LUISS

Corso di laurea in International Relations

Cattedra Diplomacy and Negotiation

Cyber-diplomacy and Global Order: Negotiating Cooperation or Managing Competition?

Prof. Pasquale Ferrara

RELATORE

Prof. Alfonso Giordano

CORRELATORE

Sara Ciardiello Matr. 655912

CANDIDATO

Anno Accademico 2024/2025

Cyber-diplomacy and Global Order:
Negotiating Cooperation or Managing Competition?

Abstract

In what ways do negotiation mechanisms influence the attitude of States in cyberspace, and how effective are they in managing conflicts and advancing global cybersecurity cooperation? This thesis addresses this question by placing cyber-diplomacy at its core, understood as the adaptation of traditional diplomatic tools to the challenges of the digital age. It traces the historical development and international efforts, particularly by the United Nations and the OSCE, to establish norms and confidence-building measures to regulate this emerging field of diplomacy.

The study examines the strategic postures of major actors – the United States, China, Russia, and the European Union – to show how their foreign policies shape the diplomatic landscape of cyberspace. It then applies negotiation theory, including Game Theory models, to explain how dialogue, bargaining, and compromise influence State behavior in this domain.

The decisive stress case is the cyberwarfare in Ukraine, which puts to the test the resilience and limitations of existing diplomatic frameworks under conditions of high-intensity conflict. The findings demonstrate that while cyber-diplomacy provides essential mechanisms for managing tensions, its effectiveness ultimately depends on multi-stakeholder involvement that complements State-led diplomacy.

Summary

1. Introduction

> *"Technology is shaping the most consequential issues in our foreign policy today, from winning the war in Ukraine to managing competition with China, from defending human rights in the digital age to shaping the governance of artificial intelligence. Diplomacy is most important when it is most challenging. The work of today's technology diplomats [...] will shape the global technology ecosystem for decades to come."*
>
> Nathaniel C. Fick
> Ambassador at Large
> Cyberspace & Digital Policy
> US Department of State

This Statement highlights not only the growing salience of technology in international relations but also underscores the enduring centrality of diplomacy as a practice and institution. As Berridge defines it, diplomacy is "the conduct of relations between sovereign States and other international actors by official agents and peaceful means," with negotiation at its very core. Cyber-diplomacy, therefore, is both a continuation and an adaptation of traditional diplomacy to the challenges of the digital age.

As the world evolves, becoming increasingly interconnected through digital technologies, there is a growing need for global collaboration in addressing the challenges of cyberspace[1]. Cyber-diplomacy has been defined in the literature as 'the use of diplomatic tools and mindsets in resolving or at least managing, the problems in cyberspace'[2] and the use of 'diplomatic tools and diplomatic thinking'[3] to address issues arising in cyberspace.

These tools draw from established diplomatic theories of negotiation, including distributive versus integrative bargaining, Track I (official, State-led) and Track II (unofficial, multi-stakeholder) diplomacy, and consensus-building approaches. This thesis will explore how these frameworks apply to cyber negotiations and test their

[1] Ioana-Cristina Vasiloiu (2023). Cyber-diplomacy: A New Frontier for Global Cooperation in the Digital Age. Informatica Economica, 27(1), pp.41–50

[2] Riordan, S. (2019). Cyber-diplomacy: Managing Security and Governance Online, Cambridge: Polity Press, 2019

[3] Carmen Elena Circu, Addressing the Gap in Strategic Cyber Policy, The Market of Ideas, 2019

explanatory power across case studies of international cyber governance and conflict prevention.

As cyber threats have emerged as a critical concern for national security and foreign policy, a new profession – cyber-diplomacy – has taken shape. Diplomacy's primary goal is to advance the interests of the State one represents, not just for cyberspace but for the larger security, economic and political interests of the nation as they shape and are affected by cyberspace and by digital technologies. Cyber diplomats lead international negotiations, prevent conflicts, shape the public opinion and foster agreements in global and regional cyber forums[4].

The diplomacy of cyberspace, has become part of the diplomatic portfolio of every nation: a series of multilateral and bilateral diplomatic efforts have sought to create common understanding, reduce risk and improve stability. These efforts have produced successes in the UN and other multilateral forums, but much remains to be done.

If traditional diplomacy remains primarily concerned with State-to-State relations in its various formats, cyber-diplomacy expands the arena of actors far beyond governments. The private sector, academia, and civil society play crucial roles in building, innovating, and maintaining the functionality of cyberspace. This diversification of stakeholders reflects what Keohane and Nye describe as *complex interdependence* – a condition in which multiple channels connect societies, power is dispersed across State and non-State actors, and military force is less central than cooperation and negotiation[5].

[4] Salvi, A., Tiirmaa-Klaar, H. and Lewis, J. (2025). A Handbook for the Practice of Cyber-diplomacy. Luxembourg: EU Institute for Security Studies.

[5] Keohane, R.O. and Nye, J.S. (2012). Power and interdependence, 4th ed. Glenview, IL: Pearson Education, Inc.

In this context, cyber-diplomacy is best understood not only through the lens of Track I diplomacy (official, State-led negotiations) but also as an arena where Track II (informal, expert-driven) come into play. This “multi-track diplomacy” framework captures how cyberspace actors – governments, organizations, corporations, the private sector, and civil society – collaborate, compete, and negotiate to shape norms and develop cyber capabilities to ensure a safe digital space through cyber-diplomacy[6]. By framing cyber-diplomacy in these terms, the shift from traditional State-centric negotiation to a more plural, multi-actor process, becomes clear.

The transboundary nature of cyber requires all States to cooperate to advance the adoption of a multilateral system of voluntary rules, norms, principles and coordinated capacity building. For cyber-diplomacy to be effective and meaningful, States will need to continue to strengthen multilateralism[7]. By working internationally, countries can combine their resources, intelligence, and skills to detect, prevent, and respond to cyber-attacks with global implications[8].

This master's thesis examines how diplomatic negotiation methods impact global cybersecurity governance and international relations, focusing on the question: “*In what ways do negotiation mechanisms influence the attitude of States in cyberspace, and how effective are they in managing conflicts and advancing global cybersecurity cooperation?*”

This study examines whether cyber-diplomacy promotes international collaboration or instead intensifies geopolitical competition. It focuses on the strategic approaches of major actors such as the United States, China, Russia, and the

[6] Ioana-Cristina Vasiloiu (2023). Cyber-diplomacy: A New Frontier for Global Cooperation in the Digital Age. Informatica Economica, 27(1), pp.41–50

[7] Salvi, A., Tiirmaa-Klaar, H. and Lewis, J. (2025). A Handbook for the Practice of Cyber-diplomacy. Luxembourg: EU Institute for Security Studies

[8] Petar Radanliev (2025) Cyber-diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing, Journal of Cyber Security Technology, 9:1, 28-78

European Union. The central hypothesis is that these actors adopt different negotiation stances: some rely on cooperative, integrative strategies aimed at building norms and fostering stability, while others pursue competitive, distributive approaches that mirror broader geopolitical rivalries. By testing this hypothesis across case studies, the thesis explores how divergent strategies shape international cyber negotiations and whether cyber-diplomacy can function as a stabilizing force in global security. Furthermore, it evaluates the effectiveness of existing diplomatic instruments – such as Track I (official, State-led) and Track II (informal, multi-stakeholder) diplomacy – in reducing the risks of cyber conflict. Case studies, including Russian cyber operations in Ukraine, illustrate both the challenges and the consequences for the future of armed conflict.[9].

Cyber-diplomacy is presented as a crucial tool for managing both the risks and opportunities of cyberspace. While the challenges are substantial, the potential benefits of stronger international cooperation are equally significant. Policymakers therefore need to prioritize collaboration and work toward shared standards and norms that can help create a more stable, secure, and predictable digital environment[10].

Finally, this thesis situates cyber-diplomacy within classical and modern negotiation theory, assessing the capacity of diplomatic mechanisms to reduce conflict in cyberspace and to strengthen international cooperation.

[9] Duguin, S. and Pavlova, P. (2023). The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict. Brussels: European Parliament

[10] Ioana-Cristina Vasiloiu (2023). Cyber-diplomacy: A New Frontier for Global Cooperation in the Digital Age. Informatica Economica, 27(1), pp.41–50

1. The Emergence of Cyber-Diplomacy

This chapter represents the foundational component of this thesis. The primary aim is to explore the historical evolution of cyber-diplomacy, outlining its essential principles and concepts. Furthermore, it aims to clarify the roles and impact of principal stakeholders in this sector, encompassing governments, corporate entities, and international organizations. The chapter further situates cyber-diplomacy within classical diplomatic theory, highlighting how established diplomatic principles are applied and modified in the context of the digital age.

In a progressively digitally interconnected world, global collaboration has become essential for addressing challenges within cyberspace. The rising need to deal with threats that could possibly have enormous consequences on national security and foreign policy has led to the emergence of cyber-diplomacy, a specialized branch of diplomacy. Landmark incidents such as the Moonlight Maze cyber operation, the 2007 cyberattacks against Estonia, the 2008 cyber sabotage during the Russian invasion of Georgia, and the Stuxnet computer virus in 2009-2010, highlighted the urgent need for a diplomatic framework to manage these threats. In this context, negotiations serve to prevent escalation and build mutual assurances. Particularly, confidence-building measures (CBMs), diplomatic tools designed to reduce mistrust, increase transparency, and foster predictability among States in situations of potential conflict, become essential diplomatic tools, enabling States to reduce mistrust, establish communication channels, and create shared understandings that mitigate the risk of cyber incidents spiraling into broader conflicts.

Cyber-diplomacy refers to "*the use of diplomatic tools and strategies to govern cyberspace, address security issues, and foster international collaboration*", as it will be later explained. The primary objectives include promoting responsible State conduct, enhancing cybersecurity, ensuring stability in the digital realm, and enabling collaborative responses to common cyber threats. It differs from traditional foreign policy by involving a broader spectrum of actors beyond just States. The private sector, academia, and civil society are integral to the functionality and security of cyberspace, necessitating their active participation in diplomatic efforts. This has led to the rise of multistakeholder diplomacy, an approach that integrates diverse perspectives and expertise from non-governmental organizations (NGOs), private companies, and inter-governmental organizations (IGOs) to address complex global challenges that cannot be resolved by States alone. Market actors, alongside civil society organizations and academic bodies, are now considered essential partners in discussions on cyber stability.

The chapter will also examine how State actors are actively shaping cyber-diplomacy through the creation of new diplomatic roles and specialized government entities. These institutional changes not only reflect a strategic prioritization of cyber issues but also enhance States' negotiation capacity, enabling them to engage more effectively in international cyber dialogues and strengthen their ability to shape norms and agreements in cyberspace.

By exploring these fundamental aspects – the historical context, definitions, key actors, and the evolution of norms – this chapter lays the groundwork for understanding how diplomatic negotiation mechanisms can effectively mitigate cyber conflicts and enhance international cybersecurity cooperation, setting the stage for the detailed analyses presented in subsequent chapters.

1.1 Theoretical Framework

Outlining the theoretical framework that strengthens the analysis is essential before digging deeper into the content of what follows. The reader will engage with this work better if the perspective from which it is developed is clarified.

The traditional schools of thought that make up international relations theory provide a number of perspectives for understanding recent global developments. As Berridge emphasizes, diplomacy is not merely a theory of international relations; it is also the practice of negotiation – the process through which agreements are reached, which constitutes the ultimate goal of diplomatic activity[11]. Cyber-

[11] Berridge, G.R. (2023). Theory and Practice: Negotiations. [online] DiploFoundation. Available at: https://asef.org/wp-content/uploads/2020/10/ModelASEM_Diplo_Negotiations.pdf.

diplomacy makes the duty even more complex as it is an intricate field that encompasses domains like international law, engineering, human rights, and ICT.

Since the role of diplomacy in this context is the main focus of this thesis, the factors that impact those who formulate international policy will receive the majority of the attention. International relations theory offers crucial resources for figuring out substantial concepts, such as recognizing the increasing role played by non-governmental organizations (NGOs), private companies and inter-governmental organizations (IGOs) on the international arena.
Globalization and the information revolution at the beginning of the XXI Century have empowered decentralized networks and challenged State-centered hierarchies. Non-State actors bring critical resources, legitimacy, and technical expertise, which enhance their negotiation leverage and shift the balance of bargaining power in international diplomacy, including in the cyber domain.

The necessity of dealing with issues of increasing technical and social complexity has required wider engagement beyond conventional State-to-State diplomacy. Increased participation, action, and accountability from different non-State actors have been part of this expansion. This has long been the case for environmental law and the domain of cybersecurity is no different[12].

Although networks had always existed, information and communication technologies have rapidly reduced physical and economic barriers that once limited network expansion.

[12] Johnstone, I., Sukumar, A. and Trachtman, J. (2023). Building cybersecurity through multistakeholder diplomacy: Politics, processes, and prospects.

Networks became flexible and agile in time. They have democratized access to power, reducing many of the advantages previously enjoyed only by States: large corporations, such as IBM, have excelled in that[13].

From the collaboration with the private sector, societies haves gained numerous advantages, the main one being the creativity and the adaptability needed to respond to new realities and advance interests globally. In other words, non-State actors have added long-term vision to diplomacy activities[14]. In light of this, entities such as NGOs, private companies, and IGOs, which share the common denominator of not being representative of States, have shifted in perception – from being mere target audiences to being regarded as stakeholders and active participants.

The approach outlined is proper of the so-called *multistakeholder diplomacy*, which saw its rising since when diplomacy became no longer confined to issues of war and peace and, instead, started to address every activity of the modern State, which itself is far more active than the one of the previous Century, regulating and acting in many different spheres of life.

The growth of multi-stakeholder involvement in cyber-diplomacy has been greatly facilitated by three crucial variables.

First, market actors now have more options to either flee or abandon a system or institution – for example, a company moving abroad to avoid unfavorable regulations – or to voice their disapproval and attempt to affect change from within, such as through lobbying, negotiations, or policy changes. This is due to the increased cross-border mobility of capital and goods.

[13] Metzl, J.F. (2001). Network Diplomacy. Georgetown Journal of International Affairs, 2(1), pp.77–87.

[14] Lee, G. and Ayhan, K. (2015). Why Do We Need Non-State Actors in Public Diplomacy?: Theoretical Discussion of Relational, Networked and Collaborative Public Diplomacy. Journal of International and Area Studies, 22(1), pp.57–77.

Second, non-State actors are now better equipped to coordinate and conduct cross-border operations. Third, the global ideational superstructure has changed, favoring theories that support private-led governance models.

Market actors, such as Microsoft, FireEye, CrowdStrike, civil society organizations and academia are today essential interlocutors in cyber stability discussions, whether in norm articulation or in implementation[15]. Companies often serve as quasi-mediators or agenda-setters in cyber negotiations, shaping priorities and facilitating dialogue among States and other stakeholders. From a negotiation perspective, this reflects coalition-building dynamics, as States increasingly form alliances with private actors to strengthen their bargaining positions and advance their strategic interests in multilateral cyber negotiations.

The way States negotiate cyber-diplomacy agreements and help minimize cyber conflicts has also changed as a result of non-governmental actors being included in the decision-making process. Global multistakeholder initiatives bring together the activist, bureaucrat, engineer, entrepreneur, funder, journalist, researcher, as well as others, integrating different perspectives and experiences. In the end, the underlying intuition is that combining different sources of understanding and expertise might result in improved global problem-solving[16].

As it will be outlined within this chapter, the inclusion of multiple stakeholders has been crucial in reaching a consensus on the first stance.

