Retrieved from: https://digitalcommons.law.yale.edu/fss_papers/4854
- Jensen, E.T., The Tallinn Manual 2.0: Highlights and Insights, 48 Georgetown Journal of International Law, 735 (2017). Retrieved from: https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf
- Leetaru, Kalev, What Tallinn Manual 2.0 teaches us about the new cyber order, Forbes, 2017. Retrieved from: https://www.forbes.com/sites/kalevleetaru/2017/02/09/what-tallinn-manual-2-0-teaches-us-about-the-new-cyber-order/#1780f04d928b
- Libicki M., Cyberspace Is Not a Warfighting Domain, A Journal of Law and Policy for the Information Society, v. 8, no. 2, Fall 2012, p. 325-340. Retrieved from: https://kb.osu.edu/bitstream/handle/1811/73111/1/ISJLP_V8N2_321.pdf
- Libicki, M. C., Expectations of Cyber Deterrence, Strategic Studies Quarterly, Winter 2018, The Air University Press. Retrieved from: https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-12_Issue-4/Libicki.pdf
- Live FireEye Cyber Threat Map, available at: https://www.fireeye.com/cyber-map/threat-map.html
- Lu Chuanying, China’s Emerging Cyberspace Strategy, The Diplomat, 2016. Retrieved from: https://thediplomat.com/2016/05/chinas-emerging-cyberspace-strategy/
- Mauer, T., Cybersecurity in a Complex Environment: Transatlantic Divergences and Diplomatic Achievements, VEREINTE NATIONEN – German Review on the United Nations, Vol. 64, 2/2016, pp. 51–55. Retrieved from: https://dgvn.de/fileadmin/publications/PDFs/Zeitschrift_VN/VN_2016/Heft_2_2016/Maurer_Cyberraum_VN_2_16_engl_web.pdf
- Mearsheimer, JJ, The False Promise of International Institutions, The MIT Press, International Security, Vol. 19, No. 3, p. 5–49, 1994. Retrieved from: http://www.jstor.org/stable/2539078
- Michael Connell and Sarah Vogler, Russia’s Approach to Cyber Warfare, CAN Analysis and Solutions, March 2017. https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf
- Nye, J. S., Deterrence and Dissuasion in Cyberspace, International Security, 41, 2017, 44-71. Retrieved from: https://www.mitpressjournals.org/doi/full/10.1162/ISEC_a_00266
- Nye, J. S., The Future of Power, New York: Public Affairs, Vol.11-No. 8, 2011. Retrieved from: https://www.files.ethz.ch/isn/154756/issuesinsights_vol11no08.pdf

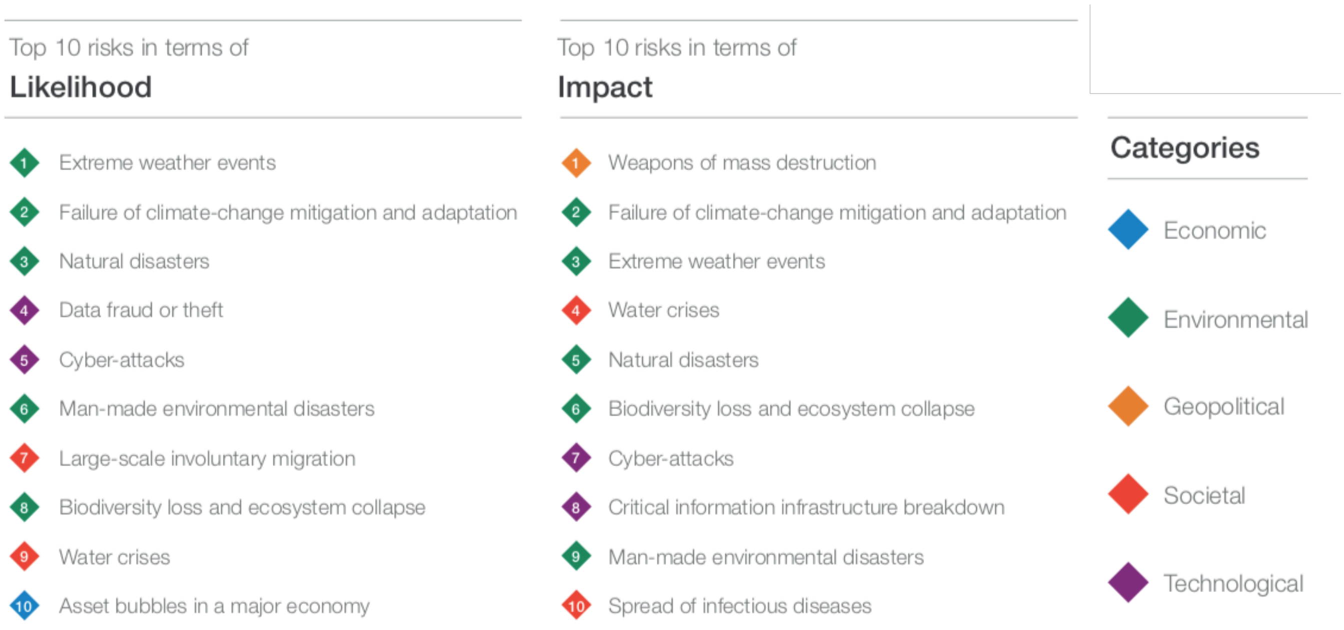
- Nye, Joseph S., Cyber Power, Belfer Center for Science and International Affairs, Harvard Kennedy School, 2010. Retrieved from: https://projects.csail.mit.edu/ecir/wiki/images/d/da/Nye_Cyber_Powe1.pdf
- Raik, K., Järvenpää, P., A New Era of EU-NATO Cooperation: How to Make the Best of a Marriage of Necessity, Report, International Centre for Defence and Security, May 2017. Available at: https://icds.ee/wp-content/uploads/2018/ICDS_Report_A_New_Era_of_EU-NATO.pdf
- Rand Corporation, Challenges and Opportunities in Cyberspace, available at: https://www.rand.org/research/primers/cyber.html
- Rovner, Joshua and Tyler Moore, Does the Internet Need a Hegemon?, Journal of Global Security Studies, 2017. Published by Oxford University Press on behalf of the International Studies Association. Retrieved from https://academic.oup.com/jogss/article/2/3/184/4082200
- Ryan David Kiggins, US Leadership in Cyberspace: Transnational Cyber Security and Global Governance, in Kremer J., and Müller B., Cyberspace and International Relations: Theory, Prospects and Challenges, Heidelberg ; New York ; Dordrecht ; London : Springer, 2014.
- Samm Sacks, Beijing Wants to Rewrite the Rules of the Internet, the Atlantic, 2018. Retrieved from: https://www.theatlantic.com/international/archive/2018/06/zte-huawei-china-trump-trade-cyber/563033/
- Samm Sacks, China’s Emerging Cyber Governance System, Center for Strategic and International Studies, 2019. Retrieved from: https://www.csis.org/chinas-emerging-cyber-governance-system
- Samuele De Tomas Colatin, A surprising turn of events: UN creates two working groups on cyberspace, NATO Cooperative Cyber Defence Centre of Excellence, available at: https://ccdcoe.org/incyder-articles/a-surprising-turn-of-events-un-creates-two-working-groups-on-cyberspace/
- Sarah Mckune, Shazeda Ahmed, The Contestation and Shaping of Cyber Norms Through China’s Internet Sovereignty Agenda, International Journal of Communication 12(2018), 3835–3855. Retrieved from: https://www.google.it/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwjKuqHLwcjkAhURtosKHVq9BBcQFjAAegQIAhAC&url=https%3A%2F%2Fijoc.org%2Findex.php%2Fijoc%2Farticle%2Fdownload%2F8540%2F2461&usg=AOvVaw3TqT55DKCoVsK9CKoxjI1f
- Segal A., Year in Review: Chinese Cyber Sovereignty in Action, Council on Foreign Relations, 2018. Retrieved from: https://www.cfr.org/blog/year-review-chinese-cyber-sovereignty-action

