LUISS

Department of Political Sciences
Degree Program in International Relations

Chair of Security Policies

Cyber Proxy Wars: International Normative Regulation

Prof. Carlo Magrassi
SUPERVISOR

Prof. Alfonso Giordano
CO-SUPERVISOR

Matr. 647752

Sabrina Sileoni

CANDIDATE

Academic year 2022/23

Index

Abstract

In today's highly interconnected world, the internet's rapid growth has brought immense benefits but also introduced complex cybersecurity challenges. This thesis explores the phenomena of cyber proxy wars and tries to identify the stages of normative regulation in today’s discussion at international and regional forums such as the UN GGE and OEWG, and the OSCE.

Cybersecurity is now a top-tier national security concern, recognized by global leaders as a significant threat to the world economy. The dilemma that most institutions and governments are facing today is how to deal with this threat. The notion of sovereignty has historically characterized the international system, but in cyberspace, the lack of geographical borders, as well as the dominance of the private sector and non-State actors, has put this principle into question. This id further exacerbated by the emergence of non-State and proxy actors. With most treaties and conventions being obsolete or not applicable to the matter in question, States are navigating this new realm with no plan in place. What is needed is are clear norms of responsible State behavior in cyberspace and a treaty comparable to the Geneva Convention that establishes the norms of engagement for nation States in cyberspace and a legal framework for international prosecution of violators. This is why actors are able to conduct harmful cyberattacks with relative impunity: when there are no rules for acceptable behaviour in cyberspace, everything is allowed. While normative foundations related to State and its proxy’s behavior can be found in current international law principles such as sovereignty, attribution, and neutrality. Their application is far from being achieved.

To address these challenges, the international community must work proactively and cooperatively to promote implementation of norms and rules for State and proxy behavior in cyberspace. The study employs Martha Finnemore's constructivist theory of norms to analyze the evolution of norms in the cybersecurity sector, emphasizing their social construction and influence on State behavior.

The research draws upon a wide range of academic and professional sources, including studies on the delegation of power by States into cyberspace, the normative regulation of cyber relations, and institutional reports on cyber regulation. Additionally, it

examines the normative constraints on cyber proxy conflict and the role of advocacy networks and norm entrepreneurs in shaping cyber norms. This is done by analyzing three key diplomatic processes, at the international level the GGE and the OEWG, while at the regional level we have the OSCE's work on CBMs.

Ultimately, this dissertation aims to provide insights into the evolving dynamics of international relations in the age of cyberspace and contribute to the ongoing discourse on establishing a framework for responsible State behavior in this critical domain.

List of Acronyms and Abbreviations

- Agenzia per la Cybersicurezza Nazionale (ACN)
- Computer Security Incident Response Teams (CSIRTs)
- Conference for Security and Cooperation in Europe (CSCE)
- Confidence Building Measure (CBM)
- Department of Defense (DoD)
- Domain Name System (DNS)
- Private military companies (PMCs)
- Draft Articles on Responsibility of States for Internationally Wrongful Acts (DARSIWA)
- European Union Agency for Cybersecurity (ENISA)
- Information and Communication Technologies (ICTs)
- International Court of Justice (ICJ)
- International Criminal Tribunal for the former Yugoslavia (ICTY)
- International Humanitarian Law (IHL)
- Internet Assigned Numbers Authority (IANA)
- Internet Corporation for Assigned Names and Numbers (ICANN)
- Law of Armed Conflict (LOAC)
- Non-Governmental Organizations (NGOs)
- North Atlantic Treaty Organization (NATO)
- Office of Cyber Security and Information Assurance (OCSIA)
- Open Ended Working Group (OEWG)
- Organization for Security and Cooperation in Europe (OSCE)
- Points of Contact (PoCs)
- Program of Action (PoA)
- UN General Assembly (UNGA)
- United Nations (UN)
- United Nations Group of Governmental Experts (UN GGE)
- United Nations' Institute for Disarmament Research (UNIDIR)
- People's Protection Units" (YPG)

Introduction

1. Relevance of the topic

We live in a world that is extremely interconnected. The Internet's growing popularity and its historically unprecedented expansion has brought plenty of social and economic benefits. Nonetheless, the connection between computers and humans poses a dilemma. It creates a wide range of opportunities for companies and businesses for the delivery of public goods and services, as well as new ways for citizens to participate in civil society; however, it also creates incredible opportunities for the world's most sophisticated militaries and their various adversaries, both State and non-State actors, to employ new and potentially harmful strategic means of action, which are arguably more difficult to defend and complex to deter. As a matter of fact, in a 'networked society,' new elites draw their power from an increased capacity to penetrate the layers of hardware and software that make up the cyberspace. These new capacities result in the significant increase of malicious actors' powers and potential, as opposed to the continuous lagging behind of institutions and professionals. As a consequence, the Internet is becoming a more dangerous place for individuals, organizations, and governments all over the world.

Cyber security has become a critical national security concern, and cyberspace has become a new sphere of statecraft, bringing a number of difficulties to international relations. According to the World Economic Forum (WEF) Global Risk Report 2021, the fourth most pressing short-term risks to the world is cybersecurity.[1] Nearly 40% of WEF leaders cited cybersecurity as a “clear and present danger” to the global economy.[2]

The dilemma that most institutions and governments are facing today is how to deal with this threat. The notion of sovereignty has historically characterized the international system, but in cyberspace, the lack of geographical borders, as well as the dominance of the private sector and non-State actors, has put this principle into question. With most treaties and conventions being obsolete or not applicable to the matter in question, States are navigating this new realm with no plan in place. What is needed is are clear norms of responsible State and proxy behavior in cyberspace and a treaty comparable to the Geneva Convention that establishes the norms of engagement for nation States in cyberspace and a

[1] McLennan, Marsh. "The Global Risks Report 2021 16th Edition."
[2] Ibidem.

legal framework for international prosecution of violators. This is why actors are able to conduct harmful cyberattacks with relative impunity: when there are no rules for acceptable behaviour in cyberspace, everything is allowed. While there is considerable consensus on how current international law should be applied to cyberspace, many political issues remain unsettled, such as sovereignty, attribution, and neutrality. Creating rules and norms for State behaviour in cyberspace can and must help in reducing this risk.

2. Literature review

This dissertation will rely on many sources of academic and professional knowledge regarding the normative regulation of proxy cyber relations. These will be reviewed here in a thematic organization.

The first group of sources to analyse are those which have as a central topic the delegation of power by States into the cyber realm, mainly through proxies. The most important source on the topic of the State's power projection for this dissertation is Tim Maurer's *Cyber mercenaries*[3], in which we investigate the covert links between governments and hackers. According to Maurer, cyberspace has become the new battlefield for geopolitics, and nations have begun to use hackers as proxies to project influence. Increasingly, nations are utilizing independent hackers as proxies to project influence both domestically and internationally. Over 30 countries, according to some estimates, are actively developing offensive cyber capabilities. Third-party groups—so-called cyber mercenaries—are increasingly exploiting the accountability dilemma by conducting cyber operations. Maurer believes we have not done enough to defend against this rising threat to national security for legislators, military leaders, and companies alike. The author looks at how different nations seek different models for their proxy connections, but they all face the same dilemma of balancing the advantages of these ties with the cyber operations and possible hazards of escalation.

The State-proxy relationship is further analysed by James Collier in his article *Proxy Actors in the Cyber Domain*[4]. Here the author adds to the information given by Maurer by providing a taxonomy of States' use of proxy players in the cyber domain,

[3] Maurer, Tim. Cyber mercenaries. Cambridge University Press, 2018.
[4] Collier, Jamie. "Proxy Actors in the Cyber Domain: Implications for State Strategy." St Antony's International Review 13, no. 1 (2017): 25–47.

defining the proxy actors accessible to a State, the reasons proxy actors appeal, and the structure of State-proxy relationships.

In *Cyberspace and the State: Towards a Strategy for Cyber-Power*[5], Betz and Stevens take the reader through the key ideas of power, sovereignty, war, and dominion to help them comprehend how they interact, as well as the intricacy of the greater cyber world. The authors set the tone by looking at prevalent internet vocabulary, its influence, and the challenge of attribution. This basis leads to a consideration of power, beginning with how power manifests itself in the cyber realm. It then goes into the discussion over sovereignty (legal sovereignty, Westphalian sovereignty, domestic sovereignty, and interdependence sovereignty). Betz further analyses the cyber domain in his article *Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed*[6]. Here he concentrates again on cyber power, arguing that it does not have independent war-winning capability.

In *Proxy Wars in Cyberspace: The Evolving International Law of Attribution*[7], the authors put under the magnifying glass the State as an actor prone to hostile activity against other States and examine the legal landscape of proxy cyber operations.

The second group of sources are those that analyse the process of normative regulation. Many studies have focused on the relationship between cyber security and normative regulation. The key normative restrictions on cyber proxy wars have been analysed by Nye, one of the most prominent scholars in IR, in his paper *Normative Restraints on Cyber Conflict*.[8] The author's study focuses on the recent evolution of international standards to provide insights into the emergence of normative restrictions in the cyberspace. Nye draws on constructivist scholar Martha Finnemore when discussing the normative constraints on States, explaining how political actors frequently cross the lines that academic theorists establish between the categories of law, norms, principles, and codes of behaviour.

---

[5] Betz, D. J. & Stevens, T., 2011. Cyberspace and the State: Towards a Strategy for Cyber-Power. Abingdon: Routledge/International Institute for Strategic Studies.

[6] Betz, D., 2012. Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed. Journal of Strategic Studies, 35(5).

[7] Schmitt, Michael N., and Liis Vihul. "Proxy wars in cyberspace: the evolving international law of attribution." *Fletcher Sec. Rev.* 1 (2014).

[8] Nye, Joseph S. "Normative restraints on cyber conflict." Cyber Security: A Peer-Reviewed Journal 1.4 (2018): 331-342.

The topic of laws, norms, principles and norms of behaviour was indeed pioneered by Finnemore and her work on the lifecycle of norms. Specifically, in her article titled *International Norm Dynamics and Political Change*[9], Finnemore and Sikkink advance three broad arguments: 1) The current ideational 'turn' is essentially a return to some of the discipline's historic objectives. 2) Norms have a three-stage 'life cycle', each with its own origin, method of impact, and circumstances under which norms will affect international politics. 3) The inclination to pit standards against logic fails to understand the most important political processes. Instead, we must acknowledge that "rationality cannot be divorced from any politically relevant episode of normative influence or normative change, just as each episode of rational decision is constrained by the normative environment."

The third group of sources analysed are institutional reports on the matter of cyber regulation. These range from the four GGE reports (2010, 2013, 2015, 2021)[10] to both of the Tallinn Manuals on the international law applicable to cyber warfare (2013, 2017)[11] and furthermore to the International Law Commission's *Draft Articles on Responsibility of States for Internationally Wrongful Acts* (DARSIWA)[12]. The 2010 GGE report stated that governments agreed cyber-conflict had become a threat to international peace and stability, and that a catastrophic cyber event may evolve into a larger conflict due to a lack of international direction. As a result, it advocated a dialogue on international cyberspace standards, as well as confidence-building measures to promote international security and stability. The 2013 report contained a significant milestone of consensus in international law. The 2015 study also included 11 additional norms and principles recommendations. However, it is debatable whether the GGE reports have any norm-setting influence. The findings were only mentioned in subsequent General Assembly decisions, and the GGE membership is not widely represented. The 2015 report also failed to make any headway on the Law of Armed Conflict's (LOAC) applicability to cyberspace, and China and Russia

[9] Finnemore, Martha, and Kathryn Sikkink. "International norm dynamics and political change." International organization 52.4 (1998).
[10] United Nations Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", A/70/174, 2010, 2013,2015,2021.
[11] Tallinn Manual on the International Law Applicable to Cyber Warfare, by Michael N. Schmitt, Cambridge University Press, Cambridge, 2013
[12] International Law Commission. "Draft articles on responsibility of states for internationally wrongful acts." Yearbook of the International Law Commission 2.2 (2001).

appear to have abandoned their 2013 agreement that international law applies online. The Tallinn Manuals, on the other hand, were the first complete and authoritative examination of international law's applicability to cyber warfare. The first Tallinn Manual analyses international law concepts that apply to cyber warfare and lists 95 ‘black-letter rules’ that regulate such battles. Sovereignty, State responsibility, the jus ad bellum, international humanitarian law, and the rule of neutrality are all discussed. Tallinn Manual 2.0 instead expands on the original edition's extremely important coverage by covering malicious cyber activities that do not rise to the threshold of acts of war. It lists 154 ‘black letter’ laws that govern these sorts of cyber activities and gives detailed discussion on each one. It covers subjects including human rights and the law of air, space, and sea, in addition to sovereignty and State accountability.

Nevertheless, not all States agree on the international application of the Tallinn Manual. The official position of the Russian Federation regarding the Tallinn Manual is one of significant scepticism. The Russian government views the Tallinn Manual as a research document that carries inherent political bias, potentially serving to legitimize the military application of IT technologies. This perception is rooted in several factors that raise questions about the impartiality and inclusivity of the manual's development process. One noteworthy concern is that the individuals responsible for crafting the Tallinn Manual primarily hail from backgrounds associated with the United States and certain European countries, which might create an inherent bias in the manual's perspective. Critics argue that this bias is evident in the absence of legal experts from countries like China and the Russian Federation, which could have contributed diverse viewpoints and insights. The context of the Manual's creation is also a point of contention. It is noted that the manual was conceived as a response to cyber-attacks, including those allegedly orchestrated by the Russian Federation in 2007. Consequently, some argue that the manual's genesis may reflect a specific agenda or viewpoint rather than a truly neutral and comprehensive examination of international cyber-related matters. In contrast, the Russian Federation has advocated for the development of a new international legal framework governing the use of information and communication technologies (ICTs) and a thorough review of existing international law principles such as jus ad bellum and jus in bello. This position is grounded in the belief that a comprehensive and balanced international legal framework is essential to address the challenges posed by ICTs and to prevent conflicts arising from their

misuse. While the Tallinn Manual is acknowledged within this context, critics contend that it is not given due consideration and is perceived as an effort by NATO experts whose views are perceived as conflicting with Russia's goal of averting military and political confrontations in the realm of information space.

The *Draft Articles on Responsibility of States for Internationally Wrongful Acts* (DARSIWA) aim to codify and expand gradually the fundamental principles of international law governing States' accountability for their globally unlawful activities. The focus is on the secondary standards of State accountability, or the broad requirements under international law for the State to be held accountable for wrongdoings or omissions, and the resulting legal ramifications. The provisions make no attempt to specify the specifics of the international commitments, whose violation results in liability. The basic norms serve this purpose, and codifying them would require restating the majority of important customary and conventional international law.

3. Methodology of the research

The methodology of this research drew upon Finnemore's constructivist theory of norms.[13] The emphasis on the social construction of norms and their influence on State conduct in Finnemore's constructivist theory of norms makes it particularly relevant to the topic of cybersecurity. Cybersecurity in the context of international relations is impacted by norms that direct State behaviour and interactions in cyberspace as well as more conventional legal frameworks.

Finnemore contends that social norms are created via processes of interaction and interpretation rather than being inherent or set. They develop as common perceptions among players in a certain setting, and they have the power to influence behaviour. Norms are essential in influencing State behaviours, collaboration, and dispute resolution in the context of cybersecurity.

The constructivist viewpoint emphasizes the significance of norms in determining what constitutes appropriate and improper conduct in cyberspace. It acknowledges that interactions and agreements among States, non-State actors, and international organizations can lead to norms evolving and changing over time. This is especially true in the field of

[13] Martha Finnemore and Kathryn Sikkink, "International Norm Dynamics and Political Change," International Organization 52:4 (1998), 891.

cybersecurity, where new dangers and difficulties necessitate ongoing adaptation and updating of rules.

The importance of socialization in the spread of norms is also emphasized by Finnemore's constructivist theory. Through processes of social learning, imitation, and persuasion, States develop and internalize norms. By encouraging responsible behaviour and lowering the possibility of cyber disputes, norms can assist nations develop uniform expectations and standards of conduct in the area of cybersecurity.

The constructivist approach also emphasizes the importance of advocacy networks and norm entrepreneurs in establishing norms. These individuals are essential in advancing and galvanizing support for certain cybersecurity rules. They participate in discourse, articulating problems and emphasizing the significance of certain actions or routines that might affect societal norms and State conduct.

Overall, Finnemore's constructivist theory of norms offers a useful framework for appreciating and examining the evolution of norms in the cybersecurity sector. It clarifies how social norms are created, change through time, and influence State behaviour and online interactions. We may better understand the difficulties and potential for creating a cooperative and secure cyber environment by looking at norms through this lens.

This theory was then applied to the current problem of cyber delegation of power by States to proxies, with the aim to analyse the current issues of normative regulations and understand at which stage of the ‘norm cycle’ we currently are. The research mainly used qualitative data in order to interpret patterns and meanings in the data. The data was primarily secondary, pooling form historical examples of cyber breaches and attacks by State and non-State actors.

4. Research questions

In this thesis we will attempt to answer the two research questions: (I). What are the normative foundations of the cyber proxy wars regulations? And (II). Are these norms internalized?

5. Hypothesis

The evolution of cyber proxy warfare and the development of norms regulating it present complex global challenges. There are principles and laws in international relations

which are recognised by many States as being applicable to cyberspace. Yet, of how to implement those rules is still an unresolved issue. The establishment of cyber norms is in its early stages, mirroring the initial phase of 'norm emergence.' The rise of non-state actors and State proxies in cyberspace reshapes international security but also underscores the urgency of robust cyber norms. Soft power dynamics influence States' adherence to these norms, including prudence, reputational costs, and national political pressures. International legal norms face challenges in cyberspace, especially regarding non-state actors and State proxies.

While progress in cyber norm development is evident, it remains a complex process which is long from reaching the 3rd stage of the life cycle of norms. The international community must continue proactive and cooperative efforts to build and internalize norms governing cyber proxy warfare, safeguarding global peace and stability in this ever-evolving domain.

6. Structure outline

This thesis will be divided into four chapters. The first chapter will set the pace for the research. It will begin by defining what is cyberspace and what are the cyber threats in the military and political realm. This chapter will be specifically inspired by Tim Maurer's work in *Cyber Mercenaries: the State, Hackers and Power* [14]. In his book, Maurer gives valuable insight into how States utilize non-State actors in offensive cyber operations, demonstrating that States are only one category of players with substantial offensive cyber capabilities. Maurer's analysis highlights the underappreciated phenomenon of governments outsourcing certain duties to non-State actors, as well as identifying the grey area of reality in which States cultivate informal connections with players that are not technically part of the State and yet benefit it. We begin by defining the core principles of proxies in cyberspace.

The second section of this chapter will deconstruct and define cyber proxy relations. Most proxy relations, according to Maurer, may be divided into three categories: delegation, orchestration, and sanctioning.[15] *Delegation* captures the more conventional concept of proxies (defined as the primary delegating its "authority to an agent to act on its

[14] Maurer, Tim. Cyber mercenaries. Cambridge University Press, 2018.
[15] Ibidem.

behalf"), [16] as shown by the US government's relationship with its defense contractors. *Orchestration* is defined as the " enlistment of intermediary actors on a voluntary basis, by providing them with ideational and material support, and using them to address target actors in pursuit of political goals".[17] Finally, *sanctioning* occurs when a State chooses to passively assist a non-State actor by deciding to "tolerate the actor's activities while having the power to do otherwise".[18]

The second chapter will cover the issue of the normative regulation of international relations in the cyberspace. Great powers compete in a variety of domains to protect their interests and ensure their security. Perhaps the most striking area of this increased competition has been the internet. As previously stated, the extent and diversity of cyber-enabled forms of competition has been increasing to encompass acts such as interfering in democratic processes and the theft of industrial secrets on a larger and more sophisticated scale. Such tools have the potential to jeopardize the stability of major power relations more than nearly any other area of competition by posing direct dangers to political and economic security in national homelands.

The main instruments of statecraft for encouraging cybersecurity remain investments in cyber resilience and threats of punishment. Other areas of competition, on the other hand, have long used formally or informally negotiated rules of the road and international conventions to help restrain disruptive features of competition and create a situation in which deterrence and defense strategies would be more successful. Extensive arms control treaties, rules of engagement in the air and on the high seas, and unwritten rules that constrain State action, such as the prohibition on the use of nuclear weapons, are examples of such rules and norms. Today's question is whether such rules and norms can contribute to control competition even in the cyber realm. Hundreds of recommendations for rules and standards to control cyber activity have been made by governments, academics, nongovernmental organizations (NGOs), and private-sector corporations, most of which are based on international law. For this section we follow the normative approach of scholar Martha Finnemore by first analysing the political issues around the normative

[16] Ibidem.
[17] Ibidem.
[18] Ibidem.

regulation of cyberspace and then exploring the importance that soft power can have in such regulation.[19]

The third chapter will regard the areas of contention, or so called 'grey areas', in international law regarding appropriate State behavior in cyberspace. Cyberspace has its own set of traits that might obstruct the formation of standards to limit State conduct. Because of the structure and complexity of cyberspace, certain international principles are considerably more difficult than in other domains, such as the principles of sovereignty, attribution, the use of force and self-defence, and the law of neutrality. Then we will examine how they influence other crucial areas of international law such as the principle of due diligence, State responsibility and countermeasures. Globalisation and technological change have long been seen as harbingers of State decline and reduction of sovereignty. The consequences of the emergence of cyberspace on State sovereignty have tended to follow a broad narrative that sees sovereignty loss as an unavoidable result of global information interchange and the dwindling importance of physical territory in cyberspace. As a result, we are in a conflict between the free flow of information and the traditional notion of sovereignty, as demonstrated by the new Russian information security law adopted in 2015, the first since 2000, which states that "[t]he special services of certain States provide information and psychological influence, aimed at destabilizing the political and social situation in various regions of the world, resulting in the undermining of the sovereignty and the territorial integrity of other States."[20]

As we previously mentioned cyberattacks are secretive by their very nature, this explains why the nature and repercussions of an incident may not be immediately apparent and attributing the source of an attack can be difficult. There have been attempts to apply international law to cyberspace, such as the 2013 Tallinn Manual on the International Law Applicable to Cyber Warfare.[21] However, they have so far failed to achieve consensus on many points. In the case of proxies, Michael Schmitt and Liis Vihul, in their 2014 article *Proxy Wars in Cyberspace: The Evolving International Law of Attributio*n, noted that States have a lot of leeway in their support of them: "the relatively high levels of support

[19] Martha Finnemore and Kathryn Sikkink, "International Norm Dynamics and Political Change," International Organization 52:4 (1998), 891.
[20] Shtepa, "Russia's Draft Information Security Doctrine."
[21] Schmitt, Michael N., ed. *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press, 2013.

that are required before a State can be held responsible for the activities of non-State groups or individuals, as distinct from their own responsibility for being involved, creates a normative safe zone for them."[22] Looking into non-governmental attribution capabilities and their consequences for international relations is indeed an important area of inquiry.

The notion of neutrality, on the other hand, is crucial in cyber warfare. A belligerent may route an attack through neutral nations' servers or conduct cyberattacks from within the neutral State's borders due to the internet's borderless international framework. Even if the neutral State's territory is not physically violated, assaults routed through its cyber infrastructure appear to breach the principle of neutrality. Thus, the principle of neutrality applies in international armed combat circumstances. However, the legal stance on whether cyberattacks are authorized acts of armed conflict is ambiguous under international law. According to the United Nations Charter an armed attack is defined as "the crossing of geographic domains by the use of armed force."[23] Keeping this in mind, it has been suggested that malicious software essentially transports a weapon capable of causing physical devastation across cyberspace, and so cyberattacks should be considered an armed attack under the United Nations Charter.[24]

The fourth and final chapter will analyse the UN GGE negotiations over cyberspace security. The GGE has long been the primary UN forum for debates on cyber stability. This policy process was created to look into current and future cyber risks, as well as possible cooperative responses. Since 2004, the GGE has held six meeting, four of which have produces reports on cybersecurity (2010, 2013, 2015, 2021) and the need for defining cyberspace standards has been emphasized throughout these GGE reports. When looking at the GGE process through Finnemore and Sikkink's model, it's clear that these standards are still in their early period in the lifecycle of norms. In 2019 a new forum was created upon the request of the Russian Federation, the OEWG. This process was much more open and concerned with the ongoing creation and improvement of the standards, norms, and principles guiding responsible State behavior. However, doubts arose as to whether this process would substitute or complement the efforts made so far through the GGE.

---

[22] Schmitt, Michael N., and Liis Vihul. "Proxy wars in cyberspace: the evolving international law of attribution." *Fletcher Sec. Rev.* 1 (2014): 53.

[23] Charter of the United Nations, art. 51.

[24] Brown, Davis. "A proposal for an international convention to regulate the use of information systems in armed conflict." *Harv. Int'l LJ* 47 (2006): 179.

Lastly, this thesis will analyse the efforts made by the OSCE in the field of cyber and ICT security. The OSCE's primary objective is to foster stability, peace, and democracy by engaging in both political discourses concerning shared values and pragmatic initiatives aimed at creating enduring positive impacts. Within the realm of cybersecurity, the OSCE confronts diverse cyber threats, encompassing cybercrimes and the exploitation of the Internet for terrorist objectives. Notably, the organization concentrates on formulating Confidence Building Measures (CBMs) among its participating States, intended to mitigate the likelihood of conflict arising from the utilization of ICTs.

7. Conclusions

The subject of cyber proxy warfare and its normative regulation in international relations represents an emerging and evolving field of study within the broader context of cybersecurity and international security. While there is a growing body of literature addressing various aspects of cyber warfare, including state-sponsored cyber activities and cyber conflict, the specific focus on cyber proxy warfare and its normative framework is relatively novel.

This research builds upon existing scholarship in the following ways:

- Cybersecurity Studies: It draws from research in the field of cybersecurity, examining the tactics, techniques, and procedures used in state-sponsored and proxy cyber operations.
- International Relations Theory: The analysis incorporates international relations theories, such as the concept of state sovereignty, to understand the challenges of regulating cyber proxy activities within the existing international framework.
- Normative Governance: The discussion integrates concepts from the literature on international norms and governance to explore the potential development of norms and agreements related to cyber proxy warfare.

The scientific novelty of this research lies in its comprehensive examination of cyber proxy warfare within the context of international relations and normative development. Key aspects of its novelty include:

- Cyber Proxy Focus: While there is extensive literature on cyber warfare, the specific focus on cyber proxy warfare, where non-state actors act on behalf of states in cyberspace, is a relatively new area of study.
- Normative Development: The research emphasizes the need for normative development in response to the evolving nature of cyber proxy warfare, filling a gap in the literature that addresses the regulatory challenges posed by this emerging form of conflict.
- Interdisciplinary Approach: By integrating insights from cybersecurity, international relations, and governance studies, this research takes an interdisciplinary approach to understanding the complex dynamics of cyber proxy warfare and potential normative solutions.

In summary, the topic of cyber proxy warfare and its normative regulation represents an emerging and interdisciplinary field of study. While it draws from existing research in cybersecurity and international relations, its focus on the specific challenges and opportunities posed by cyber proxy operations and the development of norms in this context adds a novel dimension to the broader literature on international security and governance.

Chapter 1: Methodology of the research

The importance of cyberspace in the military and political realm

As governments and non-State actors use cyberspace to reach strategic goals, this has grown to be a more contentious domain in international relations. Many analysts argue that cyberspace is the new field of conflict as a result of an increasing number of cyberattacks and instances of cyberespionage. However, it is a complex problem that demands rigorous investigation to determine whether cyberspace is the new arena for global conflicts.

This first paragraph will first introduce the complicated concept of 'cyberspace'. Secondly, in this chapter we will define what is 'cyberwarfare' and if it has or will ever take place.

The definitions of cyberspace used by various governments vary considerably, indeed there seems to be no consensus on what 'cyberspace' is nor what are its implications of conflicts. Cyberspace is described by the US Cyberspace Policy Review as the "globally-interconnected digital information and communications infrastructure [that] underpins almost every facet of modern society".[25] The UK Cyber Security Strategy, on the other hand, describes cyberspace as including "all forms of networked, digital activities; this includes the content of and actions conducted through digital networks".[26] Cyberspace is described as "the electronic world created by interconnected networks of information technology and the information on those networks"[27] in the Canadian Cyber Security Strategy. While the word 'cyberspace' is completely avoided in Australia's Cyber Security Strategy in favour of the word 'Internet.'[28]

Overall, cyberspace differs in a number of ways from other strategic domains, like land, sea, air, and space, the most significant of which is that it is the only environment that is fully created by mankind. Cyberspace is artificial. We usually think of it as a digital

[25] White House, Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure (Washington DC: US Government Printing Office, 2009), p. iii.
[26] Cabinet Office, Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space (Norwich: The Stationery Office, 2009), p. 7.
[27] Public Safety Canada, Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada (Ottawa: Government of Canada Publications), p. 2.
[28] Attorney-General's Department, Cyber Security Strategy (Canberra: Australian Government, 2009).

space between the devices we use to access it, such as computers and smartphones. Therefore, this space only exists because of the underlying infrastructure that enables it and is entirely constructed by man, which is not an observation we can easily make of other domains.

Another peculiarity of cyberspace, according to Nye, is essentially due to the fact that both natural and virtual elements contribute to its formation, the hybrid nature of which reflects the uncertainty and inability to achieve an all-encompassing sharing of the cognitive description of the term 'cyberspace'.[29] According to Martin C. Libicki, cyberspace (unlike the other natural domains such as land, water, air and outer space) is a virtual and intangible medium, the heterogeneous nature of which, Libicki continues, is to represent this reality on three levels: physical, syntactic and semantic.[30] Unlike Libicki's perception, the U.S. military while depicting cyberspace through such triple layering, prefers to add a purely 'social' level as depicted in Figure 1 in the appendix.[31]

According to this threefold representation, the first layer (the physical layer) consists of the submarine or Ethernet cables, routers and data exchange and communication devices. Above this is the logical layer made up of the codes that enable the hardware to function and communicate. The third layer consists of the social layer, made up of interaction between online users (individuals) and, increasingly, between machines. These three layers go to form the first frame of the mapping of the cyberspace. However, the essential element that distinguishes the geography of the cyberspace domain from other realities is its artificial and hybrid character.

It is precisely the hybrid character of cyberspace that has helped shape the dynamics of human interactions and outclass traditional concepts such as political participation, political debate, decision-making, peace and war. Many analysts argue that cyberspace is indeed the new field for international wars and go so far as to calling it the 'fifth dimension of conflictuality'[32], where, computer systems, especially civilian ones, are

[29] Nye Jr, Joseph S. The future of power. PublicAffairs, 2011.
[30] Libicki, Martin C. Cyberdeterrence and cyberwar. RAND corporation, 2009.
[31] Department of the Army Headquarters, United States Army.
[32] Martino, Luigi. "La quinta dimensione della conflittualità. L'ascesa del cyberspazio ei suoi effetti sulla politica internazionale." Politica & Società 7.1 (2018): 61-76.

the new centres of gravity to be protected, against an enemy that, more often than not, 'operates in the shadows' in a nuanced and asymmetric environment.