1.2 Defining Cyber-Diplomacy

Cyber-diplomacy has been understood differently in the literature and thus calls for a bit of clarification. For instance, the term “cyber-diplomacy” is often used

[15] Sukumar, A. (2023). Building an International Cybersecurity Regime: Multistakeholder Diplomacy. Edward Elgar Publishing.

[16] Scholte, J. (2020). Multistakeholderism: Filling the Global Governance Gap? School of Global Studies University of Gothenburg.

interchangeably with the ones of “e-diplomacy” and “digital diplomacy”, despite important differences[17]. Riordan clarifies the distinction between cyber and digital diplomacy by explaining that the latter refers to the use of digital tools and techniques to conduct diplomacy, while cyber-diplomacy refers to the deployment of diplomatic tools and the diplomatic mindset to deal with issue arising from cyberspace[18]. In other words, digital diplomacy, also known as e-diplomacy or diplomacy 2.0, uses governments’ and diplomats’ social media, online platforms, and digital technology to interact with international audiences, encourage communications, and carry out diplomatic outreach, whereas cyber-diplomacy involves the use of diplomatic means to regulate the cyberspace and delve into security issues, cooperating bilaterally and multilaterally[19]. It works by building strategic partnerships with other countries to promote responsible conduct, sustaining cybersecurity, and offering stability to cyberspace. Moreover, it also covers cooperation on shared threats, shaping like-minded coalitions on central policy issues, information exchange and national initiatives[20]. It explores the behaviour of States and other global players in a wide range of activities manifested in cyberspace[21]. Whereas digital diplomacy focuses on communication and outreach, cyber-diplomacy is grounded in negotiation over security, norms, and sovereignty, echoing classical diplomatic methods.

The following table will highlight and resume the main differences between digital diplomacy, e-diplomacy and cyber-diplomacy.

[17] Tallin Papers, CCDCOE

[18] Riordan, S. (2019). Cyber-diplomacy: Managing Security and Governance Online, Cambridge: Polity Press, 2019.

[19] Petar Radanliev (2025) Cyber-diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing, Journal of Cyber Security Technology, 9:1, 28-78

[20] Painter, C. (2018). Diplomacy in Cyberspace.

[21] Salvi, A., Tiirmaa-Klaar, H. and Lewis, J. (2025). A Handbook for the Practice of Cyber-diplomacy. Luxembourg: EU Institute for Security Studies.

CONCEPT	DESCRIPTION
Digital Diplomacy	Uses governments' and diplomats' social media, online platforms, and digital technology to engage international audiences, facilitate communications, and conduct diplomatic outreach
E-Diplomacy	Involves the use of electronic tools and platforms for diplomatic activities, including email diplomacy, virtual meetings, and digital communication channels to enhance diplomatic efficiency and global engagement
Cyber-diplomacy	Focuses on diplomatic efforts to regulate cyberspace, address security concerns, and collaborate internationally. It aims to build partnerships for responsible conduct, enhance cybersecurity, stabilize cyberspace, and cooperate on shared threats

Table 1: Distinction between digital diplomacy, e-diplomacy and cyber-diplomacy

The cyber-diplomacy agenda for interState relations is concerned with bilateral and multilateral cooperation mechanisms to promote international stability, security and cooperation in cyberspace issues, as well as cybersecurity capacity-related assistance. Related issues addressed are also the protection of human rights online, internet governance and technology-related foreign economic policy. Governments have begun to broaden their cyber-diplomacy portfolios to include all other foreign policy implications related to new technologies, such as military use of AI or the role of digital technologies in modern conflicts[22].

Moreover, cyber-diplomacy promotes capacity building in developing nations to improve their cybersecurity skills and strengths. This assistance can come from sharing expertise, training, and technology transfer[23]. Cyber-diplomacy also discusses topics relating to freedoms and rights in cyberspace, including decentralisation and internet governance, freedom of expression, ethics, and privacy.

[22] *Ibidem*

[23] Ioana-Cristina Vasiloiu (2023). Cyber-diplomacy: A New Frontier for Global Cooperation in the Digital Age. Informatica Economica, 27(1), pp.41–50

Unlike many other areas of traditional foreign policy, cyber-diplomacy is not just concerned with complex interdependent State-to-State relations but also with government-to-private sector relations, which control critical infrastructure, and non-governmental agencies advocating for human rights, the research-intensive academic community, and civil society. Public-private sector partnerships can therefore enable exchanges of knowledge and know-how in the area of cybersecurity[24].

When considering the emergence of the field, it is important to first understand the underlying logic of cooperation in this policy domain. Cyberspace cumulates a number of characteristics that frame diplomatic engagement among stakeholders[25].

In common with land, sea, air and space, cyberspace is now often designated as a strategic domain in its own right, but it is different from other domains in several respects, the most important of which is that it is the only environment that is entirely manmade[26]. Furthermore, cyberspace is usually considered as a "global common", defined as a "resource domain to which all nations have legal access"[27]. As such, it is considered that there should be a minimum number of rules and regulations, in order to ensure access to all and avoid conflict, which can only result from diplomatic negotiations.

There is little consistency between governmental definitions of cyberspace. The absence of shared definitions significantly complicates negotiations, as parties may struggle to even agree on what is being negotiated. The US Cyberspace Policy

[24] Petar Radanliev (2025) Cyber-diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing, Journal of Cyber Security Technology, 9:1, 28-78

[25] Barrinha, A. and Renard, T. (2017). Cyber-diplomacy: the making of an international society in the digital age. Global Affairs, 3(4-5), pp.353–364

[26] Betz, D. and Stevens, T. (2017). Cyberspace and the State. 1st ed. Routledge

[27] Buck, S.J. (1998). The Global Commons. Routledge

Review[28], for instance, defines cyberspace as the “globally-interconnected digital information and communications infrastructure that underpins almost every facet of modern society”, while the United Kingdom Cyber Security Strategy defines cyberspace as encompassing “all forms of networked, digital activities”[29]. The Canadian Cyber Security Strategy defines cyberspace as “the electronic world created by interconnected networks of information technology and the information on those networks”[30].

Alternative terms are employed in non-Anglophone contexts: Russian and Chinese official references to “cyberspace” occur primarily in translations of foreign texts or references to foreign approaches. The natural Chinese term which comes closest to English understanding of “cyberspace” is Xūnǐ zhǔjī (虛擬主機), which could be translated as *virtual host*, meaning no more than the necessary components for connecting a machine to a network for the specific purposes of communicating via protocols such as the email and so on [31].

It is easier for Russia and China, as well as other similar nations, to find a common language than for English-speaking nations to do so, despite the fact that Chinese and Russian rhetoric and official policies differ (in terms of concepts, terminology, and some practical decisions). In fact, it appears nearly impossible to achieve genuine reconciliation regarding the nature and governance of cyberspace if there

[28] CISA (2009), Cyberspace Policy Review

[29] Cyber Security Strategy of the United Kingdom safety, security and resilience in cyber space (2009), London: Cabinet Office.

[30] Government of Canada (2010). Canada’s Cyber Security Strategy: for a Stronger and More Prosperous Canada.

[31] Giles, K. and Hagestad II, W. (2013). Divided by a Common language: Cyber Definitions in Chinese, Russian and English. In: 5th International Conference on Cyber Conflict. Tallinn: NATO CCD COE Publications.

isn't even a common language to express fundamental ideas in cyber-security. This is the reason why this particular aspect becomes so relevant.

However, a comprehensive definition of cyberspace is – however – provided by the US National Institute of Standards and Technology (NIST). According to it, cyberspace is *"the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries*"[32], meaning that there are components of cyberspace that are not linked to the Internet, such as industrial control systems of critical infrastructures that provide essential services (electricity, water and transport, etc.). Moreover, specific military, intelligence, industrial and other communications systems with restricted access are separated from the world wide web.

Another concept related to cyber-diplomacy is cybersecurity, which focuses on the technical and operational aspects of securing digital systems. Cyber-diplomacy deals with the diplomatic implications of managing cyber threats: it introduces norms and rules through which cyberspace acquires a degree of stability and predictability[33].

To this matter, a large part of the work of cyber-diplomacy is the one of building confidence-building measures (CBMs), planned procedures to prevent hostilities, to avert escalation, to reduce military tension, and to build mutual trust between countries[34], that – in the case of cyberspace – help States to cooperate before

[32] CSRC Content Editor. cyberspace - Glossary | CSRC

[33] Ioana-Cristina Vasiloiu (2023). Cyber-diplomacy: A New Frontier for Global Cooperation in the Digital Age. Informatica Economica, 27(1),

[34] United Nations. Office for Disarmament Affairs. (n.d.). Military Confidence-Building Measures – UNODA.

incidents and coordinate crisis management and incident response activities, thereby preventing further damage and assisting in data recovery[35].

In conclusion, cyber-diplomacy can be seen as a chessboard with a broad spectrum of actors, policies, and platforms interrelated to each other and any area that has relevance to cyberspace is likely to be influenced by cyber-diplomacy, such as trade policy, security, freedom of governance, and freedom of speech[36].

1.3 The Genesis of Cyber-Diplomacy: A Historical Perspective

Cyber-diplomacy is complicated by its history. It did not start out as a central issue for international relations, and for sure it was not initially important for economies or trade. It is, at most, less than two decades old, making it an edifice still under construction[37]. Understanding the emergence of cyber-diplomacy is crucial to recognize the successes, the failures and opportunities in this domain[38].

1.3.1.1 The Diplomatization of Cyberspace

Cyber-diplomacy was born out of the necessity to regulate the emerging battlefield in cyberspace. One of the understandings of *diplomatization* is presented in Neumann's *At Home with the Diplomats*, which sees the concept as the appropriation of diplomatic practices by non-diplomatic groups, such as local

[35] Petar Radanliev (2025) Cyber-diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing, Journal of Cyber Security Technology, 9:1, 28-78

[36] Mihai Sebastian Chihaia and Rempala, J. (2023). Cyber-diplomacy. Springer eBooks, pp.260–264

[37] Salvi, A., Tiirmaa-Klaar, H. and Lewis, J. (2025). A Handbook for the Practice of Cyber-diplomacy. Luxembourg: EU Institute for Security Studies

[38] Barrinha, A. (2024b). Cyber-diplomacy: The Emergence of a Transient Field. The Hague Journal of Diplomacy

bureaucrats and the military, but also NGOs, businesses and even journalists[39]: the emergence of cyberattacks, hacking, cyber-crime, cyber espionage, IP theft, and disinformation were and still are all problems that required some sort of international rule set.

The need for cyber-diplomacy followed the same logic that evolved around airspace or maritime. These were all areas that at one point did not have a set of governing norms; it was only via diplomatic negotiations that international society was able to create an overarching set of standards and ultimately agree upon laws in these sectors[40].

For instance, a useful analogy is the development of the United Nations Convention on the Law of the Sea (UNCLOS) in 1982 – the most comprehensive legal framework for the world's oceans. These negotiations were highly complex, reflecting the dynamics of power between advanced and developing States, where weaker actors often had to negotiate under conditions set by stronger ones[41]. Similarly, cyber-diplomacy is shaped by asymmetries in capacity and influence, which profoundly affect the formulation of norms and rules in cyberspace.

1.3.1.2 Former Incidents

Increasingly adversarial State behaviour in cyberspace became a serious national security concern in the mid-2000s. Intrusions into government classified networks, such as the Moonlight Maze cyber operation against the US probably from Russia, have been taking place since the 1980s. The formative phase culminated with the first large-scale coordinated cyber campaign against Estonia in 2007 and with cyber sabotage to aid the military ground assault during the Russian invasion of Georgia in 2008. These times also saw other notable cyber operations that affected State

[39] Neumann, I.B. (2017). At Home with the Diplomats Inside a European Foreign Ministry. Cornell University Press

[40] Mihai Sebastian Chihaia and Rempala, J. (2023). Cyber-diplomacy. Springer eBooks, pp.260–264

[41] Schandorf, S.O. (2024). Power Relations and Maritime Justice: An Exploration of UNCLOS Negotiations. Ocean and Society, 1(Article 8791).

capabilities, such as the disruption of Iran’s nuclear enrichment facility by the Stuxnet computer virus in 2009 - 2010.

After Russia's first incursion into Ukraine in 2014, a new wave of cyber operations had regional and global impact, the most notorious being the NotPetya ransomware in 2017, which affected tens of thousands of targets in Ukraine and other parts of Europe. The pandemic due to the COVID-19 only accelerated online threats, as did the new Russian invasion of Ukraine in 2022.

With many examples from the growing field of covert cyber operations, including the loss of sensitive government data, rampant cyber espionage, intrusions into critical networks and the continued online theft of intellectual property, the scope of malicious State-organised cyber activity has expanded rapidly[42] and this led to the need to establish internationally-recognized norms and CBMs.

The following table highlights some of the milestone cyber events that have shaped the evolution of State behaviour and international concern in the cyber domain.

[42] Salvi, A., Tiirmaa-Klaar, H. and Lewis, J. (2025). A Handbook for the Practice of Cyber-diplomacy. Luxembourg: EU Institute for Security Studies

EVENT	YEAR(S)	DESCRIPTION
Moonlight Maze	Late 1990s	One of the first major cyber espionage campaigns targeting U.S. government systems, allegedly traced to Russia
Estonia Cyberattacks	2007	First large-scale coordinated cyberattack targeting a nation; disrupted government, media, and banking services in Estonia
Russia–Georgia War	2008	Cyberattacks against Georgian government and media websites coincided with Russian military invasion, showcasing cyber as a support tool in conventional war
Stuxnet	2009 – 2010	Highly sophisticated malware allegedly developed by the U.S. and Israel to sabotage Iran's nuclear enrichment program
Ukraine Conflict (Phase I)	2014	Following Russia's annexation of Crimea, Ukraine faced targeted cyberattacks on infrastructure, communications, and military systems
NotPetya	2017	Disguised as ransomware, this destructive malware crippled Ukrainian infrastructure and global companies; attributed to Russian actors
COVID-era Cyberattacks	2020 – 2021	Surge in cyberattacks on health systems, vaccine research facilities, and critical infrastructure during the global pandemic
Ukraine Invasion (Phase II)	2022 – Present	Intensified cyberattacks on Ukrainian targets and Western allies, including data wiping, disinformation, and attacks on energy and telecom sectors

Table 2: Milestone Events

1.4 Towards Norms and Confidence-Building Measures

If one would want to trace the history of the emergence of cyber-diplomacy, they would go back at the 18 September 1996, when Gordon Smith, the Canadian Foreign Affairs and International Trade deputy minister, at the Technology in Government Forum in Ottawa, for the first time even talked about "the application of information technologies to make the Department of Foreign Affairs and International Trade in Canada (DFAIT) more responsive and efficient"[43]. Most works published prior to 2010 tended to reflect this view of cyber-diplomacy.

The term "cyber-diplomacy" was hardly ever used, but the environment was already highly politicised, as demonstrated by the Russia's proposal of a UN treaty to ban electronic and information weapons in 1998 and the World Summit on the Information Society in 2003 and 2005[44].

One of the earliest studies to mention "cyber-diplomacy" as diplomacy dealing with emerging international aspects of cyber-policy and cybersecurity was only published in 2010 by the EastWest Institute, where it is suggested:

> *Because of high levels of cross-border connectivity in the cyber world, new approaches for cybersecurity must factor in the international dimension. Thus, instead of exclusively focusing on cyber defense or cyber war, it is also important to begin to develop cyber-diplomacy.*
> *Few governments have even thought about the diplomatic dimension of cybersecurity, and they certainly haven't developed diplomatic strategies commensurate with the threat*[45].