- Siim Alatalu, Irina Borogan, Elena Chernenko, Sven Herpig, Oscar Jonsson, Xymena Kurowska, Jarno Limnell, Patryk Pawlak, Piret Pernik, Thomas Reinhold, Anatoly Reshetnikov, Andrei Soldatov and Jean-Baptiste Jeangène Vilmer, Hacks, leaks and Disruptions: Russian cyber strategies, Chaillot Papers, European Union Institute for Security Studies, Paris, October 2018. Retrieved from: https://www.iss.europa.eu/content/hacks-leaks-and-disruptions-—-russian-cyber-strategies
- Simnar R. Maker, New frontier in defense: cyberspace and U.S. Foreign Policy, A national committee on American Foreign Policy Report, May 2017. Retrieved from https://www.ncafp.org/2016/wp-content/uploads/2017/05/Cyberspace-and-US-Foreign-Policy-Report-May-17.pdf
- Stadnik I., Discussing state behaviour in cyberspace: What should we expect?, Diplomacy.edu, 2019. Retrieved from: https://www.diplomacy.edu/blog/discussing-state-behaviour-cyberspace-what-should-we-expect
- Stephanie Borg Psaila, New cyber norms to protect cyberspace, GIP Digital Watch observatory, 2018. Retrieved from: https://dig.watch/trends/cyber-norms
- The Fifth Domain, Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats, Article published on Council on Foreign Relations, 2019. Retrieved from: https://www.cfr.org/book/fifth-domain
- U.N. General Assembly, "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," U.N. Doc. A/69/273 (2015), http://www.un.org/Docs/journal/asp/ws.asp?m=A/69/723.
- UN GGE and OEWG, GIP Digital Watch observatory, 2019. Retrieved from: https://dig.watch/processes/un-gge
- Walt, S.M. (1991) The Renaissance of Security Studies. *International Studies Quarterly* 35 (2), 211–39.
- Wendt A., Anarchy is what States Make of it: The Social Construction of Power Politics, International Organization, Vol. 46, No. 2, 1992, pp. 391-425, The MIT Press. Retrieved from: http://www.jstor.org/stable/2706858

Appendix

Figure 1: The Global Risks Landscape 2019

Source: World Economic Forum, The Global Risks Report 2019, 14th Edition



Top 10 risks in terms of
Likelihood

1. Extreme weather events
2. Failure of climate-change mitigation and adaptation
3. Natural disasters
4. Data fraud or theft
5. Cyber-attacks
6. Man-made environmental disasters
7. Large-scale involuntary migration
8. Biodiversity loss and ecosystem collapse
9. Water crises
10. Asset bubbles in a major economy

Top 10 risks in terms of
Impact

1. Weapons of mass destruction
2. Failure of climate-change mitigation and adaptation
3. Extreme weather events
4. Water crises
5. Natural disasters
6. Biodiversity loss and ecosystem collapse
7. Cyber-attacks
8. Critical information infrastructure breakdown
9. Man-made environmental disasters
10. Spread of infectious diseases

Categories

- Economic
- Environmental
- Geopolitical
- Societal
- Technological

[270]

Table 1: Cyber Warfare: Countries with the strongest cyber forces

Source: Valdai Discussion Club

Countries with the Strongest Cyber Forces[271]		
Countries	Financing (mnl $ per year)	Personnel
United States of America	7,000	9,0000
China	1,500	20,000
United Kingdom	450	2,000
South Korea	400	700
Russia	300	1,000
Germany	250	1,000
France	220	800
North Korea	200	4,000
Israel	150	1,000