However, not all analysts agree. Thomas Rid, for instance, asserts that the focus on the cyber domain and so-called 'cyberwarfare' would be nothing more than a publicity gimmick because the risk of cyber warfare and the hypothetically feared disasters would most certainly not present in the future: "cyber war will not take place."[33] Rather, political cyberattacks that have occurred or may occur in the future will only be a "sophisticated versions of activities that are as old as warfare itself: subversion, sabotage and espionage"[34]. Rid concludes that no act of cyberwarfare satisfies all three of Clausewitz's criteria — violence, instrumentality, and politics — on the traditional conception of what constitutes war.[35]

This argument is still compelling today, indeed we have not yet seen an 'all out' cyber war. Usually, cyber forces are today almost always used to accompany wars. However, the belief that cyber war will never happen endorses what Whetham believed to be an 'overly restrictive' interpretation of war.[36] Thus, it is important to define what we mean by warfare.

This thesis agrees with the criteria which were outlined by Clausewitz to define an act of war. It also agrees with Rid and makes the case that not all cyber-attacks, such as cyber-espionage and subversion, should be considered acts of war because this risks to confuse the notions of war and non-war. However, we argue that the use of violence is not a necessary prerequisite for what constitutes war[37]. We find it more fruitful to adopt a broader definition and interpretation of what is to be considered war, taking into account also Sun Tzu's theories on war[38]. As was noted by Amit Sharma:

"Cyber warfare derives the essence of both of these great military theorists, as it is warfare that is capable of compelling the enemy to do your will by inducing strategic

[33] Rid, Thomas. "Cyber war will not take place." Journal of strategic studies 35.1 (2012): 5-32.
[34] Ibidem.
[35] Ibidem.
[36] Whetham, David. ""Are We Fighting Yet?" Can Traditional Just War Concepts Cope with Contemporary Conflict and the Changing Character of War?." The Monist 99.1 (2016): 55-69.
[37] Ibidem.
[38] Tzu, Sun, and Lionel Giles. The art of war. Vol. 84. Oxford: Oxford University Press, 1963.

paralysis to achieve desired ends, and this seizing of the enemy is done almost without any application of physical force."[39]

Indeed, there have been several changes since 1832 and the development of cyber-weapons has simultaneously reduced the appeal of using maximum force and revived Sun Tzu's principles of minimal force and deceit.[40]

It is crucial to illustrate how future cyber warfare will manifest by illuminating how small-scale acts of violence may escalate into unfathomable atrocities. War may actually be defined as the use of limited force, provided that it results in violence, paired with instrumentality and political might. As stated by Sun Tzu, "to seize the enemy without fighting is the most skilful"[41]. This statement is applicable to cyber-attacks because it may be possible to subjugate the enemy without the use of conventional armed forces and only the barest amount of force. The Stuxnet and NotPetya attacks have shown that cyberattacks have and could meet the requirements necessary to constitute an act of war and force the enemy to carry out its will with the least amount of force, while at the same time encapsulating the art of war where the wise warrior avoids the battle[42], at least conventionally. Rid is therefore mistaken when he claims that because a cyberattack requires a relatively little amount of force, it cannot produce enough violence to qualify as an act of war.

This is further supported by the fact that, although making it plain that force is the key to war, Clausewitz never specifies how much force is required for an act to be considered an act of war. Clausewitz simply asserts that using the greatest amount of power possible will give you the upper hand in a battle. [43] In cyberspace, though, that is not the case because the advantage can be gained with little force. This is partly due to the fact that little acts of force, like performing an IP spoofing, have the potential to escalate into widespread violence, which may result in the bodily or mental harm or death of individuals or inanimate things[44]. The misleading nature of cyberattacks and the fact that they are typically not announced but rather the attacker "attacks him where he is unprepared and

[39] Sharma, Amit. "Cyber wars: A paradigm shift from means to ends." Strategic Analysis 34.1 (2010): 62-73.
[40] See note 29
[41] Ibidem.
[42] Ibidem.
[43] Clausewitz, Carl. On war. Penguin UK, 2003.
[44] Stone, John. "Cyber war will take place!." Journal of strategic studies 36.1 (2013): 101-108.

appears when he is unexpected"[45], boosts the idea that minimal force can gain the upper hand and can therefore increase damage and chances of victory.

This motivates us to show how cyberwarfare may still happen despite one of its biggest drawbacks: attribution. Because cyberattacks typically strike when their target is unprepared, these issues — attribution, anonymity, and lack of declaration — are the most difficult to solve. According to Rid, the attacked State must be able to blame the assault on another State in order to know how or where to start a response and possibly declare a war. Even while history does not record acts of war without at some point blaming someone, this does not mean it will not do so in the future. [46] It's even possible that the constantly changing nature of war will make it difficult to ever conclusively determine who committed a war crime in cyberspace. However, this does not imply that the act is not a war crime. Therefore, any attempt to discern whether an act of war meets the criteria outlined earlier in the chapter — namely, the act is innately violent, political, and instrumental — is not subject to issues of transparency and attribution.[47]

It is crucial to cross-examine Rid's mistakes in failing to accurately discern between what constitutes sabotage and an act of war in literary terms in order to demonstrate the likelihood of cyberwar. Since "things are the prime targets, not humans," Rid contends that any "deliberate attempt to weaken or destroy an economic or military system" is sabotage and cannot be classified as warfare.[48] However, Rid's analysis distinguishes between damage that only affects physical property and damage that injures or kills people on at least one side of a conflict. Rid is wrong in this regard because, according to the Oxford English Dictionary, violence need not always result in human casualties. [49] Instead, because the *mens rea* must only be for the act's commission and the outcome is inconsequential, a violent act may even have no consequences at all. Rid clearly believes that the Stuxnet attack on the Iranian enrichment plant can squarely fit within what is defined as 'sabotage' rather than realizing that the Stuxnet case was a hotly contested case that cannot squarely fit within the bracket of sabotage because of this misunderstanding of the meaning of the

[45] Tzu, Sun, and Lionel Giles. The art of war. Vol. 84. Oxford: Oxford University Press, 1963.
[46] Stone, John. "Cyber war will take place!." Journal of strategic studies 36.1 (2013): 101-108.
[47] Ibidem.
[48] Rid, Thomas. "Cyber war will not take place." Journal of strategic studies 35.1 (2012): 5-32.
[49] Stone, John. "Cyber war will take place!." Journal of strategic studies 36.1 (2013): 101-108.

word ‘violence.’ Stuxnet's inability to be recognized by Rid as an act that goes beyond sabotage may, therefore, be reasonably contested.

Firstly, we could argue that the conduct was first and foremost political, since it was “of such complexity it could only be a State behind it”. [50] Second, Stuxnet had a goal: forcing Iran to comply with the perpetrator's demand for a postponed Iranian nuclear program[51]. Therefore, we can claim that the attack was also instrumental to an end. Lastly, the fact that it was the first known incident of a physically harmful cyber weapon damaging centrifuges made it violent attack in nature. [52]

It is important to look at Stuxnet in two critical ways in order to further support the notion that it was not just a large-scale act of sabotage. First off, according to the equivalent effect test, the Stuxnet strike qualifies as an act of war since it resembles a kinetic attack and has “the effect of a cruise missile or a commando raid”.[53] The equivalent effect test is crucial for categorization because it serves as a key criterion for differentiating between an act of just hostile behaviour and an act of war. Because cyberespionage does not constitute an act of war, Rid was correct in stating that Lewis's observation that “no damage or no casualties, means no attack”. This is due to the fact that cyberspace is a hostile environment, and that hostile conduct exists there, such as cyberespionage, “but it stays below the threshold of an attack”[54]. However, Stuxnet stands out because it inflicted physical harm akin to a kinetic attack. Stuxnet largely satisfies the Schmitt test criteria because it caused “physical damage to the Iranian nuclear infrastructure, was highly invasive, its damage was quantifiable, and it was almost certainly created under the auspices of a national government” [55]. This is another way to show that Stuxnet could one day be seen as an act of war. All things considered, one issue still remains: would a commando operation by the United States of America and Israel against the Iranian nuclear site be regarded as an act of war or only sabotage because no one was killed? It is possible that it would be viewed as a war crime, or more particularly, as a clandestine action carried out by the Special Forces. Although this contestable cyberattack did not start a cyberwar, it

[50] Beaumont, Peter. "Stuxnet worm heralds new era of global cyberwar." The Guardian 30 (2010).
[51] Zetter, Kim. "Legal Experts: Stuxnet Attack on Iran Was Illegal ‘Act of Force.’." WIRED Online (2013).
[52] Ibidem.
[53] Wedermyer, Landon J. "The Changing Face of War: The Stuxnet Virus and the Need for International Regulation of Cyber Conflict." StuSch (2012).
[54] Lewis, J. "Cyber attacks, real or imagined, and cyber war." CSIS Commentary 11 (2011).
[55] Rid, Thomas. "Cyber war will not take place." Journal of strategic studies 35.1 (2012): 5-32.

does show how one might develop in the future. As a result, when Rid claims that Stuxnet has raised the bar for computer sabotage[56], he ignores the reality that this is not only a new degree of sabotage.

Furthermore, Rid is cautious to explain the differences between the immediacy and directness of a physical assault, such a drone attack and he claims that in the case of potential cyber-attacks, "the causal chain that links somebody pushing a button to somebody else being hurt is mediated, delayed, and permeated by chance and friction"[57]. Nevertheless, he claims that, despite this, they could still be regarded as acts of war if, for example, a derailment brought on by logic bombs crashed a train or caused the failure of backup air traffic control systems, resulting in numerous injuries and fatalities[58]. However, if he can acknowledge that this is a possibility, he cannot credibly deny the possibility of a cyberwar.

Finally, it is crucial to illustrate how trinitarian warfare could be used in cyberwar in the future. The government, the people, including the economy, and the defenders of the State are the three inclinations that make up the trinity and are all thought to be essential for keeping the State's machinery in motion[59]. Each member of the trinity is strong enough to overcome obstacles provided by foes on its own since it may depend on another member of the trinity to revive it. However, "the cascade effect" is generated to cause a strategic paralysis on the nation when all three components are destroyed simultaneously or, in conventional terms, are subjected to parallel warfare"[60], which plunges the State into an upheaval and uproar. All three tendencies now heavily rely on technology, especially in contemporary States. These three trends are all exposed to parallel warfare by their reliance on internet. This is presently seen in the COVID-19 pandemic, where a successful cyber-attack on the communications and health care infrastructure could have caused any State to become strategically paralyzed. The Titan Rain attacks on Estonia and Georgia, which were tactical in nature and targeted specific members of the trinity, serve to underline this point even more[61]. By contrast, applying power simultaneously at the strategic, operational,

[56] Ibidem.
[57] Ibidem.
[58] Ibidem.
[59] Sharma, Amit. "Cyber wars: A paradigm shift from means to ends." Strategic Analysis 34.1 (2010): 62-73.
[60] Ibidem.
[61] Ibidem.

and tactical levels of war would have affected all three members of the trinity. Therefore, in order for cyberattacks to qualify as acts of war, they must inflict harm comparable to that caused by a kinetic attack, and they must particularly succeed in subduing the enemy by employing the parallel warfare paradigm[62]. All things considered, even though cyberwar hasn't occurred in the past because cyberattacks haven't been effective acts of war, it doesn't mean it won't in the future.

We can conclude by arguing that although cyberwar has not yet occurred, it is obvious that it will do so in the future. This is partly due to the fact that some cyberattacks may meet the three requirements that must be present for an act of war: it must be intrinsically violent, political, and instrumental. Incomprehensible aggression can also result from seemingly innocuous actions of force, such as accessing a computer system.[63] Regarding the extremely challenging topic of attribution and declaration, even though history has never known an act of war without some form of attribution, a future in which there is never clear-cut attribution could present a unique challenge to the world. In addition, violence committed need not be fatal; it can also result in material damage and psychological harm. The Stuxnet attack on the Iranian nuclear plant, which provided the world a glimpse into what may happen but on a bigger, more sophisticated scale in the future, is one specific plausibility probe that was examined in the article and supports the claim that cyberwar will occur. Last but not least, cyberattacks have the ability to cause a 'cascade effect' in which all three members of the trinity are harmed, seizing the opponent via tactical paralysis. The issue of when a cyberwar will occur has replaced the earlier one of whether one will occur.

Many States and International Organizations have agreed with the view that cyberspace is the new field of warfare and have stated so publicly. One of the first to do so was the U.S. in 2010, when the departments of Defense and Homeland Security of the United States created the U.S. Cyber Command. In an essay written by former Deputy Defense Secretary William J. Lynn III for *Foreign Affairs* magazine, it is clearly stated that "the Pentagon has formally recognized cyberspace as a new domain of warfare."[64]

---

[62] Ibidem.
[63] Stone, John. "Cyber war will take place!." Journal of strategic studies 36.1 (2013): 101-108.
[64] Lynn III, William F. "Defending a new domain-the Pentagon's cyberstrategy." Foreign Aff. 89 (2010): 97.

Moreover, the Russian military concept from 2010 identifies information security (*informatsionnaya bezopastnost*), the semantic Russian equivalent of cybersecurity, as one of the "features of contemporary military conflicts" and states that one of the tasks of the Armed Forces is to "to develop forces and resources for information warfare".[65]

Furthermore, the 2016 Warsaw Summit Communiqué officially decrees the militarization of cyberspace. As it clearly states: "Cyber attacks present a clear challenge to the security of the Alliance and could be as harmful to modern societies as a conventional attack. We agreed in Wales that cyber defence is part of NATO's core task of collective defence. Now, in Warsaw, we reaffirm NATO's defensive mandate, and recognise cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea."[66]

These three instances highlight the growing recognition of the importance of cybersecurity in modern warfare and mark a significant shift in the national and international postures to collective security. The American recognition of cyberspace as a new domain of warfare reflects the realization that while information and communication technologies (ICTs) are used more frequently in military operations, being able to control and influence cyberspace is now crucial to maintaining national security. The Russian understanding of information warfare is important for the nation's military posture and strategy since it represents a movement toward a broader understanding of warfare that encompasses not just conventional military operations but also a variety of non-military actions such as cyberattacks, disinformation, and other types of information manipulation. This strategy is compatible with Russia's larger initiatives to increase its influence and protect its interests in the global scene. Russian military planners are embracing the value of information warfare and the potential of information and communication technology to further their national security goals. Lastly, one of the key implications of the NATO decree is the recognition of cyber-attacks as a clear challenge to the security of the Alliance. This recognition is important because it acknowledges the growing threat posed by cyber-attacks to national security and emphasizes the need for collective defence against

---

[65] "Военная доктрина Российской Федерации." 2010. Президент России. February 5, 2010. Accessed April 30, 2023. http://kremlin.ru/supplement/461. For the English translation see: https://carnegieendowment.org/files/2010russia_military_doctrine.pdf

[66] NATO. "Warsaw Summit Communiqué." NATO, July 2016, https://www.nato.int/cps/en/natohq/official_texts_133169.htm

such attacks. As stated by NATO Secretary General Jens Stoltenberg, "most crises and conflicts today have a cyber dimension."[67] Furthermore, the recognition of cyberspace as a domain of operations implies that cyber warfare is now being seen as a legitimate form of warfare. This is significant because it provides a legal framework for the use of cyber-attacks in modern warfare and emphasizes the importance of international norms and laws in governing cyber operations. Overall, the NATO decree on cyber defence marks a significant shift in the Alliance's approach to collective defence, highlighting the growing importance of cybersecurity in modern warfare. By recognizing cyberspace as a domain of operations and emphasizing the need for effective cyber defence, NATO is taking a proactive approach to maintaining national security in the face of growing cyber threats.

Anatomy of cyber-proxy relationships: the State and the intermediaries

Once we have argued that indeed cyberspace is a new field for international warfare, this paragraph will analyse the relationship between State and non-State actors, and particularly those of proxies. In doing so we will understand the concept of proxies in cyberspace, in order to better understand how they are regulated.

First, we will introduce the concept of proxy actors in cyberspace. Secondly, we will delineate their relationship with States. This chapter is specifically inspired by Tim Maurer's work in *Cyber Mercenaries: the State, Hackers and Power*[68].

Definition of the term 'proxy' in international research

One of the infamous stratagems used in Chinese military doctrine and claimed by Zi Gong is "to kill with a borrowed sword." The essence of this strategy involves leveraging a third party's power or influence to engage your adversary or persuading your ally to confront your enemy on your behalf, essentially employing a proxy to advance your objectives.

The term 'proxy' is widely debated, and there is no agreed-upon meaning. The fact that proxies are technically outside of the government and, to some extent, are independent

[67] NATO. "Cyber Defence: A Core Task for NATO in the 21st Century." NATO, June 29, 2016, https://www.nato.int/cps/en/natohq/opinions_132349.htm.
[68] Maurer, Tim. Cyber mercenaries. Cambridge University Press, 2018.

of the State is what characterizes them. They have different organizational structures, operating environments, motivations, and historical circumstances that have influenced their ups and downs. The majority of research on these actors focuses on their interactions with the State and how they have aided in the projection of State authority.[69]

The main use of proxies is power projection. Tim Maurer explains in his book that cyber proxies are connected to aggressive cyber operations.[70] In this sense, external cyber operations, as defined by former US military personnel Matthew Noyes and Robert Belk, are "cyber actions with effects on systems not owned or operated by the actor." [71] Information availability, confidentiality, and integrity may be compromised by such consequences. in most cases, an offensive cyber operation involves infiltrating an adversary's computer system or network and exploiting a weakness within that system or network to deploy a malicious payload. Both social engineering and coding vulnerability exploits can be used to gain remote access. Moreover, the vulnerability may have been intentionally included by a government agency as a backdoor or it may have been unintentional, such as a programming error.

An aggressive cyber operation may be directly or indirectly carried out through cyber proxies. Different outcomes are possible from offensive cyber operations. They can serve as stand-ins for traditional weapons, like a bomb, and they can also facilitate entirely unanticipated behaviours, such as altering financial data. The Pentagon's top cyber adviser, Eric Rosenbach, emphasized these qualities when he said the following regarding cyber operations:

“The place where I think it will be most helpful to senior policymakers is what I call in “the space between. What is the space between? ... You have diplomacy, economic sanctions ... and then you have military action. In between there’s this space, right? In cyber, there are a lot of things that you can do in that space between that can help us accomplish the national interest.”[72]

---

[69] Ibidem.
[70] Ibidem.
[71] Belk, Robert, and Matthew Noyes. On the use of offensive cyber capabilities: A policy analysis on offensive US cyber policy. JOHN F KENNEDY SCHOOL OF GOVERNMENT CAMBRIDGE MA, 2012.
[72] “Cyber Leaders: A Discussion with the Honorable Eric Rosenbach” (panel discussion, Center for Strategic and International Studies, Washington, DC, October 2, 2014), http://csis.org/event/cyber-leaders.

It is not just American thinkers that have this opinion. Similar reasoning has been put up by academics at the China Institute for International Studies, a think tank connected to China's Ministry of Foreign Affairs.[73] Therefore, utilizing proxies to project coercive authority through cyberspace is particularly alluring since the technology offers new coercive effects below the threshold of use of force in addition to plausible deniability.

Maurer summarizes what we said above in his definition of cyber proxy. He states that: "cyber proxies act as intermediaries that conduct or directly contribute to an offensive cyber action that is enabled knowingly, whether actively or passively, by a beneficiary."[74]

Different strategies are used by States to manage their interactions with cyber proxies. The interactions that nations have with these cyber proxies are often extensions of their customary methods of interaction with non-State entities. An intermediary that performs or directly participates to an aggressive cyber operation is referred to as a cyber proxy when enabled wilfully, actively, or passively by a beneficiary who benefits from its impact.[75]

The analysis in traditional study in this field frequently uses the words 'principles' and 'agents'. Nevertheless, decision-makers sometimes deal with difficult circumstances in which a State is not quite a principal: the State doesn't actively support a proxy, but rather chooses to ignore its activities. Maurer stays away from language that suggests any active sponsorship. Instead, he refers to actor A as the 'beneficiary' rather than the 'principal', and actor B as the 'proxy'.[76]

We will examine the many kinds of connections that may be made between these players in the next section.

[73] Teng Jianqun and Xu Longdi, Cyber War Preparedness, Cyberspace Arms Control and the United States (Beijing: China Institute of International Studies, 2014), 11.
[74] Maurer, Tim. Cyber mercenaries. Cambridge University Press, 2018.
[75] Ibidem.
[76] Mumford, Andrew. Proxy warfare. John Wiley & Sons, 2013.

The ‘beneficiary-proxy’ relationships

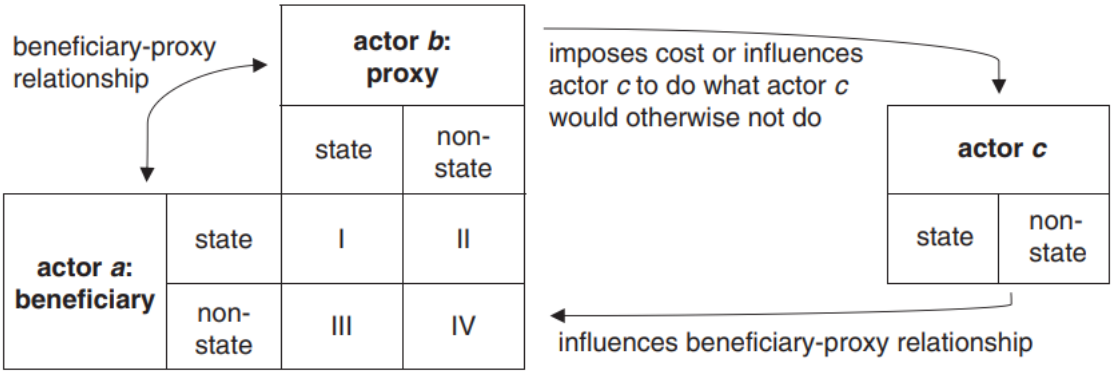


Figure 2, Beneficiary–proxy relationship directed at a third party.
Source: Maurer, Tim. Cyber mercenaries. Cambridge University Press, 2018.

Figure 2 presents a graphical representation of the various relationships that could arise between different actors in cyberspace. Each of the three actors—the beneficiary, the proxy, and the target—is classified into one of two groups, which also demonstrates the power projection towards others. Each player can either be a State or non-State actor.[77] The two-way arrows emphasize how the two actors have an impact on the other. This dynamic also applies to actor C, who is the targeted party and who, by its actions, can influence the proxy or the recipient, however, we will not cover this in our framework.

State/State Proxy Relationships

The first kind of relationship is frequently discussed in the literature on Cold War client and satellite nations as well as ‘State mercenarism.’[78] However, examples of this idea go back many centuries. The proverbial "kill with a borrowed sword", which we mentioned earlier, was used by Zi Gong, a Confucius follower who defended his native State Lu from the more powerful State of Qi in the fifth century B.C. In a complex plan, Zi Gong used the neighbouring States as ‘borrowed knives’ (i.e., proxies) to protect his home State.[79] The distinction between proxy partnerships and alliances is a common subject in the literature on State proxies. Even if asymmetry is challenging to assess, it is obvious that it is essential to the proxy connection. However, given that the Westphalian system presupposes that all sovereign nations are equal, the consideration of alliances makes this judgment more

[77] This framework does not include intergovernmental organizations and other actors that could give a more comprehensive view.
[78] Maurer, Tim. Cyber mercenaries. Cambridge University Press, 2018.
[79] Senger, Harro von, and Myron B. Gubitz. "The book of stratagems: Tactics for triumph and survival."1988

challenging. A convincing strategy is to disregard formal treaty-based alliances as proxies rather than treating it as an open empirical question for each situation.[80]

State/Non-State Proxy Relationships

The literature on privatization and the private market of force is consistent with the second type of relationship, known as State/non-State. This contains research on private military and security contractors, mercenaries, proxy conflicts, and proxy warfare. There are many instances of these connections: the conflict in Syria, which employs both domestic and external proxies, is one of the most notorious examples. Despite its comparatively recent development, the world of cyber power exhibits a comparable set of interactions. For instance, the head of research at Kaspersky Lab, said in an interview with Reuters in 2013 that "what we have here is the emergence of small groups of cyber-mercenaries available to perform targeted attacks (...) We actually believe they have contracts, and they are interested in fulfilling whatever the contract requirements are."[81]

Non-State/State Proxy Relationships

By emphasizing a non-State actor as the recipient or beneficiary, the third type of connection, non-State/State, departs from the traditional State-centric approach often seen in most assessments. This kind of relationship can be seen in numerous instances of States being invaded by organized crime groups and being used as a front. This kind of instance is provided in the literature on 'weak States' and organized crime. This relationship recognizes that a substantial percentage of previous scholarly work does not apply to nations where public institutions have been corrupted by certain individuals to further their own agendas. Indicating this situation, Atanas Atanasov, a former counterintelligence head and current lawmaker in Bulgaria, said, "Other countries have the mafia, but in Bulgaria, the mafia controls the country."[82]

Non-State/Non-State Proxy Relationships

The fourth relationship, illustrates the reality that proxy interactions do not always have to involve a State. For instance, Andrew Mumford, in his book addressing this topic,

[80] Maurer, Tim. Cyber mercenaries. Cambridge University Press, 2018.
[81] Menn, Joseph. "Hacker'mercenaries' linked to Japan, South Korea spying: researchers." Reuters, September 29 (2013).
[82] Naím, Moisés. "Mafia states: Organized crime takes office." Foreign Aff. 91 (2012): 100.

emphasized that proxy warfare is no longer exclusively a State-driven form of conflict. He pointed out that the proliferation of global al-Qaeda 'franchises' has significantly altered the manner in which regional conflicts can be influenced through the proxy engagement of these networked cells.[83]

Throughout the relatively brief history of cyberspace, instances of such cyber proxies have not been rare. For instance, hacker Robert Anderson disclosed to Wired in 2007 that he had been recruited by the Motion Picture Association of America to take part in website hacking as part of their attempts to battle pirated movies.[84]

It is significant to note that the streamlined structure shown in Figure 2 is not comprehensive of many elements such as intergovernmental actors, it does not take into account circumstances revolving around many beneficiaries and a single proxy, or vice-versa, or even instances when the affected third party or actor C may use a proxy to affect actor A, actor B, or perhaps another actor completely.

Three main types of proxy relationships

Once we have defined the actors involved and how they interact, we may now continue by analysing the degree of their connections. Proxy connections may be divided into three main categories: delegation, orchestration, and sanctioning.[85] Delegation describes situations where the recipient exercises significant control on the proxy. Orchestration refers to circumstances where proxies function with a degree of freedom but are nonetheless supported by the State without being given specific instructions. Lastly, circumstances where the State purposely ignores the conduct of non-State actors while creating the conditions for them to engage in harmful behaviours are known as sanctioning or passive support.[86]

Table 1: Three main types of proxy relationships

[83] Mumford, Andrew. Proxy warfare. John Wiley & Sons, 2013.
[84] Kravets, David. "Exclusive: I was a hacker for the MPAA." Wired Magazine (2007).
[85] Maurer, Tim. Cyber mercenaries. Cambridge University Press, 2018.
[86] Ibidem.

Type of proxy relationship		*Beneficiary (actor a)*	⟶	*Proxy (actor b)*	⟶	
Active	Delegation	Principal	⟶	Agent	⟶	Target
	Orchestration *"Blitz orchestration"*	Orchestrator	⟶	Intermediary	⟶	*(actor c)*
Passive	Sanctioning	Sanctioner	⟶	Sanctionee	⟶	

Source: Maurer, Tim. Cyber mercenaries. Cambridge University Press, 2018.

The concept presented by Maurer decides to include the phenomena of sanctioning by stating that offensive cyber acts carried out by proxies are enabled with the knowledge and assistance of a beneficiary. Using the phrase 'on behalf of' a State, however, suggests a more limited connection, comparable to contractual delegation in principal-agent theory or the 'effective control' level in international law. This constrained viewpoint leaves out the most difficult part of proxies: circumstances in which a State, despite obvious involvement in some capacity, either overlooks such activities or purposefully builds sufficient distance to avoid public responsibility.

To underline that the connection goes beyond the purview of delegation as defined in principle-agent models, Maurer uses the term 'beneficiary' instead of 'principal', as stated earlier.[87]

Delegation

A beneficiary may delegate authority to an agent to act on their behalf in a proxy relationship. In this principal-agent relationship, contracts are required to control the agent's behaviour.[88] In the ideal scenario, the agent would adhere to the beneficiary's orders precisely, but in reality, issues between their goals frequently result in undesired behaviour. It is difficult for the principle to entirely avert such divergent conduct because the principal may not have a complete understanding of the agent.

Furthermore, the number of beneficiaries engaged affects an agent's level of autonomy, with more beneficiaries providing the agent more flexibility. This structure

[87] Ibidem.
[88] Abbott, Kenneth W., et al., eds. International organizations as orchestrators. Cambridge University Press, 2015.

exposes the beneficiary to risks. Due to the agent's unpredictable actions, the beneficiary might need to provide more assistance and cover more expenses.

One of the 'agency problems' that might arise is the possibility that a government could create something that grows to be unmanageable. This is known as the 'Frankenstein problem', presented by the researcher Idean Salehyan.[89] Beyond extreme harm to other parties, this issue can also result in the agent rising up against the beneficiary. In order to avoid the danger of insurrection or desertion, Salehyan observes that leaders must achieve an extremely challenging equilibrium.[90] To reduce the likelihood of divergent conduct and expenses, beneficiaries frequently include constraint and control measures from the start of proxy relationships. Screening and selection, monitoring, and punitive measures are the three main tools beneficiaries employ to reduce the divergence of interests and conduct.[91]

Due to the difficulty that beneficiaries confront in not fully comprehending what their proxies' goals are, rigorous screening and selection are required. Mandatory audits, contractor reports, and the usage of 'fire alarms' given by outside parties that inform the beneficiary of unwanted activity by the agent are just a few of the techniques that may be used to monitor the acts of proxies.[92] A noteworthy fire alarm mechanism in the area of cybersecurity is the advent of private cyber threat intelligence organizations that publish reports on individual threat actors and their actions.[93] Compared to covert proxy connections designed to preserve plausible deniability, transparent and contractual proxy partnerships provide additional options for monitoring.[94]

Orchestration

Delegation is different from orchestration, which instead highlights the ideational side of the interaction while still recognizing the importance of rational interests.[95] Daniel

[89] Salehyan, Idean. "The delegation of war to rebel organizations." Journal of Conflict Resolution 54.3 (2010): 493-515.
[90] Ibidem.
[91] Ibidem.
[92] Byman, Daniel, and Sarah E. Kreps. "Agents of destruction? Applying principal-agent analysis to state-sponsored terrorism." International Studies Perspectives 11.1 (2010): 1-18.
[93] Ibidem.
[94] Ibidem.
[95] Abbott, Kenneth W., et al., eds. International organizations as orchestrators. Cambridge University Press, 2015.

Byman and Sarah Kreps noticed that the need for extra control mechanisms is frequently reduced by strong ideological bonds.[96]

Orchestration can provide a further method to achieve one's political objectives and engage target actors, as it entails recruiting intermediary players freely and giving them material and ideational assistance.[97] The relationship between the orchestrator and the middleman is also determined by their connected aims, claim Kenneth Abbott and his co-authors. They suggest that correlated objectives are necessary for orchestration to work.[98]

Therefore, finding connected goals, selecting suitable intermediates, tracking correlation across time, and planning for remedial action are all important steps in orchestration.[99] Delegation is the term used in international law to describe proxy connections that are above the level of effective control and are referred to as 'State-sponsored' in counterterrorism literature. Contrarily, orchestration includes a wide variety of operations that fall below this threshold, such as funding, the provision of weapons, the sharing of intelligence, and logistical assistance, which can nevertheless be regarded as 'State-supported'.[100]

Orchestration has in common with delegation the screening and monitoring process. Indeed, these are still used to minimize divergence and evaluate the proxy.