[43] Barrinha, A. (2024b). Cyber-diplomacy: The Emergence of a Transient Field. The Hague Journal of Diplomacy

[44] *Ibidem*

[45] Gady, F.-S. and Austin, G. (2010). Russia, The United States, And Cyber-diplomacy Opening the Doors. New York: EastWest Institute

Two years later, in 2012, Paul Meyer, a retired Canadian diplomat, published an article on the *Rusi Journal* in which he argued the diplomatic process of exploring possible international cooperation to build resilience in cyberspace against threats[46].

1.4.1.1 UN and OSCE Efforts

Recognizing the important role of non-State actors in securing digital networks and infrastructure, intergovernmental forums have gradually opened the door for multistakeholder participation in the formulation, articulation and implementation of cyber norms. As a result, the secretariats of organizations such as the United Nations and the European Union have become active players in helping to steer cyber-diplomacy and regime-building[47].

In tracing the timeline of diplomatic initiatives in cyberspace, the earliest and most notable starting point is the initiative launched by the United Nations. In 1998, starting from a Russian proposal, the United Nations' General Assembly (UNGA) approved the Resolution 53/70 with the aim of valuing the mechanisms in order to mitigate the risks caused by the malicious use of the ICT and develop cooperation in the cyberspace[48]. After the adoption of the resolution, the General Assembly established a Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security.

Since 2004, the GGE had primarily focused on examining the threats and challenges to international security arising from cyberspace, with the aim of proposing measures to enhance stability and foster international cooperation. For instance, the 2013 report recommended laying the groundwork for the development of "*norms,*

[46] Meyer, P. (2012). Diplomatic Alternatives to Cyber-Warfare. The RUSI Journal, 157(1), pp.14 – 19

[47] Johnstone, I., Sukumar, A. and Trachtman, J. (2023a). Building cybersecurity through multistakeholder diplomacy: Politics, processes, and prospects.

[48] UN General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security (A/RES/53/70), December, 4th 1998

rules or principles of responsible behavior of States and confidence-building measures with regard to information space"[49]. In its 2015 report, the GGE identified as key priorities the need to further analyze the applicability of existing international law to the cyber domain, as well as the necessity to develop measures aimed at building trust, transparency, and cooperation among States. However, the GGE faced two main limitations: the voluntary nature of the implementation of its proposed norms by States, and the difficulty in adapting its internal discussions to the changing geopolitical context, as evidenced, for example, by the cyberattacks against Ukraine in 2015[50]. From a negotiation theory perspective, the GGE's "exclusive club" structure can be understood as a small-group negotiation format, where limited participation may facilitate coordination among members but often exacerbates deadlocks in multilateral decision-making. Consensus becomes harder to achieve because excluded stakeholders are unable to influence the agenda or express their interests, leading to perceived inequities and stalled negotiations. In contrast, the later OEWG represents a plenary negotiation format, with broader multistakeholder involvement, which increases legitimacy and reduces the likelihood of deadlock by allowing more parties to participate in shaping outcomes and sharing their perspectives. However, the principal one for sure was the perception of the GGE being an "exclusive club", due to the exclusion not only of a significant number of States, but also of non-State actors[51].

[49] UN General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/68/98), June, 24th 2013

[50] Ruhl, C., Maurer, T., Hoffman, W. and Hollis, D.B. (2020). Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads. Washigton DC: Carnegie Endowment for International Peace.

[51] *Ibidem*

Throughout their negotiations, member States have been using UN organizations as organizational platforms for their competing agendas[52]. At the same time, appeals by non-State actors for greater access or input into the GGE process may highlight a process which proves inadequate in addressing issues where the majority of relevant stakeholders remain excluded from the dialogue. The inability to include a broader range of stakeholders also constrained the GGE's capacity to foster genuine trust, transparency, and cooperation[53].

Despite evident shortcomings, any assessment of the initiatives promoted within the United Nations framework must also recognize the notably efficient role played by the Organization for Security and Cooperation in Europe (OSCE), especially in the work done for the adoption of CBMs in cyberspace[54].

The initiative began with the establishment of the Informal Working Group (IWG), tasked with discussing the dynamics of the cyber domain in order to enhance stability and security within the OSCE framework, building on the premise that they had already proven effective as a crisis prevention mechanism during the Cold War[55].

In 2013, the 57 OSCE participating States approved the first set of CBMs – a total of eleven – primarily focused on establishing transparency measures, communication channels, and trust among States. In 2016, a second set, comprising

[52] Maurer, T. (2011). Cyber norm emergence at the United Nations - An Analysis of the Activities at the UN Regarding Cyber-security. Cambridge: Belfer Center for Science and International Affairs - Harvard Kennedy School.

[53] Ruhl, C., Hollis, D., Hoffman, W. and Maurer, T. (2020a). Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads.

[54] Pawlak, P. (2016). Confidence-Building Measures in Cyberspace: Current Debates and Trends Confidence-Building Measures in Cyberspace: Current Debates and Trends. In: H. Rõigas and A.-M. Osula eds., International Cyber Norms Legal, Policy & Industry Perspectives. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, pp.129–153.

[55] *Ibidem*

five additional measures was adopted, resulting in the development of the first internationally recognized framework of non-binding measures in the cyber domain[56]. Unfortunately, the initiatives implemented within the OSCE framework were influenced by the political and ideological tensions emerged within the GGE, which ultimately led to the suspension of the approval process for the third set of CBMs, entirely focused on addressing the "how" of applying existing international law to the cyber domain[57].

Tension further exacerbated the dialogues to the point that in 2018, through Resolution 73/27 of the UNGA proposed by the Russian Federation, an Open-Ended Working Group (OEWG) was established, to which all UN member States were invited to participate.

The OEWG's main task was to continue developing rules, norms, and principles for the responsible behavior of States, discussing their implementation methods and the possibility of establishing an institutional dialogue under the auspices of the UN.

Russian political perception of the OEWG was the one of a potent counterweight to the GGE, outnumbered by the US and its allies. Indeed, the OEWG's publication of a final report, subsequently adopted by the UN General Assembly, was articulated as a "triumphant success of diplomacy" by Russia[58].

This time, the frustrations provoked by "exclusive club" approach of the GGE were left out, ensuring greater representativeness. In December 2019, the OEWG organized an informal, intersessional meeting in a multistakeholder format: chaired

[56] OSCE, Permanent Council Decision No. 1202, March, 10th 2016

[57] Pawlak, P. (2016). Confidence-Building Measures in Cyberspace: Current Debates and Trends Confidence-Building Measures in Cyberspace: Current Debates and Trends. In: H. Rõigas and A.-M. Osula eds., International Cyber Norms Legal, Policy & Industry Perspectives. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, pp.129–153

[58] Sukumar, A. (2023). The geopolitics of multistakeholder cyber-diplomacy: A comparative analysis. In: Building an International Cybersecurity Regime: Multistakeholder Diplomacy. Edward Elgar Publishing, pp. 20 - 58

by Singapore, this meeting was the first multistakeholder meeting on cyber norms held under the aegis of the UN. NGOs were permitted to participate in substantive sessions, a significant shift from their previous roles as mere observers or occasional participants in UN intergovernmental gatherings. This was a departure from the traditional method of involving non-governmental entities as observers or participants in UN inter-governmental meetings. The chair of the OEWG and other representatives from the Group, also participated in a number of informal multistakeholder sessions. This broadened multistakeholder involvement extended even into the substantive sessions of the OEWG[59].

As a result of opening its participation to non-governmental entities, the OEWG also received written inputs from a number of stakeholders on the pre-draft, Zero Draft, and First Draft on the Group's report.

1.4.1.2 G7 Initiatives

The initiatives were taking place also outside the UN framework. The Group of Seven (G7) in 2016 created the Ise-Shima Cyber Group (ISCG), a permanent platform dedicated entirely to cyber-related issues. The ISCG held its first meeting in 2017 during the G7 presidency of Italy, with the goal of establishing "responsible State behavior norms in cyberspace", in line with the provisions of the UN GGE[60]. The work carried out under the Italian presidency was an attempt to emphasize the need to shift from a predominantly technical approach to a political-diplomatic process, aimed at developing an initial framework of shared rules of conduct for cyberspace[61].

[59] *Ibidem*

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

[61] Martino, L. (2021). Le iniziative diplomatiche per il cyberspazio: punti di forza e di debolezza. IAI Istituto Affari Internazionali. Rome: IAI

The European Union also devoted significant attention and resources to strengthening cyber resilience in its internal market policy area. The Council of Europe adopted the Convention for Cybercrime in the early years of advancing global connectivity in 2001. Known as the Budapest Convention, it provides a common framework for international cooperation for its members and aims to harmonize cybercrime legislation. With its global reach, the Convention not only offered the most comprehensive guideline for investigating and prosecuting cybercrime but also provided a 24/7 law enforcement network to facilitate information sharing and operational cooperation between its members[62]. Further development within the EU cyber-diplomacy efforts will be discussed later in the paragraph “The European Union cyber-diplomacy initiatives“.

Back to the research question, whether or not diplomatic negotiation mechanisms can mitigate cyber conflicts and improve international cybersecurity cooperation, it is possible to draw the conclusion from historical and factual evaluation that the multistakeholderism approach improves the legitimacy and acceptance of outcomes, making them last longer. the OEWG's outcomes demonstrate that diplomatic mechanisms can, in fact, aid in the reduction of cyber conflicts. Furthermore, a broad range of actors' active participation supports in reducing competing points of view and reducing geopolitical tensions.

As the following paragraph demonstrates, this is one reason why many States have nominated Tech Ambassadors and whole departments within their foreign affairs ministers that concentrate exclusively on cyberspace. The main goal of such efforts is to build relationships not just with diplomats but also with tech companies alongside other non-State actors.

[62] Salvi, A., Tiirmaa-Klaar, H. and Lewis, J. (2025). A Handbook for the Practice of Cyber-diplomacy. Luxembourg: EU Institute for Security Studies

1.5 State Actors Shaping Cyber-Diplomacy: Emerging Diplomatic Figures

When designing a tech-integrated foreign policy, governments generally choose between two main models: appointing a dedicated tech ambassador or creating a network of tech-focused diplomats. Understanding how States assign diplomatic responsibilities in cyberspace offers valuable insights into both the prioritization of cyber issues and the broader strategic posture in foreign policy. The designation of cyber-focused diplomatic roles serves not only as an indicator of institutional commitment but also reflects how each State conceptualizes the cyber domain, its intersection with other policy areas, and the level of integration into national security and international engagement strategies[63].

A dedicated tech ambassador is a high-level representative responsible for building direct relationships with major technology companies and key stakeholders, often based in strategic locations such as Silicon Valley. This model is especially useful for smaller countries seeking visibility and access to influential actors in the tech sector. However, it can be expensive to establish and requires specific expertise and strong central coordination. In contrast, a network of tech diplomats involves placing multiple specialists in embassies across different countries. This model allows for wider geographical coverage and more flexibility in responding to emerging trends or challenges in global technology policy. The downside is that it requires careful coordination. Countries like Denmark and the UK have used the ambassador model, while China and the United States have developed broader networks to monitor and engage with global tech developments. Each approach

[63] Salvi, A., Tiirmaa-Klaar, H. and Lewis, J. (2025). A Handbook for the Practice of Cyber-diplomacy. Luxembourg: EU Institute for Security Studies

offers distinct advantages depending on a country's diplomatic goals, resources, and strategic priorities[64].

There is a clear divide between those countries leading in cyber-diplomacy and those still developing foundational capabilities. While the OEWG within the UN process has stimulated broader participation, many Global South countries have only recently begun engaging with cyber-diplomatic mechanisms[65]. Some promising examples of emerging engagement include Brazil's appointment of a dedicated tech diplomat based in Silicon Valley, a strategic move to interface directly with major technology stakeholders. Pakistan's Ministry of Foreign Affairs is actively exploring how digital technologies can be leveraged to address social and economic development challenges. Similarly, India has created a Division for New and Emerging Strategic Technologies within its foreign ministry, showing its intention to play a more active role in shaping global technology governance. Senegal has also expressed interest in enhancing its tech diplomacy footprint, notably by considering the appointment of a "digital ambassador" to better engage with the technology sector[66]. In contrast, countries in the Global North have been moving toward more complex and integrative approaches.

Denmark was among the first to appoint a Tech Ambassador with a global mandate. France followed suit with the creation of the "Ambassadeur du Numérique", emphasizing the country's commitment to shaping digital norms. Australia broadened its scope by expanding the role of its Ambassador for Cyber Affairs to include Critical Technologies, a move that reflects the increasingly interconnected nature of cybersecurity and emerging technologies. The United States further

[64] Erzse, A. and Garson, M. (2022). A Leaders' Guide to Building a Tech- Forward Foreign Policy. London: Tony Blair Institute for Global Change

[65] Höne, K. (2022). What is Tech Diplomacy? Heinrich-Böll-Stiftung.

[66] Cheney, C. (2022). Why more lower-income nations are engaging in tech diplomacy. [online] Devex. Available at: https://www.devex.com/news/why-more-lower-income-nations-are-engaging-in-tech-diplomacy-104006

institutionalized its approach with the 2022 establishment of the Bureau of Cyberspace and Digital Policy, staffed by nearly 100 personnel, and the appointment of Nathaniel C. Fick as the first Ambassador at Large for Cyberspace and Digital Policy[67].

In this sense, cyberspace, cybersecurity, and cyber-diplomacy are floating signifiers with indeterminate content that are defined by the vantage points and agendas of diplomatic actors. They depend on a State's institutional arrangement, political configuration, and geopolitical standing. A State's internal dynamics, such as the shape of its bureaucracy, political objectives, and technological expertise, effectively dictate how it "*diplomatises*" cyberspace. At the same time, these domestic factors are interconnected with external ones, such as the level of international agreement on cyber norms or the strategic position of States in the global cyber order[68].

Like many other diplomats, cyber diplomats should cover a wide range of interrelated issues and be able to move quickly between complex subject areas. They are integral to ensuring that national policies and regulations are aligned with international trends and best practices. Their duties involve not only advising on domestic policy but also coordinating and aligning these policies with international multilateral, minilateral, and bilateral agreements. Through these efforts, they help present a cohesive, unified, whole-of-government policy position in global discussions, advancing their country's interests in international fora. Furthermore, tech diplomats are tasked with defining and promoting their nation's values,

[67]Schaffer, A. (2022). It's a big day at the State Department for U.S. cyberdiplomacy. Washington Post. [online] Available at: https://www.washingtonpost.com/politics/2022/04/04/its-big-day-State-department-us-cyberdiplomacy/

[68] Barrinha, A. (2024a). Cyber-diplomacy: The Emergence of a Transient Field. The Hague Journal of Diplomacy, 19(3), pp.1–28

technological capabilities, and priorities abroad, thereby influencing global cyber governance, innovation, and security frameworks[69].

[69] Salvi, A., Tiirmaa-Klaar, H. and Lewis, J. (2025). A Handbook for the Practice of Cyber-diplomacy. Luxembourg: EU Institute for Security Studies

COUNTRY	MODEL	KEY FEATURES	STRATEGIC FOCUS
Denmark	**Tech Ambassador Model**	First country to appoint a Tech Ambassador with a global mandate; based in Silicon Valley.	Direct engagement with tech firms; visibility; norm-setting.
United States	**Networked Institutional Model**	Created Bureau of Cyberspace and Digital Policy (2022); Ambassador at Large; nearly 100 staff.	Integration of cyber/digital policy into national security; global engagement.
India	**Hybrid Institutional Model**	Established Division for New and Emerging Strategic Technologies within MEA.	Emerging tech policy; shaping global digital norms.
France	**Ambassador Model**	Appointed "Ambassadeur du Numérique" to represent France in digital diplomacy.	Digital sovereignty; regulation; cyber governance.
Australia	***Expanded Ambassadorial Role***	Expanded Cyber Ambassador's portfolio to include Critical Technologies.	Cybersecurity-tech policy integration; regional influence.
Brazil	**Tech Envoy Initiative**	Appointed tech diplomat in Silicon Valley to connect directly with global tech stakeholders.	Building diplomatic capacity; increasing visibility in the global tech ecosystem.