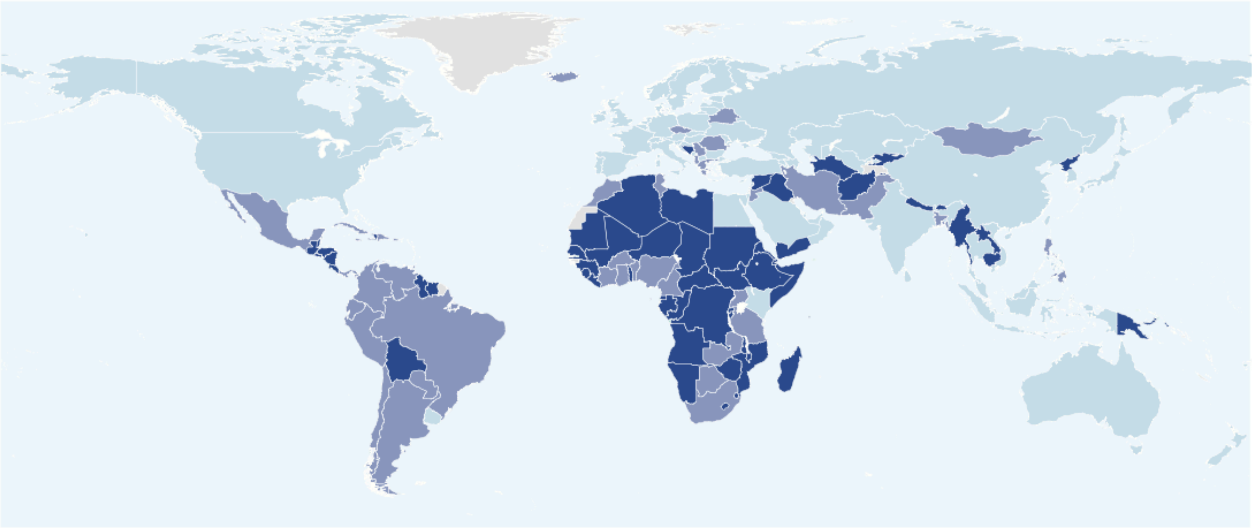
[270] World Economic Forum, The Global Risks Report 2019 14th Edition, Geneva, 2019. Available at: http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

[271] Cyber Warfare Infographics, Valdai Discussion Club, 27.08.2019, available at: http://valdaiclub.com/multimedia/infographics/cyber-warfare/

Figure 2: Geographical cyber commitment around the world

Source: International Telecommunication Union (ITU) report on the 2018 Global Cybersecurity Index (GCI).

Heat map showing geographical commitment around the world



The colours in the heat map above indicate differences in the level of commitment with high, medium, and low scores in a range of colours from light blue (peak commitment) to dark blue (low commitment).

[272]

Table 2: Comparison of National Strategies

Object	Russian Federation	People's Republic of China	United States of America
Security concept	Information security and cultural security	Network sovereignty, regulation and control	Cybersecurity and critical infrastructure
Field of concern for security	All field of society and State	All field of society and State	Political and military field
Relevant official documents	National Security Strategy published (September 2000); Foreign Policy Concept of the Russian Federation (November 2016); Official document of the Russian Federation on the Doctrine of Information Security (December 2016)	National Cybersecurity Strategy (2016), Cybersecurity Law (2017)	2018 National Defense Strategy of the United States of America; Presidential Executive Order "Cybersecurity for the Nation" (2017); Task Force on Cyber Deterrence (2017)
International effort for tacking the threat	Commitment to United Nations initiatives since 1990s, creation of OEWG, regional commitment with SCO members for an International code of	Recognition of United Nations initiatives to tackle the threats arising from cyberspace, but stronger commitment on a regional (SCO) and	Commitment to United Nations as main promoter of the application of UN Charter to cyberspace, creation of UN GGE format, regional

[272] This image is taken from the International Telecommunication Union (ITU) report on the 2018 Global Cybersecurity Index (GCI), p. 13.

	conduct for information security.	bilateral level (Belt and Roald initiative)	commitment (NATO and partnership with EU).

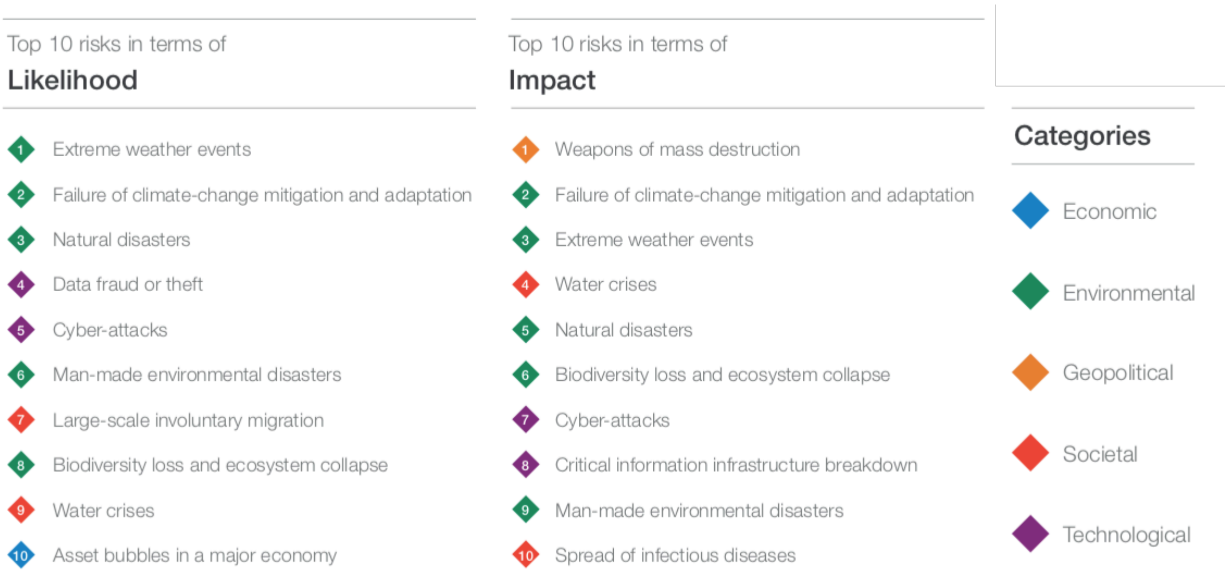
This table intends to summarize the main traits of each national strategies taken into analysis in the second part of the work. The main object of study for Russian Federation, People's Republic of China and the United States are: security concept applied to the field of cybersecurity, field of concern for security, list of the most relevant official documents and, finally, international and regional efforts in tackling the issues arising from cybersecurity. This table shows important differences of approach to the problem and explains the knots complicating cooperation.