Sanctioning

The idea of passive support is the foundation of sanctioning, according to counterterrorism literature.[101] When a State deliberately decides to put up with a non-State actor's action while still having the power to step in, this is called passive support. No delegation or orchestration is necessary in these situations, but the State's decision to do nothing effectively turns the non-State actor into a proxy.[102]

---

[96] Byman, Daniel, and Sarah E. Kreps. "Agents of destruction? Applying principal-agent analysis to state-sponsored terrorism." International Studies Perspectives 11.1 (2010): 1-18.
[97] Abbott, Kenneth W., et al., eds. International organizations as orchestrators. Cambridge University Press, 2015.
[98] Ibidem.
[99] Ibidem.
[100] Byman, Daniel, and Sarah E. Kreps. "Agents of destruction? Applying principal-agent analysis to state-sponsored terrorism." International Studies Perspectives 11.1 (2010): 1-18.
[101] Maurer, Tim. Cyber mercenaries. Cambridge University Press, 2018.
[102] Ibidem.

Several reasons can lead a State to permit malevolent actions committed by a non-State actor from within its borders. First off, the non-State actor may have a lot of domestic support, which could result in consequences if the State took action against them. In reality, such domestic backing might also go beyond simple tolerance and lead to later official acceptance.[103]

Second, if a State does not see a non-State player as posing a direct danger, it may decide to tolerate them. For instance, in 1979, the Muslim Student Followers of the Imam's Line, a group of extremist Iranian students, supported the Islamic revolution and the newly elected government.[104] Therefore, they did not pose a threat to the government.

When inactivity has a low cyber operations or an indirect advantage, this is a third element that influences sanctions. Byman emphasizes that because passive support is less overt, it is frequently seen as more acceptable globally and has less diplomatic repercussions.[105] By remaining silent, a State may acquire domestic support or influence its enemy in ways that surpass any possible cyber threat incurred as a result of the adversary's objections. This low level of inaction applies in particular to cyber-attacks, which are non-physical in nature and manifest themselves after a long time.

Disparity between a State's anticipated capability or aspirational position and its real capabilities and power is a fourth element that might influence punishment. To put it another way, a State may try to portray itself as a regional or global force, suggesting that it has all the essential internal resources to intervene. However, in practice, its capability could be severely constrained. In such circumstances, a failed attempt to punish a non-State actor might reveal this disparity, causing the State shame.[106]

Regarding State accountability for private actors' conduct in particular, the phenomena of sanctioning has had an influence on the core concepts of agency under pre-existing international law. This impact is highlighted by Tal Becker, who claims that:

"When President Bush declared, on the evening of September 11th, that the United States would "make no distinction between the terrorists who committed the attacks and

[103] Ibidem.
[104] Mahdi, Ali Akbar. "The student movement in the Islamic Republic of Iran." Journal of Iranian Research and Analysis 15.2 (1999): 5-32.
[105] Byman, Daniel. "Passive sponsors of terrorism." Survival 47.4 (2005): 117-144.
[106] Maurer, Tim. Cyber mercenaries. Cambridge University Press, 2018.

those who harbor them" he made no claim that State responsibility was grounded in an agency relationship. The Taliban was held directly responsible for the September 11th attacks because it 'allowed' Al-Qaeda to operate, not because it directed or controlled their activities. And yet, the overwhelming number of nations that appeared to endorse this policy, and to support the targeting of both the Taliban regime and Al-Qaeda – seemed remarkably unconcerned by this departure from agency standards."[107]

The importance of due diligence as a subject of discussion among the 2016–2017 United Nations Group of Governmental Experts (UN GGE) members is highlighted by its controversial character.[108] This discussion centres around the possible dangers of overstretching the idea of State responsibility, particularly in terms of efficiently balancing legal and political duties in proportion to a State's actual implementation capabilities.

Conclusion

In conclusion, the potential role of cyberspace as the next battlefield remains a subject of ongoing debate. While some argue that cyberspace should be recognized as the 'fifth dimension of conflictuality,' others, like Thomas Rid, view cyberattacks as advanced forms of espionage, subversion, and sabotage, suggesting that not all cyberattacks should be categorized as acts of war.

Nevertheless, there are contrasting arguments in favor of the idea that cyberspace constitutes a novel arena for conflict. These arguments call for a broader definition of warfare that includes cyber activities, emphasizing the ability of even minor cyberforce to coerce adversaries and achieve strategic paralysis without resorting to physical assault. Despite the ongoing dispute, several developments underscore the growing recognition of the significance of cybersecurity in contemporary combat.

Significant shifts in national and global security postures are evident, such as the establishment of organizations like the U.S. Cyber Command, the acknowledgment of cybersecurity's importance by the Russian military in military conflicts, and the emphasis placed on effective cyber defense in the 2016 Warsaw Summit Communiqué. These

[107] Becker, Tal. Terrorism and the state: rethinking the rules of state responsibility. Bloomsbury Publishing, 2006.
[108] Schmitt, Michael N. "In defense of due diligence in cyberspace." Yale LJF 125 (2015): 68.

developments highlight the necessity for collective defense in the current operational environment of cyberspace.

In light of these arguments and advancements, this thesis contends that, despite the ongoing debate, cyberspace has indeed become the new theater of warfare. Given the evolving nature of military operations in cyberspace, there is an increasing need to establish international standards and legislation to effectively regulate cyberwarfare and safeguard national security against evolving cyber threats.

In summary, this thesis posits that governments employ non-state actors, often referred to as proxies, in various ways to assert authority in cyberspace. These proxies function as intermediaries, carrying out tasks on behalf of the government. Three types of interactions between governments and proxies are identified: delegation, orchestration, and sanctioning. Delegation involves granting the proxy authority, while orchestration entails working with like-minded middlemen. Sanctioning occurs when a state allows a non-state actor to act without direct permission. These proxy relationships offer advantages such as plausible deniability and the ability to exert force below the threshold of conventional military power.

Proxy actors engage in offensive cyber operations that target systems not owned or operated by the actor in cyberspace. Analyzing the role of proxies and their impact on cybersecurity necessitates a comprehensive understanding of the dynamics of these relationships. Consequently, governments delegate responsibilities, plan operations, and sanction or support the actions of non-state actors as a means of projecting power in the realm of cyberspace.

Chapter 2: The applicability of international norms to international relations regulation in cyberspace

Cybersecurity hazards are pervasive in all areas of technology and can have a significant negative impact on society. It is essential that nation-States, corporations, and customers everywhere give cybersecurity top priority on a global level. States and stakeholders are increasingly adopting norms as the preferred policy instrument for guaranteeing the security of information and communications technologies (ICTs) and cyberspace in general as conversations on how and when to secure it are in progress. Should the constraint on governments and non-governmental organizations (NGOs) to use technology to undermine crucial democratic infrastructures be enshrined into law? Can international bodies and a variety of stakeholders come to a consensus that such conduct should be forbidden? A normative agreement that defines a cybersecurity standard appropriate for the digital era may be observed in such a consensus on the use and behaviour of ICTs, cybersecurity, and cyberspace. The adoption of such a rule is the first stage in a long process of increasing security.[109]

According to Peter Katzenstein, norms set expectations for actors' behaviour within a certain setting.[110] In its broadest sense, a norm is a precept that unites group members and governs their behaviour, acting as a standard for deciding what is suitable and acceptable.[111] In political science and international relations, the study of norms aims to comprehend how individual moral convictions might influence societal norms and expectations.[112]

The noticeable lack of normative conduct in the fields of cybersecurity, cyberspace, and ICTs is a major concern for States and other actors internationally. Because there are so few rules, people lose trust in digital processes, which leads to more and more limitations in the digital space over time. The robustness and balance of the global order is

[109] Finnemore, Martha, and Duncan B. Hollis. "Constructing norms for global cybersecurity." American Journal of International Law 110.3 (2016): 425-479.
[110] Katzenstein, Peter J., ed. The culture of national security: Norms and identity in world politics. Columbia University Press, 1996.
[111] Merriam-Webster, Merriam-Webster: Definition of 'Norm', https://www.merriam-webster.com/dictionary/norm , 2021.
[112] Risse, Thomas, and Kathryn Sikkink. "The socialization of international human rights norms into domestic practices: introduction." Cambridge Studies in International Relations 66 (1999): 1-38.

weakened as a result. Consequently, the need to develop 'cyber norms' to control and improve the security of cyberspace is growing.

In 2018, UN Secretary General António Guterres, for instance, underlined the need for international norms to lessen the harm that electronic warfare does to civilians, confirming that in his opinion cyberspace is indeed a new field of warfare.[113] Leaders have continuously urged for the regulation of cyberspace over the years. The creation of such norms, however, confronts several obstacles.

Existing norms from a wide variety of fields, such as national laws, international laws, professional standards, political agreements, and technological protocols, are already present in cyberspace. These normative frameworks are at various phases of development and distribution and entail significant commitments. Many of these endeavors, nevertheless, have turned out to be fruitless. Therefore, this chapter aims to explore the obstacles that impeded the establishment of normative international regulations in cyberspace and attempt to set the theoretical foundations needed to answer the first research question: (I). What are the normative foundations of the cyber proxy wars regulations? And later to answer the second (II). Are these norms internalized?

Before understanding at which state of normative regulation are cyber proxy wars we must understand norms and their processes. We will start this chapter by delineating cybersecurity norm types. Then we will see how Finnemore & Sikkink's constructivist theory on the 'Norm Life Cycle'[114] applies in cyberspace, and lastly, we will talk about the constraints on nation States.

The typology of international norm and norm's life cycle theory applicability in cyberspace

In contrast to the concept of cybersecurity, the concept of a norm is well-established and explicitly defined in the domains of sociology and political science. Norms are defined as the "collective expectations for the proper behaviour of actors with a given

[113] Khalip, Andrei. "UN chief urges global rules for cyber warfare." Reuters, February 19 (2018).
[114] Finnemore, Martha, and Kathryn Sikkink. "International norm dynamics and political change." International organization 52.4 (1998): 887-917.

identity", according to Katzenstein's commonly used definition. [115] The four key components of this concept are community expectations, behaviour, identity, and propriety.

Identity refers to the particular group to whom a standard is applicable. Nation-States are the most notable illustration. The UN Group of Governmental Experts (GGE) and Shanghai Cooperation Organization's explain that norms are meant for all nations, however there may be more exclusive groupings of governments that unite behind certain standards. Regional organizations like the European Union, which created the Directive on Data Protection as a normative framework, is an example of such groups.[116]

As seen in the cybersecurity guidelines established for members of the Organization for Security and Cooperation in Europe (OSCE)[117] or the North Atlantic Treaty Organization (NATO)[118], groups may also include 'like-minded' and regional governments. Even bilateral interactions between certain nations might lead to the emergence of norms. It is vital to remember that cyber rules might apply to a variety of identities other than those of governments. Even victims of cyberattacks, for instance, might create a group or 'identity' to create cyber norms that mandate certain activities.[119]

Behaviour, instead, describes the particular acts that are required by social standards. While some norms clearly forbid certain behaviours, such as regulative norms. Others dictate what acts should be done, such as constitutive norms. The emergence of 'systems administrators' and the creation of organizations like the Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Assigned Numbers Authority (IANA) are examples of how constitutive norms have the potential to create new actors and institutions.[120] Both regulative and constitutive norms' behavioural aspects might differ in their level of specificity.

---

[115] Katzenstein, Peter J., ed. The culture of national security: Norms and identity in world politics. Columbia University Press, 1996.
[116] Finnemore, Martha, and Duncan B. Hollis. "Constructing norms for global cybersecurity." American Journal of International Law 110.3 (2016): 425-479.
[117] Cyber/ICT Security. OSCE. https://www.osce.org/cyber-ict-security
[118] North Atlantic Treaty Organization, Cyber Defence, 2016, at http://www.nato.int/cps/en/natohq/ topics_78170.htm.
[119] Finnemore, Martha, and Duncan B. Hollis. "Constructing norms for global cybersecurity." American Journal of International Law 110.3 (2016): 425-479.
[120] Ibidem.

Propriety is the standard by which social standards judge whether a conduct is appropriate or inappropriate. The appropriateness of norms may be attributed to a number of sources, most notably the law but not less important are politics, culture, professional standards, and religion. Promoting "voluntary, nonbinding" standards as an alternative to legislation, together with the creation of a comprehensive international cybersecurity treaty have received the majority of attention in talks on cyber norms.[121] Law and norms, however, are notions that are linked and do not conflict. Therefore, to provide a foundation for appropriateness, those participating in law making or treaty discussions might turn to norms as a useful tool. A treaty is a favoured instrument because it has a lengthy history of legitimacy and stability, which raises the credibility of the expectations it sets. Law, which is closely tied to numerous standards, thus plays a clear role in defining appropriate and inappropriate behaviour in cyberspace. Many cyber-norms, however, rely on grounds other than the law for their appropriateness. Political agreements among nation States may serve as the basis for cyber-norms, such as the Parliamentary Declaration & Resolution on Cybersecurity of the OSCE.[122]

Cyber-norms' appropriateness, or the intrinsic moral or ethical worth of their normative assertions, can come from sources other than those of law and politics, the most notable example is from culture. Multiple varied cultures intertwine in cyberspace, giving birth to a wide variety of normative assertions.[123] The social and intersubjective aspect of norms is referred to as collective expectations. Rather than being unilateral orders, norms are common understandings about proper conduct held by members of a certain community. Norms are what social scientists refer to as "social constructions", existing solely because of our collective belief in their existence.[124] Additionally, norms have the power to create or form new social phenomena, agents, and organizational systems. Their

[121] Assembly, UN General. "Developments in the field of information and telecommunications in the context of international security." United Nations General Assembly. Search in (2015).
[122] OSCE, PA. "Istanbul Declaration and Resolutions Adopted by the OSCE Parliamentary Assembly at the Twenty-Second Annual Session." (2013).
[123] Finnemore, Martha, and Kathryn Sikkink. "International norm dynamics and political change." International organization 52.4 (1998): 887-917.
[124] Wendt, Alexander. "Anarchy is what states make of it: the social construction of power politics." International organization 46.2 (1992): 391-425.

degree of internalization can vary, and they might get their normative power or validity from a variety of cultures and situations, including but not limited to the law.[125]

The cybersecurity environment includes a variety of settings, and efforts to create new cyber-norms must take this normative heterogeneity into consideration. However, in order for such initiatives to be successful, it is essential to comprehend the mechanisms through which norms form and influence behaviour.

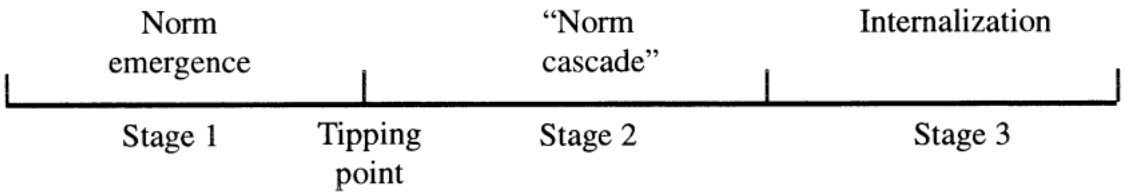
Next, we shall expand on the definition of 'norms' that was provided above. We will achieve this by drawing on significant work from the field of international relations (IR), particularly from the diverse perspectives known as 'normative IR theory' and 'constructivism'.

Because one of the main areas of norm research is the influence of norms on State conduct, it is essential to operationalize a standard in a way that is distinct from the behaviour of States or non-State actors it aims to explain. The 'life cycle' of norms is the term used by constructivist researchers Finnemore and Sikkink to provide a method for understanding the dynamics of this process.[126] They show how the level of agreement on a developing norm across a large number of players may increase to the point where it becomes widely accepted across many empirical examples. Furthermore, the authors highlight two elements that are necessary for the successful creation of a norm: 'norm entrepreneurs' and their organizational platforms.[127]

Finnemore and Sikkink use a three-stage process model to illustrate norm influence as shown in Figure 3. The authors argue that change at each stage is characterized by different actors, motives, and mechanisms of influence.[128]

Figure 3. The lifecycle of norms

[125] Finnemore, Martha, and Kathryn Sikkink. "International norm dynamics and political change." International organization 52.4 (1998): 887-917.
[126] Ibidem.
[127] Ibidem.
[128] Ibidem.



Source: Martha Finnemore and Kathryn Sikkink. *International norm dynamics and political change*. International organization 52.4 (1998): p. 896.

'Norm emergence,' the first step of the norm life cycle, is the formulation and subsequent debate of the normative behaviour. By convincing a significant number of nations, often referred to as norm leaders, to embrace these new standards, norm entrepreneurs play an important role in this stage.[129] They want to persuade and win over these powerful individuals.

'Norm cascade,' the second step, is when the norm becomes broadly accepted by all pertinent players or actors.[130] In this phase, individuals adopt the norm and follow suit, frequently motivated by an imitation dynamic. The goal of norm leaders is to actively influence other governments to adopt the norm. Although the driving forces behind this cascading impact may vary, we contend that a number of elements, including conformity, demands, the pursuit of international legitimacy, and State leaders' desires to boost their self-esteem, all play an important role.[131]

The last phase of the norm life cycle is 'norm internalization,' during which the norm is well internalized and no longer open to extensive public discussion. At this point, the norm is seen as 'taken for granted' and is acknowledged as the acceptable manner of acting.[132]

There is a critical stage in the norm life cycle known as the 'tipping point,' which is positioned between the first and second stage. The passage from a theoretical norm to a conceptualized and accepted norm, which opens the door for the internalization and adoption process, occurs at this tipping point.[133] While it is important to look at each step of the norm life cycle since they all help norms evolve and spread and may even lead to

[129] Ibidem.
[130] Ibidem.
[131] Ibidem.
[132] Ibidem.
[133] Ibidem.

their integration into legal frameworks in the future, this stage is crucial for the development of norms.

The starting stage, known as 'emergence,' is where there is the most uncertainty, the authors note.[134] The question of whether the general public and pertinent stakeholders would view the norm as substantial enough to support and act upon it is raised when the standard is first proposed and discussed. Nevertheless, it is critical to recognize that at any stage of their development, norms are susceptible to difficulties and failure.

As Finnemore and Sikkink contend, international relations' norms are not only drawn from theoretical frameworks, but they also need to be introduced and promoted by individuals or organizations in order to be kept current.[135] These actors or organizations, referred to as 'norm entrepreneurs', are extremely important in influencing the conversation surrounding norms. They persuade other actors to adhere to particular standards or groups of norms through a variety of persuasive techniques. Norm entrepreneurs are viewed in this perspective as 'norm protagonists' who use language to describe, interpret, and dramatize issues in order to call attention to them and sometimes even to create new issues entirely.[136] According to social movement theorists, this process is called 'framing' and it entails reinterpreting or renaming current situations in order to develop new views of appropriateness and interest.[137] However, these rising new norms and frames must compete with already existing norms and frames in order to gain legitimacy and this is no easy task. Norm entrepreneurs may occasionally need to purposefully act in ways that defy accepted standards in order to question and alter dominant ideas of appropriateness. The understanding of how a 'logic of appropriateness' relates to norms becomes clearer through the contestation of those norms.[138]

Yet, why are norms entrepreneurs committed to help a new norm emerge? Without taking into account elements like empathy, altruism, and ideational commitment, it might be challenging to understand the motives that are behind a typical norm entrepreneur (see Table 2). Depending on the particular norm and entrepreneur involved, these motives

[134] Ibidem.
[135] Ibidem.
[136] Ibidem.
[137] Snow, David A., et al. "Frame alignment processes, micromobilization, and movement participation." American sociological review (1986): 464-481.
[138] Olsen, Johan P., and James G. March. The logic of appropriateness. No. 9. ARENA, 2004.

change. When actors are able to comprehend and relate to the thoughts and feelings of others, empathy becomes important. Even when it doesn't immediately contribute to their own security or monetary well-being, this sympathetic interdependence encourages genuine care for the welfare of others.[139] Contrarily, altruism entails acting in a way that benefits others regardless of the danger to one's own safety.[140] The core of compassion, according to Kristen Monroe, is to recognize and acknowledge our shared humanity and the claim to certain rights based on this similarity.[141] Last but not least, regardless of whether their pursuit of these standards has a direct influence on their personal well-being, entrepreneurs who really believe in the principles and values represented by the norms they advocate are motivated by ideational commitment (see Table 2).

Table 2. Stages and Motivations of norms

	Stage 1 *Norm emergence*	*Stage 2* *Norm cascade*	*Stage 3* *Internalization*
Actors	Norm entrepreneurs with organizational platforms	States, international organizations, networks	Law, professions, bureaucracy
Motives	Altruism, empathy, ideational, commitment	Legitimacy, reputation, esteem	Conformity
Dominant mechanisms	Persuasion	Socialization, institutionalization, demonstration	Habit, institutionalization

Source: Martha Finnemore and Kathryn Sikkink. *International norm dynamics and political change*. International organization 52.4 (1998), p.898.

To advocate for their standards, all proponents of international norms need an organizational platform. Some NGOs, such as Greenpeace and the Red Cross have built platforms particularly for supporting a given standard. These NGOs frequently join broader

[139] Keohane, Robert O. "After hegemony: transatlantic economic relations in the next decade." The International Spectator 19.1 (1984): 3-9.
[140] Monroe, Kristen Renwick. "Explicating altruism." (2002).
[141] Ibidem.

international advocacy networks that concentrate on human rights, environmental standards, or the banning of land mines.[142]

Norm entrepreneurs do, however, also work inside established international organizations with objectives and agendas that go beyond simply advancing a particular norm.[143] The goals of these groups can greatly influence the content of the standards they support. The capacity of contemporary organizations, particularly multinational ones, to use knowledge and information to affect the actions of other players is a significant aspect in their impact. Empirical studies have demonstrated how the professional training of bureaucrats within these organizations may either help or hinder the propagation of new norms within the organization. This expertise is often found among professionals within these organizations.[144]

Regardless of the platform they choose, norm entrepreneurs and the organizations they work for frequently need the help of State actors to advance their agendas and obtain acceptance for their norms. Entrepreneurs can accomplish this aim using a variety of organizational platforms' tools and strategies.[145]

According to Sandholtz, the normative context of a given historical period has a significant impact on the first stage of the norm life cycle.[146] Indeed, we will see in our analysis of the case studies that most of the international decisions regarding cyber-norms have been influenced by the historical context in which they took place. At this stage, important players make judgments based on their prior experiences and relations, which impact how they see the larger community and its expectations for enforcing new laws. In essence, the choice to spread a new standard among more people frequently depends on precedent. People who are active in the spread of norms could be reluctant to lead the development of new norms if prior norms encountered opposition in a society that is resistant to change.

---

[142] Finnemore, Martha, and Kathryn Sikkink. "International norm dynamics and political change." International organization 52.4 (1998)
[143] Ibidem.
[144] Ibidem.
[145] Ibidem.
[146] Sandholtz, Wayne. Prohibiting plunder: how norms change. Oxford University Press, 2007.

The link between social norms and laws is complex, even though it is frequently considered a sign of a norm's success when it becomes a law.[147] Strong social norms are known to ease the load on law enforcement, and laws that are supported by social norms are more likely to be upheld by the government.[148] This issue is further complicated by the growing reliance of the physical world on cyberspace and ICTs. The essential infrastructure of the globe depends more and more on cyberspace and ICTs as a result of technological advancements, an increase in Internet users brought on by globalization and incidents like the COVID-19 epidemic, and other factors. The rules and processes regulating both spheres must be more closely integrated as a result of their interconnectedness.

Political issues of the normative regulation

After having introduced the definition of 'norm' and the constructivist theory of lifecycle of norms, we will now delve into the soft power constraints to the normative regulation of cyberspace. As we have seen, in order for a norm to become internalized it must go through 3 phases. We will introduce and analyse some soft power tools that operate as obstacles towards the implementation of norms in cyberspace during said phases.

Why do sovereign governments occasionally allow normative factors to constrain their behaviour? There are several causes, but the most obvious and frequently cited one is the beneficial coordination results that follow from abiding by common legal, normative, and ethical norms. For instance, there has been ardent debate regarding the Internet Corporation for Assigned Names and Numbers (ICANN). The US Department of Commerce began a contract with ICANN, a private non-profit organisation. This was established at the government's request with the goal of privatizing the Domain Name System (DNS), the addressing system that underpins the Internet. Outside of the US, domain name registrars are questioning the unfairness of the ICANN procedure for authorizing new domains, stating they want the option to leave ICANN and create their own networks. Nevertheless, nations have avoided making substantial changes to the DNS and have prioritized a consistent and agreed-upon system for domain name allocation and

[147] Etzioni, Amitai. "Social norms: Internalization, persuasion, and history." Law and society review (2000): 157-178.
[148] Ibidem.

management, recognizing that normative factors in governing the DNS helps facilitate a cohesive global digital landscape.[149]

Additionally, the recent expansion of cybersecurity norms and standards has been made possible by the market for cyber insurance expanding quickly and the development of accounting standards. This is an illustration of how private organizations may assist governments in creating standards to coordinate the behaviour of international corporations.[150]

Coordination games, however, only cover a small subset of State behaviour. We will now look at three variables that might influence a government's position to normative restrictions on how they should behave in cyberspace. (1) To start, there is the aspect of prudence and caution against uncertain outcomes. (2) A second normative restriction is related with reputational consequences. (3) Thirdly, as standards are internalized by a State, domestic political pressure may also develop.

1. Prudence and caution against uncertainty

Certain standards and actions have been significantly shaped by prudence and caution against negative outcomes. In order to better understand how these could apply to cyber-norms, we will use examples such as the fight for regulating nuclear weapons during the last century. Tactical nuclear weapons were adopted by the US military's deployed forces after Hiroshima because they were largely seen as appropriate. However, President Dwight Eisenhower rejected the idea made by the Chairman of the Joint Chiefs of Staff in 1954 and 1955 to deploy nuclear bombs to defend Dien Bien Phu in Vietnam and offshore islands near Taiwan, in part because he was worried about unforeseen consequences.[151] The decision-making cyber operations connected with using nuclear bombs rose as this cautious approach finally became the norm. Thomas Schelling claims that one of the most important developments in weapons control over the past 70 years has been the creation of this standard.[152]

---

[149] Fuller, Kathleen E. "ICANN: The debate over governing the internet." Duke L. & Tech. Rev. 1 (2001): 1.
[150] Herr, Trey. "Cyber insurance and private governance: The enforcement power of markets." Regulation & Governance 15.1 (2021): 98-114.
[151] Nye Jr, Joseph S. "Deterrence and dissuasion in cyberspace." International security 41.3 (2016).
[152] Schelling, Thomas C. "An astonishing 60 years: The legacy of Hiroshima." Proceedings of the National Academy of Sciences 103.16 (2006): 6089-6093.

In cyberspace, attacks against crucial systems like the DNS or the IANA may be constrained out of concern about endangering the financial gains received from the Internet. Additionally, caution and self-control may evolve into norms of non-use, limited usage, or limited targeting due to the relatively new development of cyber warfare and the unpredictable nature of its effects. Furthermore, inactivity fuelled by self-interest and uncertainty might emerge and finally establish itself as the norm.

The policy that outlawed privateering in the 19th century serves as a powerful illustration of the evolution of norms, with implications for cyber security and the problem of private 'hack-back.' According to Egloff, this transformation is a result of State-sanctioned and State-tolerated non-State violence's unintended repercussions.[153] As governments struggled to manage privateers and saw the damaging effects they had on the economy, attitudes changed and new norms arose. The long-term development of security dynamics in a certain area becomes more significant over time for stakeholders. The ecology of security actors develops rather than undergoing quick change. Over time, policy decisions are influenced by unintended repercussions, feedback loops, and conflicting agendas. Furthermore, as the importance of the domain develops for all engaged parties, the stakes rise, generating incentives for stability. According to Maurer and other researchers, caution and new rules may continue to emerge if the unintended effects of State dependence on internet become more obvious and expensive.[154] Different nations may see private proxies differently and may have different control arrangements with them, but as a result of unexpected consequences and an increase in reliance on cyberspace, caution may eventually lead to the development of new norms and an evolution of prudence.[155]

2. Reputational cyber operations

After World War I, the restricted employment of some weapons was mostly due to external reputational harm. This is clear from the 1925 Geneva Protocol's ban on the

[153] Egloff, F. J. "Cybersecurity and the age of privateering: A historical analogy." (2015).
[154] Tim Maurer, "Cyber mercenaries", Cambridge University Press, (2018).
[155] Ibidem.

possession and use of chemical and biological weapons.[156] The negative connotations associated with these weapons led to a cyber operation to a nation's soft power that pertained to both their use and even simple ownership. Such taboos, however, did not totally stop nations like the Soviet Union and other non-State entities from owning and developing biological weapons, mostly because of insufficient verification mechanisms. Moreover, the benefits of breaching the taboo were often seen as outweighing the drawbacks.

However, these standards did have an influence on how people saw the cyber operations and advantages of certain acts, such as the dismantling of the majority of Syria's chemical weapons in 2014 or the bombing in 2017 that specifically targeted Syrian chemical weapons.[157] The Biological Warfare Convention has been adopted by 185 governments, therefore nations looking to develop biological weapons must do it clandestinely and illegally at the risk of receiving strong international censure if proof of their actions were to be made public.[158] Therefore, since norms have been created to discourage their dissemination, external reputational harm and unclear rewards play a vital role in restricting the acquisition of such weapons.

Conventional taboos could still be applicable in the arena of online activities even though it is not as simple as the possession of conventional arms. Unlike other areas, the cyber realm is not universally perceived as being dangerous, and some even admire it as a tool for ‘bloodless war.’ Whether a computer program is used for malicious purposes is determined mainly upon the intent of the user, therefore it can be challenging to prohibit the development, acquisition, or even installation of certain computer programs for espionage. As a result, it is difficult for cyber weapons control to imitate the Cold War-era nuclear armaments control systems. Contrary to nuclear weapons, it is difficult to consistently ban the possession of a particular kind of cyber weapon.

Focusing on the targets of cybercrime, while leveraging the current and well-established international legal framework, is a more practical approach to normative

[156] United Nations, Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or other Gases, and of Bacteriological Methods of Warfare, 17 June 1925, available at: https://www.refworld.org/docid/4a54bc07d.html

[157] Timeline of Syrian Chemical Weapons Activity, 2012-2022 | Arms Control Association. (n.d.). https://www.armscontrol.org/factsheets/Timeline-of-Syrian-Chemical-Weapons-Activity

[158] Alexander, K. (n.d.). UNODA Treaties. https://treaties.unoda.org/t/bwc

regulations in cyber weaponry. The idea that purposeful assaults on civilians employing cyber weapons are prohibited by the standards of discrimination and proportionality, as included in the widely accepted LOAC, has been promoted by the United States. The 2015 UN GGE report[159] supported confidence-building measures like commitments to offer forensic assistance and non-interference with the activities of computer security incident response teams (CSIRTs), and it endorsed this strategy for norms in cyber arms control.