Table 3: Comparative Overview of National Approaches to Tech-Integrated Foreign Policy

1.5.1 National Approaches in Cyber-Diplomatic Engagement

While the preceding section emphasized the behavior of State actors in defining the norms, principles, and diplomatic structures of cyber-diplomacy at the international level, the following section focus on the act of operationalizing them within the national frame. The investigation on national framings shows whether States embodying cyber-diplomatic goals and how they transform these into national strategies, institutional designs, and even foreign policy agendas.

As cyber threats continue to grow in scale and complexity, most States have developed their own national agendas for cyber-diplomacy. National agendas reflect each country's strategic interests, legal traditions, and foreign policy priorities in the cyber domain.

Some countries focus on promoting international norms and cooperation, others on cybersecurity capacity building, cybercrime prevention, or developing national digital sovereignty. National cyber-diplomacy initiatives typically involve a mix of legal, political, technical, and military tools, and require coordination among different government institutions, such as foreign ministries, cybersecurity agencies, and ministries of defense. The following sections give concrete examples of State activities in cyber-diplomacy, highlighting the diversity of approaches and contributions to international cyber stability.

1.5.1.1 The Case of Denmark’s Tech Ambassador

Denmark’s appointment of the world’s first Tech Ambassador in 2017 marked a significant shift in how States can engage with global technological power structures. By nominating Casper Klynge to the position, the Danish government took a strategic decision to broaden the scope of diplomacy beyond traditional State-to-State relations and include large technology companies including Meta, Google, and others as central geopolitical actors because of their global influence in areas such as cybersecurity, data governance, artificial intelligence, and digital regulation.

Denmark designed a model of cyber-diplomacy grounded in high-level representation, assigning the ambassador a global mandate while establishing operational offices in Copenhagen, Silicon Valley and Beijing[70].

The Danish *TechPlomacy* strategy is built around six core functions: to represent Denmark's interests in relation to the global tech industry; to gather and transmit strategic knowledge to government agencies; to support innovation and ensure technology remains central to foreign and security policy discussions; to build international coalitions with both public and private actors; to contribute to domestic public debates on the role of technology; and to promote Danish tech and investment opportunities abroad. These goals highlight Denmark's ambition to not only react to the global tech landscape, but to actively shape it in accordance with its national interests and democratic values. The ambassador's role involved a mix of classic diplomatic tools, such as bilateral meetings and international negotiations, with modern communication methods, including social media outreach, video briefings, and public engagement[71].

Furthermore, Denmark's tech diplomacy is supported by several institutional mechanisms. The Tech Advisory Board, composed of experts from academia, the private sector, and civil society, provides strategic guidance and promotes reflection on complex tech-policy issues. A tech network across Danish embassies and multilateral missions reinforces global coordination and ensures that emerging technological developments are monitored and addressed from a variety of regional perspectives. Unlike many top-down diplomatic initiatives, Denmark also emphasizes citizen engagement as a core component of its tech diplomacy. Annual polls, public events, and dialogue with civil society are used to ensure that the

[70] Satariano, A. (2019). The World's First Ambassador to the Tech Industry (Published 2019). The New York Times. [online] 3 Sep. Available at: https://www.nytimes.com/2019/09/03/technology/denmark-tech-ambassador.html

[71] Office of the Danish Tech Ambassador. The TechPlomacy Approach. [online] Ministry of Foreign Affairs of Denmark. Available at: https://techamb.um.dk/the-techplomacy-approach.

country's foreign policy remains connected to domestic values, concerns, and democratic accountability[72].

However, despite innovative initiatives, Denmark's strategy concerning cyber and technological diplomacy has come across many roadblocks.

Internally, there were issues of coordination and dedication among government ministries. Several staff members within the Ministry of Foreign Affairs perceived the *TechPlomacy* as mainly symbolic rather than pragmatic initiative. Denmark faced challenges in exerting influence over major technology companies, which frequently demonstrated little interest in recommendations from what they considered a minor nation. Consequently, Denmark shifted to building alliances with like-minded States and NGOs to amplify its influence on global technological matters[73].

Denmark created a TechPlomacy model that included operational offices in Beijing, Silicon Valley, and Copenhagen along with high-level ambassadorial representation. Although creative, the project had trouble influencing big tech companies and producing quantifiable results, and it was occasionally viewed internally as more symbolic than useful. In order to boost its influence, Denmark consequently started forming partnerships with like-minded governments and non-governmental organizations.

Representing Danish interests in the international tech sector, gathering and disseminating strategic knowledge to government agencies, fostering innovation and incorporating technology into foreign and security policy, forming international alliances, and participating in domestic technological discussions and promoting Danish tech and investment abroad are the six main pillars of the strategy.

[72] Office of the Danish Tech Ambassador (2021). Tech Diplomatic Results (2021-2023). [online] Ministry of Foreign Affairs of Denmark. Available at: https://techamb.um.dk/impact/tech-diplomatic-results

[73] Jacobsen, J.T. (2024). Commitment and compromise in Danish cyber and tech diplomacy. International Affairs, 100(6), pp.2361–2378.

In keeping with Denmark's goal to influence the global tech scene in a way that aligns with its democratic values and national interests, the ambassador used both conventional diplomatic instruments and contemporary communication techniques.

Nevertheless, Denmark's model fits into the definition of cyber-diplomacy given in this work. The strategy encompassed the development of new roles and institutions, the development of norms, engagement with different groups of stakeholders, and capacity-building initiatives within multilateral forums. Denmark's strategy demonstrates the potential and complexity of using diplomatic tools in the cyber domain. The example shows that although small Countries can exhibit creativity and proactivity, their success frequently depends on internal cohesion and readiness of external actors to collaborate.

1.5.1.2 US State Department's Office of the Coordinator for Cyber Issues

In the United States, the efforts made by the government to advance its interests in cyberspace have evolved over the years. The institutional development began in 2011, when Secretary of State Hillary Clinton announced the establishment of the Office of the Coordinator for Cyber Issues (State/S/CCI) within the State Department. The announcement came shortly before the release of the Obama administration's International Strategy for Cyberspace in the same year, making clear the rapidly growing significance the administration attributed to tech in foreign policy[74]. S/CCI's coordination function spans the full spectrum of cyber-related issues to include security, economic issues, freedom of expression, and free flow of information on the Internet[75].

The Office is nowadays currently led by Christopher Painter, and it brings together the many elements in the State Department working on cyber issues. Its

[74] *Ibidem*

[75] U.S. Department of State. (2017). Office of the Coordinator for Cyber Issues. [online] Available at: https://2009-2017.State.gov/s/cyberissues/index.htm

responsibilities include coordinating the Department's global diplomatic engagement on cyber issues, serving as the Department's liaison to the White House and federal departments and agencies on these issues, advising the Secretary and Deputy Secretaries on cyber issues and engagements, acting as liaison to public and private sector entities on cyber issues and coordinating the work of regional and functional bureaus within the Department engaged in these areas[76].

In 2016, the Department of State International Cyberspace Policy Strategy affirmed the elevation of cyberspace policy as a foreign policy imperative and the prioritization of State's efforts to mainstream cyberspace policy issues in its diplomatic activities[77]. Two years later, in 2018, pursuant to Executive Order 13800, the government led the development of an international engagement strategy in coordination with other federal agencies to strengthen the cooperation with other countries and international organizations[78].

This foundational work culminated in a more prominent and comprehensive structure. In January 2019, members of Congress introduced the *Cyber-diplomacy Act*, which established a new office to lead State's international cyberspace efforts. Examined issue this time were international cybersecurity, digital economy, and internet freedom, among others[79].

[76] U.S. government accountability office. (2025). Gao-25-108445, cyber-diplomacy: the Bureau of Cyberspace and Digital Policy's Efforts to Advance U.S. Interests. [online] Available at: https://files.gao.gov/reports/GAO-25-108445/index.html#_ftn3

[77] Department of State International Cyberspace Policy Strategy, March 2016. https://ccdcoe.org/uploads/2018/10/USA_Department-of-State_-International-Cyberspace-Policy-Strategy_2016.pdf

[78] U.S. Government Accountability Office. (2025). Gao-25-108445, cyber-diplomacy: The Bureau of Cyberspace and Digital Policy's Efforts to Advance U.S. Interests. [online] Available at: https://files.gao.gov/reports/GAO-25-108445/index.html#_ftn3

[79] Cyber-diplomacy Act of 2019, H.R. 739, 116th Cong. (2019)

In April 2022, the Bureau of Cyberspace and Digital Policy (CDP) was established, headed by a Senate-confirmed Ambassador-at-Large and staffed by nearly 100 personnel, with a mission to address national security challenges, economic opportunities, and implications associated with cyberspace, digital technologies, and digital policy. The office was, to elevate cyberspace as an organizing concept for U.S. diplomacy by consolidating efforts and leadership of cyberspace-related activities into a single unit[80].

Ensuring coherence across the diverse landscape of US actors – including the Department of Defense (DoD), Department of Homeland Security (DHS), National Security Agency (NSA), and the State Department – is a continuous effort proactively addressed through established mechanisms. Both S/CCI and CDP were designed with strong inter-agency coordination in mind: S/CCI initially served as the State Department's “liaison to the White House and federal departments and agencies” on cyber issues, formalizing communication channels across the executive branch. CDP also facilitates bilateral diplomacy efforts to achieve desired outcomes through activities such as communication with partner nations to discuss common interests. According to State officials, such engagement encourages global coordination on a collective strategy to achieve common policy outcomes. For instance, in 2022, State worked with Denmark to advance the Copenhagen Pledge on Tech for Democracy (the Pledge) that counters digital authoritarianism across the globe and advances digital freedom[81]. In addition, CDP works with other agencies through formal interagency agreements and informal processes to leverage expertise and develop a whole-of-government approach to executing key cyber-diplomacy activities.

[80] United States Department of State. (n.d.). Key Topics - Bureau of Cyberspace and Digital Policy. [online] Available at: https://www.State.gov/bureaus-offices/deputy-secretary-of-State/bureau-of-cyberspace-and-digital-policy/

[81] U.S. Department of State. (2022). DENMARK – Summit for Democracy. [online] Available at: https://www.State.gov/wp-content/uploads/2022/02/DENMARK-Summit-for-Democracy-Written-Statement-Accessible.pdf

The US strategy appears to be a meticulously orchestrated symphony, in which every component (DoD, DHS, NSA, State Department) fulfils its distinct role, while the conductor (CDP) guarantees that each of the instruments are coordinated and synchronized to deliver a cohesive performance on the international stage.

1.5.1.3 The European Union cyber-diplomacy initiatives

To understand the European Union's approach to cyber-diplomacy, it is essential to examine its strategies and the main pillars of its external actions in this domain.

The EU's approach to cyber-diplomacy is unique due to its institutional structure, value-driven policies and robust regulatory frameworks that harmonize the approaches of its 27 Member States. Unlike individual nation-States, the EU unites diverse national strategies under a shared policy and legal framework, while its Member States retain responsibility for national security. This structure enables the EU to establish a regional baseline for cybersecurity, foster strong solidarity and cooperation among Member States, and present a unified stance on the international stage[82].

In time, the European Union has taken several important steps to develop a strong and unified approach to cyber-diplomacy.
Diplomacy in the cyberspace in the EU formally began with the establishment of a dedicated cyber policy taskforce within the European External Action Service (EEAS) in 2012 and the adoption by the European Commission and the High Representative for Foreign Affairs and Security Policy of the first comprehensive EU Cybersecurity Strategy in 2013[83]

[82] Le Blanc, M. and Salvi, A. (2024). European Cyber Policy and Cyber-diplomacy. In: A. Salvi, H. Tiirmaa-Klaar and J.A. Lewis, eds., A Handbook for the Practice of Cyber-diplomacy. Luxembourg: Publications Office of the European Union, pp.58–70

[83] European Commission. (2013). Cybersecurity Strategy of the European Union: An open, safe and secure cyberspace. [online] Available at: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

The Council Conclusions on Cyber-diplomacy of 11 February 2015[84] outlined the EU's commitment to developing a common and comprehensive global approach to cyber-diplomacy that upholds human rights, democracy, and the rule of law. The document emphasized that freedom of expression, privacy, and gender equality must be respected in cyberspace, and stressed the importance of cybersecurity, cybercrime prevention, international cooperation, and capacity building in third countries.

On 14 March 2017, the EEAS and the European Commission presented a paper on a joint EU diplomatic response to cyber operations. The paper was examined by the Horizontal Working Party on Cyber Issues, established in 2016, responsible for coordination of Council's work on cyber issues. The Political and Security Committee (PSC), whose main interests are foreign and security policy, later received and discussed the draft. On June 2017, the Council of the European Union adopted the draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities – the *Cyber-diplomacy Toolbox* – which includes diplomatic "restrictive" measures within the EU Common Foreign and Security Policy that can be used against malicious operations directed against member States in cyberspace.

The Toolbox is part of the EU's approach to cyber-diplomacy within the Common Foreign and Security Policy, and it contributes to conflict prevention, the mitigation of cybersecurity threats, and greater stability in international relations. The EU diplomatic response to malicious cyber activities is proportionate to the scope, scale, duration, intensity, complexity, sophistication and impact of each cyber activity. All diplomatic efforts promote security and stability in cyberspace through

[84] Council Conclusions on Cyber-diplomacy. (2015). [online] Council of the European Union. Available at: https://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf

increased international cooperation, and reduce the risk of misperception, escalation and conflict that may stem from ICT incidents[85].

Soon after the adoption of the Cyber-diplomacy Toolbox, the Political and Security Committee adopted the corresponding implementing guidelines, which listed five categories of measures within the Cyber-diplomacy Toolkit. These included restrictive measures and the procedure for imposing such measures, as well as preventive, cooperative, stability measures and possible support to Member States' lawful responses[86].

The measures presented in the guidelines for the implementation of the toolbox are a combination of diplomatic, political and economic actions. These can be used to both prevent or respond to a malicious cyber activity, including in situations where the incident does not rise to the level of internationally wrongful acts but can still be considered as an unfriendly act. The measures can be used independently, or in parallel, either by an individual Member State, collectively with other Member States, by Member States in cooperation with the EU institutions or by the EU institutions themselves. Coordination with like-minded partners and international organizations is encouraged[87].

On 16 December 2020, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented a new EU Cybersecurity Strategy which allows the EU to step up leadership on international norms and standards in cyberspace, and to strengthen cooperation with partners

[85] Understanding the EU's approach to cyber-diplomacy and cyber defence. (2020). [online] European Parliament. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651937/EPRS_BRI(2020)651937_EN.pdf

[86] Kasper, A., Osula, A.-M. and Molnár, A. (2021). EU cybersecurity and cyber-diplomacy. In: Revista de Internet, Derecho Y Politica. Universitat Oberta de Catalunya

[87] Implementing Guidelines of the Cyber-diplomacy Toolbox. (2023). [online] pp.14–15. Available at: https://data.consilium.europa.eu/doc/document/ST-10289-2023-INIT/en/pdf

around the world to promote a global, open, stable and secure cyberspace, grounded in the rule of law, human rights, fundamental freedoms and democratic values[88].