Executive Summary

Introduction

The 21st century has been experiencing a rising number of new cyber threats that governments cannot face on their own by means of traditional tools. Technology has played one of the most important role in reshaping social interactions and progress over few generations, determining as well important implications for security.

Figure 1: WEF: The Global Risks Landscape 2019[273]



Top 10 risks in terms of **Likelihood**	Top 10 risks in terms of **Impact**
🟩 1 Extreme weather events	🟧 1 Weapons of mass destruction
🟩 2 Failure of climate-change mitigation and adaptation	🟩 2 Failure of climate-change mitigation and adaptation
🟩 3 Natural disasters	🟩 3 Extreme weather events
🟪 4 Data fraud or theft	🟥 4 Water crises
🟪 5 Cyber-attacks	🟩 5 Natural disasters
🟩 6 Man-made environmental disasters	🟩 6 Biodiversity loss and ecosystem collapse
🟥 7 Large-scale involuntary migration	🟪 7 Cyber-attacks
🟩 8 Biodiversity loss and ecosystem collapse	🟪 8 Critical information infrastructure breakdown
🟥 9 Water crises	🟩 9 Man-made environmental disasters
🟦 10 Asset bubbles in a major economy	🟥 10 Spread of infectious diseases

Categories

🟦 Economic

🟩 Environmental

🟧 Geopolitical

🟥 Societal

🟪 Technological

According to the assessment of the World Economic Forum (Figure 1), cyber-attacks (in purple) are among the five most likely dangers that may occur in 2019, and among the ten most impactful threats that the world could suffer in the same year. In this uncertain scenario, this work intends to explore the elements related to cyber-international interactions within the framework of International Relations theories in order to analyse and explain States' behaviours in cyberspace dynamics. Furthermore, the work is committed to explore national strategies, in particular those of Russia, China and the United States, in order to understand whether the different theoretical patterns are applicable to current national behaviours. Finally, the investigation allows to develop some perspective trends of cooperation in the field, beware of the difficulties that have emerged through the theoretical analysis and the comparison of national strategies. Examples of cooperation are bestowed among the United Nations Members, EU and NATO Members (with a specific focus on the Italian case) and with public-private partnership. Questions are addressed on whether the creation of a legal shared framework will reveal itself as a complex global governance action and on the difficulties that may arise in the cooperation process, considering the challenges originating from national interests and mistrust between States. Thus, the final aim is to provide recommendations to researchers and policy makers in order to offer valuable and plausible solutions for tackling the threats

[273] World Economic Forum, The Global Risks Report 2019 14th Edition, Geneva, 2019.

and the risks originating from cyberattacks and for creating a global security regime dedicated to cyberspace.

Research question: *in which way the technical difficulties arising from cyberspace and the different perceptions of States that define their national strategies shape the current and future patterns of cooperation in the field of cybersecurity*?

Methodology

In this work, an exploratory, descriptive and comparative research was performed to investigate the main aspects of a relatively-new researched topic and to expand the scientific understanding on the matter of cybersecurity and international cooperation.

The research encompasses a comprehensive and extensive literature:

1. *Literature on the theories of International Relations: Realism, Liberalism and Constructivism;*
2. *Literature on cybersecurity;*
3. *Official Documents on national strategies of Russia, China, the United States and Italy;*
4. *Document review of International and Regional organizations (in particular, United Nations, North Atlantic Treaty Organization, European Union, Shanghai Cooperation Organization and International Telecommunication Union).*

The work contains as well an Information Security Glossary in order to provide a more specific definition of cyber technical features.

The *relevancy* of this research is given by the fact that cyber strategies have come of age and can produce detrimental impacts. Major powers currently employ cyber strategies to gain a position of advantage relatively to their rivals, while small States and non-State actors attempt to use cyber operations to punch above their weight to maximize their potential goals.[274] Therefore, the topic is consistent with one of the major trend in the ongoing security debate. The *practical importance* of this work is to understand how national perceptions and technological features are shaping the current pattern of cooperation in cybersecurity. Therefore, the conclusions of this research are instructive in order to forecast perspective trends of cooperation in the field.

Part One – Theory and methodology of the research

1.1 Classical theories of International Relations

1.1.1 Realism and the Security Dilemma

The first part of the work outlines a general enquiry of the main traits that characterize the Realist theory of International Relations (IR), focusing on the features of the security dilemma and of the competitive interactions among States, which lead to a continuing negative spiral of

[274] Valeriano B., Jensen, B., & Maness R., Cyber Strategy: The Evolving Character of Power and Coercion, New York: Oxford University Press, 2018, p.1-2.

deteriorating political relations.[275] The few possibilities of establishing a certain level of security are determined by a mix of military arsenal reinforcement and diplomacy, aimed at the establishment of an arms control treaty in order to consolidate an advantageous position in the world order. The realist approach is instructive to understand competitive cyberspace dynamics and it is useful for the analysis in its categorization of actors, power and structure.

1.1.2 Liberalism and International Cooperation

While Realist theories provide a pessimistic approach towards cooperation, Liberalism tends to offer a much more positive view about improving cooperation in the field of international politics. What characterizes Liberal theories is its multi-centric approach, conveying attention to a plethora of different actors other than States. Moreover, Liberalism offers a different solution to the security dilemma by demonstrating that it is not through self-help or balance of power that such dilemma is resolved but through cooperation and collective efforts. Central to the Liberal theory is the concept of collective security, which is only realized when each State accepts that the security of an actor is a concern for all and is willing to join in a collective response against the aggressor.[276]

1.1.3 Constructivism and the role of ideas in shaping States' behavior

Constructivism understands the concept of security as a construction, exploring its origins, characteristics and the reason for which threats are perceived differently by States due to their background experiences. As a consequence, every single actor decides to apply a process of securitization to a certain object. From this process, Constructivist theory enables to assess and confront why Countries give birth to different national strategies.