The 2015 report focused on the necessity for caution in strikes on specified civilian targets rather than the outright prohibition of certain lines of code by drawing on the established international rules of LOAC.[160]

From Russia's perspective, the activities of American government-funded organizations like the National Endowment for Democracy, which worked to oppose authoritarian practices in Ukraine or Russia, differed in degree rather than kind from that of their cyber activities, which used botnets to manipulate social media and sow discord in the American political system. Following the 2016 presidential election, it became clear that Russia had to bear significant political and reputational consequences as a result of its cyberattacks. Three Russian firms and 13 people were indicted on criminal charges by a special prosecutor, and because of the unexpected repercussions of its activities, relations between Russia and the United States remained strained. However, it is doubtful that these unintended effects will encourage caution without a stronger response from the United States.[161]

Given the divergent viewpoints on the degree or kind of cyberattacks, it is doubtful if future negotiations in this area may result in an agreement on mutual restriction. However, it is evident that the broad strokes provided in the 2015 UN GGE report did adequately not address the issue at hand.

---

[159] United Nations Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", A/70/174, July 22, 2015.

[160] Ibidem.

[161] Nye, Joseph S. "Normative restraints on cyber conflict." Cyber Security: A Peer-Reviewed Journal 1.4 (2018): 331-342.

Contrarily, China and the United States adopted a new norm in 2015 that aims to restrict their disputes over cyber espionage. It is significant to highlight that espionage between States is a long-standing activity and is not prohibited under international law.

The Obama administration's response to Chinese economic espionage, both in rhetoric and action, is a good example of the US' entrepreneurial endeavours as norm entrepreneur. Indicting officials and signing an executive order authorizing the US to place severe financial limitations on people or businesses who engage in or profit from cyber-enabled economic espionage are two examples of how the US has taken punitive steps in favour of this emerging norm. [162]

The use of rhetoric has also been a strong tool in the norm-building process by the US. President Obama has called intellectual property and State secret theft an "act of aggression" and a "core national security danger," and China has been publicly recognized and condemned.[163]

At first, China had rejected the American efforts. However, it changed its position and accepted the new standard during the summit conference in September 2015. Through bilateral agreements, this standard was subsequently expanded to include a number of other nations. Generally speaking, the process of multilateralizing standards is extremely important in raising the reputational cyber operations related to engaging in bad behaviour.[164]

3. Domestic political pressure

Domestic politics are a further issue that can persuade leaders to accept normative restrictions on their actions on the outside. As mentioned in previously, norms can reach tipping points, resulting in cascades of acceptance and internalization, when the conduct of a significant number of actors within a group becomes important to their identity as members of that group. This then translates into ideas that have political repercussions at

[162] Libicki, Martin. "The coming of cyber espionage norms." 2017 9th International Conference on Cyber Conflict (CyCon). IEEE, 2017.
[163] Lee, Malcolm R. "Will the United States impose cyber sanctions on China?.", 2015.
[164] Burke, Evan. "The Obama-Xi Summit and the prospects for a global norm against commercial IP theft." Carnegie Endowment for International Peace. June 14 (2021): 2021.

home, discouraging leaders from doing specific external measures.[165] Such norms might have their roots in the development of home social attitudes or be imported from other sources. Examples of both situations may be found in the historical evolution of standards surrounding the abolition of the slave trade in the 19th century or the advancement of human rights in the second half of the 20th century. After World War II, many States felt obligated to support the Universal Declaration of Human Rights as a result of the leadership of the Western victorious nations and their Latin American allies. As a result, these regimes felt limited by American pressure and worried about their soft power reputations. However, it is also clear that the influence of standards that have been absorbed by their domestic public opinion places restrictions on certain governments.[166]

States' internalization of standards can also be influenced by domestic political and economic factors. Companies may put pressure on governments to create uniform standards and norms in these areas since they suffer from the negative effects of conflicting privacy and data localization regulations. Similar to how the cyber insurance sector is rapidly growing, this might lead to internal demands for standards and norms to be established, particularly with regard to industrial processors and supervisory control systems incorporated into the growing number of networked devices. The practice of ‘build quickly and patch later’ may eventually be replaced by standards and regulations that place a higher priority on security.

The UN GGE is one of the major advocates of norms when it comes to normative restrictions on cyber tools, and together with the First Committee of the United Nations General Assembly, it could continue to do so in the future. The public's participation and general antipathy to these issues, however, can lag behind. Furthermore, there is no firm estimate of the length of this hypothetical cycle, and there is no assurance that one will ever occur. For instance, regression is undoubtedly a possibility if general relations between States worsen. However, if we go farther out than the next ten years, domestic pressure for normative restrictions may rise.

---

[165] Finnemore, Martha, and Kathryn Sikkink. "International norm dynamics and political change." International organization 52.4 (1998): pp. 887-917.

[166] Simmons, Beth A. Mobilizing for human rights: international law in domestic politics. Cambridge University Press, 2009.

The evolution of proxy norms: from the Cold War to the Cyber age

In the transition from the post-Cold War era to the cyber age, the evolution of norms concerning proxy warfare has followed a trajectory guided by Martha Finnemore's theory of norm lifecycles.[167] Initially, during the Cold War, norms emerged that accepted proxy wars as instrumental tools for superpowers to compete indirectly while avoiding direct nuclear confrontation. These proxy conflicts played a pivotal role in the concept of nuclear deterrence, allowing the United States and the Soviet Union to engage in strategic rivalry through conflicts such as the Vietnam War, where they backed opposing sides.[168] These norms surrounding proxy wars provided a framework for the two superpowers to maneuver within the boundaries of nuclear-armed stalemate.

However, the collapse of the Soviet Union in the early 1990s marked a significant turning point in the evolution of norms related to proxy warfare. With the demise of the bipolar world order, a unipolar system emerged, with the United States as the predominant global power. This shift in power dynamics led to a re-evaluation of proxy wars and their utility. The appeal of proxy wars persisted for global powers, but for different reasons. Firstly, they offered a means to avoid direct confrontation with other major nuclear-armed states, thereby reducing the risk of nuclear escalation. Secondly, proxy wars allowed powerful states to protect their interests and exert influence in strategically important regions without incurring the high costs, both human and economic, associated with direct military interventions.[169]

Out of the context of the Cold War, however, proxy wars became more complex and controversial to define. In the absence of a clear bipolar rivalry, the definition of what constituted a "proxy war" became a subject of debate. Two contrasting definitions emerged: one that emphasized the direct and equal involvement of two major powers supporting opposite sides, and another that encompassed any conflict in which outside states were involved due to vested interests. The choice between these definitions could significantly impact the analysis of a conflict, leading to disputes over whether certain conflicts, such as the Syrian Civil War, qualified as proxy wars.

---

[167] Finnemore, Martha, and Kathryn Sikkink. "International norm dynamics and political change." International organization 52.4 (1998)

[168] Rondeaux, Candace, and David Sterman. "Twenty-first century proxy warfare: confronting strategic innovation in a multipolar world." New America (2019).

[169] Ibidem.

For the purpose of this analysis, proxy wars are defined broadly as conflicts in which external states become involved due to their vested interests, irrespective of whether they are major global powers or regional actors. This definition allows for a more inclusive understanding of contemporary proxy conflicts.

The evolution of norms surrounding proxy warfare is closely linked to changes in the ideological justifications for intervention.[170] During the Cold War, proxy wars were often framed within the context of competing ideologies, primarily communism and democracy. However, in the post-Cold War era, conflicts began to develop based on new ideological premises and interests. For instance, the United States' involvement in the civil war in Somalia was justified on the grounds of humanitarian intervention, marking a departure from the ideological struggles of the past.[171] This shift demonstrated the adaptability of norms as they evolved to accommodate changing justifications for international involvement.

Despite evolving norms, a significant challenge emerged in the form of imbalanced benefits derived from proxy warfare. Major powers reaped financial and political advantages from proxy conflicts, but the countries where these conflicts played out often bore the brunt of the suffering. This imbalance of benefits contributed to the prolonged nature of proxy wars, both during the Cold War and in the years that followed. Conflicts like the Syrian Civil War, the Darfur conflict, and the Yemeni Crisis have persisted for years, marked by fluctuating international interventions.[172]

The protracted nature of proxy wars often serves as a strategic choice, creating a kind of stalemate that forces the adversary to reconsider its strategy. However, the involvement of external parties prolongs conflicts and makes definitive victory elusive. This dynamic harkens back to the intractable nature of Cold War-era conflicts like the Vietnam War, highlighting the enduring challenges of third-party involvement.

The evolving landscape of proxy wars has also been shaped by the emergence of new actors, including non-state actors and rising global powers like China. The United

---

[170] Giberson, J. (2019, January 13). The realities of proxy wars in the post Cold War Era – McGill Journal of Political Studies. https://mjps.ssmu.ca/2019/01/13/realities-proxy-wars-post-cold-war-era/
[171] Ibidem.
[172] Rondeaux, Candace, and David Sterman. "Twenty-first century proxy warfare: confronting strategic innovation in a multipolar world." New America (2019).

States' "War on Terror" exemplifies its willingness to employ proxy warfare to protect its interests and combat terrorist organizations.[173] Non-state actors, such as terrorist groups, pose unique challenges as they operate across borders, making them difficult to combat. In response, major powers, including the United States, have engaged in various proxy conflicts across regions, employing local proxy forces familiar with the specific terrain and dynamics.[174]

One notable example is the United States' involvement in the Syrian Civil War through proxy actors, particularly the Kurdish "People's Protection Units" (YPG).[175] By providing training and intelligence to the Kurdish forces, the United States has maintained a presence in the conflict without committing substantial troop deployments. In contrast, the U.S. war in Afghanistan represents a more direct involvement, with a significant deployment of troops and resources.[176]

Another significant development in proxy warfare is the rise of private military companies (PMCs) as essential tools for Western countries to engage in security practices and proxy conflict participation. These PMCs have been utilized by governments to gather intelligence, protect civilian leaders, and procure weapons. For states, PMCs have allowed for a substantial reduction in military personnel in national armies. Furthermore, the deaths of private military contractors do not carry the same political weight as those of national soldiers. Private contractors are often buried without the official government ceremonies and media coverage that accompany traditional military casualties. This shift in the nature of proxy warfare has had profound implications, as evidenced by the presence of almost 200,000 private contractors in Iraq in 2008, outnumbering national troops stationed there. The United States alone spent between $6-10 billion on PMCs in Iraq.[177]

The rise of private soldiers for hire represents a turning point in how proxy conflicts play out internationally. With the risk of losing national troops mitigated by the availability of private military forces, states may be incentivized to engage in more proxy conflicts.

---

[173] Ibidem.
[174] Ibidem.
[175] Moghadam, Assaf, and Michel Wyss. "The political power of proxies: Why nonstate actors use local surrogates." International Security 44.4 (2020): 119-157.
[176] Ibidem.
[177] Giberson, J. (2019, January 13). The realities of proxy wars in the post Cold War Era – McGill Journal of Political Studies. https://mjps.ssmu.ca/2019/01/13/realities-proxy-wars-post-cold-war-era/

PMCs also introduce complexities in state relations, as illustrated by the 2007 Nisour Square Massacre in Baghdad, where private contractors from the PMC Blackwater opened fire on unarmed Iraqi civilians, straining Iraqi-U.S. relations and raising questions about the influence of PMCs within the U.S. government.[178]

Notably, the United States is not the only power involved in proxy conflicts. Iran, for instance, has supported Houthi rebels in Yemen, providing weapons and military support to advance its interests in the region. Iran has also recruited Shia fighters from other countries, such as Afghanistan and Lebanon, to participate in the Syrian Civil War[179]

For emerging global powers like China, proxy wars offer a means to protect their interests without facing significant backlash from important Western states, which are crucial trade partners.[180] As China continues to expand its influence, proxy wars become a strategic option to exert international influence, particularly in regions like Africa, where competition with the United States for access to natural resources escalates tensions. China has established substantial regional influence through efforts like founding and funding Confucius Institutes, which teach Mandarin to African students and promote Chinese culture.[181] As China's power grows, it threatens the influence of other global powers in the region, thereby increasing tensions and competition through proxy means.

Perhaps the most disruptive evolution in proxy warfare is the shift from a unipolar to a potentially multipolar distribution of power in the international system.[182] During the Cold War, the bipolar distribution of power positioned the United States and the Soviet Union as the two superpowers dominating global politics. However, with the emergence of new powers on the global stage, including China, Russia, and regional actors, the concept of a unipolar world order has been challenged. This shift introduces new dynamics and complexities into state behavior and international relations.

The political risks associated with directly challenging a powerful state or its allies deter such confrontations and instead encourage the use of proxy wars to protect strategic

---

[178] Ibidem.
[179] Terrill, W. Andrew. "Iranian involvement in Yemen." Orbis 58.3 (2014): 429-440.
[180] Rondeaux, Candace, and David Sterman. "Twenty-first century proxy warfare: confronting strategic innovation in a multipolar world." New America (2019).
[181] Ibidem.
[182] Giberson, J. (2019, January 13). The realities of proxy wars in the post Cold War Era – McGill Journal of Political Studies. https://mjps.ssmu.ca/2019/01/13/realities-proxy-wars-post-cold-war-era/

interests. Moreover, the specter of nuclear retaliation continues to deter direct confrontations, particularly when the very existence of a state is not at risk, echoing the Cold War dynamics of mutual assured destruction.[183]

With the introduction of more powerful states within the international system, the stakes surrounding the distribution of power are heightened. Direct state-to-state relations are evolving to avoid conventional warfare, and international disputes increasingly find expression in proxy warfare. The proliferation of private military companies, technological advancements, and the emergence of cyber warfare as a significant dimension of proxy conflicts further redefine the landscape. Moreover, Proxy wars have been regularly under-theorized and under-analyzed. The great difficulty that rises in regulating proxy wars is the fact that proxy operations are "deliberately designed to remain below the threshold of conventional military conflict and open interstate war".[184] These actions violate international norms and are motivated by broader security objectives.[185] Other terms for this concept include irregular warfare and military operations other than war, among others.[186] A variety of reasons exist for the increase in use of gray zone tactics, including the ones mentioned along this paragraph.

Furthermore, the emergence of cyber warfare introduces a further challenge to the regulation of proxy warfare. In addition to indirect third-party involvement in conflicts, cyber proxy wars take place within the realm of computer networks. As technology evolves, the physical tolls of conventional warfare, such as the loss of human life, infrastructure damage, and ecological impacts, can be circumvented by governments through the use of computer viruses and cyber attacks. The United States and other major powers have established dedicated departments for cyber operations, and States like Russia, China, and Canada have both been victims and perpetrators of such operation.

The development of ideological conflicts, shifts in methods of warfare, and evolving international power dynamics have all contributed to the transformation of proxy

[183] Ibidem.
[184] Brands, Hal. "Paradoxes of the gray zone." Available at http://www.fpri.org/article/2016/02/paradoxes-gray-zone/
[185] Naugle, Asmeret Bier, and Michael Lewis Bernard. Proxy War in the Gray Zone. No. SAND2017-3011C. Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), 2017.
[186] Ibidem.

warfare in the decades following the Cold War. While international conflicts have generally become less violent and less frequent over the past century, changes in the international distribution of power and the nature of proxy warfare have impacted state relations. As the 21st century unfolds, the increased role of technology in proxy warfare suggests that overall violence stemming from conflict may continue to decrease. However, the implications of technology on international relations remain largely unknown and will only become apparent as these conflicts play out in real time.

In conclusion, as more powerful states enter the international system, the stakes surrounding power distribution escalate. States are adapting to avoid conventional warfare, and international disputes increasingly manifest through proxy warfare. Emerging technologies, such as private military companies and drones, have reshaped the nature of proxy conflicts. The advent of cyber warfare further expands the concept of "proxy," with conflicts not only involving third-party interventions but also taking place in the virtual realm of computer networks. Nations are establishing departments dedicated to cyber operations, with hacking attacks becoming commonplace.

The fusion of technology, ideological conflicts, and shifting power dynamics has transformed proxy warfare since the Cold War. While international conflicts have become less violent and frequent over the past century, the introduction of cyber warfare in proxy conflicts is expected to further reduce overall violence. However, the impact of technology on international relations will reveal itself as these conflicts unfold in real time.

Proxy warfare is poised to shape twenty-first century conflicts for the foreseeable future, with ongoing debates regarding its normative regulation. The hope is that, especially in the context of emerging cyber proxy wars, states will recognize the inherent threats posed by underregulated proxy warfare and agree to implement norms governing responsible behavior.

Conclusion

The advent of the digital age has given rise to never-before-seen levels of connectedness and opportunity, but it has also made individuals vulnerable to serious cybersecurity risks. To address these issues, normative agreements must be made in order

to guide online conduct. Norms are essential for boosting security and stability, but international legislation in this area confront significant difficulties.

Identity, behaviour, propriety, and community expectations are some of the norms that are examined in this chapter, which also offers helpful insights into how norms are formed and influenced. It is crucial to comprehend normative processes in order to create strong cyber norms that can safeguard us in the digital world.

The evolution and influence of norms on State behaviour are guided by the norm life cycle, which includes ‘norm emergence,’ ‘norm cascade,’ and ‘norm internalization.’ Through groups like NGOs and international organisations, norm entrepreneurs advance new norms through persuasion tactics and ideational commitment.

The adoption of new standards is influenced by the normative environment of historical eras and earlier experiences. Strong social norms can lessen the need for law enforcement, which can be considered as a success even though it is possible to transform norms into laws. Additional difficulties arise from the integration of laws and procedures in the fast-developing Internet.

Examining the political ramifications of normative regulation in cyberspace, we discover that governments consent to having their actions limited by normative criteria because of caution, aversion to risk, concern for reputational harm, and domestic political pressure.

Multilateral cooperation is essential to promoting compliance by increasing the reputational cost of cyber operations associated with engaging in unfavourable behaviour. However, the efficacy and adoption of standards can be impacted by uncertainties in the changing cyber world and geopolitical upheavals.

In conclusion, broad and inclusive rules are necessary for protecting cyberspace. It is essential to comprehend the norm life cycle, the function of norm entrepreneurs, and soft power restrictions. Continuous norm adaptation and international collaboration are essential for effectively tackling new dangers and protecting our linked society as the digital era continues to develop. We can meet the difficulties of the digital age and create a safer cyberspace for everyone by adopting normative regulation.

Chapter 3: Normative foundations of cyberspace international regulation

Cyberspace has its own set of traits that might obstruct the formation of standards to limit State and non-State behavior. Defining the normative foundation of proxy wars in cyberspace requires examining the guiding principles, ethical considerations, and international norms that shape and influence the behavior of States and non-State actors involved in cyber proxy conflicts. Because of the structure and complexity of cyberspace, certain international principles are considerably more difficult to apply than in other domains, this is why there are some areas of law where the application of traditional principles and rules are yet to be settled, areas also known as *grey zones*. These grey zones represent obstacles towards the regulation of States' behavior in cyberspace and their analysis, therefore, represents a crucial point in answering the first research question (I). What are the normative foundations of the cyber proxy wars regulations?

Although norms and laws are separate ideas, they are interwoven in the digital environment. The acceptance of a norm allows for an easier acceptance of a law. That is why hope that a norm will be internalized is essentially a result of international law's limitations in regulating cyber threats, but the development of norms also depends on the acceptability of international law as it pertains to the cyberspace sphere.

Hence, in this chapter we will analyse examining the international principles and norms that shape and influence the behavior of States and non-State actors involved in cyber proxy conflicts, such as sovereignty, the principle of State responsibility, the law of neutrality and due diligence.

Most principles of international law only apply to States. However, without attribution of the cyber operation to a state as a matter of law, there is often no breach of international law, even though non-state groups' cyber operations may be illegal under the laws of a state that has authority. In other words, the question in the context of the proxy wars is whether the operation of the proxy would violate one of these laws if the state had carried it out directly, and if so, if the state is legally responsible for the proxy's actions. Therefore, the first step is to look at whether cyber operations violate international law

requirements before moving on to attribution. Respect for another state's sovereignty is the duty that a cyber operation is most likely to violate and the one we will begin with.

Sovereignty as a norm in cyberspace

Foremost, it is crucial to acknowledge that cyberspace falls under the application of the "Principle of Sovereignty."[187] Debates surrounding the impact of cyberspace on State sovereignty have often followed a general narrative, describing the decline of sovereignty as an inevitable outcome of global information exchange and the diminishing significance of physical territory in the digital realm.

Unlike power, which is commonly considered as fundamental to social interaction and governance, sovereignty is a concept that solely originates from the realm of politics. Sovereignty is indeed contingent upon the prevailing political theories and practices of a given period.[188]

In the contemporary age, sovereignty is intimately tied to the nature of the State; without a State in the traditional sense, sovereignty cannot truly exist.[189] Nevertheless, in the 20th century, the supreme authority of sovereign States has been limited by international norms such as human rights and prohibitions against genocide, as well as by supranational institutions like the United Nations and the European Union.[190]

As Robert Keohane has observed, discussions about sovereignty often outweigh its precise definition.[191] To provide some clarity, Stephen Krasner proposed four ways in which scholars and others concerned with State conduct in the international system understand 'sovereignty': domestic sovereignty, interdependence sovereignty, international legal sovereignty, and Westphalian sovereignty.[192]

Each type of sovereignty can be examined in connection with cyberspace, and it is incorrect to presume that cyberspace invariably undermines sovereignty in all its manifestations. Notably, cyberspace has minimal impact on International Legal

[187] Schmitt, Michael N., ed. Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press, 2017.
[188] Betz, David J. Cyberspace and the State: Towards a Strategy for Cyber-power. Routledge, 2017
[189] Ibidem.
[190] Keohane, Robert O. "Ironies of sovereignty: the European Union and the United States." JCMS: journal of common market studies 40.4 (2002): 743-765.
[191] Ibidem
[192] Krasner, Stephen D. "Sovereignty." Foreign Policy (2001): 20-29.

sovereignty, but it does have significant implications for the closely related notion of Westphalian sovereignty. The most pronounced effect of cyberspace is on Interdependence sovereignty, given the cross-border nature of information exchange.[193] Consequently, this can potentially influence Domestic sovereignty, and numerous instances demonstrate that this is indeed an ongoing reality.

International legal sovereignty and cyberspace

International legal sovereignty pertains to the establishment of political entities in the international system, recognized by other States as equals under international law, granting their representatives diplomatic immunity and access to the global stage.[194]

Cyberspace itself does not directly challenge the integrity of international legal sovereignty as a source of authority. However, some theorists and activists argue more vigorously that cyberspace should be acknowledged as a sovereign entity in the international political system. Their claims rest on the distinct nature of cyberspace, especially its lack of traditional territorial boundaries and non-corporeal activities.[195] Consequently, cyberspace is informally regarded as a global realm beyond traditional legal sovereignty. These advocates present the case for recognizing an "emergent cyberspace sovereignty," asserting that some States already endorse this notion.[196] Nevertheless, currently, there is no indication that any State is willing to recognize cyberspace as an independent legal sovereign entity. On the contrary, States seem less inclined than ever to relinquish authority over cyberspace.

The likelihood of any compromise to grant cyberspace recognition as a legal sovereign entity is low, especially considering that cyberspace lacks autonomy and a unified actor capable of representation.

---

[193] Betz, David J. Cyberspace and the State: Towards a Strategy for Cyber-power. Routledge, 2017.
[194] Ibidem.
[195] Johnson, David R., and David Post. "Law and borders: The rise of law in cyberspace." stanford law review (1996): 1367-1402; Barlow, John Perry. "A Declaration of the Independence of Cyberspace." Duke L. & Tech. Rev. 18 (2019): 5.
[196] Wu, Timothy S. "Cyberspace sovereignty--the Internet and the international system." Harv. JL & Tech. 10 (1996).

Westphalian sovereignty and cyberspace

Westphalian sovereignty is based on the concept that States are associated with specific physical territories, where domestic political authorities hold the legitimate power for institutional organization and policies. According to Newman, this system rests on the principles of the "sovereignty of each political unit (the State), territoriality, and non-intervention (internal sovereignty)." [197] It forms the foundation of the modern international system of sovereign States and is enshrined in the United Nations Charter, which prohibits the UN from intervening in matters within the domestic jurisdiction of any State.[198]Violations of Westphalian sovereignty occur when external actors induce changes in the structures and actions of domestic political authority. The Tallin Manual's Rule 4 explicitly states that States must not conduct cyber operations that violate the sovereignty of another State.[199]

A clear example of cyberspace's interaction with Westphalian sovereignty lies in the exercise of compulsory cyber-power. Operations targeting assets in another country inherently breach Westphalian sovereignty. Similarly, cyber operations conducted by a State, or a proxy's operation attributable to a State, in another country breach Westphalian sovereignty, akin to any other militarized action against another State. Famous instances of proxy cyber operations include the cyberattacks on Georgia and Estonia in 2008, both of which raised questions about the boundaries of Westphalian sovereignty and potential connections to external actors. In these instances, malicious cyber activity, including large-scale DDoS attacks, impacted not just important financial institutions and news sources but also official government websites. Interestingly, following the 2007 incidents, the response—or lack thereof—from the relevant state in addressing and mitigating activities originating within its borders could be viewed as a factor contributing to these actions, implying a certain level of endorsement. Such implications may provide a foundation for a state's increased engagement in similar operations.[200]

---

[197] E. Newman, 'Failing States and International Order: Constructing a Post-Westphalian World', Contemporary Security Policy, 2009, Vol. 30, No. 3, page 422.

[198] "United Nations Charter, Chapter I: Purposes and Principles". United Nations. 26 June 1945. Retrieved 13 February 2023.

[199] Schmitt, Michael N., ed. Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press, 2017.

[200] Maurer, Tim. Cyber mercenaries. Cambridge University Press, 2018.

Covert cyber-espionage targeting locations within another State is also a violation. The Stuxnet worm incident, possibly involving a combined US-Israeli operation against Iranian nuclear technologies, is another example of this type of breach.[201]

However, some exceptions may be tolerated and even encouraged, such as when one State invites another to conduct actions within its borders, as seen in transnational counter-cybercrime operations. While this too violates Westphalian sovereignty, it is deemed acceptable due to its perceived benefits to both States. For instance, the Council of Europe's Convention on Cybercrime of November 2001 involves States voluntarily allowing changes in internal legal frameworks and an increase in cross-border investigative actions.[202]

Cyberspace presents an intriguing possibility where violations of Westphalian sovereignty might become normalized over time, despite conventions or arrangements regulating computer network operations against other parties. The development of 'active defense systems' could lead to automated and institutionalized violations of Westphalian sovereignty as a de facto defense and security policy. These systems respond to attacks on friendly networks with retaliatory actions, often targeting assets outside one's own borders.[203] As more State agencies and proxies deploy active defense systems, the global level of Westphalian sovereignty violations is likely to increase, possibly becoming the status quo. This creates a paradoxical situation where violations become both the norm and the exception.

Domestic sovereignty

While Westphalian sovereignty pertains to the principle of non-intervention in the internal affairs of other States, domestic sovereignty focuses on how a State's internal affairs are conducted, including how authority is organized and the level of control exerted by its political structures.[204] The emergence of cyberspace has significantly impacted both domestic authority and control. By this, we refer to those functions that can only be carried

[201] Responsible Behaviour in Cyberspace: Global narratives and practice: EU Cyber Direct. (2023, June 29). Horizon. https://eucyberdirect.eu/research/responsible-behaviour-in-cyberspace.
[202] Council of Europe, Convention on Cybercrime, 2001, http://conventions.coe.int/treaty/en/treaties/html/185.htm.
[203] Kesan, Jay P., and Carol Mullins Hayes. "Thinking through active defense in cyberspace." Proceedings of the Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options. 2010.
[204] Krasner, Stephen D. "Sovereignty." Foreign Policy (2001): 20-29.

out by states. Elections, tax collecting, law enforcement, national crisis management, diplomacy, and national defense are a few examples. Interference happens when a cyber operation makes it significantly harder to carry out the task, such as when it momentarily interferes with electoral machines or with defensive military systems like early-warning radars.[205] Usurpation refers to carrying out fundamentally governmental duties in place of the other state, as in the case of enforcing laws against proxies by conducting remote searches or virtually seizing items on the territory of another state without that state's consent.[206]

States have adopted different pieces of legislation and built new institutions to control how cyberspace is used within their borders in response to the issues it presents. Examples include the European Union Agency for Cybersecurity (ENISA) in the EU[207], the Office of Cyber Security and Information Assurance (OCSIA) in the United Kingdom[208], and the Agenzia per la Cybersicurezza Nazionale (ACN) in Italy[209]. These actions demonstrate how an increasing number of States view cyberspace as a potential threat to their domestic sovereignty.

A clear manifestation of this dynamic is evident in the efforts by several States to control their citizens' access to information, citing certain content and activities as threats to internal order and authority. For instance, in an episode of information amplification before the 2017 Catalan independence vote, certain media outlets with suspected affiliations exploited social media profiles connected to Venezuela and Chavista interests. These accounts actively promoted the hashtag #VenezuelaSalutesCatalonia, insinuating solidarity between Venezuela and Catalonia's push for independence.[210]

While cyberspace has posed challenges to governments' ability to exercise domestic sovereignty as extensively as before, they have been actively seeking ways to reassert

---

[205] Johnson, Durward E., and Michael N. Schmitt. "Responding to proxy cyber operations under international law." The Cyber Defense Review 6.4 (2021): 15-34.
[206] Ibidem.
[207] About ENISA - The European Union Agency for Cybersecurity. ENISA. https://www.enisa.europa.eu/about-enisa
[208] Cabinet Office. A strong Britain in an age of uncertainty: the national security strategy. Vol. 7953. The Stationery Office, 2010.
[209] Chi siamo - Agenzia per la cybersicurezza nazionale. (n.d.). ACN - Agenzia per La Cybersicurezza Nazionale. https://www.acn.gov.it/agenzia/chi-siamo.
[210] Alandete, David. "Russian network used Venezuelan accounts to deepen Catalan crisis." El País 11 (2017): 2017.

control over information sources to maintain internal authority. The impact of cyberspace on domestic sovereignty largely stems from its tendency to bypass governments' control over information flow across borders. Despite being a medium of information exchange, cyberspace's transmitted information is often interpreted as persuasive ideas and ideologies or converted into capital in the form of goods and services. Consequently, both desirable and dangerous information are subject to robust attempts at control. The struggle between managing desired and dangerous information defines the contemporary cyberspace policy landscape.[211]

Interdependence sovereignty

The concept of control is central to interdependence sovereignty, which deals with regulating the flow of goods, people, pollutants, diseases, and ideas across territorial borders. When considering the loss of sovereignty as a result of globalization, this sort of sovereignty is frequently mentioned.[212]

Global cyberspace thrives precisely because information flows relatively freely across national boundaries, as famously expressed by the Internet axiom, "national borders aren't even speed bumps on the information superhighway".[213] While domestic authority may not necessarily be impacted by depleted interdependence sovereignty, domestic control is often weakened. If a State cannot effectively regulate what enters its borders, it will struggle to maintain control over internal affairs.[214] Indeed, in cyberspace, it is challenging to control the influence of foreign citizens on a State's own population.