Most recently, on 24 February 2025 a new Cybersecurity Blueprint was proposed to improve crisis coordination during large-scale cyber incidents, and it builds on the EU Cyber-diplomacy Toolbox.[89]

The Blueprint also foster a more structured cooperation between civilian and military actors, including cooperation with North Atlantic Treaty Organisation (NATO), given that a large-scale cyber incident affecting Union civilian infrastructure on which the military rely may also activate NATO response mechanisms. Although non-binding, the Blueprint updates earlier guidance and reflects lessons learned from past EU-level cyber exercises. Together, these initiatives show the EU's growing role in shaping global cyber-diplomacy, enhancing cybersecurity, and promoting peace and security in the digital world[90].

Given the increasingly dominant role of the internet and other digital technologies in issues pertaining to security, economic growth, and the design of societies across the globe, the relevance of tech diplomacy, as an attempt to manage international relations, will only grow in the next years[91].

[88] European Commission. (2020). The EU's Cybersecurity Strategy for the Digital Decade | Shaping Europe's digital future. [online] Available at: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

[89]Shaping Europe's digital future. (2025). Commission launches new cybersecurity blueprint to enhance EU cyber crisis coordination. [online] Available at: https://digital-strategy.ec.europa.eu/en/news/commission-launches-new-cybersecurity-blueprint-enhance-eu-cyber-crisis-coordination

[90] Shaping Europe's digital future. (2025b). Cyber Blueprint - Draft Council Recommendation. [online] Available at: https://digital-strategy.ec.europa.eu/en/library/cyber-blueprint-draft-council-recommendation

[91] Höne, K. (2022). What is Tech Diplomacy? Heinrich-Böll-Stiftung.

1.6 Beyond the State: The Growing Impact of Non-State Actors in Cyber-Diplomacy

Cyber Non-State Actors (CNSA) are key figures in the globalized world of nowadays: their operations could have a significant impact on international affairs, politics, and on the economy[92].

To address complex challenges, multilateralism alone is no longer enough. A new and dynamic response is required, a multi-stakeholder diplomacy approach brings together all relevant parties to tackle issues too complex to be resolved by any one of them. This approach does not imply that industry or civil society take decisions that should be taken by governments, but rather that all parties come together to ensure the stability, security and trustworthiness of the internet. It is about empowering States to take the most informed and, by extension, the best possible decisions. In essence, it is about giving civil society and industry a voice rather than a vote[93]. Private enterprises and corporations can have an important role in the Internet: they contribute to cyber-diplomacy by forming public-private partnerships, sharing threat intelligence, and working with governments to improve cybersecurity and safeguard key infrastructure[94].

NGOs and think tanks contribute to cyber-diplomacy by conducting research, giving expert analysis, and advocating for safe cyber practices. They frequently

[92] Paganini, P. (2022). Non-State Actors in Cyberspace: an Attempt to a Taxonomic classification, role, Impact and Relations with a State's socio- Economic Structure. Università degli Studi di Firenze: Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali (CCSSII). [online]
Available at: https://www.cssii.unifi.it/upload/sub/Pubblicazioni/2022_Paganini_Pierluigi.pdf

[93] Malisevic, N. (2024). The Future of Cybersecurity: Embracing Multistakeholder Diplomacy. In: A. Salvi, H. Tiirmaa-Klaar and J.A. Lewis, eds., A Handbook for the Practice of Cyber-diplomacy. Luxembourg: Publications Office of the European Union, pp.94–95

[94] Radanliev, P. (2024). Cyber-diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing. Journal of Cyber Security Technology, [online] pp.1–51

provide policy suggestions and work with governments and international agencies. In cyber-diplomacy conversations, cybersecurity experts, researchers, and technical specialists share useful insights and ideas. Their knowledge contributes to developing policies, tactics, and international cybersecurity activities[95].

Microsoft Corporation is arguably the most active company in the field; in 2017, it called for a “Digital Geneva Convention” that would reaffirm the “tech sector's” status as a “neutral Digital Switzerland”. Later, in November 2018, Microsoft organized an event called “An Evening on Digital Peace” at the Peace Palace in The Hague, bringing together diplomats, research scholars, and technical experts. The event was organized in partnership with the Institute for Accountability in the Digital Age, a non-profit think tank[96]. In 2018, Microsoft also announced the “Cybersecurity Tech Accord” (CTA), which prompted technology companies to promise to protect their users and customers from cyberattacks, regardless of the attacker's “criminal or geopolitical” motivation. At the time of writing, almost 200 companies have “adopted” the CTA[97]. This supports the idea that collaboration with the private sector can help extend the tenure of diplomats serving in government roles.

The NCS Guide 2021, the 2nd Edition of the Guide to developing a National Cybersecurity Strategy, is likely the most tangible result of the private-public sector partnership. The partners, in which Deloitte and Microsoft appear, came together with an appreciation of the need to strengthen cooperation and coordination across the international community on cybersecurity capacity-building. The objective of

[95] *Ibidem*

[96] Microsoft Netherlands (2018). The Need for Digital Peace at the Peace Palace, The Hague. [online] YouTube. Available at: https://www.youtube.com/watch?v=rMXJMMcHjYs [Accessed 23 Jun. 2025]

[97] Sukumar, A. (2023). The geopolitics of multistakeholder cyber-diplomacy: A comparative analysis. In: Building an International Cybersecurity Regime: Multistakeholder Diplomacy. Edward Elgar Publishing, pp. 20 – 58

this effort was to support national leaders and policymakers in the development of defensive and proactive responses to cyber risks, in the form of a National Cybersecurity Strategy, and in thinking strategically about cybersecurity, cyber-preparedness, response and resilience, and building confidence and security in the use of ICTs[98].

In this sense, negotiations and diplomatic efforts may significantly be affected by the work of non-State actors, particularly those encouraged by the input from multiple stakeholders. These initiatives promote openness, harmonize national and global agendas, and establish a basis for reciprocal comprehension and responsibility.

1.6.1 The Global Commission on the Stability of Cyberspace: a successful example of multi-stakeholder cyber-diplomacy

A useful example is the Global Commission on the Stability of Cyberspace (GCSC)[99], which began its work convinced that an issue traditionally reserved to States – international peace and security – could no longer be addressed without engaging other stakeholders. The initiative was launched in February 2017, published its final report in November 2019, and concluded its activities after the publication of the CyberStability Paper Series in December 2021[100].

The Commission brought together a diverse set of members, including State representatives such as the Foreign Ministers of the Netherlands and France, and the Chief Executive of the Cyber Security Agency of Singapore, alongside

[98] ITU (2021). Guide to Developing a National Cybersecurity Strategy 2nd Edition | Strategic Engagement in Cybersecurity Guide to Developing a National Cybersecurity Strategy.

[99] Global Commission on the Stability of Cyberspace (2019). The Global Commission on the Stability of Cyberspace: Promoting stability in cyberspace to build peace and prosperity . [online] Available at: https://cyberstability.org.

[100] The Hague Centre for Strategic Studies (2021). Global Commission on the Stability of Cyberspace. [online] HCSS. Available at: https://hcss.nl/global-commission-on-the-stability-of-cyberspace-homepage/.

representatives from private companies, civil society, and academia. The main goal was not only to put forward proposals for norms and policies to enhance security and stability in cyberspace, but also engage the full range of stakeholders to develop shared understandings, with the aim of advancing cyber stability by supporting information exchange and capacity building, basic research, and advocacy[101].

1.7 Conclusion

This chapter provided a key comprehensive understanding of the emergence and evolution of cyber-diplomacy, recognizing it as an increasingly important domain within international relations.

As it has been demonstrated, the growing relevance of digital technologies in foreign policy involves the "*diplomatization* of cyberspace", encouraged by multiple antagonistic State actions and notable cyber events, ranging from Moonlight Maze to the extensive operations in Ukraine.

The chapter has defined cyber-diplomacy not merely as the use of digital tools for diplomatic activities (as for e-diplomacy and digital diplomacy), but as the application of diplomatic tools to address issues arising from cyberspace, including security, economic concerns, human rights, and internet governance.

A major finding is the intrinsically multistakeholder characteristic of cyber-diplomacy, distinguishing it from conventional State-to-State interactions. It requires strong collaboration between governments, the private sector, academia, and civil society, whose active participation is vital for building, maintaining, and innovating cyberspace.

The chapter further highlighted the progression towards establishing norms and confidence-building measures within international forums, notably through the

[101] Global Commission on the Stability of Cyberspace (GCSC) (2019). Advancing Cyber-stability Final Report Global Commission On The Stability Of Cyberspace. [online] Available at: https://hcss.nl/wp-content/uploads/2019/11/GCSC-Final-Report-November-2019.pdf.

United Nations' Group of Governmental Experts and Open-Ended Working Group, and efforts by the OSCE and G7 initiatives.

Based on critical examination, cyber-diplomacy is still a “edifice still under construction”, despite having made significant progress in creating a framework for global engagement. It represents a fundamental shift from traditional State-to-State negotiations to complex, multi-actor processes, where States and non-State actors alike negotiate over security, norms, and governance in cyberspace.

Building upon this chapter two will explicitly explore the diplomatic mechanisms for managing cyber conflicts, analyzing different negotiation approaches. It will examine the critical roles of international organizations, the use of Track II diplomacy and further elaborate on the application of CBMs, trying to provide a comprehensive analysis of the tools and strategies employed to foster stability and cooperation.

2. Strategic Posture in Cyberspace: International and National Stances

Building on the previous chapter, which examined the evolution of cyber-diplomacy over time and described the roles of key actors like nations, international organizations and the private sector, this second section emphasizes the theoretical and practical methods through which cyber-diplomacy is carried out.
As cyberspace has emerged as a critical domain for international relations, the need for structured negotiation processes to handle cyber incidents, prevent escalation, and foster mutual trust has become increasingly crucial.

This dynamic can be framed through the lens of preventive diplomacy. Preventive diplomacy is a proactive approach in international relations that focuses on avoiding the escalation of conflicts and managing disputes before they turn violent. Its central goal is not merely to resolve crises once they erupt but to stop them from intensifying in the first place, thereby distinguishing it from post-conflict peacemaking. In practice, this involves preventive negotiation – a process of structured communication, often facilitated by third parties, designed to produce outcomes acceptable to all sides. Preventive diplomacy also depends on early warning systems, timely intervention, and efforts to foster attitudinal change between parties, reshaping their perceptions and expectations to reduce the risk of confrontation[102].

Applied to cyberspace, this framework highlights how negotiations among key actors serve as a form of preventive diplomacy. Through dialogue, CBMs and norm-setting, States and non-State actors seek to identify problems early, generate alternative solutions, and use a mix of incentives and disincentives to steer behavior toward restraint and cooperation. In this sense, cyber-diplomacy is not only a response to existing threats but also a preventive tool designed to manage vulnerabilities before they escalate into full-blown cyber conflict.

[102] I. William Zartmann (2001). Preventive negotiation: avoiding conflict escalation. Lanham, Md.: Rowman & Littlefield.

The passage seeks to offer an exhaustive understanding of national and regional approaches, including China, Russia, the United States and the European Union.

The topic then moves to the role of international organizations (UN, OSCE, NATO) which provide institutional frameworks for cooperation, norm development, and crisis management in the cyber domain. Here, the work will assess the negotiation approaches of leading States, distinguishing between cooperative and confrontational postures, and relate these to classical negotiation frameworks such as distributive and integrative models.

2.1 Diplomatic mechanisms for managing cyber conflicts

Nowadays, internet-based platforms and infrastructures continue to grow in importance for the delivery of basic services and become part of critical national infrastructure. The importance of the matter makes the risk of conflict higher, as well as the possibilities of misunderstandings or misperceptions between Countries.

It is cyber-diplomacy that prevent these conflicts from happening and contributes to building bridges between States to establish norms and crisis management frameworks in the field[103]. The international community has engaged in several regional and global processes focusing on clarifying how the existing international law applies to cyberspace, the development of norms of responsible State behavior, mutual non-aggression and information sharing in cyberspace and the development of confidence-building measures.

[103] Zwarts, H., Du Toit, J. and Von Solms, B. (2022). A Cyber-Diplomacy and Cybersecurity Awareness Framework (CDAF) for Developing Countries. European Conference on Cyber Warfare and Security, 21(1), pp.341 – 349.

During the years, bilateral, trilateral and multilateral agreements on cyber security have been signed as means to handle conflicts as well as tackle conflict of interests arising from cyberspace[104].

A nation's involvement in policy processes is influenced by at least two main broad dimensions: the political dimension and the functional dimension[105].When applied to the practice of cyber-diplomacy, on a political level this is translated into the importance a country attributes to cyber issues compared to other policy priorities, while the functional dimension involves a Country's capacity to engage in discussions and negotiations on the issues.

Nations that are most likely to be inactive in cyber-diplomacy are usually those which do not have the necessary resources to engage in the matter and those that consider cyber issues as low on their political agendas.

This dynamic can be explained through the "social delegation cycle", a theory which emphasizes the role of power – defined as an actor's ability to achieve goals – in determining participation and influence in negotiations. In collective bargaining processes, only objectives that the group has the power to achieve are treated as viable outcomes, and an individual actor's relative power shapes its ability to secure favorable terms. For weaker States, limited resources and capabilities restrict their ability to propose or shape collective goals, leaving them with little leverage to negotiate on equal terms with stronger actors. As a result, these States often become norm-takers rather than norm-shapers, compelled to accept the frameworks established by more powerful players[106].

[104] Sustainability Directory (2025). Cyber-diplomacy Strategies. [online] Available at: https://pollution.sustainability-directory.com/term/cyber-diplomacy-strategies/

[105] EuropeAid (2010) Toolkit for Capacity Development. Tools and Methods Series, Reference Document No. 6, European Commission. Available at https://europa.eu/capacity4dev/t-and-m-series/document/reference-document-nr-6-toolkit-capacity-development-2010

[106] Boella, G. and Van Der Torre, L. (2007). Power in Norm Negotiation.

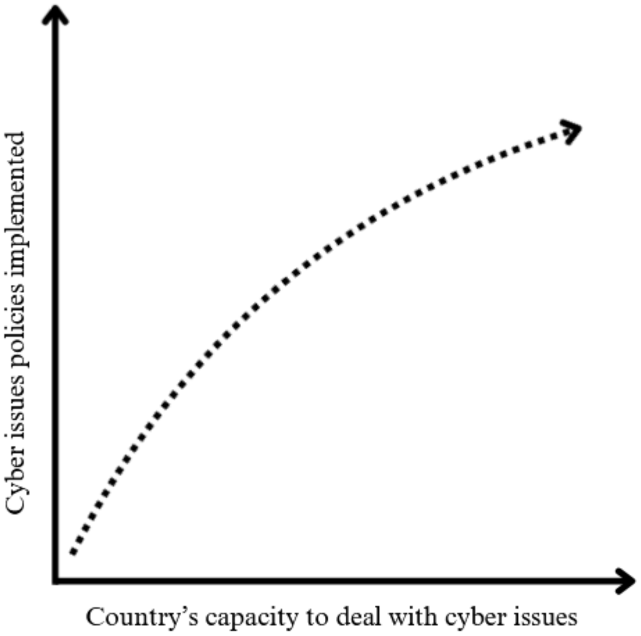
This dynamic explains why negotiation arenas in cyber-diplomacy are frequently dominated by stronger States, while weaker ones accept norms largely for the sake of maintaining stability and avoiding disproportionate costs of non-compliance.