1.2 Defining the cyber domain

This section presents different definitions of "cyberspace", showing there is no unitary approach to the issue. For example, Joseph Nye considers cyberspace both a complex set of network systems and a new domain of power.[277] Even when discussing about security in the fifth domain, we encounter two different concepts: cybersecurity and information security. A further issue related to cyberspace is anonymity, which is expressed by the ability to execute operations in any dimension, holding no price or risk to the perpetrators most of the time. Such scenario creates a highly debated issue of legality, fueling the misrepresentation of cyberthreats. A third aspect is the global character of the Internet, which plays an important role in defining the terms for establishing an international regime of governance in the domain. Indeed, the competition between Countries is not solely based on the classical principle of resource scarcity but is reshaped accordingly to the characteristics attributed to digital resources. Consequently, the question of governance is built up differently: rather

[275] Mazzei F., Marchetti R., Petito F., Manuale di Politica Internazionale, Egea, 2010.
[276] Mazzei F., Marchetti R., Petito F., Manuale di Politica Internazionale, Egea, 2010
[277] Nye, Joseph S., Cyber Power, Belfer Center for Science and International Affairs, Harvard Kennedy School, 2010.

than on the classic problem of distribution, in cyberspace the principles of representation, power and legitimacy are risen by means of interoperability and communication.[278]

1.3 The applicability of IR theory to the analysis of cybersecurity

1.3.1 Cyber Actors: uncertainty and the rising importance of non-State actors

The first object of the analysis deals with actors and their characteristics. Considering that, in 2018, more than 57.8%[279] of world population had Internet access worldwide, we may assume that more than half of world population could potentially use the Internet for malicious purposes. The expanding number of possible hackers, which is happening according to Joseph Nye (2011) due to a process of power diffusion, raises issues in terms of responsibility and punishment.[280] A further knot consists in what is generally defined as the attribution problem. Substantial progress in technology, in many cases, have allowed understanding the origins of the intrusions. However, while it is actually possible to assess the geographical location of the computer, it is much more difficult to establish the individual who acted maliciously behind it.[281]

1.3.2 Cyber power: adding flexibility and fluidity to a traditional concept

This work understands the meaning of cyber power with the significance of influence, as different techniques of cyberwarfare are designed with the aim of limiting someone's autonomy and of exerting control over someone's capabilities. In this precise context, control has not defined characteristics, it is technological and it is not solely State-centric or real. Therefore, in order to adapt to a changing environment, a flexible interpretation of power must be applied to predict and understand new control methods and techniques. For example, a measurement can be provided by data on financing cyber-related activities (Table 1).

Table 1: Cyber Warfare: Countries with the strongest cyber forces[282]

Countries with the Strongest Cyber Forces		
Countries	Financing (mnl $ per year)	Personnel
United States of America	7,000	9,0000
China	1,500	20,000
United Kingdom	450	2,000
South Korea	400	700
Russia	300	1,000
Germany	250	1,000
France	220	800

[278] Singer, P. W., & Friedman, A., Cybersecurity and cyberwar: What everyone needs to know. Oxford: Oxford University Press, 2014.

[279] International Telecommunication Union, ITU Annual Progress Report 2018.

[280] Nye, Joseph S., The Future of Power, New York: Public Affairs, Vol.11-No. 8, 2011.

[281] Buchanan B., The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations, New York: Oxford University Press, 2017.

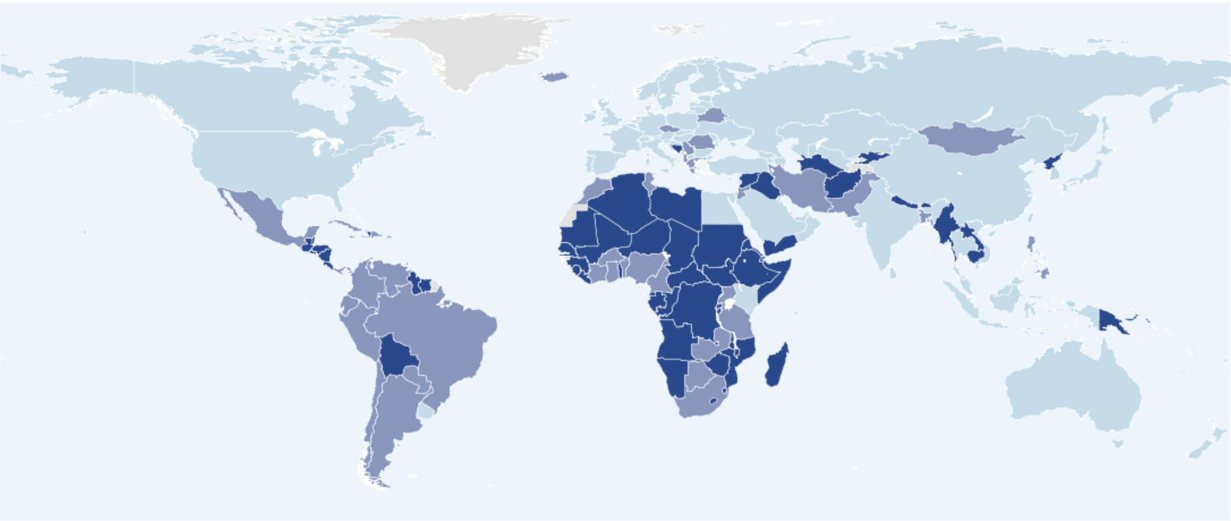
[282] Cyber Warfare Infographics, Valdai Discussion Club, 27.08.2019, available at: http://valdaiclub.com/multimedia/infographics/cyber-warfare/

North Korea	200	4,000
Israel	150	1,000

According to Martin Libicki's (2009) formulation, power in cyberspace can be as well conceived as the States' capacity of cyber defense, built upon the principles of robustness, system integrity and confidentiality.[283] An empirical example is offered by the 2018 Global Cybersecurity Index by the International Telecommunication Union (ITU), which presents a classification of States which have a high, medium or low commitment to cybersecurity in the year 2018 (Figure 2).

Figure 2: Geographical cyber commitment around the world[284]

Heat map showing geographical commitment around the world



The colours in the heat map above indicate differences in the level of commitment with high, medium, and low scores in a range of colours from light blue (peak commitment) to dark blue (low commitment).