Attempts by governments to restore interdependence sovereignty have faced limited success, leading to a paradoxical situation. Governments attempt to restrict information flows for grounds of national security while simultaneously promoting cyberspace as an engine of economic growth and the propagation of democratic principles. It is challenging to balance the conflict between advancing international Internet freedom and preserving national security.[215]

---

[211] Ibidem.
[212] Krasner, Stephen D. "Sovereignty." Foreign Policy (2001): 20-29.
[213] This is attributed to Tim May, former chief scientist at Intel and co-founder of the Cypherpunks mailing list, found in Betz, David J. Cyberspace and the State: Towards a Strategy for Cyber-power. Routledge, 2017.
[214] Krasner, Stephen D. "Sovereignty." Foreign Policy (2001): 20-29.
[215] Betz, David J. Cyberspace and the State: Towards a Strategy for Cyber-power. Routledge, 2017.

If national security concerns outweigh all other considerations, the logical outcome is a highly regulated online environment, where national cyberspaces mirror physical borders and national norms—a form of political 'balkanization' of cyberspace.[216] Alternatively, political-economic blocs of like-minded nations may emerge, where interdependence sovereignty is relinquished in favor of asserting pooled sovereignty at the borders of these multinational groupings.

China's 'Golden Shield' censorship and surveillance project, also known as the Great Firewall of China, exemplifies how strict regulation of the telecommunications sector can substantially aid in controlling cyberspace. While not entirely impenetrable, the normative impact of persistent and pervasive Internet filtering and monitoring is crucial alongside its technical effectiveness. By controlling aspects of interdependence sovereignty, China aims to protect its domestic sovereignty from subversive political and cultural ideas, while also leveraging cyberspace for economic and political influence.[217]

Attribution and State Responsibility over acts committed by proxies

As we previously mentioned cyberattacks are secretive by their very nature, this explains why the nature and repercussions of an incident may not be immediately apparent and attributing the source of an attack can be difficult. There have been attempts to apply international law to cyberspace, such as the 2013 Tallinn Manual on the International Law Applicable to Cyber Warfare.[218] However, they have so far failed to achieve consensus on many points. In the case of proxies, Michael Schmitt and Liis Vihul, in their 2014 article *Proxy Wars in Cyberspace: The Evolving International Law of Attribution*, noted that States have a lot of leeway in their support of them: "the relatively high levels of support that are required before a State can be held responsible for the activities of non-State groups or individuals, as distinct from their own responsibility for being involved, creates a

[216] The Economist, "A virtual counter-revolution", The Economist Group Limited, 2010, at https://www.economist.com/briefing/2010/09/02/a-virtual-counter-revolution.
[217] Walton, Greg. China's golden shield: Corporations and the development of surveillance technology in the People's Republic of China. Rights & Democracy, 2001.
[218] Schmitt, Michael N., ed. *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press, 2013.

normative safe zone for them."[219]This paragraph will analyse the principle of attribution of proxy actors in cyberspace.

Cyberspace is not exempt from the application of international law, which governs activities occurring within it. Consequently, secondary rules of international law, such as the law of State responsibility, are foundational to operations originating in cyberspace. The law of State responsibility deals with the legal consequences when a State violates international law. According to the International Law Commission's DARSIWA, States are held accountable for their "internationally wrongful acts," meaning acts that infringe upon their international obligations and cause injury to another State.[220]

For an act to be considered an internationally wrongful act, two distinct elements must be present. First, there must be an action or omission that breaches an international legal obligation. Second, this act must be attributable to the responsible State, meaning it is perceived as a State-act under international law.[221]

In the event that a responsible State violates an obligation owed to another State, it is required to immediately cease the offending conduct or fulfill the required duty and provide full reparation to the injured State.[222] This framework applies entirely to State cyber operations that violate international obligations owed to the target State. Therefore, it is indisputable that a State conducting a cyber operation that violates a treaty or customary international law duty to another State is obligated to immediately terminate the operation.

Attributing a cyber operation conducted by a proxy actor in cyberspace to the State itself is a complex and challenging endeavor, primarily due to the intricate nature of proxy relationships and the evolving tactics employed by State actors. As mentioned, the process of attribution involves identifying the actual perpetrators of cyber operations, and when proxies are involved, this task becomes even more tedious. Firstly, technical attribution involves identifying the actual perpetrators of cyber operations through forensic investigations, which can be challenging in the case of proxy actors due to some techniques

[219] Schmitt, Michael N., and Liis Vihul. "Proxy wars in cyberspace: the evolving international law of attribution." *Fletcher Sec. Rev.* 1 (2014): 53.
[220] International Law Commission. "Draft articles on responsibility of states for internationally wrongful acts." Yearbook of the International Law Commission 2.2 (2001): 49.
[221] Ibid., art. 2.
[222] Ibid., arts. 30(a), 31.

used to evade technical attribution such as botnets, meaning networks of computers that have been taken over and used to commit different frauds and cyberattacks without the knowledge of the computer's owner[223], and IP spoofing, which is the process of creating Internet Protocol (IP) packets with a fictitious source IP address in order to pretend to be another computer system.[224] Many State-sponsored cyber operations are conducted using botnets or networks of compromised computers. These botnets may span multiple countries and involve computers owned by unsuspecting individuals or organizations. Proxies can leverage these botnets, making it appear as if the operation originates from various locations, further obscuring attribution. Therefore, mere evidence that a cyber operation originates from governmental cyber infrastructure or involves malware reporting back to another State's infrastructure is typically insufficient to attribute the operation to that State.[225]

Legal attribution, as described in the law of State responsibility, is essentially the process of connecting a specific action or omission to a State.[226] Hence, "State responsibility applies regardless of whether such acts are carried out by a State or non-State actors instructed, directed or controlled by a State [..] States cannot waive their responsibility by carrying out malicious cyber operations via non-State actors and proxies."[227]

Regarding the engagement of States and its intermediaries in cyber operations, we identify four modes of legal attribution derived from customary international law. These are significant in delineating the limits according to which an action committed by a proxy actor could be attributed to the State itself.

The first mode of attribution, outlined in Article 4 of DARSIWA (*Conduct of organs of a State*), pertains to the conduct of State organs, such as the armed forces, which

---

[223] What is a Botnet? (2023, June 30). usa.kaspersky.com. https://usa.kaspersky.com/resource-center/threats/botnet-attacks

[224] IP spoofing: How it works and how to prevent it. (2023, May 18). www.kaspersky.com. https://www.kaspersky.com/resource-center/threats/ip-spoofing

[225] Ottis, Rain. "Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective." Proceedings of the 7th European Conference on Information Warfare. Reading, MA: Academic Publishing Limited, 2008.

[226] UNGA, Report of the International Law Commission – Fifty-Third Session, 36, para. 12.

[227] Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States, UNODA, A/76/136 (August 2021) 27-28.

are considered State acts under international law.[228] The functions and positions of these State organs are irrelevant; what matters is that they hold the status of a State organ as determined by the national law of that State.[229]

The second mode of attribution, governed by Article 5 of DARSIWA (*Conduct of persons or entities exercising elements of governmental authorities*), addresses the conduct of individuals or entities empowered by a State's domestic law to exercise elements of governmental authority and acting in that capacity.[230] This means that if semi-public entities, private companies, or other actors carry out governmental functions as mandated by the State's internal law and breach the State's international obligations, the State can be held responsible.[231] This rule particularly applies to those proxies whose action fall under the category of 'delegation'.

The third applicable mode of attribution is covered by Article 11 of DARSIWA (*Conduct acknowledged and adopted by a State as its own*), which deals with situations where non-State actors' actions or omissions are acknowledged and adopted by a State as its own.[232] The formal acknowledgement of the activity by the State is necessary for the State to be held accountable for a cyber operation carried out through a proxy. This particular requirement calls for a State to admit the existence of the hostile cyber activity, either explicitly or by its actions. Additionally, the state must take affirmative steps to terminate its proxy's actions. It is crucial to note that situations such as these are extremely uncommon because nations frequently use proxies in order to preserve plausible deniability and establish a degree of distance from the adversarial cyber operation. Hence, while it is rare for States to openly acknowledge and adopt such operations as their own, if they do, the grounds for attribution presented in Articles 4, 5, and 11 of DARSIWA are expected to apply.[233]

The fourth mode of attribution, covered in Article 8 of DARSIWA (*Conduct directed or controlled by a State*), relates to the conduct of non-State actors or proxies

---

[228] International Law Commission. "Draft articles on responsibility of states for internationally wrongful acts." Yearbook of the International Law Commission 2.2 (2001)
[229] Crawford, James. State responsibility: the general part. No. 100. Cambridge University Press, 2013.
[230] International Law Commission. "Draft articles on responsibility of states for internationally wrongful acts." Yearbook of the International Law Commission 2.2 (2001)
[231] Ibidem.
[232] Ibidem.
[233] Ibidem.

operating on instructions or under the direction and control of a State.[234] This describes a relationship of 'delegation', seen in the first chapter, which illustrates situations where the recipient exercises significant control on the proxy. In the case of instructions, a State's intentions must be clearly indicated regarding the authorized violations of international law.[235] In the case of direction, a State must consistently direct the commission of those violations by providing instructions to non-State actors.[236] Proving the giving of instructions or direction can be very challenging. Hence relationships where the tie between the State and the proxy is even more subtle, such as 'orchestration' or 'sanctioning', prove almost impossible to control. State control is a more practically relevant means of legally attributing private conduct under Article 8 of DARSIWA, but it also presents several legal challenges.[237]

Control theories in the age of cyber

Only when proxies are acting "on the instructions" of a given State or operating under its "direction or control" is their behavior considered attributable to that of that State. [238] This poses a strong issue for proxies in cyberspace. Next, we will analyse how judicial systems test for controls and their implications on proxy's actions.

Two control theories are used to address the issue of State control over cyber operations and the actors involved because the law of State accountability does not have a clear definition of acting "on the instructions" or acting under the "direction or control" of a State. The effective control test proposed by the International Court of Justice (ICJ) and the overall control test (also known as the "Cassese test" used by the International Criminal Tribunal for the latter.

The overall control test offers a more lenient threshold for attributing cyber activities to States. It focuses on the State's broader involvement, coordination, and support for non-State actors. The Tallinn Manual discusses both theories, but the 2.0 version

[234] Ibidem.
[235] United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran), ICJ Reports 1980 (ICJ, 24 May 1980) (Tehran Hostages judgment), 30–31, para. 59.
[236] International Law Commission. "Draft articles on responsibility of states for internationally wrongful acts." Yearbook of the International Law Commission 2.2 (2001)
[237] Ibidem.
[238] Schmitt, Michael N., and Liis Vihul. "Proxy wars in cyberspace: the evolving international law of attribution." *Fletcher Sec. Rev.* 1 (2014).

mainly focuses on the ICJ's perspective, considering it as the leading theory for attribution.[239]

The effective control test has a high threshold and is challenging to meet in practice. It requires a State to effectively determine how cyber operations, which breach international law obligations, are conducted and continuously monitor their execution.[240] In the Bosnian Genocide case, the ICJ endorsed the effective control theory for the purposes of Article 8 of DARSIWA, rejecting the easier-to-meet overall control test used by the ICTY in the Tadić decision.[241] However, there are arguments for applying a control theory with a lower threshold to prevent States from evading international responsibility by using controlled non-State actors. Meeting the criteria of the effective control test is exceptionally demanding, especially in the context of cyberspace. Cyber proxy operations often involve a degree of autonomy for the proxies, making it difficult to prove continuous State control. This stringent requirement can lead to challenges in attributing cyberattacks to States, even when proxies are involved.

Merely involving the State in financing, equipping, providing training, or participating in operational planning and general control would not be sufficient to conclude that the State directed or enforced acts contrary to international law.[242] The effective control test's stringent requirements make it challenging to attribute cyber operations committed by State proxies to States themselves, as they must have significant and continuous control over the actions.

It is argued that a control theory with a lower threshold is necessary to prevent States from escaping international responsibility when using non-State actors under their control.[243] While the ICJ's endorsement of the effective control theory in the Bosnian Genocide case may seem conclusive, the need for a control theory with a lower threshold persists.

---

[239] Schmitt, Michael N., ed. Tallinn manual on the international law applicable to cyber warfare. Cambridge University Press, 2013.
[240] Delerue, François. Cyber operations and international law. Vol. 146. Cambridge University Press, 2020.
[241] See note 219.
[242] Schmitt, Michael N., ed. Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press, 2017.
[243] Responsible Behaviour in Cyberspace: Global narratives and practice: EU Cyber Direct. (2023, June 29). Horizon. https://eucyberdirect.eu/research/responsible-behaviour-in-cyberspace.

The ICTY's Appeals Chamber's rationale suggests that the level of State control over individuals and groups can differ in nature, as acknowledged by Vice-President Awn Shawkat Al-Khasawneh of the ICJ in the Bosnian Genocide case[244].

In the realm of cyberspace, two scenarios are distinguished: (1) proxies such as private individuals or unorganized groups carrying out cyber operations on behalf of States, and (2) organized and hierarchically structured groups responsible for violations.[245]

For the first scenario, legal attribution necessitates establishing effective State control over cyber operations.[246] This requires significant and continuous State control over private individuals or unorganized groups engaging in cyber operations that breach international law.

Conversely, for the second scenario involving organized and hierarchically structured groups, a more general level of State control would suffice.[247] This means States must not only provide financing and equipment but also coordinate activities and contribute to the overall planning of these groups. Notably, State control over non-State actors like militias or paramilitary groups can take on an overall nature, without necessarily involving specific orders or direction from the State. Instead, the State's role in organizing, coordinating, or planning actions, along with providing financial, training, and operational support, is taken into account. [248]

In summary, the level of State control required for legal attribution in cyberspace may vary depending on the actors involved and the organizational structure of the groups responsible for violations. Effective control may be necessary for private individuals or unorganized groups, while an overall level of control would be sufficient for organized and hierarchically structured cyber groups.

[244] Dissenting Opinion of the Vice-President of the ICJ A. S. Al-Khasawneh in Bosnian Genocide judgment (Dissenting opinion of Al-Khasawneh, Bosnian Genocide judgment), 216–217, para. 37.
[245] Cassese, Antonio. "The Nicaragua and Tadić tests revisited in light of the ICJ judgment on genocide in Bosnia." European journal of international Law 18.4 (2007): 649-668.
[246] Tadić judgment, 56, para. 131.
[247] Ibidem.
[248] Ibid., 58–59, para. 137.

The attribution rules of DARSIWA concerning State control do not prescribe a specific control theory for different contexts.[249] Relying solely on the hard-to-meet criteria of the effective control test, which has a high threshold, would not align with the fundamental premise of State responsibility doctrine, potentially allowing States to avoid international responsibility.[250] Moreover, it would be impractical to hold States accountable if only the effective control requirements were applied.

Considering the rapid technological developments, the law of international responsibility, including attribution rules rooted in customary international law, is continually evolving and should not be seen as static. Flexibility in adopting attribution standards can be observed for instance in the area of anti-terrorism.[251]

Emphasizing the role of overall control theory is crucial. This test is supported by State and judicial practice, has a lower threshold than the effective control theory, and is valuable in establishing the actual close relationship between States and organized, hierarchically structured cyber groups.[252] These groups must have a structure, chain of command, rules of operation, and certain outward symbols of authority.[253] While the Tadić decision was made decades ago when cyber-attacks were less prevalent, it may be appropriate to re-evaluate the elements of the overall control test given the current landscape where hackers' collectives and other organized groups are involved in cyber operations.

The group's structure does not need to be of military nature, and a well-structured group requires a chain of command, ensuring members are under the authority of superiors who guide their activities.[254] A set of rules, both written and unwritten, should be followed by group members. It is conceivable that these criteria could be met by groups acting on behalf of States in cyberspace.

---

[249] International Law Commission. "Draft articles on responsibility of states for internationally wrongful acts." Yearbook of the International Law Commission 2.2 (2001)
[250] Cassese, Antonio. "The Nicaragua and Tadić tests revisited in light of the ICJ judgment on genocide in Bosnia." European journal of international Law 18.4 (2007): 649-668.
[251] Jinks, Derek. "State responsibility for the acts of private armed groups." Chi. J. Int'l L. 4 (2003): 83.
[252] Delerue, François. Cyber operations and international law. Vol. 146. Cambridge University Press, 2020.
[253] Tadić judgment, 49, para. 120.
[254] Ibidem.

The fourth requirement, concerning outward symbols of authority, is more relevant to military and paramilitary units in armed conflicts, such as uniforms and insignia.[255] However, it may not be the core criterion for groups involved in cyber operations on behalf of States in cyberspace.

In conclusion, the choice between the effective control test and the overall control test has far-reaching implications for attributing cyber proxy operations to States. The threshold set by these control theories plays a pivotal role in determining State responsibility, impacting efforts to hold States accountable for cyber activities conducted by proxies. As the cyber landscape continues to evolve, the adaptability and application of these control theories in cyberspace will remain a topic of significance in international law and State responsibility. Given technological advancements, these theories are not limited to military operations and should be applied in the cyber context depending on specific case circumstances involving individuals and groups.

The Use of Force and Self-Defence

Article 2(4) of the United Nations Charter enunciates the imperative for all Member States to abstain from employing or threatening force in their international dealings, ensuring the territorial integrity and political independence of any State, and adhering to the objectives of the United Nations. This fundamental principle of international law is widely acknowledged as customary[256], and there is a consensus that it fully applies to cyber operations conducted by or attributable to States and their proxies.[257] This was further stated in the proposal of the Russian Federation for the "updated concept of the Convention of the UN on ensuring international information security".[258] Here Russia proposed the adoption of the UN Convention on Ensuring International Information Security, which would govern the relationships between States regarding the security and use of information and communications technologies. This convention could incorporate provisions based on recommendations from annual UN GA resolutions, as well as the

[255] Ibidem.
[256] The charter of the United Nations, art. 2(4). Oxford, UK: 1995.
[257] Schmitt, Michael N., ed. Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press, (2017).
[258] Russian Federation, UPDATED CONCEPT OF THE CONVENTION OF THE UNITED NATIONS ON ENSURING INTERNATIONAL INFORMATION SECURITY, (2020), https://namib.online/en/basic-documents-in-the-field-of-international-information-security/

consensus reports of relevant UN OEWGs and GGEs from various years. Among the principles and proposals for the Convention there is that of "refraining in international relations from the threat or use of force against another State's information and communication infrastructure or as a means of conflict resolution.[259]

However, uncertainty surrounds the precise threshold for determining the use of force in the context of cyber activities. In addition, a proxy's cyber activity must be traceable to a state in order to breach the prohibition on the use of force, much like with the sovereignty and intervention requirements. If it is not, under the domestic laws of the states with authority over the situation, it is only a crime.

It is generally accepted that a cyber operation resulting in physical damage or injury constitutes an unlawful use of force, unless authorized by international law, such as in cases of self defense with authorization[260], United Nations Security Council mandate under Chapter VII of the UN Charter,[261] or the consent of the affected State.

The first edition of the Tallinn Manual concluded that certain operations without such severe consequences might still meet the use of force threshold.[262] This conclusion was drawn from the International Court of Justice's ruling in the Nicaragua case, which declared that arming and training guerrilla forces against another State qualifies as a use of force against that State.[263] By analogy, the Manual's Experts concurred that providing malware and training to non-State groups for its use against another State also constitutes a use of force.[264] When reviewing the relevant text for Tallinn Manual 2.0, no subsequent State practice or opinio juris warranted revision.[265] However, reaching a clear-cut test for categorizing non-destructive cyber operations as a use of force proved challenging. Consequently, the Experts proposed an approach that considers how likely States are to perceive a cyber operation as such. This approach is predicated on the premise that, in the absence of a definitive threshold, States involved in or targeted by cyber operations must

[259] Ibidem.
[260] See note 238.
[261] Ibid., ch. VII.
[262] Schmitt, Michael N., ed. Tallinn manual on the international law applicable to cyber warfare. Cambridge University Press, 2013.
[263] Leigh, Monroe. "Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America). 1984 ICJ Reports 392." American Journal of International Law (1985).
[264] See note 239.
[265] Ibidem.

be mindful of how the international community is likely to assess whether the operations violate the prohibition on the use of force.[266]

The method identifies factors that States are likely to take into account when making determinations regarding the use of force. Key factors encompass the severity, immediacy, directness, and invasiveness of the consequences; the measurability and military character of the operation; the extent of State involvement; and any presumptive legality concerning the type of operation, such as psychological operations or espionage.[267] The Experts also identified other relevant factors, including the prevailing political environment, whether the cyber operation indicates a future use of military force, the identity of the examiner, any record of cyber operations by the attacker, and the nature of the target.[268] While no single factor alone is likely to qualify a cyber operation as a use of force, these and other factors are jointly considered when assessing the likelihood of an operation being categorized as such.

The absence of a consensus on the use of force threshold and the resulting approach proposed by the Experts, which considers a varied and context-based list of factors, highlights the ambiguity surrounding the prohibition on the use of force for States and their proxies.[269]

The issue of self-defence is somewhat clearer, though still unsettled. According to Article 51 of the UN Charter, the inherent right to individual or collective self-defence remains intact when a Member of the United Nations faces an armed attack until the Security Council acts for international peace and security. There is broad agreement that this article reflects customary international law and applies to defending against cyber armed attacks. [270]

The key to comprehending self-defence in the cyber context lies in interpreting the term ‘armed attack,’ which lacks a specific definition in international law. The prevailing view distinguishes the most severe forms of force, constituting armed attacks, from less

[266] Ibidem.
[267] Schmitt, Michael N., ed. Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press, (2017).
[268] Ibidem.
[269] Leigh, Monroe. "Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America). 1984 ICJ Reports 392." American Journal of International Law (1985).
[270] See note 247.

grave forms, as exemplified in the Nicaragua case by the ICJ.[271] However, the United States' assertion that there is no distinction between the use of force and armed attack thresholds, a view not widely accepted, adds to the uncertainty surrounding self-defence.[272]

The difficulty for other States is determining which cyber-uses of force would reach this threshold. A cyber activity that causes severe injuries, deaths, considerable property damage, or destruction obviously satisfies the size and effects criteria.[273] Consensus rapidly declines below this point. For instance, the first edition Tallinn Manual experts disagreed on whether the 2010 Stuxnet operation, which destroyed Iranian centrifuges, constituted as an armed strike even though they all agreed it involved the use of force.[274] While some experts contend that a cyber operation must result in physical harm or destruction in order to be deemed an armed strike, others rightly emphasize the seriousness of the repercussions.

Complexity is increased in scenarios where a number of cyber activities are involved but none of them independently match the criteria for an armed strike. It is uncertain if States, particularly when using the severity method, can add up the effects of these actions to exceed the armed assault threshold. According to the experts, aggregation is acceptable when one State or organization is in charge of all activities, and they would also permit aggregation when several States or groups cooperate.[275] However, as this matter is not covered by international law and there is little State practice or jurisprudential opinion, their conclusion remains speculative.

Another concern that contributes to the ambiguity surrounding self-defence is whether non-State actors have the right to launch an armed attack when their online behavior cannot be connected to a State. After the 9/11 attacks, when the world community perceived Al Qaeda's acts as an armed assault, the right to self and collective defense was

---

[271] See note 249.
[272] Blank, Laurie R. "Irreconcilable Differences: The Thresholds for Armed Attack and International Armed Conflict." Notre Dame L. Rev. 96 (2020): 249.
[273] Schmitt, Michael N., ed. Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press, (2017).
[274] Sanger, David E. "Obama order sped up wave of cyberattacks against Iran." The New York Times 1.06 (2012): 2012.
[275] See note 254.

asserted.[276] This approach is in line with Article 51, which omits explicitly identifying States as the initiators of the required military attack. Accordingly, the same justification holds valid for cyber operations carried out by non-State actors, according to several States, academia, and the majority of Tallinn Manual experts.[277]

However, this tactic was called into doubt by the ICJ in its Wall advisory opinion and Armed Activities decision.[278] In such cases, the court did not appear to want to extend the right to self-defence to situations in which it was impossible to connect the activities of non-State entities to a State. In view of State practice and *opinio juris* to that effect, the court has come under justified criticism for its unwillingness to interpret the right as including assaults by non-State actors, particularly by members of the court itself. It is, however, challenging to make a case for a right of self-defence against non-State actors who engage in armed attack-level cyber operations in light of its remarks.

The Law of Neutrality

The concept of 'neutrality' refers to the legal status of a State that is not involved in an international armed conflict.[279] Despite doubts arising from conflicts occurring since World War II, the law of neutrality is still considered valid. Some neutral governments have tried to hide their involvement in conflicts, indicating their adherence to this law. Even those openly supporting one side justify their actions, acknowledging the continued application of neutrality law. Various military manuals and international law associations also recognize the relevance of neutrality in international armed conflicts.[280]

Under the UN Charter, it is possible to distinguish between aggressors and victims, but this doesn't permit States to unilaterally exempt themselves from neutrality obligations. However, if the UN Security Council decides on preventive or enforcement measures

[276] Shiryaev, Yaroslav. "The right of armed self-defence in international law and self-defence arguments used in the second Lebanon war." Acta Societatis Martensis 3 (2007): 80.
[277] See note 254.
[278] Ventura, Manuel J. "Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda)(Reparations Judgment)(ICJ)." International Legal Materials 62.3 (2023): 399-527.
[279] Convention No. V Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, Oct. 18, 1907, 36 Stat. 2310 [hereinafter Hague V]. Convention No. XIII Concerning the Rights and Duties of Neutral Powers in Naval War, Oct. 18, 1907, 36 Stat. 2415 [hereinafter Hague XIII].
[280] Heintschel von Heinegg, Wolff. "Territorial sovereignty and neutrality in cyberspace." International Law Studies 89.1 (2013).

under Chapter VII of the Charter, the scope of neutrality law may be reduced, and the 1907 Hague Conventions become inapplicable.[281]

Considering the above, it is assumed that, except for UN Security Council decisions, the traditional law of neutrality applies to States not involved in international armed conflicts. The focus will now shift to exploring the application of this law in cyberspace and identifying the obligations of belligerents and neutrals concerning military operations in that domain.

The Law of Neutrality in cyberspace and for cyber proxies

The core principles and rules of the law of neutrality, which apply to international armed conflicts characterized by the use of traditional kinetic weapons, are valid. However, some may question their applicability when it comes to hostilities and hostile acts conducted in or through cyberspace. Considering cyberspace as a new 'fifth dimension' with unique characteristics, it might seem challenging to maintain the law of neutrality's relevance.

Yet, if we acknowledge that cyberspace requires a physical architecture to exist, many of the difficulties in applying the law of neutrality can be addressed. The law of neutrality serves a dual protective purpose: to protect the territorial sovereignty of neutral States and their nationals against the harmful effects of ongoing hostilities, and to safeguard belligerent interests against interference by neutral States and their nationals to the advantage of one belligerent and to the detriment of the other.[282]

In the context of cyberspace, it can be reasonably concluded that the law of neutrality protects cyber infrastructure located in the territory of a neutral State or residing in sovereign immune platforms and other objects used by the neutral State for non-commercial government purposes.[283] Belligerents are obligated to respect the sovereignty and inviolability of States not participating in the conflict by refraining from any harmful interference with the cyber infrastructure located in neutral territory. Neutral States, in turn,

---

[281] Doswald-Beck, Louise. "The San Remo Manual on international law applicable to armed conflicts at sea." American Journal of International Law 89.1 (1995): 192-208.

[282] HEADQUARTERS, US, MARINE CORPS, and US COAST GUARD. "THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS." (2007).

[283] Heintschel von Heinegg, Wolff. "Territorial sovereignty and neutrality in cyberspace." International Law Studies 89.1 (2013).

must remain impartial and refrain from engaging in cyber activities that support one belligerent's military actions to the detriment of the opposing belligerent. They are also obliged to take feasible measures to terminate any abuse of cyber infrastructure within their territory or on their sovereign immune platforms by belligerents.[284]

Although these findings are based on a teleological interpretation of the law of neutrality and might be subject to question, they are supported by the majority of authors addressing neutrality in the cyber context and are also backed by State practice.[285] For instance, the U.S. Department of Defense (DoD) has taken the position that long-standing international norms guiding State behavior, both in times of peace and conflict, apply in cyberspace.[286] The DoD's Cyberspace Policy Report emphasizes the criticality of applying the tenets of the law of armed conflict and addresses activities taking place in neutral third countries.[287]

Furthermore, the recent HPCR Manual has acknowledged the applicability of the law of neutrality to cyberspace, and its endorsement by a considerable number of governments reflects the consensus of those States on the issues it addresses.[288] However, it is worth noting that the traditional rules of the law of neutrality, while generally applicable to cyberspace, might require clarification or even modification due to cyberspace's unique characteristics.

Nevertheless, there is a position that is becoming more common that argues the complete application of IHL to internet within the community of like-minded Western States. It follows for these States that the concept of neutrality, as a fundamental tenet of IHL, has full application in the context of cyberspace and cyber operations.

The ICJ's 1996 Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons provides the rationale for expanding the application of the concept of neutrality

---

[284] Ibidem.
[285] Walker, George K. "Information warfare and neutrality." Vand. J. Transnat'l L. 33 (2000); Todd, Graham H. "Armed attack in cyberspace: deterring asymmetric warfare with an asymmetric definition." AFL Rev. 64 (2009): 65.
[286] United States. Department of Defense. Department of Defense Strategy for Operating in Cyberspace. DIANE Publishing, 2012.
[287] Ibidem.
[288] Harvard School of Public Health. Program on Humanitarian Policy, and Conflict Research. HPCR manual on international law applicable to air and missile warfare. Cambridge University Press, 2013.

to cyberspace.[289] In this advisory opinion, the ICJ unequivocally stated that the principle of neutrality, whatever its precise definition may be, is applicable to all international armed conflicts, regardless of the type of weaponry used.

While acknowledging the extensive applicability of established international law, such as the law of neutrality, it becomes more difficult to define if, how, when, and how much these existing legal frameworks apply to the realm of cyberspace. This process is expected to develop gradually, affected by a combination of talks, official declarations, State practices, and codification, as noted by the OEWG. Regarding the law of neutrality, historical precedent suggests that the creation of obligations and regulations has often followed years of state practice and legal actions, such as we identified in the 'lifecycle of norms' by Finnemore[290] and as shown in the 1871 Alabama arbitration[291] or the Corfu Channel case[292] decided by the ICJ in 1949. Examining State practices and legal opinions is frequently required in order to demonstrate the internalization of a norm of international law. Therefore, identifying customary neutrality principles that apply to cyberspace requires assessing whether there is a significant, pervasive, and consistent pattern of State practice, as well as an Opinio Juris that specifically addresses the applicability and content of the law of neutrality in cyberspace.[293] According to State practice, there haven't yet been any instances when a State openly alleged that a belligerent had violated its neutrality after a cyber operation. Additionally, relatively few States have publicly expressed their views on how international law should be applied to cyberspace, albeit this tendency is rapidly changing, in part because the OEWG's final report recommends publishing legal opinions.[294]

States that uphold permanent neutrality must also be subject to certain responsibilities. These responsibilities, in particular, include a responsibility "not to accept

[289] International Court of Justice (ICJ), Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996, p. 226, 8 July 1996, available at: https://www.refworld.org/cases,ICJ,4b2913d62.html
[290] Finnemore, Martha, and Kathryn Sikkink. "International norm dynamics and political change." International organization 52.4 (1998): pp. 887-917.
[291] Bingham, Tom. "The Alabama claims arbitration." International & Comparative Law Quarterly 54.1 (2005): 1-25.
[292] Wright, Quincy. "The corfu channel case." American Journal of International Law 43.3 (1949): 491-494.
[293] Neuman, Noam. "Neutrality and Cyberspace: Bridging the Gap between Theory and Reality." International Law Studies 97.1 (2021): 33.
[294] UN OEWG in 2023 - DW Observatory. (1998, September 30). Digital Watch Observatory. https://dig.watch/processes/un-gge

any military obligations and to refrain from acts which would make the fulfilment of its obligations of neutrality impossible should the armed conflict occur"[295]. But how these commitments from peacetime are applied to the online environment is still largely unexplored. The best way to specify these commitments would be through the policies and procedures that the neutral States themselves establish, or through joint efforts on the part of the international community. However, it is clear that permanent neutral States are typically not allowed to join military alliances or make other commitments having a military component relevant to cyberspace. Therefore, multilateral cooperation on non-military aspects, such as discussions of international law or the development of norms, should be legally permissible for permanent neutral States, even though NATO membership is categorically excluded. A number of such countries, such as Switzerland, Finland, Austria, and Sweden, already engage in multilateral processes without having their neutrality policies violated. Although such cooperation arrangements may not legally involve military duties, it is important to keep in mind that they may nonetheless have an impact on the political standing of permanent neutral States. They can simultaneously contribute to improving their capabilities and perhaps to deterrent postures. As a result, depending on each neutral State's chosen neutrality posture and unique national interests and goals, the level of cooperation on cyber-related issues is likely to vary.