Capacity levels and policy priorities are closely related and can have a significant influence on one another. As the graph illustrates, a nation is more likely to invest in strengthening its cyber-diplomacy capacity when it perceives cyber issues as a top priority. Conversely, countries that rank cyber issues low on their political agendas are unlikely to develop such capacities. This dynamic helps explain why negotiation arenas are often dominated by States with both high priority and strong capacity, enabling them to shape the agenda and influence outcomes more effectively than less-engaged actors[107].

However, even for States that place cyber issues lower on their national agendas, the safety and well-being of citizens – both online and offline – remains a top concern. This creates a security dilemma in cyber negotiations: as States seek to protect their populations, their actions may be perceived as threatening by others, generating mistrust or prompting competitive measures. Negotiating norms, rules,

[107] Borg Psaila, S. (2021). Improving the practice of cyber-diplomacy: A gap analysis of training, tools, and other resources. DiploFoundation. Commisioned by the Global Forum on Cyber Expertise (GFCE)

and confidence-building measures thus becomes essential to safeguard citizens while preventing escalation and maintaining stability in cyberspace.


Cyber issues policies implemented
Country's capacity to deal with cyber issues

Graph 1: Cyber issues engagement – Direct relation

Ignoring the issue of cyber threats and, as a result, failing to create appropriate policies, would also imply the exclusion from international engagement and adapt to decisions taken by others.

The next sections will examine national and regional approaches, analyzing China, Russia and US national strategies, as well as the one of the European Union and Latin America and Caribbean at a regional level.

2.2.1. National and regional approaches

2.1.1 China

Domestic political demands and a strategic ambition to challenge the current global system are the main drivers of China's increasing involvement in cyber-

diplomacy[108]. Although this term is rarely used formally in official policy documents, the Chinese government usually refers to Science and Technology (S&T) diplomacy when addressing cyber-related issues[109]. As science and technology become increasingly important in international relations, Beijing has integrated these components more prominently into its foreign policy, however, over the last several years, S&T diplomacy has undergone through a gradual overall transformation. This change has been caused by foreign political pressures.
China's primary S&T diplomacy partners in the past were developed nations. Towards them, the main focus was “diplomacy for S&T”, meaning the encouragement of scientific cooperation and personnel exchange to enhance domestic technological capacity. However, cut back on cooperation, especially from the United States, led to a shift of attention towards developing nations, especially those participating in the Belt and Road Initiative and emerging economies like the BRICS[110].

S&T diplomacy with developing nations takes the form of “S&T for diplomacy”, using technological cooperation to strengthen diplomatic ties and improve Country’s reputation[111]. In this new phase, China increasingly uses S&T not merely as a tool for cooperation, but as negotiation leverage. By linking technological

[108] Bozhkov, N. (2020). China’s Cyber-diplomacy: A Primer :: EU Cyber Direct. [online] eucyberdirect.eu. Available at: https://eucyberdirect.eu/research/chinas-cyber-diplomacy-a-primer.

[109] Asian Research Policy: KISTEP Korea Institute of S&T Evaluation and Planning. [online] KISTEP Korea Institute of S&T Evaluation and Planning. Available at: https://www.kistep.re.kr/arpIssue.es?act=content_view&list_no=225&act=content_view&mid=a20802000000.

[110] Segal, A. (2020). China’s Alternative Cyber Governance Regime Hearing on A ‘China Model?’ Beijing’s Promotion of Alternative Global Norms and Standards. [online] Available at: https://www.uscc.gov/sites/default/files/testimonies/March%2013%20Hearing_Panel%203_Adam%20Segal%20CFR.pdf.

[111] Asian Research Policy: KISTEP Korea Institute of S&T Evaluation and Planning. [online] KISTEP Korea Institute of S&T Evaluation and Planning. Available at: https://www.kistep.re.kr/arpIssue.es?act=content_view&list_no=225&act=content_view&mid=a20802000000.

collaboration – such as joint research, cybersecurity assistance, or infrastructure projects – to other strategic objectives, China applies an issue linkage strategy. Issue linkage involves discussing multiple issues together so that agreements or concessions on one area are contingent on outcomes in another.

This approach increases the likelihood of reaching negotiated settlements and encourages States to remain committed, as backing out would risk losing benefits across several connected domains. In practice, China ties S&T cooperation to objectives such as alignment on cyber norms, trade advantages, or political support in multilateral forums, transforming S&T diplomacy from a technical or cooperative activity into a deliberate instrument of strategic bargaining, shaping both the agenda and the behavior of other actors in international negotiations[112].

Through the Belt and Road Initiative (BRI) and its digital component – the Digital Silk Road – China exports its domestic cyber governance model, technical standards, and digital infrastructure. Since 2015, they have made significant investments in cross-border optical cables, cloud computing, fintech, and big data services in foreign countries. One strategic goal, for instance, is to expand the coverage of the BeiDou Navigation System to reduce reliance on the U.S.-controlled GPS network. These activities serve to internationalize Chinese technologies and create a broader coalition of countries aligned with its vision.

The nation is changing its approach to S&T diplomacy from a factor-based approach to a rule-based one. Project-based cooperation activities involving staff, funds, equipment, and information exchange are all part of factor-based S&T diplomacy, while the rule-based approach emphasizes active involvement in the creation of ethical governance structures, standard-setting procedures, and scientific regulations. Clearly, these rule-based activities often take place through regional or multilateral platforms and have higher entry thresholds. As China takes

[112] Poast, P. (2013). Issue linkage and international cooperation: An empirical investigation. Conflict Management and Peace Science, 30(3), pp.286–303.

a more active role in international rule-making processes, its responsibilities and expectations are increasing[113].

The Country promotes a multilateral, democratic, and transparent approach to global Internet governance and supports a leading role for the United Nations in setting cyber norms[114]. It actively participates in UN processes such as the Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG), advocating for the application of State sovereignty in cyberspace.

Beijing has maintained this territorialized approach to governing cyberspace since the beginning of international discussions on “the field of ICTs in the context of international security”. Under the auspices of the United Nations, China has repeatedly insisted that the Internet should be subject to “domestic legislation” and that traffic in cyberspace should be controlled “under the premises of national sovereignty and security” taking into account “historical, cultural and political differences among countries”[115].

Bilaterally, the relations with the Europe reflects broader tensions. The EU is China’s largest trading partner, and both parties agreed to a Strategic Agenda for Cooperation in 2013, covering a broad range of issues, including cyberspace[116]. The 2017 Europol-China agreement also aimed to address transnational cybercrime[117]. However, substantial differences remain. China’s emphasis on cyber sovereignty

[113] The Royal Society (2010) [online] Available at: https://royalsociety.org/-/media/policy/publications/2010/4294969468.pdf.

[114] Segal, A. (2018). When China Rules the Web. [online] Foreign Affairs. Available at: https://www.foreignaffairs.com/china/when-china-rules-web.

[115] Bozhkov, N. (2020). China’s Cyber-diplomacy: A Primer :: EU Cyber Direct. [online] eucyberdirect.eu. Available at: https://eucyberdirect.eu/research/chinas-cyber-diplomacy-a-primer.

[116] EEAS (n.d.). EU-China 2020 Strategic Agenda for Cooperation. [online] Available at: https://www.eeas.europa.eu/sites/default/files/20131123.pdf.

[117] Bozhkov, N. (2020). China’s Cyber-diplomacy: A Primer :: EU Cyber Direct. [online] eucyberdirect.eu. Available at: https://eucyberdirect.eu/research/chinas-cyber-diplomacy-a-primer.

conflicts with the EU's regulatory frameworks such as the General Data Protection Regulation (GDPR) and the NIS Directive, which prioritize privacy, openness, and cross-border data flows[118].

The EU promotes a decentralized, rights-based approach to cybersecurity, which contrasts sharply with China's top-down, Party-centric model.

China's emphasis on cyber sovereignty and centralized control clashes with the EU's regulatory frameworks, reflecting a value-based negotiation deadlock. Despite that, both sides recognize shared vulnerabilities – such as hybrid threats and AI-driven disinformation – and the potential value of continued dialogue.

In conclusion, the implementation of transformation of Chinese S&T diplomacy remains limited because of internal challenges. Despite enormous efforts, China lacks a sufficient number of highly skilled tech diplomats, and its domestic system still suffers from inefficiencies in resource management. In this regard, China's domestic S&T system continues to be inefficient in managing its resources, and the country does not have enough highly qualified S&T diplomats. Compared to 368 Americans, in 2019, only 98 Chinese people occupied important roles in significant international academic organizations[119]. It is true that it takes a sustained investment in professional experience and education to develop such expertise, but apparently China has not yet achieved a qualitative change in S&T diplomacy, despite its quantitative growth.

[118] *Ibidem*

[119] Asian Research Policy: KISTEP Korea Institute of S&T Evaluation and Planning. [online] KISTEP Korea Institute of S&T Evaluation and Planning. Available at: https://www.kistep.re.kr/arpIssue.es?act=content_view&list_no=225&act=content_view&mid=a20802000000.

2.1.2 Russia

Historically, Russia's diplomatic efforts concerning the impact of ICT on international relations have always been carried out with the intention of preventing conflicts and a cyber arms race[120].

The Russian Information Security Doctrine, which was adopted in September 2000, largely shaped Russia's position in international fora. It defined information security as the “protection of its [Russia’s] national interests in the information sphere defined by the totality of balanced interests of the individual, society, and the State”[121]. According to the Russian narrative, the international community is at the edge of perpetual cyberwar, with the “the information arms race […] gaining momentum” and the world facing an “existential” choice “between global cyber peace and cyberwarfare”. Moreover, all UN member States “are equally vulnerable […] and feel an urgent need to come out with a global response”[122].

Due to its perceived inferiority in communications technology, Russia envisions an international environment that it could control and prevent cyber-attacks and digital “arms race”[123]. This strategy exemplifies coercive diplomacy, as Russia attempts to build blocs of aligned actors and isolate Western positions in order to advance its interests and shape the norms of cyberspace.

The first resolution on "Developments in the Field of Information and Telecommunications in the Context of International Security" was submitted to the

[120] Popescu, N., Secrieru, S., Alatalu, S., Borogan, I., Chernenko, E., Herpig, S., Jonsson, O., Kurowska, X., Limnell, J., Pawlak, P., Pernik, P., Reinhold, T., Reshetnikov, A., Soldatov, A. and Vilmer, J.-B. (2018). Hacks, leaks and disruptions Russian cyber strategies EDITED BY Chaillot Papers. [online] Available at: https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf.

[121] Gady, F.-S. and Austin, G. (2010b). Russia, The United States, And Cyber-diplomacy Opening the Doors. [online] Available at: https://www.files.ethz.ch/isn/121211/USRussiaCyber_WEB.pdf.

[122] Hansel, M. (2023). Great power narratives on the challenges of cyber norm building. Policy Design and Practice, pp.1–16.

[123] *Ibidem*

UN General Assembly by Moscow in 1998. The document was pushed by concerns on the potential use of new technologies and means that could have been used “for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the security of States”[124].

In 1999 Russia introduced a new similar resolution but added two points: namely, that cyberspace may be misused for military purposes and that the international community should come up with principles on how to mitigate such dangers.
In accordance with the U.N. General Assembly Resolution No. 58/32 and to advance its cybersecurity agenda, Russia chaired the U.N. GGE in 2003 and continued to play a leading role until 2010.

The Russian Federation has established special partnerships on information security with the members of the Collective Security Treaty Organization as well as with the Shanghai Cooperation Organization[125] in 2009. The agreement – in the view of a leading Russian official –is considered one of the “most significant” development and is intended to “to create the political, legal and organizational foundations for strengthening confidence and developing cooperation among the parties and relevant national agencies”[126].

Over the decade, the desire of Moscow to establish sovereignty in cyberspace has emerged as a dominant theme, becoming widespread in the relevant regulatory legal acts. On May 1, 2019, Vladimir Putin signed the law “On Amendments to Certain Legislative Acts of the Russian Federation,” known as the “Law on the Sovereign

[124] UN General Assembly (2025). Resolution Adopted By The General Assembly: Developments in the field of information and telecommunications in the context of international security. [online] Un.org. Available at: https://docs.un.org/en/A/RES/53/70.

[125] Gady, F.-S. and Austin, G. (2010b). Russia, The United States, And Cyber-diplomacy Opening the Doors. [online] Available at: https://www.files.ethz.ch/isn/121211/USRussiaCyber_WEB.pdf.

[126] Mr. S. Shestakov (2010). Statement by Mr. S. Shestakov, representative of the Russian federation, at the joint meeting of the OSCE forum for security co-operation and the OSCE permanent council. [online] Available at: https://www.osce.org/files/f/documents/f/9/68693.pdf.

Internet", which prescribes the creation of an alternative system with the purpose of ensuring the functioning of the Internet in Russia in the event of its disconnection from the global network. This Act partially entered into force on November 1, 2019, and into full force in 2021[127].

The Russian involvement in cyber-diplomacy and its stance in the international system will be further explored in the next chapter. Because the Russian Federation's State-sponsored attacks are the most common, this work will concentrate on the analysis of Russia's role in international forums and the cyberattacks carried out against Ukraine and other nations.

2.1.3 United States

Since cyber threats affect each actor in the same way, the United States has constantly positioned cyber-diplomacy as a key component of its foreign policy in the twenty-first century, acknowledging that this implies international coordination, engagement, and cooperation at an unprecedented level.

As already mentioned in the first chapter of this work, a fundamental institutional move was the creation of the Office of the Coordinator for Cyber Issues (State/S/CCI) at the State Department in 2011, establishing a new foreign policy focus[128].

Promoting an information and communications infrastructure that facilitates global trade, strengthens security, promotes free speech and innovation, and guides State actions with norms of responsible behavior and the rule of law. Early international initiatives, like the 2013 and 2015 United Nations Group of Governmental Experts reports, confirmed that State sovereignty and international norms apply to

[127] Kurbalija, J. (2016). An introduction to internet governance 7th edition. [online] Available at: https://www.diplomacy.edu/wp-content/uploads/2021/12/AnIntroductiontoIG_7th-edition.pdf.

[128] Painter, C. (2018). Diplomacy in Cyberspace. [online] afsa.org. Available at: https://afsa.org/diplomacy-cyberspace

infrastructure and activities related to information and communications technology. This period also saw significant bilateral commitments, including a September 2015 agreement with China against cyber-enabled intellectual property (IP) theft for commercial gain, a commitment later endorsed by the G20 at the Antalya Summit in November 2015[129].

By March 2016, the Department of State's International Cyberspace Policy Strategy anticipated a continued increase in cyber-focused diplomatic efforts, signaling cyberspace policy as a foreign policy imperative.
This effort was reinforced by a December 2016 recommendation from the Commission on Enhancing National Cybersecurity to appoint an Ambassador for Cybersecurity. Further, the 2017 Group of 7 Declaration on Responsible State Behavior in Cyberspace recognized the urgent need for increased international cooperation to promote cybersecurity and stability, reaffirming the applicability of international law, promoting voluntary norms, and developing confidence-building measures.

President Donald J. Trump's Executive Order 13800 in May 2017 also designated the Secretary of State to lead an interagency effort to develop an international cooperation strategy for cybersecurity, emphasizing the promotion of an open, interoperable, reliable, and secure internet[130].