However, Libicki also argues that persuasion is an optimal tool for deterrence, by convincing another actor that the chances of failure of an attack are much more than the one of success.[285] Given this scenario, it is possible to affirm that it is difficult to objectively assess cyber power and the outcomes of its employment.

1.3.3 The structure of the international system applied to the cyber domain

In a world in which the principle of collective security is not applied to the global cyber regime yet, it looks like a realist international system prevails over any other formulation, being cyber tools coadjutants in the fight for personal interests. Furthermore, this order finds no regulating scheme because a solid juridical framework is clearly missing. It is evident as well that the Internet has revolutionized the way in which someone can exert its own influence over the structure of the

[283] Libicki, Martin C., Cyberdeterrence and cyberwar, RAND Corporation, 2009.

[284] This image is taken from the International Telecommunication Union (ITU) report on the 2018 Global Cybersecurity Index (GCI), p. 13.

[285] Ibidem.

international system, as cyber tools gave both to small States and non-State actors the chance to play the game. As a result, according to Nye (2017), the configuration of power that shapes the international system has something old, which is represented by more traditional concepts of power and capabilities, and something new, which deals with the development and implementation of new technologies.[286] Therefore, the structure of the cyber-international system is rather unsettled.

1.4 The Offense-Defense Theory in the fifth domain

1.4.1 Threat assessment in cyberspace: offense over defense

The process of threat assessment is highly compromised by the virtual nature of cyber weapons, making it difficult to identify the capabilities and vulnerabilities of the opponent as well as the adversary's actual intent. The question on whether a new technology could favor the offense or the defense posture is a critical issue when discussing about cybersecurity. As it is widely shared that the future use of cyber weapons will be offensive, larger spending on cyber offense has been implemented worldwide. Therefore, in order to create balance in cyber warfare, it is important to develop defensive mechanisms, because States can only maximize their security by minimizing the probability of positive outcome of the cyber-attacks.[287] Nevertheless, the path toward developing a substantive and effective defensive system meets several difficulties, both technical and based on misperception.

1.4.2 Mutually Assured Destruction or Mutually Assured Stability?

As argued by Ben Buchanan (2017), States' offensive behavior and subjective perception of the attacker's intentions fuel the cybersecurity dilemma.[288] Nonetheless, ambiguities of attribution and the diversity of adversaries do not make deterrence and dissuasion impossible to be achieved in cyberspace, as they can be mitigated by information sharing and confidence-building measures (CBMs). One of the main problem is that the discussion has been focusing on peacetime deterrence and dissuasion of cyberattacks, thus, there is little empirical evidence of warfare because no full-scale cyberwar has occurred yet. It is therefore extremely difficult to assess whether *Mutually Assured Destruction* or *Mutually Assured Stability* has prevailed. However, it is important to rethink escalation and deterrence as they are applied differently in the cyber-world of International Relations.

1.5 Results of the applied analysis

The main conclusion of this analysis identifies the need of rethinking the classical principles of International Relations when applying them to cyberspace, which – by now – do not find exhaustive applicability. Furthermore, because this topic is rather new to policymakers and

[286] Nye J. S., Deterrence and Dissuasion in Cyberspace, International Security, 41, 2017.
[287] Singer, P. W., & Friedman, A., Cybersecurity and cyberwar: What everyone needs to know. Oxford: Oxford University Press, 2014
[288] Buchanan B., The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations, New York: Oxford University Press, 2017.

researchers, we may envisage additional discussion on the matter and probably a more organized discourse on the topic in the future. It is undeniable that cyber-attacks are becoming the "new normal", therefore, we may expect to appreciate them as the new normal and build research upon that.

Part two – Major Cyber Rivals: towards cooperation or self-help?

2.1 States' cyber postures: a selected analysis of national security strategies

The main idea behind this chapter is to better understand the degree of cooperation between States, in the specific case of Russia, China and the United States, in the field of cybersecurity by means of analyzing the postures of the main rival actors and their official strategies; Constructivism has been fundamental in this assessment. It will be demonstrated that cooperation in the fifth domain develops at a slow peace, because there are some technical and relational aspects that need to be first addressed and overcome before calling for the instrument of international law to regulate international relations in the cyber domain.

2.1.1 The Russian Information Security Strategy

The Russian strategy is formulated on the elaboration of the comprehensive concept of international information security, which is defined as a "state of global information space in which the possibility of violating the rights of the individual, society and the rights of the State in the information sphere, as well as destructive and unlawful effects on elements of the national critical information infrastructure, are excluded".[289] The most important document outlining the strategy is the Foreign Policy Concept approved by President Vladimir Putin on November 30, 2016 which affirms the willing to protect national digital interests. The Russian cyber diplomacy has been outstanding in the field as Russia has pioneered the international commitment to cybersecurity by being the first State to address the issue at the United Nations.[290] The Country's commitment to information security has been developed also at the regional level among the members of the Shanghai Cooperation Organization. Despite Russian efforts, there are two main boundaries that prevent Russia from moving forward both on a multilateral and on a bilateral level: a conceptual issue, which is determined by different formulations and terminology of concepts regarding cyberspace, and a trust issue, determined by the accusation of being responsible for several cyberattacks.[291]

2.1.2 The Chinese International Cyber Agenda

[289] Дмитрий Грибков, Референт аппарата Совета безопасности Российской Федерации, О формировании системы международной информационной безопасности, журнала «Международная жизнь», МИД РФ, 2015. https://interaffairs.ru/jauthor/material/1352

[290] Elena Chernenko in Hacks, leaks and Disruptions: Russian cyber strategies, Chaillot Papers, European Union Institute for Security Studies, Paris, October 2018

[291] Valeriano B., Jensen, B., & Maness R., Cyber Strategy: The Evolving Character of Power and Coercion, New York: Oxford University Press, 2018

The 2016 Chinese National Cybersecurity Strategy depicts cyberspace as a new, but Chinese owned, territory for national sovereignty which require government-led cyber control in order to ensure its security. Hence, defending cyberspace sovereignty is fundamental in protecting national security and the critical information infrastructure – concept which is shared among other members of the SCO. Strategically, cyberspace represents an opportunity for using a new space to catch up to the West. In a very paradoxical way, the fifth domain consists for China both of a critical capability, because it is a source of knowledge, and a long-term vulnerability, as the Country cannot rely forever on the technology created by others.[292] Globally, China has internationally advocated the concept of cyber sovereignty by participating in the discussion on how to build a proper and working international Internet governance on an equal footing with the rest of the world and by promoting the respect for the principle of non-interference in other Countries' sovereignty.