Neutral States are obligated to uphold a negative obligation of non-participation in order to protect their right to territorial inviolability. This translates to a ban on engaging in cyber activities or acts that directly or indirectly aid one belligerent's military objectives at the expense of another in cyberspace.[296] This responsibility would include things like conducting cyber operations against the belligerents or offering them military support, including the use of cyberweapons or the hiring of cyber proxies. Governments may use proxies to maintain plausible denial throughout a war; this tactic is particularly common in the cyberspace, as demonstrated by the participation of Russian patriotic hackers in conflicts involving Estonia, Georgia, and Ukraine. Notably, Article 6 of Hague Convention V (HC V) states that neutral States are exempt from liability when "persons cross the

[295] Bothe, M. (2013). The Law of Neutrality, in The Handbook of International Humanitarian Law, 3rd edn, edited by Dieter Fleck (Oxford: Oxford University Press), p. 554

[296] Heintschel, Wolff, and Von Heinegg. "Benevolent third states in international armed conflicts: the Myth of the irrelevance of the law of neutrality." International Law and Armed Conflict: Exploring the Faultlines. Brill Nijhoff, 2007. 543-568.

frontier separately to offer their services to one of the belligerents."[297] This is also the case for the Ukrainian IT Army, which refers to a collective of individuals, including both international and Ukrainian volunteer hackers, who collaborate with Ukrainian defense ministry authorities. Their primary objective is to engage with and potentially disrupt Russian infrastructure and websites. This group operates through a Telegram channel, where they regularly compile and share lists of potential Russian targets for willing volunteers to undertake cyber activities against.[298] There has been some academic interest in revisiting Article 4 of HC V because it states that "corps of combatants cannot be formed nor recruiting agencies opened on the territory of a neutral power to assist the belligerents."[299] This is due to the prevalence of malicious campaigns organized by Advanced Persistent Threats (APTs) and other proxies. This poses a number of concerns when applied to cyberspace and cyberwarfare.

First off, figuring out the level of government encouragement necessary for a behavior to qualify as recruiting may be difficult, especially when it comes to online recruitment, where attribution can be especially difficult. Second, only organizations structured within a military framework are covered by Article 4 of HC V. This distinction becomes crucial when determining whether organizations of neutral individuals, either patriotic or potentially contracted hacking gangs, may be categorized as such. They could be held accountable for this responsibility, for example, if it can be proven that a group of hacktivists employs a hierarchical organization and a distinct line of command.[300] However, hacktivists would probably not be covered under Article 4 HC V if they operate in a decentralized, dispersed, or self-imposed framework. By extension, this clause would not apply to lone hacktivists who choose to participate in online activities after receiving an anonymous call to action (such as in Ukraine). [301] Such people would be regarded as volunteers under international law. Thirdly, Article 4 HC V does not specifically address the status of lone volunteers who do not serve in the armed services but conduct operations

[297] Levie, Howard S. "1907 HAGUE CONVENTION V RESPECTING THE RIGHTS AND DUTIES OF NEUTRAL POWERS AND PERSONS IN CASE OF WAR ON LAND (18 October 1907)." International Law Studies 60.1 (1979): 36.
[298] Connect the dots on State-Sponsored Cyber Incidents - Ukrainian IT Army. Council on Foreign Relations. https://www.cfr.org/cyber-operations/ukrainian-it-army
[299] Ibidem.
[300] Ibidem.
[301] Ibidem.

from neutral territory.[302] Volunteers would generally come under Article 6 HC V in this situation. Roscini points out that Article 6 does not take into account instances in which volunteers do hostile activities (from behind their computers) on neutral territory without actually crossing the border.[303] However, neutral States are bound by a preventative responsibility under Article 5 HC V, which forbids them from tolerating any hostilities on their soil without identifying the perpetrator.[304] As a result, it is conceivable to speculate or presume that this provision may be expanded to include crimes committed by volunteers acting from neutral territory.[305] Fourthly, whether or not these contractors took part in acts that amounted to direct hostilities depends on the extent to which the hiring of private contractors or mercenaries by a belligerent within neutral territory breaches Article 4 HC V.[306] If this is not the case, then, in accordance with Roscini, the scenario would come under the neutrality laws governing business contacts between neutral States and belligerents, and it would be legal provided that it is carried out impartially.[307] A breach of Article 4 HC V or a foundation for legal attribution are unlikely to result from political alignment and shared operational aims, even if they may be sufficient for political attribution.

Last but not least, neutral citizens lose their protected status in both situations—corps of combatants or volunteers—once they engage in hostile acts against a belligerent or enlist, as stated in Article 17 HC V on the Legality of the Threat or Use of Nuclear Weapons. [308]

Due Diligence

As the world witnessed the rise of interconnectedness and the advent of cyberspace, conflicts and transnational activities underwent a transformative change. In response,

[302] Ibidem.
[303] Roscini, Marco. Cyber operations and the use of force in international law. Oxford University Press, USA, 2014.
[304] Levie, Howard S. "1907 HAGUE CONVENTION V RESPECTING THE RIGHTS AND DUTIES OF NEUTRAL POWERS AND PERSONS IN CASE OF WAR ON LAND (18 October 1907)." International Law Studies 60.1 (1979)
[305] Roscini, Marco. Cyber operations and the use of force in international law. Oxford University Press, USA, 2014.
[306] Levie, Howard S. "1907 HAGUE CONVENTION V RESPECTING THE RIGHTS AND DUTIES OF NEUTRAL POWERS AND PERSONS IN CASE OF WAR ON LAND (18 October 1907)." International Law Studies 60.1 (1979)
[307] Ibidem.
[308] Ibidem.

international law adapted to effectively address these contemporary challenges. The law of neutrality, while upholding its core objectives, recognized the importance of adopting a proactive and preventive approach - the due diligence principle.

This evolution created a crucial intersection between the traditional principles of the law of neutrality and the modern concepts of due diligence, offering a comprehensive framework to regulate State and proxy behavior in cyberspace. This framework safeguards the rights and sovereignty of nations while holding States accountable for taking responsible measures to prevent potential harm and violations in the digital realm.

The laws of neutrality were specifically crafted to address the complex and delicate situations that arise in the grey zone around armed conflicts, where due diligence becomes essential in regulating the interactions between belligerents and neutrals who may have disputes related to the conflict but remain at peace with each other. In fact, the concept of due diligence was originally introduced in international law to fulfil this specific function within the laws of neutrality.

Today's challenge is determining whether due diligence requirements apply as particular regulations in cyberspace and, second, if a specialized due diligence system has already emerged for cyberspace. Strangely, the first question appears to have a negative outcome while the second appears to have a positive one.

Due diligence is the norm that governments must follow in order to stop their territory from being used to damage other countries. Indeed, States not only enjoy rights but must also fulfil certain obligations under international law. According to Tallinn Manual Rule 6, “a State must exercise due diligence in not allowing its territory, or territory of cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States.”[309]

Due diligence's position as a legally enforceable norm in cyberspace is still up for controversy and lacks international agreement. When a state wants to stop hostile cyber action but is unable to do so, the question of whether due diligence applies arises,

[309]Schmitt, Michael N. "Due Diligence." Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge UP, 2017. 30-50. Print.

especially when dealing with proxy actors, in regards to activities that are below the "sanctioning" level. The main points of contention in this discussion are whether a state should ask for or approve international help in such circumstances and how much due diligence other governments should exercise. Which acts are still sanctioned and which are deemed to be outside of that scope will depend on the expectations of proper governmental behavior and vigilance.

Additionally, the 2015 UN GGE study included a number of topics important to the debate over due diligence.[310] Firstly, it asserted that (1) "States possess jurisdiction over the ICT infrastructure within their borders" and (2) "States must prevent proxies from committing internationally wrongful acts using ICTs and ensure their territory isn't utilized by non-State actors for such acts." However, the report also introduced qualifications, stating that (3) "merely identifying an ICT activity originating from a State's territory or infrastructure may not be adequate for attribution to that State." It emphasized the need for substantiated evidence when accusing States of wrongful acts. Overall, the UN GGE report's references to proxies and international law suggest its focus on non-state actors operating under a state's effective control.

Various reports and studies have revealed differing viewpoints on the matter. For instance, a report by Duncan Hollis for the Organization of American States in 2020 found that most Latin American States consider due diligence to be binding in cyberspace, but some disagree.[311] Similarly, New Zealand has expressed uncertainty about the crystallization of a specific 'due diligence' obligation in international law.[312] The views of the USA and six European States on the law of cyberspace also differ, with five States agreeing to a binding due diligence norm, while the USA and the UK have not publicly committed to that position.[313]

---

[310] United Nations Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", A/70/174, July 22, 2015.

[311] Hollis, D. "Improving Transparency. International Law and State Cyber Operations. Fourth report to the Organization of American States. OEA/Ser. Q. CJI/doc. 603/20." (2020).

[312] Tanzi, Attila, et al. International Law and Cyberspace. Ministry of Foreign Affairs and International Cooperation, (2021). https://www.esteri.it/wp-content/uploads/2021/12/UNIBO_Applicazione-dei-principi-della-Carta-delle-Nazioni-Unite-nello-spazio-cibernetico.pdf.

[313] Ibidem.

The endorsement of the US government could significantly impact the debate, given its global political and technological influence, but so far, Washington has been reluctant to take such a stance. The United Nations' Institute for Disarmament Research (UNIDIR) paper from November 2021 also highlights the divergent positions of States regarding the voluntary nature, rule, or principle of due diligence as an international law norm in cyberspace.[314]

Interestingly, in multilateral documents, States appear united in their desire to create a specialized due diligence regime for cyberspace, while simultaneously denying the norm's binding nature. For instance, the 2015 UN GGE's report endorsed by the Group of Seven and the Group of Twenty organizations uses language that echoes the classic formulation of due diligence duties in the 1949 Corfu Channel case.[315] However, the use of 'should' instead of 'must' indicates that it is a recommendation rather than a binding law.[316] The report consequently includes a wider variety of players than only those who are effectively under the authority of a state because it does not identify the type of actor or degree of control.

Critics, including Francois Delerue, argue that while new specific rules reflecting the governance needs of cyberspace may be necessary, there is no reason to assume that a new field of international law begins without pre-existing legal duties.[317] Nevertheless, the community of States has treated the due diligence norm in cyberspace as voluntary and non-binding, adding to the complexity of the debate.

In some cases, opposition to due diligence in cyberspace extends further, with the OEWG removing and relegating the section on due diligence in its final report in March 2021.[318] Diplomats involved in the drafting process confirm that although a majority of

---

[314] UNIDIR, "Due diligence in cyberspace: Normative expectations of reciprocal protection of international legal rights", (2021), https://www.unidir.org/publication/due-diligence-cyberspace-normative-expectations-reciprocal-protection-international

[315] Wright, Quincy. "The corfu channel case." American Journal of International Law 43.3 (1949): 491-494.

[316] United Nations Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", A/70/174, July 22, 2015.

[317] Delerue, François. Cyber operations and international law. Vol. 146. Cambridge University Press, 2020.

[318] Assembly, UN General. "Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security." (2021).

States support due diligence, it was sacrificed to ensure universal agreement on the final document, with the wording weakened to “should seek to ensure” rather than "should."[319]

The necessity for states to take preventative action is not discussed in the 2015 UNGGE report. Schmitt and Watts note that there is disagreement over whether governments are required to "prevent cyber infrastructure within their borders from being used for activities that violate obligations to other states" as part of their due diligence. They contend that the more advantageous position is that nations should only be compelled to halt current or impending cyber activities, and that in doing so, they should take whatever steps are deemed acceptable in the particular situation.[320]

Some powerful States express apprehension about the due diligence norm in cyberspace, fearing potential future burdens resulting from detailed requirements. As a result, there is limited interest in precisely defining the current scope of the norm in multilateral documents. The lack of consensus on the norm's scope, knowledge conditions, standards, and thresholds, is evident in various States' ambiguous language.[321] Even the five States acknowledging a binding due diligence norm relied on vague terms, emphasizing the need for "reasonable measures" without providing specific details.[322] The Tallinn Manual 2.0, compiled by experts in 2017, serves as a valuable guide, but it too highlights the unsettled nature of the due diligence principle's precise scope of action. While the Manual discusses numerous actions States could take to fulfil their due diligence duty, it refrains from endorsing any as binding requirements. Interestingly, it deviates from UN-sponsored texts by asserting that a State must exercise due diligence in preventing its territory or cyber infrastructure under its governmental control from being used for cyber operations that adversely affect other States' rights.[323]

During the drafting process, concerned States ensured that due diligence obligations remained non-binding, leading to its exclusion from the final version of the OEWG's

---

[319] Ibidem.
[320] Schmitt, Michael N., and Sean Watts. "Beyond state-centrism: international law and non-state actors in cyberspace." Journal of Conflict and Security Law 21.3 (2016): 595-611.
[321] See note 252
[322] Tanzi, Attila, et al. International Law and Cyberspace. Ministry of Foreign Affairs and International Cooperation, (2021). https://www.esteri.it/wp-content/uploads/2021/12/UNIBO_Applicazione-dei-principi-della-Carta-delle-Nazioni-Unite-nello-spazio-cibernetico.pdf.
[323] Schmitt, Michael N., ed. Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press, 2017.

report. However, its reappearance in the UN GGE report published shortly afterward was notable. Nevertheless, the expression of the norm remained vague, merely stating that it raises the expectation that a State will take reasonable steps within its capacity to end ongoing activity in its territory.

The lack of clarity on the expected "reasonable efforts" for due diligence obligations hinders cyber capacity building and escalates risks in future cyber conflicts. The absence of agreed legal foundations increases the likelihood of tensions and escalation when dealing with cyber operations routed through third States. Hence, there is a clear and precise need for clarity on responsible State behavior in cyberspace in order to avoid potential crises and minimize risks of escalation.

Conclusion

The examination conducted in this article has brought to light the unique complexities presented by cyberspace, which pose obstacles in establishing clear standards to govern State conduct. The intricate and multifaceted nature of cyberspace makes it challenging to apply certain traditional international principles, resulting in areas where rules and principles remain unsettled, commonly referred to as ‘grey zones.’ These grey zones impede the regulation of State and non-State actors’ behavior in cyberspace, making them a focal point in addressing the research question (I). What are the normative foundations of the cyber proxy wars regulations?

In this chapter, we have explored crucial areas of contention within cyberspace, including sovereignty, attribution, the use of force and self-defence, and the law of neutrality. Each of these aspects contributes to the complexity of governing State conduct in cyberspace and necessitates thorough examination to establish effective governance. The interplay between these areas and the challenges they present underscores the importance of comprehensive approaches to tackle State behavior in cyberspace.

As we navigate the complexities of regulating cyberspace, it becomes evident that States must actively express their perspectives not only on the applicability of international legal regimes in cyberspace but also on the implementation of specific rules. Effectively managing cyberspace requires continuous dialogue and collaboration among States to

develop coherent and robust frameworks that can adapt to the dynamic nature of cyberspace.

In conclusion, the emergence of non-State actors and State proxies in cyberspace create a need for proactive and cooperative efforts from the international community to address the grey zones and challenges that hinder the regulation of State and proxy behavior. By conducting a comprehensive analysis of contentious areas and their implications on broader aspects of international law, States can establish a more secure and stable cyberspace environment, promoting responsible behavior and upholding international law principles in the digital realm.

Chapter 4: Case study: UN GGEs, OEWGs and OSCE negotiations on the regulation of cyberspace and proxy wars

In recent years, global attention has increasingly focused on the conduct of States in cyberspace, particularly their use of cyberattacks through State proxies, in relation to international peace and security. While cyber proxy wars are a significant concern, international forums, such as the UN, have placed a stronger emphasis on examining State behavior in cyberspace.

The first forum to confront this new and upcoming threat was within the United Nations, here from 2004 to 2021 the UN GGE was established. Presently, the focus has shifted toward the activities of the UN OEWG, established in 2021, on security and use of information and communications technologies. Furthermore, diverse multilateral organizations, encompassing regional and trans-regional entities like the Organization for Security and Cooperation in Europe (OSCE), have made noteworthy contributions to the global discourse on cyber matters thanks to their cyber confidence building measures (CBMs).

This chapter undertakes an examination of three case studies of cyber norm processes: the GGE, the OEWG, and the OSCE's measures pertaining to Cyber/ICT Security. This exploration allows for a comprehensive understanding of the development and evolution of norms within the realm of cybersecurity and the broader context of international relations.

The UN GGEs

The UN talks on cyber norms date back nearly to the creation of the World Wide Web. The beginning of the 1990s saw the rise of the United States to a dominating position in technical development, which was reflected in its military superiority, underscoring the fundamental significance of technology in the political-military setting. Given this emerging position of the United States in ICTs, the Russian Federation suggested in 1998 that ICT concerns be discussed in the context of global security at the UN. The optimum course of action was determined to be the formation of a Group of Governmental Experts

under the Disarmament Committee after many attempts to launch discussions using various UN forums. Therefore, in order to examine dangers and potential cooperation actions in cyberspace, the GGE was established, according to a UN General Assembly (UNGA) resolution that the Russian Federation sponsored in 2002.[324]

Since its establishment the GGE was one of the more restrictive and State-centric approaches to cyber standards, only allowing experts from 15 States to participate in the meetings. This number was then increased to 20 in 2015 and to 25 in 2017. Additionally, representatives from 25 member States' governments were represented in the 2019 sessions.[325] Representatives chosen by each of the five permanent members of the UN Security Council make up the GGE's 17 members. The remaining experts are picked by their governments after the States are chosen from a list of applicants by the Office of the High Representative for Disarmament Affairs based on attaining an equal geographic distribution, among other criteria.

The GGE process is based around consensus. Each GGE has issued a consensus report, marking important advancements in the discussion of global standards for cyberspace. GGE meetings are held in secret session, and neither official nor unofficial observers are present.[326] Nevertheless, the group announced in 2018 that it would conduct six discussions with regional groups, notably with the Organization for Security Cooperation in Europe, to increase its regional outreach efforts.[327] There have been six GGEs on cyber issues since 2004.

The first GGE to address cyber issues met in 2004. Due to a number of reasons, this initial effort did not result in a consensus report. Notably, the permanent members of the UN Security Council were reluctant to support the report's recommendations, and at that

---

[324] Assembly, General. "Resolution adopted by the General Assembly." Agenda 21.7 (2002): 11, at https://digitallibrary.un.org/record/453522?ln=en#record-files-collapse-header

[325]The list of 2019–2021 States with GGE members is 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, United States, and Uruguay.

[326] UN OEWG in 2023 - DW Observatory. (1998, September 30). Digital Watch Observatory. https://dig.watch/processes/un-gge

[327] UN. General Assembly (73rd sess. : 2018-2019). (2018, December 11). Developments in the field of information and telecommunications in the context of international security :: resolution /: adopted by the General Assembly. United Nations Digital Library System. https://digitallibrary.un.org/record/1655670?ln=en

time there was little interest worldwide in matters pertaining to cyber stability. In fact, few influential decision-makers, diplomats, and military leaders were aware of cyber risks until 2007. In both the public and commercial sectors, information security teams and IT departments were responsible for managing cybersecurity. [328]

The tipping point occurred in 2007, when a series of cyber operations started to unsettle the general opinion on the strategic dangers associated with the cyber domain. For instance, Estonia was the subject of a significant cyber operation that caused extensive digital disruptions.[329] This incident served as a wake-up call, highlighting the potential for cyberattacks and hybrid techniques to advance foreign policy goals when used within a geopolitical context. Senior decision-makers in the fields of foreign and security policy began to pay close attention to cybersecurity. The confrontation between Russia and Georgia in 2008 also witnessed the use of cyber operations, underscoring the strategic importance of these actions in contemporary warfare.[330]

Following these events, the UN GGE process started to gain momentum. 2009 saw the start of the UN GGE's second session, which had the mandate to "...continue to study existing and potential threats in the sphere of information security and possible cooperative measures to address them."[331] This era, which emerged against the backdrop of an increasing number of serious cyber events, represented the real beginning of defining boundaries for State action in cyberspace.

The conclusion of the 2009–2010 GGE negotiations was a suggestion for continuous State-to-State discussions targeted at risk mitigation and the protection of vital infrastructure. Additionally, the section on suggestions underlined the significance of "confidence-building, stability, and risk reduction measures to address the implications of State use of ICTs."[332]

---

[328] Tiirma-Klaar, H. "The Evolution of the UN Group of Governmental Experts on Cyber Issues from a Marginal Group to a Major International Security Norm-Setting Body." Cyberstability Paper Series (2021).
[329] Ottis, Rain. "Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective." Proceedings of the 7th European Conference on Information Warfare. Reading, MA: Academic Publishing Limited, 2008.
[330] Markoff, John. "Before the gunfire, cyberattacks." New York Times 12 (2008): 27-28.
[331] 2010 UN GGE - Report of the group of governmental experts on developments in the field of information and telecommunications in the context of international security (A/70/174) (res. A/65/201) | Digital Watch Observatory. Digital Watch Observatory. https://dig.watch/resource/un-gge-report-2010-res-a65201
[332] Ibidem.

The 2009–2010 process was crucial in building a developing global cyber community and in identifying a group of countries that devoted time and money in developing global regulations for State behavior in cyberspace. It also established a precedent by bringing cybersecurity problems up on the international security agenda of the UN First Committee, thereby refuting the idea that cybersecurity was only relevant in secret server rooms.[333]

Moving forward, the GGE for 2012–2013 reached an unparalleled level of agreement on the application of international law, including the UN Charter, in both online and offline contexts. This report made reference to all four crucial elements that would later lay the groundwork for responsible State activity in cyberspace.[334] The declaration States that international law is applicable in cyberspace, including the UN Charter and the Universal Declaration of Human Rights, that "the application of norms derived from existing international law relevant to the use of ICTs by States is an essential measure to reduce risks to international peace, security, and stability."[335] Moreover, three crucial duties for State behaviour are encapsulated in paragraph 23 and, as we have seen in the previous chapter on international law, are still relevant: "States must uphold their international responsibilities with regard to international crimes that are imputed to them. States shall not commit international unlawful actions through the use of proxies. States should take proactive measures to prevent non-State entities from using ICTs illegally on their territory.[336]

The 2013 report remained ambiguous in its practical application but, nevertheless, paved the way for the 2015 report, which is considered one of the most important documents setting boundaries of norm behavior in cyberspace.[337]

One of the most important contributions to the control of State behavior in cyberspace is the 2014-2015 GGE report.[338] In this report, 11 voluntary standards for

---

[333] Ibidem.

[334]"Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," United Nations , June 24, 2013, UN Doc. A/68/98

[335] Ibidem.

[336] Ibidem.

[337] Tiirma-Klaar, H. "The Evolution of the UN Group of Governmental Experts on Cyber Issues from a Marginal Group to a Major International Security Norm-Setting Body." Cyberstability Paper Series (2021).

responsible State behavior in times of peace were developed. These norms include promises to cooperate in cyber incidents, refrain from actions that may harm vital infrastructure, and safeguard computer incident response teams. Compared to the 2013 report, it also included new components including attribution, supplier chain, and vulnerability disclosure. The recommendations for efforts to boost confidence and capability were also strongly shown.[339]

Fig.2: The UN norms of responsible State behaviour in cyberspace

Source: Australian Strategic Policy Institute, 2022.

Despite initial optimism, a number of issues contributed to the 2016–2017 GGE discussions' failure to come to an agreement, including disagreements over international law and rising geopolitical tensions, which were particularly worsened by Russia's interference in the 2016 U.S. presidential election.[340]

The need to revive the conversation on cyber rules lasted throughout the 2018 UNGA73 session. The fallout from the earlier failure, however, threw a pall over current discussions. Two cyber resolutions were presented at this time, one by the United States and the other by Russia. In addition to a separate annex summarizing State contributions on the application of international law in cyberspace, the U.S. resolution called for the formation of a new GGE to offer implementation insights for agreed standards.[341]

---

[338] United Nations Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", A/70/174, July 22, 2015.

[339] Ibidem.

[340] Tiirma-Klaar, H. "The Evolution of the UN Group of Governmental Experts on Cyber Issues from a Marginal Group to a Major International Security Norm-Setting Body." Cyberstability Paper Series (2021).

[341] Developments in the field of information and telecommunications in the context of international security – UNODA. 2018. A/RES/73/27, https://disarmament.unoda.org/ict-security/

The establishment of the extensive OEWG, on the other hand, was proposed in Russia's resolution, as elaborated in the subsequent section. An essential milestone in these negotiations occurred when the international law matter was ultimately addressed during the GGE meetings in 2021. It's worth noting that while an official compendium of positions was acknowledged, it is essential to recognize that these positions exhibit significant diversity.[342]

To build on the GGE 2019–2021 agreement, countries taking part in the conference had substantial OEWG deliberations in September 2019. They aimed to maintain successes and highlight the worth of the present GGE. Representatives emphasized the four established principles from prior GGEs as a guiding framework at the OEWG session, demonstrating international unanimity. The European Union's member States formally enacted the 'acquis,' their previously reached GGE agreement. The GGE concentrated on responsible State behavior norms within a smaller group, while the inclusive OEWG sought to foster awareness and consensus on international law, norms, confidence-building, and capacity-building. Despite initial reservations about the OEWG formation, optimism grew as two complementary processes emerged.[343]

The 2019-2020 GGE was disrupted by the surging COVID-19 pandemic. Yet, the final report of the GGE might be viewed as a singular success of multilateral diplomacy, with advances perceived by all participants to the negotiations. Important references to international law, in-depth text on crediting others, and standards for protecting important infrastructure were all secured by Western nations. Russia was successfully included a reference to the new OEWG, while China was achieved its desired wording on supply chains. The report's recommendations for more collaboration, consultations, and capacity-building features were well received by developing nations.[344]

---

[342] Assembly, UN General. "Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution (2021)." (2021).

[343] UN OEWG in 2023 - DW Observatory. (1998a, September 30). Digital Watch Observatory. https://dig.watch/processes/un-gge

[344] Tiirma-Klaar, H. "The Evolution of the UN Group of Governmental Experts on Cyber Issues from a Marginal Group to a Major International Security Norm-Setting Body." Cyberstability Paper Series (2021).

In a broader assessment, it can be concluded that the GGEs attained consensus under specific geopolitical circumstances marked by relatively low tensions among major powers or shared interests that encouraged agreement. The successful negotiation outcomes were influenced by various factors, including the competence of the chairs, group members' expectations, regional dynamics, effective behind-the-scenes discussions, and the growing expertise of GGE participants.

It is debatable, nevertheless, whether the GGE reports genuinely have any norm-setting authority. Action that is otherwise compliant with international law is not something that norms attempt to restrict or forbid. It's interesting to notice that rules "allow the international community to assess the activities of States" according to the GGE 2015 and OEWG 2021 reports, yet this statement is absent from the GGE 2021 report. The GGE process as viewed via Finnemore and Sikkink's model further emphasizes how early in the cycle these standards are. It is not yet obvious if a wide variety of governments have embraced these norms, even though the 2015 GGE study shows a process of socialization and activity by norm entrepreneurs. But a norm cascade is frequently made possible by the institutionalization of norms through international laws and organizations. By defining their substance and what constitutes a breach, the ongoing GGE process may push nations to adopt these standards.[345]

GGE and Proxies

The UN GGE reports from 2013, 2015, and 2021 constitute valuable sources of information regarding the international community's perspective on establishing guidelines for responsible conduct in cyberspace, particularly concerning the role of proxy actors. These reports have significantly contributed to shaping the discourse surrounding norms in cyberspace. Notably, they articulate the principle that states should refrain from employing proxies to “commit internationally wrongful acts using ICTs,” and emphasize the importance of states' efforts to prevent such acts from originating within their territorial jurisdiction. This unequivocal stance underscores the applicability of international law in

[345] Martha Finnemore and Kathryn Sikkink, “International Norm Dynamics and Political Change,” International Organization, (1998).

the digital realm, aligning it with conventional legal frameworks applicable in offline contexts.[346]

However, it is essential to highlight that none of the UN GGE reports provide an explicit definition of the term “proxy”. Consequently, the term presents challenges when translating it into other languages, thereby affecting its precise interpretation. For instance, the Russian version of the 2013 report uses the terms "посредников" and "представителей," which can be translated as "intermediary" or "middleman."[347] Furthermore, it elaborates on a proxy as an entity that "acts in the interests of states." Similarly, the Arabic version can be interpreted as referring to "entities acting on behalf of states" or "indirect means/ways." While comprehensive information concerning the diverse interpretations of the UN GGE language on proxies by different states remains largely undisclosed, certain details regarding the United States government's understanding of this term are available. During a workshop in 2012, focusing on proxy actors in cyberspace and hosted by the ASEAN Regional Forum in Vietnam, Dr. Sharri Clark, a foreign service officer at the U.S. Department of State, delineated proxy actors as "groups and individuals who, on behalf of a state take malicious cyber actions against the governments, the private sector, and citizens of other states".[348]

Subsequently, in a speech delivered at the National Security Agency (NSA) later in the same year, Harold Hongju Koh, who served as the 22nd Legal Adviser of the U.S. Department of State at the time, expounded on the legal responsibilities of states regarding activities conducted through "proxy actors."[349] He argued that states are legally liable for the deeds of nominally private individuals acting on the orders of, or under the authority of, the state. Koh underlined that existing international law covers the issue of proxy actors even in the area of cyber operations, where it is possible to mask one's name and location

[346] United Nations, “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, UN Doc. A/68/98; United Nations Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, “Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security”, A/70/174, July 22, 2015.

[347] Организация Объединенных Наций, “Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности”, June 24, 2013, UN Doc. A/68/98.

[348] Co-Chairs’ Summary Report ARF Workshop on Proxy Actors in Cyberspace. Hoi An City, Vietnam. 15/03/2012

[349] Hongju Koh, Harold. "International law in cyberspace." (2012).

and problems with attribution may develop. When a state has extensive control over nominally private persons or groups that conduct international crimes, the state is held accountable for those crimes in the same way that it would be if its official agents had committed the crimes themselves. These legal rules are designed to prevent nations from escaping responsibility for their international crimes by using purportedly private individuals.