Legislative proposals like the Cyber-diplomacy Act of 2017, outlined a policy to promote an “open, interoperable, reliable, unfettered, and secure internet” governed by the multi-stakeholder model, which safeguards human rights, democracy, rule of law, freedom of expression, innovation, communication, and economic prosperity,

[129] US Congress (2025). U.S. Cyber-diplomacy in an Era of Growing Threats. [online] Congress of the United States. Available at: https://www.congress.gov/event/115th-congress/house-event/106830/text

[130] Cyber-diplomacy Toolbox (n.d.). Cyber-diplomacy in the USA. [online] Available at: https://www.cyber-diplomacy-toolbox.com/Cyber_Diplomacy_USA.html

while protecting against deception, fraud, and theft[131]. To implement this policy, objectives included clarifying international laws and norms, reducing escalation risks, cooperating with like-minded democracies, and securing commitments on responsible State behavior, such as refraining from IP theft, avoiding damage to critical infrastructure, underscoring the critical importance of cybersecurity and digital communications to the US mission[132].

The Cyber-diplomacy Act of 2021, which followed similar proposals like the 2017 Act, was the result of a legislative push to formally codify and elevate US cyber-diplomacy.

In order to protect human rights, democracy, the rule of law, freedom of expression, innovation, communication, and economic prosperity, this Act built a clear policy: to promote "an open, interoperable, reliable, unfettered, and secure internet" governed by the multi-stakeholder model[133]. Outlining international laws and norms, lowering the risk of escalation, collaborating with like-minded democracies, and obtaining pledges on responsible State behavior – such as abstaining from intellectual property theft, preventing damage to vital infrastructure, and defending human rights online – were among the main goals of this policy's implementation.

Most importantly, the Act required the Department of State to create a Bureau of International Cyberspace Policy, headed by an ambassador-ranked official appointed by the President with Senate consent. This Bureau, now known as the Bureau of Cyberspace and Digital Policy (CDP), was in fact established in April 2022 to elevate cyberspace as an organizing concept for US diplomacy. Leading

[131] Kerry, C. (2017). The Cyber-diplomacy Act of 2017: Giving Cyber the Importance It Needs at the State Department. [online] Lawfare. Available at: https://www.lawfaremedia.org/article/cyber-diplomacy-act-2017-giving-cyber-importance-it-needs-State-department

[132] Office, A. (2025). Cyber-diplomacy: The Bureau of Cyberspace and Digital Policy's Efforts to Advance U.S. Interests. [online] Gao.gov. Available at: https://www.gao.gov/assets/gao-25-108445.pdf

[133] Cyber-diplomacy Toolbox (n.d.). Cyber-diplomacy in the USA. [online] Available at: https://www.cyber-diplomacy-toolbox.com/Cyber_Diplomacy_USA.html

diplomatic initiatives pertaining to global cybersecurity, Internet access and freedom, the digital economy, cybercrime, and deterrence are among the Bureau's main responsibilities[134].

In order to ensure coordination in cyberspace policy throughout the US Government and within the Department of State, the Bureau also complies with GAO's recommendations for efficiently involving federal stakeholders and organizing State-sponsored initiatives.

Also, it serves as a liaison to the private sector and civil society in the effort of establishing a global deterrence framework for malicious cyber activity.

In its 2025 Report, GAO noted that CDP faced organizational challenges (such as defining roles, hiring staff, and ensuring sufficient expertise), however the office increased US global involvement in cyber-diplomacy[135].

Despite these challenges, the Department of State released its United States International Cyberspace and Digital Policy Strategy, the most recent comprehensive articulation of the US approach, in May 2024[136].

The idea of "digital solidarity" is emphasized in this strategy, which focusses on redistributing accountability for cyber defence, realigning incentives for sustained cybersecurity investment through partnerships, information sharing, and diplomacy, and establishing coalitions against threats. It identifies four key areas of action: promoting an open digital ecosystem; coordinating rights-respecting approaches to digital and data governance; promoting responsible State conduct and thwarting threats; and strengthening cyber capacity and digital policy with

[134] U.S. Department of State (2024). United States International Cyberspace & Digital Policy Strategy - United States Department of State. [online] United States Department of State. Available at: https://2021-2025.State.gov/united-States-international-cyberspace-and-digital-policy-strategy/

[135] Office, A. (2025). Cyber-diplomacy: The Bureau of Cyberspace and Digital Policy's Efforts to Advance U.S. Interests. [online] Gao.gov. Available at: https://www.gao.gov/assets/gao-25-108445.pdf

[136] Reed, J. (2024). State department international cyberspace digital policy strategy. IBM

international partners. In an increasingly complicated digital setting, these areas aim to promote shared values and increase resilience.

In order to align the future of technology with US interests and values, the strategy also emphasizes the significance of proactive participation in international, multilateral, and multistakeholder bodies[137]. This institutional framework supports the US policy in the international arena.

Through these evolving structures, the US engages in strategic dialogue by building strategic partnerships and multilateral engagement across various forums like the UN (including the Group of Governmental Experts, GGE), OSCE, G7, and G20, aiming to advance a common vision of cyberspace[138]. Examples of fundamental US diplomatic endeavors include the development of voluntary, non-binding peacetime norms (such as forbidding attacks on critical infrastructure), the promotion of a strategic framework for cyber stability, the use of confidence-building measures to lower escalation risks, and the argument that international law applies to State activity in cyberspace[139]. Concrete engagement has been registered not only in multilateral fora but also in bilateral agreement, like the landmark agreement with China against intellectual property theft[140] and the one with Denmark to counter digital authoritarianism through the Copenhagen Pledge. Furthermore, US cyber-diplomacy supports capacity-building initiatives for developing countries to

[137] U.S. Department of State (2024). United States International Cyberspace & Digital Policy Strategy - United States Department of State. [online] United States Department of State. Available at: https://2021-2025.State.gov/united-States-international-cyberspace-and-digital-policy-strategy/

[138] U.S Congress (2021). 117th Congress (2021-2022): Cyber-diplomacy Act of 2021. [online] Congress.gov. Available at: https://www.congress.gov/bill/117th-congress/house-bill/1251/text

[139] Cyber-diplomacy Toolbox (n.d.). Cyber-diplomacy in the USA. [online] Available at: https://www.cyber-diplomacy-toolbox.com/Cyber_Diplomacy_USA.html

[140] Qian, X. (2019). Cyberspace Security and U.S.-China Relations. Proceedings of the 2019 International Conference on Artificial Intelligence and Computer Science.

enhance their cybercrime-fighting capabilities and establish national cyber strategies, thereby improving global network security[141].

Despite notable advancements, challenges are still present, especially in reaching a more comprehensive global agreement on standards and ensuring the proper application of international law[142].

2.1.4 European Union

Cyber security is an issue not only for States but for the European Union as well. It extends beyond the resilience of networks, the digital single market or the prosecution of cyber criminals, and also concerns the EU's Common Foreign and Security Policy (CFSP) and Common Security and Defence Policy (CSDP).

At European level, the Horizontal Working Party on Cyber Issues was created in 2015 to coordinate the political aspects of cyberspace within the Council. The Horizontal Working Party on Cyber Issues, chaired by the rotating Presidency, and the Political and Security Committee (PSC) are responsible for appropriate implementation measures. Legally Member States are free to launch initiatives. It can participate in both legislative and non-legislative activities. Furthermore, member States decided in February 2015 to strengthen cyber-diplomacy at communitarian level in the European External Action Service. This was confirmed in November 2016 by the implementation plan on security and defence[143].

[141] Office, U.S.G.A. (2024). Cyber-diplomacy: State's Efforts Aim to Support U.S. Interests and Elevate Priorities | U.S. GAO. [online] www.gao.gov. Available at: https://www.gao.gov/products/gao-24-105563

[142] Office, A. (2025). Cyber-diplomacy: The Bureau of Cyberspace and Digital Policy's Efforts to Advance U.S. Interests. [online] Gao.gov. Available at: https://www.gao.gov/products/gao-25-108445

[143] Annegret Bendiek (2024). The EU as a Force for Peace in International Cyber-diplomacy. [online] Stiftung Wissenschaft und Politik (SWP). Available at: https://www.swp-berlin.org/publikation/the-eu-as-a-force-for-peace-in-international-cyber-diplomacy.

The 2016 EU Global Strategy emphasized the importance of cooperation with third parties in the cyber domain as a key aspect of the European Union's foreign and security policy and stressed the “State and Societal Resilience” of neighborhood Countries[144]. The 2020 EU’s Cybersecurity Strategy addresses also key aspects related to capacity building with surrounding areas, such as supporting the development of legislation and policies in line with European cyber-diplomacy policies and standards; and assistance to address malicious cyber activities[145]. The 2022 EU Strategic Compass recognizes the interconnected nature of cyber threats and the need for collaborative efforts to address them effectively. It emphasizes the importance of cyber cooperation and enhancing cyber resilience and capabilities not only within the Union but also in its neighboring regions, as a key aspect of its security and defence strategy[146].

The EU aims to protect, detect, defend, and deter cyberattacks through various policies and initiatives. Collaboration is crucial in countering hybrid threats, foreign information manipulation, and interference. Supporting partners in enhancing cyber resilience and deploying experts in case of cyber crises are fundamental elements of capacity building. Overall, the Strategic Compass underscores the importance of cyber cooperation and capacity building neighborhood Countries as part of a comprehensive approach to enhancing cybersecurity and addressing cyberthreats collaboratively and inclusively[147].

[144] Shared Vision, Common Action: A Stronger Europe A Global Strategy for the European Union’s Foreign And Security Policy. (2016). Available at: https://eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf.

[145] European Union (2020). The EU Security Union Strategy. Available at: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

[146] European Union External Action Service (2020). A Strategic Compass for Security and Defence. https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en

[147] *Ibidem*

Meanwhile, the European Union's cyber legal framework incorporated three other relevant documents that encompass capacity-building aspects. While the Regulation 2019/881 – Cyber Security Act – primarily focuses on enhancing cybersecurity within the European Union, some provisions indirectly address cooperation and capacity-building with EU surrounding regions in the context of cybersecurity, through ENISA[148]. That could potentially have positive effects by promoting best practices, information sharing, and collaboration in neighboring regions.

The Cyber Resilience Act also highlights the importance of cooperation and capacity building with surrounding regions in the context of cybersecurity, via bilateral Mutual Recognition Agreements for "conformity assessment and marking of regulated products"; the promotion of a global cyber resilience environment to strengthen the cybersecurity framework within and outside the union. Moreover, it addresses the cross-border nature of cybersecurity threats and the risks faced by Member States for the same products with digital elements[149].

In line with this extensive framework, the EU Cyber Solidarity Act proposed by the European Commission and entered into force in February 2025, endorses strengthening the readiness of critical entities across the EU and enhancing solidarity by establishing common response capacities against "significant or large-scale cybersecurity incidents", by providing support to cyber-incidents for third countries associated with the Digital Europe Programme[150]. Alongside the

[148] EUR-Lex (2019). Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). [online] Europa.eu. Available at: https://eur-lex.europa.eu/eli/reg/2019/881/.

[149] European Commission (2024). EU Cyber Resilience Act | Shaping Europe's digital future. [online] digital-strategy.ec.europa.eu. Available at: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act.

[150] European Commission (2025). The EU Cyber Solidarity Act | Shaping Europe's digital future. [online] Available at: https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity.

normative framework, the European Union has been promoting cyber capacity building in its surrounding regions through various initiatives and programs, such as extending the benefits of the EU Digital Single Market to the Eastern Partnership through the EU4Digital Initiative; enhancing cybersecurity and cyber resilience in Eastern Partnership (EaP) and third countries via Cybersecurity East the EU Cyber Capacity Building (EU CCB) Program; Supporting the improvement of cybersecurity frameworks and capabilities in the Western Balkan countries; Providing short-term technical assistance to neighboring countries to help them align with EU standards and practices through Technical Assistance and Information Exchange (TAIEX)[151].

2.2 The role of international organizations

Since the adoption of the concept of cyber-diplomacy in the foreign policies of different countries, they have predominantly relied upon signing of bilateral, tri-lateral and multilateral agreements on cyber security, mutual non-aggression and information sharing in cyberspace as the means to handle conflicts as well as tackle conflict of interests arising from cyberspace.

One of the milestones in global cyber-diplomacy arrangement begins with the Budapest Convention on Cybercrime. This arrangement, which was proposed in 2001 and came into force in 2004, is the first international convention dealing with crimes perpetrated via the Internet and other computer networks, with a focus on copyright infringements, computer-related fraud, child pornography, and network security violations. It also contains a series of powers and procedures such as the search of computer networks and interception. Its primary goal as laid forth in the Preamble is the adoption, notably via the adoption of suitable laws and promoting international cooperation of a common crime strategy to safeguard society from

[151] Barmpaliou, N. and Pawlak, P. (2025). Between ambition and pragmatism: The future of cyber capacity-building in a fragmented world. [online] European Union Institute for Security Studies. Available at: https://www.iss.europa.eu/publications/reports/between-ambition-and-pragmatism-future-cyber-capacity-building-fragmented.

cybercrime. This convention is the first multilateral legally binding instrument to regulate cybercrime and is the first global cyber diplomatic agreement. The Budapest Convention is also supplemented by a Protocol on Xenophobia and Racism committed through computer systems[152]. Nevertheless, this convention cannot be called truly global yet as the two largest populated countries, China and India are not signatories to the arrangement. Also, Russia, a powerful cyber actor in the globe has refused to sign the convention citing sovereignty concerns[153].

Initiatives such as the United Nations Group of Governmental Experts and the Open-ended Working Group have been established to reform the behavior of Countries in cyberspace.

As already examined in the first chapter of this work, the initiatives within the UN framework have been the foundational and crucial occasions of confront for norm development in the field. The UN GGE has evolved from a relatively marginal group in the early 2000s into a central body by 2021 and continued its work until recent days[154].

Four crucial elements, above all the others, including the application of existing international law, voluntary non-binding peacetime norms, confidence building,

[152] Council of Europe (2014). Budapest Convention and Related Standards. [online] Council of Europe. Available at: https://www.coe.int/en/web/cybercrime/the-budapest-convention.

[153] Chart of signatures and ratifications of Treaty 185 (2021, June 11). Retrieved from Council of Europe. Available at: https://www.coe.int/en/web/conventions/full-list?Module=signatures-by-treaty&treatynum=185

[154] Tiirmaa-Klaar, H. (2021). The Evolution of the UN Group of Governmental Experts on Cyber Issues From a Marginal Group to a Major International Security Norm-Setting Body Heli Tiirmaa-Klaar Ambassador for Cyber-diplomacy, Estonian Ministry of Foreign Affairs Cyberstability Paper Series New Conditions and Constellations in Cyber. [online] Available at: https://hcss.nl/wp-content/uploads/2021/12/Klaar.pdf.

and capacity-building measures form a normative framework for responsible State behavior[155], have been the main topics in both UN and international context.

The UNGGE work led to significant progress in norm development in the cyber-diplomacy field. Members States, in years, agreed on the applicability of international law, in particular the UN Charter, to the cyber-sphere, defined that State sovereignty is relevant for States' conduct of ICT-related activities and that State efforts to address the security of ICTs must go hand-in-hand with respect for human rights and fundamental freedoms[156] [157].

Several other international organizations have also played a role.

The OSCE Transnational Threats Department, every year from 2022, foster cooperation between partners by offering a training event on international cyber-diplomacy, following the idea that it is essential for all States to develop a good understanding of the main issues, so that equal resources can lead to meaningful contributions for the development of CBMs, which is, on the basis of the Decision No. 1039[158] on the development of confidence-building measures to reduce the

[155] *Ibidem*

[156] UN Secretary-General and UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2015). Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. digitallibrary.un.org. [online] Available at: https://digitallibrary.un.org/record/799853?v=pdf.