2.1.3 The American Cyber Strategy

The United States of America have been the author of an open network system by making it a worldwide accessible source. With time, cyberspace has been approached by the Pentagon as the fifth warfighting domain requiring a strategy for national defense.[293] Because the US is the most connected Country that heavily relies on network systems, it is as well one of the most targeted one. Hence, deterrence is a central posture in the American counter-intrusion policy.[294] The latest presidencies have worked in order to favor the prioritization of investments in resilience, reconstitution, and operations in order to assure the development of their own cyberspace capabilities and the continued integration of those into the full spectrum of military operations.[295] The American international and regional commitment to cybersecurity has been consisting in participating in the development of international norms of behavior in cyberspace and in promoting collaboration in cybercrime investigation.[296] Most of all, the United States have presented itself as a leading Country for guiding the establishment process of a solid international cyber governance. Nevertheless, its efforts have already been put into practice through NATO cybersecurity programs and exercises devoted to enhancing cybersecurity nationally and regionally.

2.2 Drawing conclusions on the analyzed States' strategies: common or divergent paths?

[292] Ibidem.

[293] D. Allen, P., Gilbert, D. , "The Information Sphere Domain Increasing Understanding and Cooperation", Johns Hopkins University, Applied Physics Lab, Booz Allen Hamilton, 2018.

[294] Final Report of the Defense Science Board (DSB) Task Force on Cyber Deterrence, Office of the Secretary of Defense, February 2017.

[295] Mattis Jim, Summary of the 2018 National Defense Strategy of the United States of America, Department of Defense of the United States of America.

[296] NATO, "Cyber Defence", 2017, February 17, NATO Official Website.

Table 2: Comparison of National Strategies

Object	Russian Federation	People's Republic of China	United States of America
Security concept	Information security and cultural security	Network sovereignty, regulation and control	Cybersecurity and critical infrastructure
Field of concern for security	All field of society and State	All field of society and State	Political and military field
Relevant official documents	National Security Strategy published (September 2000); Foreign Policy Concept of the Russian Federation (November 2016); Official document of the Russian Federation on the Doctrine of Information Security (December 2016)	National Cybersecurity Strategy (2016), Cybersecurity Law (2017)	2018 National Defense Strategy of the United States of America; Presidential Executive Order "Cybersecurity for the Nation" (2017); Task Force on Cyber Deterrence (2017)
International effort for tacking the threat	Commitment to United Nations initiatives since 1990s, creation of OEWG, regional commitment with SCO members for an International code of conduct for information security	Recognition of United Nations initiatives to tackle the threats arising from cyberspace, but stronger commitment on a regional (SCO) and bilateral level (Belt and Roald initiative)	Commitment to United Nations as main promoter of the application of UN Charter to cyberspace, creation of UN GGE format, regional commitment (NATO and partnership with EU)

The analysis carried in the second chapter demonstrates that, notwithstanding the overall acknowledgement of the security issues that arise from cyberspace, there are two main obstacles that make cooperation challenging among those Countries. The first issue is the widespread lack of trust among States at the level of cyberspace, due to the acquiescence on the use of cyber tools, especially with regards to espionage practices, and the lack of clarity or transparency on their purposes. The second issue deals with language and terminology, not only because there is a concrete difficulty with different languages, which anyway could be overcome by translators, but because there is a lack of agreement on the use of specific cyber terminology and related significance. Those differences have resulted in denouncing some countries, and in particular the US, for the imposition of crafted network structures and Internet control. Therefore, Countries like China and Russia strongly call for advanced inclusion and participation in the decision making process of Internet regimentation and in influencing the cyber global governance scenario.

Part Three – Perspective trends of cyber collaboration

3.1 A World Wide Governance for a World Wide Web: assessing the current role of International Institutions in guaranteeing a more secure Internet

Global institutions are called to both regulate the use of cyber tools to guarantee a sufficient level of cybersecurity worldwide, and to ensure that the benefits of a worldwide open access to the Internet are respected. The role of institution is posed under scrutiny and strongly subjected to criticism, therefore the question of what roles the old international organizations should play when it comes to a new feature, as in the case of the Internet, is very difficult to determine. For what concerns the creation of a cyberspace treaty, by applying the law of armed conflict to the warfighting fifth domain, there is no united front of action, due to different interests and priorities in cyberspace and the complexities of assessing cyber capabilities.[297] Nevertheless, the pessimism regarding the feasibility of cyber arms control agreements does not imply that there are no avenues for cooperation between cyber adversaries, such as CBMs and information sharing.

3.2 The Public-Private Partnership in the field of Cyber Security

The discussion on cybersecurity encompasses also the private sector. Governments are meeting the challenges of understanding how to foster information security without trying to dismantle the open character of the Internet. States should deal with the structural limitations of their power, because they no longer have direct control over most of the key sectors, as they are largely held in private hands. Thus, the challenge consists in how to better coordinate defense not only with other Countries', but with private actors, as cybersecurity requires a multi-stakeholder model for a public-private approach.[298] In this realm, the tech industry has proposed itself as a norm-developer actor with some interesting proposals advanced by Microsoft and Google, among others.[299]

3.3 Setting the international agenda: the UNIDIR 2019 Cyber Stability Conference and International ICT-security at the United Nations

The UNIDIR 2019 Cyber Stability Conference has remarked the United Nations commitment to foster cybersecurity worldwide, which is mainly sustained by the activities of the two working groups: UN GGE and OEWG. Despite their common goals, there are substantial differences between this two entities. The UN GGEs consists in an established practice, founded in 2004 and composed by an elected number of Countries committed to answering the challenges arising from cyberspace. Conversely, the OEWG has been recently created in response to the ineffectiveness of the previous group in delivering substantial results.[300] The main characteristic is inclusivity in contrast to the limited number of GGEs members. Inevitably, the creation of two separated groups have raised some controversies, especially with regards to their overlapping and competitive functions.[301] Complementarity seems to be the most appropriate pathway towards an effective mechanism for developing cybersecurity worldwide.