However, compared to the UN GGE process, the reports produced by the OEWG do not provide as much insight into the topic of cyber proxies. In fact, the OEWG has not yet produced any documents or reports that mention the subject of cyber proxies.

The UN OEWGs

The establishment of the OEWG was a turning point in the evolution of cyber norms since it provided a forum accessible to all UN members and even allowed non-State actors to participate during its intersessional discussions. However, there were early difficulties with this technique. The simultaneous sponsorship of the GGE by the US and of the OEWG by Russia hinted to possible conflicts between the two initiatives. It seemed that improvements made in one area may encounter opposition or counterproductive recommendations in the other, adding to the complicated dynamic between the two forums.[350]

Unlike the GGE's twenty-five handpicked member States, the OEWG was open to all interested UN member States. The OEWG's mandate is similar to, yet slightly broader than, the 2019–2021 GGE. The OEWG has been given a number of important duties that together will help shape the future of responsible State conduct in the cyberspace environment.

The OEWG is first and foremost concerned with the ongoing creation and improvement of the standards, norms, and principles guiding responsible State behavior. International cyber exchanges are founded upon these principles, which are reflected in the

[350] Ruhl, Christian, et al. Cyberspace and geopolitics: Assessing global cybersecurity norm processes at a crossroads. Carnegie Endowment for International Peace., 2020.

2015 UN GGE guidelines. The OEWG's duty includes improving these norms as well as producing feasible plans for their efficient application.[351]

The OEWG has the power to recommend changes to the current standards or even whole new codes of conduct, in keeping with the dynamic character of cyberspace. This adaptability is crucial in addressing emerging challenges and staying ahead of the curve in an environment characterized by rapid technological advancements. [352]

The OEWG is tasked with conducting continuing research on risks affecting information security, which fall within its scope. This comprises a thorough analysis of both current and future cyber hazards.[353]

Examining the complex interactions between international law and how nations use information and communications technology is also a crucial part of the OEWG's mandate. [354]

Moreover, the OEWG focuses on developing confidence-building measures (CBMs).[355] These policies are intended to encourage trust, openness, and collaboration between nations in cyberspace, ultimately fostering stability and responsible online conduct.

Finally, the OEWG acknowledges the significance of enhancing nations' capacities to handle cyber issues. It aims to create strategies for capacity-building and to set standards for international telecommunications. The OEWG helps to a more robust and secure cyber environment by boosting States' technological capabilities and encouraging the adoption of best practices.[356]

The OEWG was also entrusted with developing a Program of Action (PoA) for encouraging responsible State behavior in cyberspace, creating "a permanent UN forum to consider the use of ICTs by States in the context of international security." The PoA will be developed during the OEWG 2021–25 as a permanent, inclusive, action-oriented program,

[351] UN OEWG in 2023 - DW Observatory. (1998a, September 30). Digital Watch Observatory. https://dig.watch/processes/un-gge
[352] Ibidem.
[353] Ibidem.
[354] Ibidem.
[355] Ibidem.
[356] Developments in the field of information and telecommunications in the context of international security – UNODA. 2018. A/RES/73/27, section 5. https://disarmament.unoda.org/ict-security/

in accordance with a resolution adopted by the UNGA during the first committee in 2022.[357]

The PoA is envisioned as a venue where discussion of current and prospective concerns in the area of cyber activities would take precedence. This element emphasizes the necessity of thorough discussion aimed at comprehending the changing environment of digital issues.

In order to execute and advance pledges that are consistent with the general framework for responsible State behavior, the PoA also aims to empower and build State capacities. Beyond implementation, this also includes the potential for going back and improving the framework in light of new dynamics, assuring its flexibility to changing conditions.[358]

The arrangement also highlights the value of interaction and cooperation with a wide variety of stakeholders. This inclusive strategy recognizes the interconnectedness of today's digital concerns and strives to foster synergies among many players engaged in cyber-related initiatives.[359]

Additionally, the PoA's mandate includes regular evaluations of implementation success, encouraging accountability and openness. In addition, the PoA's involvement in determining its future course highlights its potential as a flexible mechanism that may change pace with the quickly shifting cyber scene.[360]

In essence, the creation of the Permanent Organizational Arrangement represents a concerted effort to create a comprehensive and long-lasting framework, able to not only address current cyberthreats but also to support the ongoing development of policies governing State behavior in the digital sphere.

---

[357] Albania et al. (2022, October 13). Programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security :: draft resolution /: 40 states. United Nations Digital Library System. https://digitallibrary.un.org/record/3991743?ln=en
[358] UN OEWG in 2023 - DW Observatory. (1998c, September 30). Digital Watch Observatory. https://dig.watch/processes/un-gge#The-future-process---PoA
[359] Ibidem.
[360] Ibidem.

History

In 2018 the Russian Federation led calls for a new OEWG at the UN, the reasoning behind this was to provide a “more democratic, inclusive, and transparent” process for cyber norms and related efforts.[361] Therefore, in two different UN General Assembly resolutions, member States of the UN authorized both a new GGE and an OEWG, rather than voting to support one procedure over the other. In 2019, the first OEWG meetings began. As a result, the GGE and the OEWG collaborated during 2019–2021 in a variety of contexts, as can be seen in Figure 3 in the Appendix.-On the basis of the OEWG's first substantive meeting and its open multistakeholder structure, workshop attendees expressed hope about its future. The overlapping missions of the GGE and OEWG do, in fact, imply that they may function as a whole that is more effective than the sum of its parts by expanding areas of overlapping agreement in ways that are advantageous to all nation-States. The chairs of the two forums have expressed their knowledge of this potential result and their intention to strive to work toward it in accordance with their respective mandates from the UN General Assembly.[362]

The novelty of the OEWG was that it established a crucial foundation for a more inclusive discussion on global cybersecurity. Over 100 NGOs participated in the session as observers, and 193 nations joined the OEWG.[363]

The OEWG's mandate was to "further develop the rules, norms and principles of responsible behaviour of States," as stated by the GGE, in the resolution that resulted in its formation. [364] The OEWG report, however, omitted important issues and failed to achieve any substantial changes. The absence of references to accountability and international humanitarian law (IHL) being the report's two major omissions.

---

[361] Developments in the field of information and telecommunications in the context of international security – UNODA. 2018. A/RES/73/27, section 5. https://disarmament.unoda.org/ict-security/

[362] Ruhl, Christian, et al. Cyberspace and geopolitics: Assessing global cybersecurity norm processes at a crossroads. Carnegie Endowment for International Peace., 2020.

[363] Hurel, Louise Marie. "The Rocky Road to Cyber Norms at the United Nations." Council on Foreign Relations (2022).

[364] Developments in the field of information and telecommunications in the context of international security – UNODA. 2018. A/RES/73/27, https://disarmament.unoda.org/ict-security/

However, substantial tasks remained to be addressed, prompting the renewal of the OEWG for the period of 2021-2025 following a proposition put forth by the Russian Federation.[365]

This edition was characterized by disagreements owing to the geopolitical events surrounding the sessions. There were several issues of debate, as can be seen in the Annual Progress Report of 2022, which summarized the first, second, and third sessions of the OEWG for 2021-2025.

The talks on norms were concentrated on the strategic decision of whether to stress the adoption of voluntary standards for responsible State conduct that already existed, the development of new standards, or a hybrid of both. States like the USA, Germany, Canada, and the Czech Republic argued primarily in favor of giving the present rules' implementation top priority. They suggested working together to improve their application and commented on pertinent findings and suggestions. Kenya, on the other hand, recommended the establishment of OEWG work groups to exchange best practices, particularly in the contextualization of current laws, customs, and values within national policy. Iran, however, strongly objected to the notion that the recommendations for putting into effect current rules were 'action-oriented.' They said that such language would minimize the significance of creating a legally enforceable instrument and, in turn, would shift the OEWG's attention away from its assigned task. Russia and Iran persisted in their position that new rules are necessary, especially Russia's demand for new, legally enforceable ones, which was opposed by Canada and Mauritius.[366]

In contrast, some nations such as South Africa, Botswana, and the Democratic Republic of the Congo highlighted the incompatibility of creating new rules while also putting them into practice, noting worries about the excessive load it may place on smaller developing nations. The Republic of Korea, Singapore, Peru, Nicaragua, and other nations, on the other hand, expressed support for the adoption of current norms while remaining

[365] Developments in the field of information and telecommunications in the context of international security (A/RES/75/240) | Digital Watch Observatory. (n.d.). Digital Watch Observatory. https://dig.watch/resource/developments-field-information-and-telecommunications-context-international-security

[366] Gavrilovic, A. (2022, December 13). What's new with cybersecurity negotiations: The OEWG 2021–2025 annual report adopted - Diplo. Diplo. https://www.diplomacy.edu/blog/whats-new-with-cybersecurity-negotiations-the-oewg-2021-2025-annual-report-adopted/#top

open to the development of new ones, particularly in areas like the safeguarding of electoral infrastructure and the general integrity and accessibility of the internet.[367]

The discussion of norms included the creation of standard definitions for technical ICT words. Australia opposed the plan, but China, Cuba, Iran, Lao PDR, and Nicaragua supported it. States might disclose their national viewpoints on ICT terms, according to a proposal made by the USA and the Netherlands, to increase transparency.[368]

The fundamental issue of whether voluntary standards are sufficient for international law or if additional legally obligatory commitments are necessary was a recurrent subject. Some nations, like Russia, Pakistan, the Democratic Republic of the Congo, Iran, Egypt, and Nicaragua, stressed how crucial it is to keep talking about a deal that is binding. They claimed that while norms are beneficial in times of peace, they may become ineffective in times of war. IHL has been confirmed to be applicable in cyberspace by Switzerland on behalf of a group of sixteen nations. They argued for talks led by experts under the aegis of the OEWG and emphasized the importance of defining how IHL relates to cyber operations in armed situations. This position was shared by a number of other nations, including the UK, Ecuador, Congo, New Zealand, and others. Cuba and Nicaragua, however, questioned the value of bringing up IHL in the context of ICT usage in international security since they thought it may lead to the militarization of cyberspace.[369]

Numerous viewpoints were expressed throughout the talks on subjects like due diligence. Notably, the OEWG 2021 report included suggestions about the potential for creating a legally binding agreement and addressing the applicability of international humanitarian law in cases of armed conflict. Although more debate on the subject of due diligence was recommended, there was no reference of cyber attribution in the final document.[370]

Similar to the GGE, the OEWG has a mechanism that is housed in the First Committee of the UN and is focused on multilateral agreements and a disarmament attitude. This approach has both merits and disadvantages. However, the OEWG varies

[367] Ibidem.
[368] Ibidem.
[369] Ibidem.
[370] Ibidem.

significantly from the GGE in that it allows for larger involvement in a more open environment. This structure implies the prospect of broader (and speedier) dispersion of the OEWG's results if it can come to an agreement. As a result, this would stimulate the passage from a theoretical norm to a conceptualized and accepted norm, essentially overcoming the 'tipping point' and encouraging norm cascade. However, more States participating in talks may make it more challenging for participants to reach a compromise than in the more intimate, confined environment of the GGE.

The new OEWG's largest task is figuring out how to make progress in the face of widening gaps between Western nations and Russia and China. The OEWG's first year reveals how these geopolitical conflicts have compelled members to exclude stakeholders from meetings and steer clear of in-depth talks. If these and other problems persist, they may jeopardize the work of the present OEWG and limit its ability to pursue initiatives to put cyber standards into effect.

The OSCE

With a membership comprising 57 nations across North America, Europe, and Asia, the OSCE stands as the largest regional security organization globally. The OSCE's primary objective is to foster stability, peace, and democracy by engaging in both political discourse concerning shared values and pragmatic initiatives aimed at creating enduring positive impacts.[371]

Functioning as a platform for political dialogues spanning an array of security concerns, the OSCE serves as a collaborative arena for coordinated efforts to enhance the well-being of individuals and communities. Employing a comprehensive security approach encompassing the politico-military, economic, environmental, and human dimensions, the organization facilitates cooperative endeavors among States, aiming to bridge disparities and establish trust through endeavors related to conflict prevention, crisis management, and post-conflict rehabilitation.

Moreover, the OSCE dedicates attention to security challenges transcending borders, encompassing areas such as climate change, terrorism, radicalization, violent extremism, organized crime, drug trafficking, arms proliferation, human trafficking, and

[371] Who we are. (n.d.). OSCE. https://www.osce.org/who-we-are

cybercrime. Within the realm of cybersecurity, the OSCE confronts diverse cyber threats, encompassing cybercrimes and the exploitation of the Internet for terrorist objectives. Notably, the organization concentrates on formulating CBMs among its participating States, intended to mitigate the likelihood of conflict arising from the utilization of ICTs. [372]

In this context, the OSCE undertakes initiatives to craft voluntary and practical confidence-building measures, striving to curtail conflict risks. This pursuit originated in 2011, when the organization resolved to host a conference to examine the potential role of the OSCE in enhancing cybersecurity. Commencing in 2013, OSCE member States embraced 16 distinct confidence-building measures centered on cyber and ICT security, positioning the OSCE as the inaugural regional entity to establish such measures. The OSCE's pioneering stance continues, as recent United Nations initiatives on international ICT security acknowledge the significance of regional and sub-regional organizations in formulating and executing confidence-building measures within their respective domains.[373]

However, it is important to note that the effectiveness of the OSCE's cybersecurity mechanism has been declining since 2016. Recognizing the need for change, the Russian Foreign Minister, Sergey Lavrov, proposed the so-called "The Peaceful Cyberplan for OSCE" at the 2016 OSCE ministerial council—an annual meeting of OSCE foreign ministers. This plan aimed to make OSCE cyber security activities more fruitful.[374]

Before we analyse them, we must explain what CBMs are and how they differ from what we have discussed so far – norms.

CBMs and Norms

During the Cold War, the initial intent of CBMs was to address particular military concerns and ease tensions between the East and West. In 1955, a UN resolution that was inspired by US President Eisenhower's Open Skies initiative used the phrase for the first

[372] What we do. (n.d.). OSCE. https://www.osce.org/what-we-do
[373] Emerging Practices in Cybersecurity-Related Public-Private Partnerships and Collaboration in OSCE participating States. (2023). OSCE. https://www.osce.org/secretariat/539108
[374] Тасс. (2017, November 3). РФ предложила провести в 2018 году конференцию о роли ОБСЕ в сфере кибербезопасности. ТАСС. https://tass.ru/politika/4701198; also found at https://mid.ru/en/foreign_policy/rso/1556306/

time.[375] CBMs were incorporated into the Helsinki discussions in 1975 by the Conference for Security and Cooperation in Europe (CSCE), the organization that preceded the OSCE.[376] These measures had previously largely consisted of technical agreements related to weapons control, aimed at reducing the threat of European conflict and limiting the political use of military power.

The CSCE, on the other hand, expanded the use of CBMs outside the context of weapons control by supporting their voluntary implementation without official verification. The Helsinki Final Act was a turning point since it inspired several CBMs outside the realm of weapons control. The first generation of accepted and defined CBMs resulted from this process, which allowed Cold War rivals to continuously communicate with one another.[377] A second wave of CBMs resulted from the 1986 Stockholm Document, which shifted the emphasis from capabilities to operational constraints.[378] Surprisingly, this measure also marked the debut of politically and militarily binding CBMs in Europe.

Furthermore, the Vienna Document, which was published in 1990, added routine military contact and quick risk reduction to CBMs.[379] This included the information sharing and verification of military operations and the armed forces. Although the OSCE CBMs from Helsinki were largely focused on 'hard security' concerns, they also included a wider variety of non-military CBMs. These characteristics translated some fundamental cooperative features of fostering confidence into the fields of business and the environment.

Since their creation, CBMs have been used to build confidence and mutual understanding between nations, explaining policies and preventing misunderstandings that might heighten military or political tensions. They encourage partnership-based, cooperative security by facilitating transparency, predictability, and cooperation. These

[375] UN General Assembly Resolution 914 (X) (16 Dec. 1955), https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/103/94/IMG/NR010394.pdf?OpenElement.
[376] Helsinki Final Act, 1975. OSCE. https://www.osce.org/it/mc/39504
[377] Kavanagh, Camino, and Laura Crespo. "Confidence Building Measures and ICT." European Foreign Affairs Review 24.2 (2019).
[378] Document of the Stockholm Conference, 1986. OSCE. https://www.osce.org/fsc/41238
[379] Vienna Document 1990 (it). OSCE. https://www.osce.org/it/fsc/41248

metrics can serve as a guide for prudent activity during tense times, encouraging State behavior principles, cooperative behaviors, and enduring security partnerships.[380]

CBMs assume a new relevance in the changing landscape of global power dynamics, accommodating many governments with the ability to project power. These topics are becoming more and more important as traditional crisis management tactics are put to the test by malevolent international cyber operations and digital interdependence in all types of conflicts.

The current discussions about acceptable State conduct norms are strongly related to the discourse around CBMs in cyberspace. International expectations in cyberspace are governed by norms, but CBMs offer useful instruments for managing and modifying these expectations in accordance with the capabilities of specific States. The operationalization of norms is aided by CBMs, which provide avenues for dialogue, collaboration, and information sharing. For example, the norm which affirms that "States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs"[381] or the Tallinn Manual Rule 6, "a State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States"[382], both establish an understanding that States will employ every tool at their disposal to stop such illegal actions from happening. As a result, it gives States a clear expectation. Such expectations must be modified, nevertheless, to account for the ability of any State to fulfill its duties. Such modifications are made possible by confidence-building tactics, which include creating communication channels, information sharing, and practical collaboration throughout investigations.

It is crucial to understand that while international law has legal force and application to cyberspace, it does not provide a universal answer to the complex problems associated with internet uncertainty. Notably, maintaining peace and stability as well as promoting an open, safe, and accessible ICT environment all depend on international law,

[380] Kavanagh, Camino, and Laura Crespo. "Confidence Building Measures and ICT." European Foreign Affairs Review 24.2 (2019).
[381] Hogeveen, Bart, "The UN norms of responsible state behaviour in cyberspace". The Australian Strategic Policy Institute Limited 2022.
[382] Ibidem.

which is best reflected by the UN Charter. Nevertheless, continuous analyses highlight the need for turning these legal frameworks into actual implementations that operate. CBMs are crucial in this situation because they set the stage for talks and actions. CBMs serve as instruments to make sure that States consistently understand and uphold their normative commitments. In order to foster trust and strengthen adherence to normative frameworks, these measures also operate as platforms for reciprocal interaction, enabling stakeholders to communicate insights regarding shared expectations, practices, and operational methods. [383]

In essence, norms' and CBMs' developmental paths are interconnected and dependent on one another. While norms provide the standards for acceptable State conduct, a suitable combination of CBMs—from those that improve situational awareness to those that promote resilience and encourage collaboration—serves as a practical mechanism for States to meet these standards. This association is comparable to the all-encompassing strategy shown in Table 3.

CBMs on cyber behavior

The OSCE has played a key role in an innovative project that has received official governmental funding and is focused on developing and implementing CBMs. Since 2011, these initiatives, which mostly consist of transparent and cooperative tactics, have been a top priority. As a result, a total of 16 CBMs have been adopted inside the OSCE framework.

The OSCE first acknowledged the growth of cybersecurity risks in declarations and resolutions in 2008 in Astana.[384] The 2011 Belgrade Declaration subsequently pushed for international collaboration, information sharing, and the creation of specialized countermeasures to cyberthreats while attempting to develop universal norms of behavior for cyberspace.[385] Moreover, the Informal Working Group on CBMs related to ICTs, which the OSCE Permanent Council established in 2012, was an unofficial, open-ended working

[383] Pawlak, Patryk. "Confidence-Building Measures in Cyberspace: Current Debates and Trends." International cyber norms: Legal, policy & industry perspectives 20 (2016): 129-153.
[384]OSCEPA, 'Astana Declaration of the OSCE Parliamentary Assembly and Resolution Adopted at the Seventeenth Annual Session' (29 June to 3 July 2008), https://www.oscepa.org/en/documents/annual-sessions/2008-astana/summary-report-11/289-2008-astana-annual-session-report-english/file
[385] OSCEPA, 'Belgrade Declaration of the OSCE Parliamentary Assembly and Resolution Adopted at the Twentieth Annual Session' (6-10 July 2011), https://www.oscepa.org/en/documents/annual-sessions/2011-belgrade/declaration-4/3024-belgrade-declaration-eng/file

group tasked with creating CBMs that promote interstate cooperation, transparency, predictability, stability, and the mitigation of potential risks related to the use of ICTs.[386] At the first meeting of this working group, more than 50 CBM ideas from different participating governments were presented.[387] Eleven CBMs were ultimately adopted.

The proposed CBMs can be broadly classified into three clusters[388]:

- CBMs allowing States to interpret one another's actions in cyberspace (CBMs 1, 4, 7, and 10), enhancing predictability.

- CBMs facilitating timely communication and collaboration to defuse tensions (CBMs 3, 5, and 8).

- CBMs emphasizing national readiness and diligence to address cyber/ICT challenges (CBMs 3, 6, and 8).

The chair gave a brief analysis, focusing on three main types of measures: stability measures to avoid destabilizing actions in cyberspace, cooperative crisis prevention and resolution approaches, and transparency and confidence-building measures for improved predictability. At the 2012 Ministerial Council in Dublin, a proposal for a Ministerial Council resolution on CBMs was put out, but it was rejected because of Russia's reservations. The Istanbul Declaration of 2013 demanded that the OSCE create policies to promote cyber security and reduce the likelihood of cyber war in response.[389] Due to this, a procedure to adopt a set of CBMs was started. This process culminated in Decision N.1106 in December 2013, which accepted a compromise on eleven voluntary CBMs.[390]

With Decision N.1202 in 2016, five new CBMs were added, including national vulnerability reporting, collaboration for the protection of key infrastructure, and the

---

[386] Permanent Council Decision No. 1039, 2012. OSCE. https://www.osce.org/pc/90169

[387] OSCE, 'Follow-Up on Recommendations in the OSCE PA's Monaco Declaration: Final Report for the 2013 Annual Session', https:// www.oscepa.org/documents/all-documents/annual-sessions/2013-istanbul/follow-up-report-3/1782-2013-annual-session-follow-up-final-report-1st-committee-english/file

[388] From: https://aseanregionalforum.asean.org/wp-content/uploads/2019/10/Session-2-Presentation-by-the-OSCE.pdf

[389] OSCE, Istanbul Declaration and Resolution Adopted by the OSCE Parliamentary Assembly at the Twenty-Second Annual Session (2013), https://www.oscepa.org/en/documents/annual-sessions/2013-istanbul/declaration/1801-istanbul-declaration-eng-1/file

[390] Permanent Council Decision No. 1106, 2013. OSCE. https://www.osce.org/pc/109168

creation of secure communication channels to prevent disputes resulting from the use of ICT.[391]

CBM 14 emphasizes the promotion of public-private partnerships on a voluntary basis and the sharing of best practices in response to common security issues brought on by ICT use. This cooperative approach recognizes the need of incorporating diverse stakeholders, notably the commercial sector, in cyber/ICT security and seeks to strengthen cyber resilience and readiness.[392]

In 2017, it was recognized how crucial it is to strengthen the OSCE's efforts to foster trust while reducing tensions brought on by information and communication technology. Hence, a conference titled *Cyber Security for Critical Infrastructure: Strengthening Confidence Building in the OSCE* was organized by the Austrian Chairmanship to promote direct communication between national CBM 8 PoCs and create dependable communication lines among participating nations.[393]

[391] Permanent Council Decision No.1202. (2016). OSCE. https://www.osce.org/it/pc/228511
[392] Emerging Practices in Cybersecurity-Related Public-Private Partnerships and Collaboration in OSCE participating States. (2023). OSCE. https://www.osce.org/secretariat/539108
[393] Austrian OSCE Chairmanship Conference on Cyber Security. (2017). OSCE. https://www.osce.org/event/austrian-cyber-security-2017

Table 3. Comparing Norms, CBMs and Capacity Building.

NORMS			CONFIDENCE-BUILDING MEASURES	CAPACITY-BUILDING
Norms, rules and principles of responsible behaviour (UN GGE 2015 Report)	**Challenges to implementation**		**Applicable measures (UN GGE 2015 and OSCE)**	**Corresponding capacity-building needed**
In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences.	Highly dependent on political agenda and uncertainty. CBMs are useful tools in creating 'positive expectations and good faith where doubts exist.	Facilitating cooperation	· Facilitation of cooperation between relevant national bodies (OSCE and UN GGE)	· Competent institution responsible for cyber security policy · Establishing clear division of labour within national administration
States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs	Proving if a country has known about such acts from their territory is difficult. CBMs help to determine if this is the case.	Improving situational awareness	Sharing information on national organisation, strategies, policies, and programmes (OSCE and UN GGE) · Providing a list of national terminology and definitions related to ICT security (OSCE)	· National cyber security strategy and legislation · Cyber procedures: technical, administrative, and procedural measures to protect systems · Public-private partnerships
States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats.	Such cooperation is usually based on law enforcement cooperation treaties and relatively easy to monitor. Political will might be an obstacle to implementation that needs to be addressed with CBMs.			
States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as UNGA resolutions 68/167 and 69/166 on the right to privacy in the digital age	Relatively easy to verify with regard to freedom of expression but more complicated with regard to protection of privacy online. CBMs can help improve overall climate for cooperation.	Protection of critical ICT infrastructure	· Consultations to prevent political and military tensions and protect critical national ICT infrastructure (OSCE and UN GGE) · Sharing information on categories of infrastructure considered critical and facilitating cross-border cooperation to address their vulnerabilities (UN GGE)	· Risk assessment · Developing standards · Public-private partnerships
States should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public.	This statement leaves untouched activities by non-governmental entities of which governments may be aware but not actively support. CBMs can help clarify State's position and demonstrate good faith.			

States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account UNGA resolution 58/199 on the creation of a global culture of cyber security and the protection of critical information infrastructures, and other relevant resolutions.	Some countries may not have resources to implement concrete legal or technological solutions and be more vulnerable. In such cases capacity-building amounts to an important CBM.	Fight against cyber crime	Put in place modern and effective legislation to facilitate cooperation and effective cross-border cooperation to fight cybercrime and terrorist use of ICTs (OSCE)	· Substantive and procedural laws, criminalisation of certain acts, respect for fundamental freedoms · Sustainable and scalable training for law enforcement, judges, and prosecutors · Forensics · Formal and informal channels of communication
States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, considering due regard for sovereignty.	In practical terms, such requests can be subjected to extended wait-times and undermine position of the addressee country. CBMs can help clarify reasons for possible delays or missing information.			
States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty.	These are often difficult to verify. CBMs like export controls and transparency measures – including cooperation among private sector – can be useful way for diffusing potential tensions.			
States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure.	These are relatively easy to implement through CBMs, if there is enough political will. CBMs at operational level can be more successful.	Building resilience	· Providing contact data of existing national structures that manage ICT-related incidents (OSCE and UN GGE) · Development of focal points for the exchange of information on malicious ICT use and provision of assistance in investigations (UN GGE)	· Computer Emergency Response Teams (CERTs) · 24/7 points of contact · Common protocols for sharing information regarding cyber events
States should not conduct or knowingly support activity to harm the information systems of the authorised emergency response teams of another State. A State should not use authorised emergency response teams to engage in malicious activity.	May be difficult to prove and hence CBMs – both at political and operational level – can help clarify the context and resolve conflicts.			

Source: Pawlak, Patryk. Confidence-Building Measures in Cyberspace*: Current Debates and Trends.* International cyber norms: Legal, policy & industry perspectives 20 (2016): 129-153.

As shown in Table 3, CBMs must be developed in order to guarantee the successful application of certain rules. While allowing a specific State to actively take part in the execution of the CBMs, the scope of CBMs may necessitate participating in capacity-building initiatives to guarantee that specific benchmarks of human, institutional, technological, or legal capability are fulfilled. That also suggests that further standards may need to be defined or agreed upon as capabilities continue to advance. Understanding this prospect is crucial to ensuring that decisions about capacity development do not lead to a future cyber weapons race but rather to a more reliable and stable cyberspace. This is the logic that the OSCE approach appears to be following at this stage.

Conclusion

From early debates to more formalized and inclusive frameworks within the United Nations, the development of standards of responsible state action in cyberspace has been characterized by a continuous growth. These norms have been significantly shaped by the UN GGE's and the OEWG's formation.

A small group of nations' experts from the UN GGE were originally brought together to discuss norms of responsible State behavior in cyberspace. Its membership grew over time, and consensus studies outlining norms were produced. These forums helped establish voluntary standards and directives for State conduct in times of peace. Particularly the 2014–2015 GGE report was a significant accomplishment, adopting 11 rules that prioritized collaboration, infrastructure protection, and cyber incident response.

However, difficulties emerged throughout the GGE negotiations, such as divergent views on international law and escalating geopolitical tensions. As a result, the OEWG was created as a more diverse platform. International law, norms, confidence-building, and capacity-building were all included in the OEWG's reports. Its development reflected the need for more regional and global involvement in establishing cyber rules.

The concurrent existence of the GGE and the OEWG serves as evidence of the complexity of internet norm creation. States are beginning to recognize the importance of collaboration in cyberspace, as seen by the GGE's consensus-based methodology and its effectiveness in establishing standards. Even if the GGE reports' ability to define international norms is still up for discussion, their impact on State conduct and the creation of cyber policies points to a tendency toward doing so.

Cyberspace rules are constantly changing, reflecting the dynamic character of the digital realm. The talks and results of these UN projects continue to be influenced by geopolitical conflicts, technological developments, and changes in international relations. Despite ongoing difficulties, the joint work of the GGE and the OEWG help to define responsible State conduct, promote stability, and guarantee security in the cyberspace.

A further step towards the implementation of norms of responsible State behavior in cyberspace is represented by the CBMs adopted by the OSCE. The history of the Cold War showed us how the adoption and implementation of such measures was crucial to solving issues regarding State behavior in the age of nuclear proliferation. Therefore, following these measures could help us overcome the ‘tipping point’ and lead to ‘norm cascading’.[394]

[394] Finnemore, Martha, and Duncan B. Hollis. "Constructing norms for global cybersecurity." American Journal of International Law 110.3 (2016): 425-479.

Final Remarks

In conclusion, the evolution of cyber proxy warfare and the development of norms regulating it present complex challenges on the global stage. The rise of cyber proxies represents the latest dimension in the ever-evolving landscape of international conflict, introducing multifaceted dynamics that require meticulous consideration and regulation. In response to the second research question (II). “Are the norms regulating cyber proxy wars internalized?”, our answer is that the establishment of norms within the cyber domain is still in its nascent stages, paralleling the initial phase of 'norm emergence' as outlined in the norm life cycle framework proposed by Finnemore and Sikkink.[395]

Delving into our research question, it becomes apparent that the increasing prominence of States and their proxies in cyberspace is reshaping the contemporary international security landscape. Their growing engagement in proxy relationships, driven by a combination of capabilities and political motivations, accentuates the urgency of formulating robust and comprehensive cyber norms. Despite decades of international deliberations dating back to the 1990s and the proliferation of offensive cyber operations, the body of cyber norms remains relatively fragile. While the United Nations' efforts have played a pivotal role in shaping global perceptions of cyberspace standards, significant work lies ahead before these norms advance to the stages of 'cascade' and the 'tipping point,' as described in the norm life cycle.