[297] Borghard E. D., Lonergan S. W., Why Are There No Cyber Arms Control Agreements?, Council on Foreign Relations, January 16, 2018.

[298] Brown, C., Eckersley, R., Valeriano, B., & Maness, R., International Relations Theory and Cyber Security: Threats, Conflicts, and Ethics in an Emergent Domain. In The Oxford Handbook of International Political Theory, Oxford University Press, 2018.

[299] Stephanie Borg Psaila, New cyber norms to protect cyberspace, GIP Digital Watch observatory, 2018.

[300] Mauer, T., Cybersecurity in a Complex Environment: Transatlantic Divergences and Diplomatic Achievements, Vereinte Nationen – German Review on the United Nations, Vol. 64, 2/2016, pp. 51–55.

[301] Anastasia Tolstukhina, Two Cyber Resolutions Are Better Than None, Russian International Affairs Council (RIAC), 2019.

3.4 The Tallinn Manual 2.0: an effort in understanding and applying international laws to cyber operations

The 2007 cyberattack against Estonia have been instructive for representing a constitutive case for which the discrepancy between old laws and the development of new technologies does not meet the necessity of installing the correct behavior for defending a partner Country from external attacks. With regards to the example of the Tallinn Manual, the work intends to disclose the ways in which the known international laws regulating the most classical conflicts could be applied to the context of cyber operations and cyber warfare, trying to bridge the gap between old international laws and new technologies in the most comprehensive and authoritative way. Because the Manual represents an academic research, and not a piece of international law, the Tallinn Manual has been questioned in its role and significance.

3.5 The role of the Republic of Italy in the EU-NATO cybersecurity framework: an example of regional cooperation

The 2016 EU - NATO Joint Declaration aims at, among other goals, mobilizing efficiently Members' resources to address cyber challenges and at enhancing the security of their citizens. This activity is instructive in the effort of tackling the risks emerging from cyberspace, especially in the field of cybercrime and digital market and it consists in a virtuous example of partnership in the field.[302] Despite this, the EU-NATO partnership is still limited to few subject matters. Being Italy founder of both NATO and EU, the Country represents an example of integration of different priorities. Italy endorses closer cooperation and complementarity between the two entities in their effort of promoting regional security by means of crisis management and peace-keeping operations.[303] Italy, from its side, should stand as a promoter of such cooperation both because has demonstrated to possess qualities in the area of cyber diplomacy or by working alongside other international law enforcement agencies to increase transnational cooperation on cybersecurity. Nevertheless, Italy has also an immense opportunity for amplifying its cyber expertise from both partners that have developed effective mechanisms to achieve cyber readiness, while pursuing its double goal of protecting individuals and State infrastructures.

3.6 The future of cooperation in cyberspace: what lies ahead?

Different scenarios are advanced by Healey (2011) with regards to the future of cyberspace, namely Status Quo, Domain, Balkanization, Cybergeddon and Paradise, according to the unfolding of offense over defense, the intensity and types of cyberconflicts and of cyber operations.[304] In the attempt to applying the analysis of national strategies, the US and other NATO Countries would

[302] Raik, K., Järvenpää, P., A New Era of EU-NATO Cooperation: How to Make the Best of a Marriage of Necessity, Report, International Centre for Defence and Security, May 2017

[303] Presidency of the Council of Ministers, March 2017, Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica.

[304] Healey J., The Five Futures of Cyber Conflict and Cooperation, Atlantic Council, 2011.

prefer the Paradise condition, as it would provide long-term stability and stable basis for international trade and interactions. On the other side, countries like Russia or China would much prefer a Balkanized Internet, in order to exert substantial control making it a strictly national domain that enables Countries to block access content, while transnational relations are regulated by stipulated agreements. A further question for the future of cyberspace regards the necessity of having an hegemon – probably the United States – who could lead the transition to a regimented governance of the domain. Criticism towards this view has accused the Country of not being able to provide sufficient levels of cybersecurity at a national and global level and of intending to pursue its own rather than global interests.[305]

Conclusions

There are two main conclusions that can be drawn from this study. First, there is the need of rethinking the classical assumptions of International Relations when applying them to the cyber domain, which by now do not find exhaustive applicability in the field of cyberspace. Second, the global community mission for the future consists in assuring resilience to the cyber global infrastructure, which evidently will be more pervasive in our everyday life and in the practice of business and States activities. In the process of avoiding total anarchy, the commitment of governments covers a fundamental role. Notwithstanding the different ideologies that Countries reasonably assume according to their strategies, interests and values, each State bears the responsibility of working for the goal of cyber resilience. It is undeniable that cybersecurity is a global good and, thus, should be treated as a global concern. There are four main tasks that government should accomplish:

1. invest in enhancing training and research in order to build resilient systems both for States' infrastructures and for private entities and individuals;
2. commit to the process of information exchange and CBMs in order to reduce the current levels of uncertainty and overcome the problem of attribution;
3. develop consensus on a normative framework to regulate the sharing of information and procedures for deterring and contrasting international criminal acts in cyberspace;
4. contribute to the development of a cyber weapons non-proliferation regime, which is a long-term and rather ambitious goal, but would produce the effect of limiting the number of cyber threats to which a State must develop counter measures, while States are able to enjoy better defense systems thanks to their investments.

Thus, governments need creativity in shaping the ways and the tools for pursuing such recommendations. Definitely, regional and bilateral cooperation could represent models from which to start this cooperative process, which can be later applied at the international level.

[305] Rovner, Joshua and Tyler Moore, Does the Internet Need a Hegemon?, Journal of Global Security Studies, 2017. Published by Oxford University Press on behalf of the International Studies Association.