Our exploration of the second research question affords us the opportunity to delve deeper into the intricacies and obstacles associated with regulating cyberspace. From the vantage point of norms, we have identified a range of soft power dynamics that influence States' adherence to international norms. These include considerations of prudence, reputational costs, and the pressures exerted by national political contexts, all of which play significant roles in shaping State behavior. Furthermore, our examination of the constraints imposed by international legal norms underscores the nuanced challenges presented by traditional principles such as sovereignty, due diligence, and attribution within the context of the cyber age. These complexities are especially pronounced when dealing with non-State actors and State proxies, compelling the international community to adopt proactive

[395] Finnemore, Martha, and Duncan B. Hollis. "Constructing norms for global cybersecurity." American Journal of International Law 110.3 (2016): 425-479.

and cooperative approaches to address the uncertainties and hurdles associated with cyberspace regulation effectively.

Our analysis of the case studies underscores tangible progress in the development of cyber norms, primarily catalysed by the UN GGE and the OEWG. These platforms have played pivotal roles in formulating voluntary standards and guidelines to govern responsible State conduct in cyberspace. Of particular note is the 2014–2015 GGE report, which stands as a significant milestone for its endorsement of 11 rules prioritizing cooperation, critical infrastructure protection, and cyber incident response. However, the path towards robust cyber norms is not without obstacles, including divergent interpretations of international law and escalating geopolitical tensions. These challenges prompted the establishment of the OEWG, highlighting the imperative of broader regional and global engagement in shaping cyber regulations.

Furthermore, the adoption of CBMs by the OSCE signifies a crucial step towards the implementation of norms governing responsible State behavior in cyberspace. Drawing upon the lessons of the Cold War era, these measures offer the potential to surmount the 'tipping point' and foster widespread acceptance of cyber norms.

In summary, while the regulation of cyber proxy warfare and the development of norms remain ongoing and intricate processes, the evidence suggests that progress is being made. The normative life cycle stages of emergence, cascade, and internalization provide a valuable framework for assessing the trajectory of these norms. As cyberspace continues its relentless evolution, and both State and non-State actors adapt to its challenges, the international community must remain resolute in its commitment to proactive and cooperative norm-building efforts. Ultimately, the journey towards the full internalization of norms governing cyber proxy warfare represents a critical endeavor in safeguarding international peace, stability, and security within this dynamic and evolving domain.

Bibliography

- "United Nations Charter, Chapter I: Purposes and Principles". United Nations. 26 June 1945. Retrieved 13 February 2023.
- “Cyber Leaders: A Discussion with the Honorable Eric Rosenbach” (panel discussion, Center for Strategic and International Studies, Washington, DC, October 2, 2014), http://csis.org/event/cyber-leaders.
- 2010 UN GGE - Report of the group of governmental experts on developments in the field of information and telecommunications in the context of international security (A/70/174) (res. A/65/201) | Digital Watch Observatory. Digital Watch Observatory. https://dig.watch/resource/un-gge-report-2010-res-a65201
- Abbott, Kenneth W., et al., eds. International organizations as orchestrators. Cambridge University Press, 2015.
- About ENISA - The European Union Agency for Cybersecurity. ENISA. https://www.enisa.europa.eu/about-enisa
- Albania et al. (2022, October 13). Programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security :: draft resolution /: 40 states. United Nations Digital Library System. https://digitallibrary.un.org/record/3991743?ln=en
- Alexander, K. (n.d.). UNODA Treaties. https://treaties.unoda.org/t/bwc
- ASEAN, 2019, https://aseanregionalforum.asean.org/wp-content/uploads/2019/10/Session-2-Presentation-by-the-OSCE.pdf
- Assembly, General. "Resolution adopted by the General Assembly." Agenda 21.7 (2002): 11, at https://digitallibrary.un.org/record/453522?ln=en#record-files-collapse-header
- Assembly, UN General. "Developments in the field of information and telecommunications in the context of international security." United Nations General Assembly. Search in (2015).
- Assembly, UN General. "Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution (2021)." (2021).
- Assembly, UN General. "Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security." (2021).
- Attorney-General’s Department, Cyber Security Strategy (Canberra: Australian Government, 2009).
- Australian Strategic Policy Institute, 2022.
- Austrian OSCE Chairmanship Conference on Cyber Security. (2017). OSCE. https://www.osce.org/event/austrian-cyber-security-2017
- Beaumont, Peter. "Stuxnet worm heralds new era of global cyberwar." The Guardian 30 (2010).

- Becker, Tal. Terrorism and the state: rethinking the rules of state responsibility. Bloomsbury Publishing, 2006.
- Belk, Robert, and Matthew Noyes. On the use of offensive cyber capabilities: A policy analysis on offensive US cyber policy. JOHN F KENNEDY SCHOOL OF GOVERNMENT CAMBRIDGE MA, 2012.
- Betz, David J. Cyberspace and the State: Towards a Strategy for Cyber-power. Routledge, 2017
- Blank, Laurie R. "Irreconcilable Differences: The Thresholds for Armed Attack and International Armed Conflict." Notre Dame L. Rev. 96 (2020): 249.
- Bothe, M. (2013). The Law of Neutrality, in The Handbook of International Humanitarian Law, 3rd edn, edited by Dieter Fleck (Oxford: Oxford University Press), p. 554
- Brands, Hal. "Paradoxes of the gray zone." Available at http://www.fpri.org/article/2016/02/paradoxes-gray-zone/
- Burke, Evan. "The Obama-Xi Summit and the prospects for a global norm against commercial IP theft." Carnegie Endowment for International Peace. June 14 (2021): 2021.
- Byman, Daniel, and Sarah E. Kreps. "Agents of destruction? Applying principal-agent analysis to state-sponsored terrorism." International Studies Perspectives 11.1 (2010): 1-18.
- Byman, Daniel. "Passive sponsors of terrorism." Survival 47.4 (2005): 117-144.
- Cabinet Office, Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space (Norwich: The Stationery Office, 2009), p. 7.
- Cabinet Office. A strong Britain in an age of uncertainty: the national security strategy. Vol. 7953. The Stationery Office, 2010.
- Cassese, Antonio. "The Nicaragua and Tadić tests revisited in light of the ICJ judgment on genocide in Bosnia." European journal of international Law 18.4 (2007): 649-668.
- Chi siamo - Agenzia per la cybersicurezza nazionale. (n.d.). ACN - Agenzia per La Cybersicurezza Nazionale. https://www.acn.gov.it/agenzia/chi-siamo.
- Clausewitz, Carl. On war. Penguin UK, 2003.
- Connect the dots on State-Sponsored Cyber Incidents - Ukrainian IT Army. Council on Foreign Relations. https://www.cfr.org/cyber-operations/ukrainian-it-army
- Convention No. V Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, Oct. 18, 1907, 36 Stat. 2310 [hereinafter Hague V]. Convention No. XIII Concerning the Rights and Duties of Neutral Powers in Naval War, Oct. 18, 1907, 36 Stat. 2415.
- Council of Europe, Convention on Cybercrime, 2001, http://conventions. coe.int/treaty/en/treaties/html/185.htm.
- Crawford, James. State responsibility: the general part. No. 100. Cambridge University Press, 2013.
- Cyber/ICT Security. OSCE. https://www.osce.org/cyber-ict-security
- Deibert, Ronald, et al. Access denied: The practice and policy of global internet filtering. The MIT Press, 2008.Kesan, Jay P., and Carol Mullins Hayes. "Thinking

through active defense in cyberspace." Proceedings of the Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options. 2010.
- Delerue, François. Cyber operations and international law. Vol. 146. Cambridge University Press, 2020.
- Department of the Army Headquarters, United States Army.
- Developments in the field of information and telecommunications in the context of international security – UNODA. 2018. A/RES/73/27, https://disarmament.unoda.org/ict-security/
- Developments in the field of information and telecommunications in the context of international security (A/RES/75/240) | Digital Watch Observatory. (n.d.). Digital Watch Observatory. https://dig.watch/resource/developments-field-information-and-telecommunications-context-international-security
- Dissenting Opinion of the Vice-President of the ICJ A. S. Al-Khasawneh in Bosnian Genocide judgment (Dissenting opinion of Al-Khasawneh, Bosnian Genocide judgment), 216–217, para. 37.
- Document of the Stockholm Conference, 1986. OSCE. https://www.osce.org/fsc/41238
- Doswald-Beck, Louise. "The San Remo Manual on international law applicable to armed conflicts at sea." American Journal of International Law 89.1 (1995): 192-208.
- Doswald-Beck, Louise. "The San Remo Manual on international law applicable to armed conflicts at sea." American Journal of International Law 89.1 (1995): 192-208.
- E. Newman, 'Failing States and International Order: Constructing a Post-Westphalian World', Contemporary Security Policy, 2009, Vol. 30, No. 3, page 422
- Egloff, F. J. "Cybersecurity and the age of privateering: A historical analogy." (2015)
- Emerging Practices in Cybersecurity-Related Public-Private Partnerships and Collaboration in OSCE participating States. (2023). OSCE. https://www.osce.org/secretariat/539108
- Etzioni, Amitai. "Social norms: Internalization, persuasion, and history." Law and society review (2000): 157-178.
- Finnemore, Martha, and Duncan B. Hollis. "Constructing norms for global cybersecurity." American Journal of International Law 110.3 (2016): 425-479.
- Fuller, Kathleen E. "ICANN: The debate over governing the internet." Duke L. & Tech. Rev. 1 (2001): 1.
- Gavrilovic, A. (2022, December 13). What's new with cybersecurity negotiations: The OEWG 2021–2025 annual report adopted - Diplo. Diplo. https://www.diplomacy.edu/blog/whats-new-with-cybersecurity-negotiations-the-oewg-2021-2025-annual-report-adopted/#top
- Giberson, J. (2019, January 13). The realities of proxy wars in the post Cold War Era – McGill Journal of Political Studies. https://mjps.ssmu.ca/2019/01/13/realities-proxy-wars-post-cold-war-era/

- Harvard School of Public Health. Program on Humanitarian Policy, and Conflict Research. HPCR manual on international law applicable to air and missile warfare. Cambridge University Press, 2013.
- HEADQUARTERS, US, MARINE CORPS, and US COAST GUARD. "THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS." (2007).
- Heintschel von Heinegg, Wolff. "Territorial sovereignty and neutrality in cyberspace." International Law Studies 89.1 (2013).
- Heintschel, Wolff, and Von Heinegg. "Benevolent third states in international armed conflicts: the Myth of the irrelevance of the law of neutrality." International Law and Armed Conflict: Exploring the Faultlines. Brill Nijhoff, 2007. 543-568.
- Helsinki Final Act, 1975. OSCE. https://www.osce.org/it/mc/39504
- Herr, Trey. "Cyber insurance and private governance: The enforcement power of markets." Regulation & Governance 15.1 (2021): 98-114.
- Hogeveen, Bart, "The UN norms of responsible state behaviour in cyberspace". The Australian Strategic Policy Institute Limited 2022.
- Hollis, D. "Improving Transparency. International Law and State Cyber Operations. Fourth report to the Organization of American States. OEA/Ser. Q. CJI/doc. 603/20." (2020).
- Hurel, Louise Marie. "The Rocky Road to Cyber Norms at the United Nations." Council on Foreign Relations (2022).
- International Court of Justice (ICJ), Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996, p. 226, 8 July 1996, available at: https://www.refworld.org/cases,ICJ,4b2913d62.html
- International Law Commission. "Draft articles on responsibility of states for internationally wrongful acts." Yearbook of the International Law Commission 2.2 (2001)
- International law in cyberspace. (n.d.). Digital Watch Observatory. https://dig.watch/event/un-oewg-2021-2025-1st-substantive-session/international-law
- IP spoofing: How it works and how to prevent it. (2023, May 18). www.kaspersky.com. https://www.kaspersky.com/resource-center/threats/ip-spoofing
- Jensen, Eric Talbot. "The Tallinn Manual 2.0: Highlights and Insights." Geo. J. Int'l L. 48 (2016): 735.
- Jinks, Derek. "State responsibility for the acts of private armed groups." Chi. J. Int'l L. 4 (2003): 83.
- Johnson, David R., and David Post. "Law and borders: The rise of law in cyberspace." stanford law review (1996): 1367-1402; Barlow, John Perry. "A Declaration of the Independence of Cyberspace." Duke L. & Tech. Rev. 18 (2019): 5.
- Johnson, Durward E., and Michael N. Schmitt. "Responding to proxy cyber operations under international law." The Cyber Defense Review 6.4 (2021): 15-34.

- Katzenstein, Peter J., ed. The culture of national security: Norms and identity in world politics. Columbia University Press, 1996.
- Kavanagh, Camino, and Laura Crespo. "Confidence Building Measures and ICT." European Foreign Affairs Review 24.2 (2019).
- Keohane, Robert O. "After hegemony: transatlantic economic relations in the next decade." The International Spectator 19.1 (1984): 3-9.
- Keohane, Robert O. "Ironies of sovereignty: the European Union and the United States." JCMS: journal of common market studies 40.4 (2002): 743-765.
- Khalip, Andrei. "UN chief urges global rules for cyber warfare." Reuters, February 19 (2018).
- Krasner, Stephen D. "Sovereignty." Foreign Policy (2001): 20-29.
- Kravets, David. "Exclusive: I was a hacker for the MPAA." Wired Magazine (2007).
- Lee, Malcolm R. "Will the United States impose cyber sanctions on China?.", 2015.
- Leigh, Monroe. "Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America). 1984 ICJ Reports 392." American Journal of International Law (1985).
- Levie, Howard S. "1907 HAGUE CONVENTION V RESPECTING THE RIGHTS AND DUTIES OF NEUTRAL POWERS AND PERSONS IN CASE OF WAR ON LAND (18 October 1907)." International Law Studies 60.1 (1979): 36.
- Lewis, J. "Cyber attacks, real or imagined, and cyber war." CSIS Commentary 11 (2011).
- Libicki, Martin C. Cyberdeterrence and cyberwar. RAND corporation, 2009.
- Libicki, Martin. "The coming of cyber espionage norms." 2017 9th International Conference on Cyber Conflict (CyCon). IEEE, 2017.
- Lynn III, William F. "Defending a new domain-the Pentagon's cyberstrategy." Foreign Aff. 89 (2010): 97.
- Mahdi, Ali Akbar. "The student movement in the Islamic Republic of Iran." Journal of Iranian Research and Analysis 15.2 (1999): 5-32.
- Markoff, John. "Before the gunfire, cyberattacks." New York Times 12 (2008): 27-28.
- Martha Finnemore and Kathryn Sikkink, “International Norm Dynamics and Political Change,” International Organization, (1998).
- Martino, Luigi. "La quinta dimensione della conflittualità. L'ascesa del cyberspazio ei suoi effetti sulla politica internazionale." Politica & Società 7.1 (2018): 61-76.
- Maurer, Tim. Cyber mercenaries. Cambridge University Press, 2018.
- Menn, Joseph. "Hacker'mercenaries' linked to Japan, South Korea spying: researchers." Reuters, September 29 (2013).
- Merriam-Webster, Merriam-Webster: Definition of ‘Norm’, https://www.merriam-webster.com/dictionary/norm , 2021.
- Moghadam, Assaf, and Michel Wyss. "The political power of proxies: Why nonstate actors use local surrogates." International Security 44.4 (2020): 119-157.
- Monroe, Kristen Renwick. "Explicating altruism." (2002).
- Mumford, Andrew. Proxy warfare. John Wiley & Sons, 2013.

- Naím, Moisés. "Mafia states: Organized crime takes office." Foreign Aff. 91 (2012): 100.
- NATO. "Cyber Defence: A Core Task for NATO in the 21st Century." NATO, June 29, 2016, https://www.nato.int/cps/en/natohq/opinions_132349.htm.
- NATO. "Warsaw Summit Communiqué." NATO, July 2016, https://www.nato.int/cps/en/natohq/official_texts_133169.htm
- Naugle, Asmeret Bier, and Michael Lewis Bernard. Proxy War in the Gray Zone. No. SAND2017-3011C. Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), 2017.
- Neuman, Noam. "Neutrality and Cyberspace: Bridging the Gap between Theory and Reality." International Law Studies 97.1 (2021): 33.
- North Atlantic Treaty Organization, Cyber Defence, 2016, at http://www.nato.int/cps/en/natohq/ topics_78170.htm.
- Nye Jr, Joseph S. "Deterrence and dissuasion in cyberspace." International security 41.3 (2016).
- Nye Jr, Joseph S. The future of power. PublicAffairs, 2011.
- Nye, Joseph S. "Normative restraints on cyber conflict." Cyber Security: A Peer-Reviewed Journal 1.4 (2018): 331-342.
- Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States, UNODA, A/76/136 (August 2021) 27-28.
- Olsen, Johan P., and James G. March. The logic of appropriateness. No. 9. ARENA, 2004.
- OSCE, 'Follow-Up on Recommendations in the OSCE PA's Monaco Declaration: Final Report for the 2013 Annual Session', https:// www.oscepa.org/documents/all-documents/annual-sessions/2013-istanbul/follow-up-report-3/1782-2013-annual-session-follow-up-final-report-1st-committee-english/file
- OSCE, Istanbul Declaration and Resolution Adopted by the OSCE Parliamentary Assembly at the Twenty-Second Annual Session (2013), https://www.oscepa.org/en/documents/annual-sessions/2013-istanbul/declaration/1801-istanbul-declaration-eng-1/file
- OSCE, PA. "Istanbul Declaration and Resolutions Adopted by the OSCE Parliamentary Assembly at the Twenty-Second Annual Session." (2013).
- OSCEPA, 'Astana Declaration of the OSCE Parliamentary Assembly and Resolution Adopted at the Seventeenth Annual Session' (29 June to 3 July 2008), https://www.oscepa.org/en/documents/annual-sessions/2008-astana/summary-report-11/289-2008-astana-annual-session-report-english/file
- OSCEPA, 'Belgrade Declaration of the OSCE Parliamentary Assembly and Resolution Adopted at the Twentieth Annual Session' (6-10 July 2011), https://www.oscepa.org/en/documents/annual-sessions/2011-belgrade/declaration-4/3024-belgrade-declaration-eng/file
- Ottis, Rain. "Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective." Proceedings of the 7th European Conference on Information Warfare. Reading, MA: Academic Publishing Limited, 2008.

- Pawlak, Patryk. "Confidence-Building Measures in Cyberspace: Current Debates and Trends." International cyber norms: Legal, policy & industry perspectives 20 (2016): 129-153.
- Permanent Council Decision No. 1039, 2012. OSCE. https://www.osce.org/pc/90169
- Permanent Council Decision No. 1106, 2013. OSCE. https://www.osce.org/pc/109168
- Permanent Council Decision No.1202, 2016. OSCE. https://www.osce.org/it/pc/228511
- Public Safety Canada, Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada (Ottawa: Government of Canada Publications), p. 2.
- Responsible Behaviour in Cyberspace: Global narratives and practice: EU Cyber Direct. (2023, June 29). Horizon. https://eucyberdirect.eu/research/responsible-behaviour-in-cyberspace.
- Rid, Thomas. "Cyber war will not take place." Journal of strategic studies 35.1 (2012): 5-32.
- Risse, Thomas, and Kathryn Sikkink. "The socialization of international human rights norms into domestic practices: introduction." Cambridge Studies in International Relations 66 (1999): 1-38.
- Rondeaux, Candace, and David Sterman. "Twenty-first century proxy warfare: confronting strategic innovation in a multipolar world." New America (2019).
- Roscini, Marco. Cyber operations and the use of force in international law. Oxford University Press, USA, 2014.
- Ruhl, Christian, et al. Cyberspace and geopolitics: Assessing global cybersecurity norm processes at a crossroads. Carnegie Endowment for International Peace., 2020.
- Salehyan, Idean. "The delegation of war to rebel organizations." Journal of Conflict Resolution 54.3 (2010): 493-515.
- Sandholtz, Wayne. Prohibiting plunder: how norms change. Oxford University Press, 2007.
- Schelling, Thomas C. "An astonishing 60 years: The legacy of Hiroshima." Proceedings of the National Academy of Sciences 103.16 (2006): 6089-6093.
- Schmitt, Michael N. "In defense of due diligence in cyberspace." Yale LJF 125 (2015): 68.
- Schmitt, Michael N., and Liis Vihul. "Proxy wars in cyberspace: the evolving international law of attribution." Fletcher Sec. Rev. 1 (2014): 53.
- Schmitt, Michael N., and Sean Watts. "Beyond state-centrism: international law and non-state actors in cyberspace." Journal of Conflict and Security Law 21.3 (2016): 595-611.
- Schmitt, Michael N., ed. Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press, 2017.
- Schmitt, Michael N., ed. Tallinn manual on the international law applicable to cyber warfare. Cambridge University Press, 2013.

- Secretary-General, U. (2013, June 24). Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security :: note /: by the Secretary-General. United Nations Digital Library System. https://digitallibrary.un.org/record/753055
- Senger, Harro von, and Myron B. Gubitz. "The book of stratagems: Tactics for triumph and survival."1988
- Sharma, Amit. "Cyber wars: A paradigm shift from means to ends." Strategic Analysis 34.1 (2010): 62-73.
- Shiryaev, Yaroslav. "The right of armed self-defence in international law and self-defence arguments used in the second Lebanon war." Acta Societatis Martensis 3 (2007): 80.
- Simmons, Beth A. Mobilizing for human rights: international law in domestic politics. Cambridge University Press, 2009.
- Snow, David A., et al. "Frame alignment processes, micromobilization, and movement participation." American sociological review (1986): 464-481.
- Stone, John. "Cyber war will take place!." Journal of strategic studies 36.1 (2013): 101-108.
- Tadić judgment, 56, para. 131.
- Tanzi, Attila, et al. International Law and Cyberspace. Ministry of Foreign Affairs and International Cooperation, (2021). https://www.esteri.it/wp-content/uploads/2021/12/UNIBO_Applicazione-dei-principi-della-Carta-delle-Nazioni-Unite-nello-spazio-cibernetico.pdf.
- Teng Jianqun and Xu Longdi, Cyber War Preparedness, Cyberspace Arms Control and the United States (Beijing: China Institute of International Studies, 2014), 11.
- Terrill, W. Andrew. "Iranian involvement in Yemen." Orbis 58.3 (2014): 429-440.
- The charter of the United Nations, art. 2(4). Oxford, UK: 1995.
- The Economist, “A virtual counter-revolution”, The Economist Group Limited, 2010, at https://www.economist.com/briefing/2010/09/02/a-virtual-counter-revolution.
- The list of 2019–2021 States with GGE members is 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, United States, and Uruguay.
- Tiirma-Klaar, H. "The Evolution of the UN Group of Governmental Experts on Cyber Issues from a Marginal Group to a Major International Security Norm-Setting Body." Cyberstability Paper Series (2021).
- Timeline of Syrian Chemical Weapons Activity, 2012-2022 | Arms Control Association. (n.d.). https://www.armscontrol.org/factsheets/Timeline-of-Syrian-Chemical-Weapons-Activity
- Tsagourias, Nicholas. "Cyber attacks, self-defence and the problem of attribution." Journal of conflict and security law 17.2 (2012): 229-244.
- Tzu, Sun, and Lionel Giles. The art of war. Vol. 84. Oxford: Oxford University Press, 1963.

- UN General Assembly Resolution 914 (X) (16 Dec. 1955), https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/103/94/IMG/NR010394.pdf?OpenElement.
- UN International Law Commission. "Draft articles on responsibility of states for internationally wrongful acts, with commentaries." Yearbook of the international law commission 2 (2001).
- UN OEWG in 2023 - DW Observatory. (1998, September 30). Digital Watch Observatory. https://dig.watch/processes/un-gge
- UN OEWG in 2023 - DW Observatory. (1998c, September 30). Digital Watch Observatory. https://dig.watch/processes/un-gge#The-future-process---PoA
- UN. General Assembly (73rd sess. : 2018-2019). (2018, December 11). Developments in the field of information and telecommunications in the context of international security :: resolution /: adopted by the General Assembly. United Nations Digital Library System. https://digitallibrary.un.org/record/1655670?ln=en
- UNGA, Report of the International Law Commission – Fifty-Third Session, 36, para. 12.
- UNIDIR, “Due diligence in cyberspace: Normative expectations of reciprocal protection of international legal rights”, (2021), https://www.unidir.org/publication/due-diligence-cyberspace-normative-expectations-reciprocal-protection-international
- United Nations Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, “Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security”, A/70/174, July 22, 2015.
- United Nations, Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or other Gases, and of Bacteriological Methods of Warfare, 17 June 1925, available at: https://www.refworld.org/docid/4a54bc07d.html
- United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran), ICJ Reports 1980 (ICJ, 24 May 1980) (Tehran Hostages judgment), 30–31, para. 59.
- United States. Department of Defense. Department of Defense Strategy for Operating in Cyberspace. DIANE Publishing, 2012.
- Ventura, Manuel J. "Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda)(Reparations Judgment)(ICJ)." International Legal Materials 62.3 (2023): 399-527.
- Vienna Document 1990 (it). OSCE. https://www.osce.org/it/fsc/41248
- Walker, George K. "Information warfare and neutrality." Vand. J. Transnat'l L. 33 (2000); Todd, Graham H. "Armed attack in cyberspace: deterring asymmetric warfare with an asymmetric definition." AFL Rev. 64 (2009): 65.
- Walker, George K. "Information warfare and neutrality." Vand. J. Transnat'l L. 33 (2000); Todd, Graham H. "Armed attack in cyberspace: deterring asymmetric warfare with an asymmetric definition." AFL Rev. 64 (2009): 65.

- Walton, Greg. China's golden shield: Corporations and the development of surveillance technology in the People's Republic of China. Rights & Democracy, 2001.
- Wedermyer, Landon J. "The Changing Face of War: The Stuxnet Virus and the Need for International Regulation of Cyber Conflict." StuSch (2012).
- Wendt, Alexander. "Anarchy is what states make of it: the social construction of power politics." International organization 46.2 (1992): 391-425.
- What is a Botnet? (2023, June 30). usa.kaspersky.com. https://usa.kaspersky.com/resource-center/threats/botnet-attacks
- What we do. (n.d.). OSCE. https://www.osce.org/what-we-do
- Whetham, David. "“Are We Fighting Yet?” Can Traditional Just War Concepts Cope with Contemporary Conflict and the Changing Character of War?." The Monist 99.1 (2016): 55-69.
- White House, Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure (Washington DC: US Government Printing Office, 2009), p. iii.
- Who we are. (n.d.). OSCE. https://www.osce.org/who-we-are
- Wright, Quincy. "The corfu channel case." American Journal of International Law 43.3 (1949): 491-494.
- Wu, Timothy S. "Cyberspace sovereignty--the Internet and the international system." Harv. JL & Tech. 10 (1996).
- Zetter, Kim. "Legal Experts: Stuxnet Attack on Iran Was Illegal ‘Act of Force.’." WIRED Online (2013).
- Военная доктрина Российской Федерации.” 2010. Президент России. February 5, 2010. Accessed April 30, 2023. http://kremlin.ru/supplement/461. For the English translation see: https://carnegieendowment.org/files/2010russia_military_doctrine.pdf
- Tacc. (2017, November 3). РФ предложила провести в 2018 году конференцию о роли ОБСЕ в сфере кибербезопасности. ТАСС. https://tass.ru/politika/4701198; also found at https://mid.ru/en/foreign_policy/rso/1556306/

Appendix

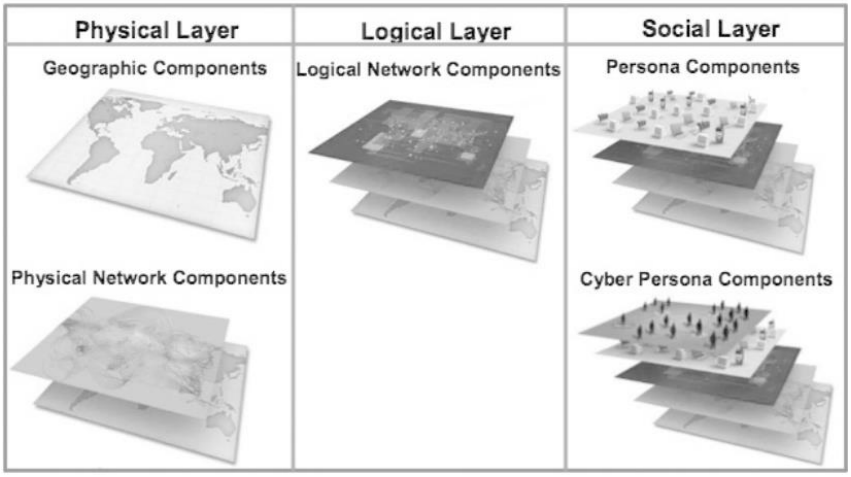


Fig. 1. Source: Department of the Army Headquarters, United States Army.

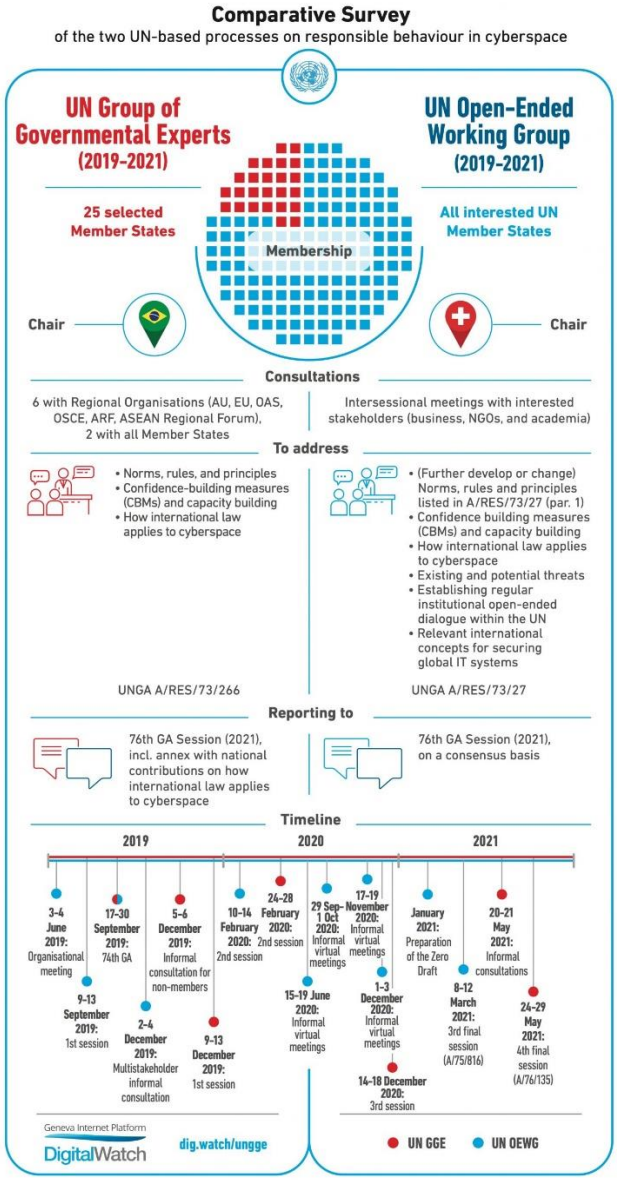


Fig.3 Comparison of UN GGE and OEWG (2019-2021). Source: Geneva Internet Platform Digital Watch.