[157] UN Secretary-General and UN Group (2013). Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. [online] United Nations Digital Library System.

Available at: https://digitallibrary.un.org/record/753055?v=pdf.

[158] OSCE (2025). Permanent Council Decision No. 1039. [online] Osce.org. Available at: https://www.osce.org/pc/90169.

risks of conflict stemming from the use of information and communication technologies of the Permanent Council, the main focus of the Organization [159]. CBMs facilitate Sates' cyber risk management efforts through diplomatic engagement, information sharing and cooperative security measures. Preventive mechanisms that form the basis of nurturing trust among nations and setting standards to reduce the consequences of cyber conflicts escalating to zero scores geopolitical crises, CBMs play this role[160].

Yet, NATO initiatives are more focused on cyber defence. By facilitating information-sharing and the exchange of best practices, as well as by conducting cyber defence exercises to develop national expertise, Allies are assisted in strengthening their national cyber defenses. A specific Memorandum of Understanding lays out arrangements for the exchange of multiple cyber defence-related information and assistance to improve cyber incident prevention, resilience and response capabilities. The instrument of the NATO's Malware Information Sharing Platform provides the instruments to share rapidly technical information and indicators of compromise, reinforcing the Alliance's overall defence posture.

With a focus on cyber defence education, consultation, lessons learnt, and research and development, the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn is a NATO-accredited multinational and interdisciplinary cyber defence hub with recognized expertise. After the incident of State-sponsored cyber-attacks occurred in Estonia in 2008, the CCDCOE sponsored a multi-year effort to gather input from a group of recognized experts on how international law applies to cyber events. The first Tallinn Manual was concerned with the law of

[159] OSCE (2024). Promoting greater engagement in international cyber-diplomacy negotiations. [online] Osce.org. Available at: https://www.osce.org/cyber-ict-security/579961.

[160] Correia, M. (2024). Securing cyberspace: threats and challenges to NATO. [online] Repositorio.ucp.pt. Available at: https://repositorio.ucp.pt/entities/publication/d68f6efe-0e0a-4b02-b3a6-d10d7bdee695.

armed conflict[161] whereas Tallinn 2.0, the second Tallinn Manual, covers a considerably larger range of cyber activities, both in and out of armed conflict[162]. In 2021, the CCDCOE is working on the Tallinn Manual 3.0 Project, a five-year project that will see existing chapters revised and new issues of State relevance will be explored[163].

Personnel from Allied (and non-NATO) nations can receive training on the operation and maintenance of NATO communications and information systems at the NATO Communications and Information Academy in Portugal. The Academy also provides instruction and training in cyber defence. To support Alliance operations, strategy, policy, doctrine, and procedures, the NATO School in Germany offers training and education in cyber defence. Strategic thinking on political-military issues, including cyber defence, is fostered at the NATO Defence College in Rome, Italy[164].

As part of their increasingly coordinated efforts to counter hybrid threats, NATO and the EU have increased their cooperation in a number of areas, including cyber defence. Exchange best practices and information among cyber response teams are encouraged by several bilateral agreements, including the Technical Arrangement on Cyber Defence between the NATO Computer Incident Response Capability (now known as the NATO Cyber Security Centre) and the Computer Emergency Response Team for the EU institutions, bodies and agencies (CERT-EU).

[161] Tallinn Manual on the International Law Applicable to Cyber Warfare (2013, March). Retrieved from Cambridge University Press. Available at: https://www.cambridge.org/core/books/tallinn-manual-on-the-international

[162] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. (2017, February). Retrieved from Cambridge University Press: https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international

[163] The Tallinn Manual 3.0. (2021). Retrieved from The NATO Cooperative Cyber Defence Centre of Excellence. Available at: https://ccdcoe.org/research/tallinn-manual/

[164] NATO (2024). Cyber defence. [online] NATO. Available at: https://www.nato.int/cps/en/natohq/topics_78170.htm.

Additionally, cooperation is being strengthened in training, research and exercises, with tangible results in countering cyber threats[165].

The Structured Dialogue on Cyber initiative is a tangible example of collaboration. The EU and NATO held their first meeting on October 4th, 2024. The discussion aimed to strengthen their cooperation on cybersecurity and cyber defence. Officials from the EU and NATO examined recent developments during the discussion and found new areas of collaboration in improving cyber resilience, safeguarding vital infrastructure, and managing cyber crises. In order to counteract malicious cyber activity, new ways to improve alignment have been explored. Additionally, the Structured Dialogue also included a scenario-based discussion using a specific fictitious cyber scenario. The conversation allowed for the identification of specific cooperative actions and the improvement of expertise on the appropriate reaction to threats and crisis coordination frameworks.

The institutions reaffirmed their commitment to continue collaborating scheduling the following meeting in 2025[166].

However, a number of factors have complicated the international organizations' progress. The issue of attribution is one of the most controversial; the 2017 Tallinn Manual 2.0 States that attributional ambiguity makes applying traditional international law to cyberspace challenging and politically charged. Another layer of complexity is added by the development of artificial intelligence, especially since its widespread adoption in 2023. Because of this development, it is much harder to manage risks like malware and the rapid escalation. Addressing these issues requires clear rules, international cooperation, and mutual trust among the nations

[165] *Ibidem*

[166] EEAS (2024). European Union and NATO hold the first Structured Dialogue on Cyber. [online] EEAS. Available at: https://www.eeas.europa.eu/eeas/european-union-and-nato-hold-first-structured-dialogue-cyber-0_en.

involved[167]. Many governments, however, have neither the knowledge nor the necessary resources to maintain basic cyber-security standards or even ascertain what attacks are being conducted via servers on their territory. Nevertheless, most States voice profound reservations over national sovereignty when presented with the idea of a central global regulatory body for security in cyberspace[168].

On July 20, 2023, Secretary-General António Guterres, presented the "Policy Brief on A New Agenda for Peace". Among others, the policy brief includes a section titled "Tackling the extension of conflict and hostilities to cyberspace". One of the recommendations of this section was to "establish an independent multilateral accountability mechanism for malicious use of cyberspace by States to reduce incentives for such conduct. This mechanism could enhance compliance with agreed norms and principles of responsible State behavior"[169].

2.3 Gender Perspectives

The integration of gender perspectives into cyber-diplomacy can be significantly advanced through the framework of Feminist Foreign Policy (FFP). FFP's universalist commitment to human rights and gender equality, its humanitarian tradition of disarmament and arms control, its rejection of force and its focus on human rather than territorial security make it directly applicable to the goal of guaranteeing a stable, secure, and global cyberspace[170].

[167] Herrero, Á. (2025). The future of global security and why cyber-diplomacy matters. [online] Diplo. Available at: https://www.diplomacy.edu/blog/the-future-of-global-security-and-why-cyber-diplomacy-matters/.

[168] Bendiek, A. (2018). The EU as a force for peace in international cyber-diplomacy. Berlin: Stiftung Wissenschaft und Politik (SWP) | *German Institute for International and Security Affairs*.

[169] Guterres, A. (2023). A New Agenda for Peace. [online] Available at: https://www.un.org/sites/un2.un.org/files/our-common-agenda-policy-brief-new-agenda-for-peace-en.pdf.

[170] UN Women Headquarters Office (2022). Feminist Foreign Policies: An Introduction. [online] New York: United Nations Entity for Gender Equality and the Empowerment of Women . Available at: https://www.unwomen.org/sites/default/files/2022-09/Brief-Feminist-foreign-policies-en.pdf.

Cyberspace is not gender-neutral. Its nature embodies a dual dynamic of empowerment and vulnerability: it gives perpetrators of gender-based violence anonymity and impunity while simultaneously enabling transnational mobilization against violations of human rights. Globally, 69% of men and 63% of women use the internet, according to data from the International Telecommunication Union (ITU), demonstrating ongoing inequalities. Additionally, according to Amnesty International, 59% of women who are victims of online violence claim that their attackers are strangers. The fact that 38% of women worldwide have experienced this type of violence, with female lawmakers and journalists being particularly at risk, demonstrates how anonymity, speed, and scale exacerbate preexisting dangers. A feminist approach therefore insists on intersectionality, acknowledging that there are multiple forms of discrimination and reaffirming that in order to ensure equitable participation and lasting peace, it is necessary to restructure established power dynamics[171].

Building on this, the first priority within cyber-diplomacy is representation. Women remain underrepresented in STEM and in decision-making due to systemic barriers and societal norms. Feminist cyber-diplomacy encourages gender-specific data collection to break down stereotypes and supports empowerment initiatives like ITU's *Her Cyber Tracks*, the European *Women4Cyber* network[172], and the UN First Committee's Women in Cyber Fellowship, and aligning with UN Security Council Resolution 1325[173], which promotes inclusive peace negotiations – including in cyber peace processes.

In multilateral negotiations under UN auspices, the OEWG's The OEWG's inclusive procedures have made it possible to bring up the digital gender divide and women's participation. However, efforts to include gender considerations in norm

[171] Salvi, A., Tiirmaa-Klaar, H. and Lewis, J. (2025). A Handbook for the Practice of Cyber-diplomacy. Luxembourg: EU Institute for Security Studies.

[172] Women4Cyber. (n.d.). About Us- Women4Cyber. https://www.women4cyber.eu

[173] Landmark resolution on Women, Peace and Security (Security Council resolution 1325). (n.d.). https://www.un.org/womenwatch/osagi/wps/

development and implementation have encountered strong resistance, with the result that most such references have been removed from final texts.

This opposition reflects a larger ideological backlash against so-called “gender ideology”, rooted in domestic political and legal contexts like Russia's constitutional ban on same-sex marriage and "anti-propaganda" laws. It is also reflected in restrictive policies in parts of the Middle East, Africa, and Asia.

Civil society actors have tried to counteract these dynamics by advancing humanitarian framings of cybersecurity governance, is increasingly limited by geopolitical antagonisms, as illustrated by the blocking of NGO engagement in OEWG sessions[174].

The second priority, on the other hand, relates to rights as technological advancement has created new opportunities for gender inequality, such as discriminatory algorithmic biases and male-normative technology design. AI-generated phishing attacks, for example, specifically target feminist figures. It has also been demonstrated that cyberattacks that precede armed conflicts have distinct and unequal effects on women; however, research on these gender-specific repercussions is remarkably lacking[175].

Addressing these vulnerabilities requires States to fulfil their duty to protect women’s rights online, for instance by integrating a cyber dimension into the Women, Peace and Security agenda.

Since resource inequality continues to be a major barrier to inclusive digital transformation, the third priority is the mobilization and redistribution of resources from and for women. Therefore, feminist cyber-diplomacy urges for gender-sensitive capacity-building and redistributive mechanisms that prioritize funding

[174] Liliya Khasanova (2023). Multilateral Cyber Negotiations and Gender Mainstreaming: A Complicated Relationship – Women In International Security [online]. Available at: https://wiisglobal.org/multilateral-cyber-negotiations-and-gender-mainstreaming-a-complicated-relationship/.

[175] Miller, K., Shires, J. and Tropina, T. (2021). Gender Approaches to Cybersecurity. unidir.org. [online] Available at: https://unidir.org/publication/gender-approaches-to-cybersecurity/.

for gender-transformative projects. It also calls for formal recognition of education and care facilities as critical infrastructure so that they receive the cybersecurity protections they need, given their crucial role in facilitating women's employment[176].

In this contested environment, advancing gender perspectives in cyber governance depends on linking them to rigorous research and clearer conceptual and legal grounding, positioning gender not as an external concern but as integral to the international security architecture itself[177].

2.4 Conclusion

This chapter has examined the way that national and international actors formulate their cyberspace strategies. It has demonstrated how national policies and frameworks for international cooperation are used to implement cyber-diplomacy.

While diplomatic negotiations have helped reduce cyber conflicts and improve global cooperation, challenges still remain. Managing cross-border cyber threats and the growing need to regulate cyberspace has led to its increasing *diplomatization*. In order to foster common values and increase resilience in the digital sphere, multilateralism and strategic alliances are essential components of many national strategies. For instance, the EU's Cyber-diplomacy Toolbox shows how economic, political, and diplomatic instruments can promote cybersecurity and prevent conflict.

International organizations such as the UN, OSCE, and NATO provide key platforms for norm-setting, crisis management, and cooperation. Through initiatives like the OEWG, GGE, and the Tallinn Manuals, they contribute to

[176] Salvi, A., Tiirmaa-Klaar, H. and Lewis, J. (2025). A Handbook for the Practice of Cyber-diplomacy. Luxembourg: EU Institute for Security Studies.

[177] Liliya Khasanova (2023). Multilateral Cyber Negotiations and Gender Mainstreaming: A Complicated Relationship – Women In International Security [online]. Available at: https://wiisglobal.org/multilateral-cyber-negotiations-and-gender-mainstreaming-a-complicated-relationship/

building trust, reducing tensions, and strengthening international legal frameworks in the cyber domain.

These initiatives suggest the increasing acknowledgment that the preservation of diplomatic relations is crucial for ensuring peace, stability, and security. The upcoming chapter will cover in detail the specific diplomatic mechanisms and negotiation strategies used in cyberspace, including track 1.5 and track 2 dialogues.

3. Playing the Diplomacy Game. Frameworks of Cyber Negotiation

After the breakdown of the origins of cyber-diplomacy and the main international initiatives, as well as the national stances adopted by the States, this chapter moves on to a more theoretical discussion. Its goal is to offer the conceptual foundations required to gain a comprehensive understanding of the case study that will be presented in the following sections of this work.

Specifically, the chapter examines how game theory can provide clarity in negotiations, helping diplomats and delegations identify the goals they aim to achieve as well as the points that are non-negotiable. Additionally, it explores how Track II diplomacy facilitates multi-stakeholder engagement, confidence-building, and norm development in situations where formal State-to-State negotiations may be limited. Together, these frameworks highlight both the strategic and procedural dimensions of negotiation in cyber-diplomacy.

While until now the ultimate purpose was to present the emergence of cyber-diplomacy, this thesis also aims at explaining why it has become relevant and why States are becoming increasingly involved in this field. In addition, it intends to contemplate the broader scope of negotiation in the context of international politics and in the process of establishing a global order.

Indeed, one of the most fundamental aspects of human interaction is the process of negotiation. From the very young age, people learn the capacity to adapt their choices to comply with the expectations of society. The act of observing rules, behave properly in public and reaching a compromise with others is a perfect example of the constant effort of balancing individual desires and collective demands.

Negotiation processes are not confined to the realm of diplomacy but rather inherent in everyday life.

The same dynamic applies to international relations. Because of the absence of a centralized authority, the international system was and is now set up in a State of anarchy. States are able to pursue their own interests and ambitions within this context; however, they must also acknowledge the necessity of coexisting with other actors. In order to avoid the ever-present possibility of conflict, States engage in mediation, cooperation, and compromise in order to achieve this balance, and negotiation becomes the primary instrument. The inability of States to reach agreements would result in open conflict and undermine trust and stability in the long term. Therefore, the ability of actors to achieve a balance between their ambitions through dialogue and compromise is essential to the maintenance of a lasting peace.

3.1 Negotiating in a World Without Borders

Maxim Kaplan, PhD candidate at the Leiden University in the Netherlands, in his final dissertation found 161 different definitions of negotiation. Of these, 115 emphasize the objective of reaching an agreement, 71 emphasize communication, 64 emphasize conflicting interests, and another 64 explain the process and behavior of negotiation.

Martin Hall and Christer Jönsson, on the other hand, do not provide a definition of diplomatic negotiation at all. Rather, they define it as a process in which diplomats work to advance the interests of their respective States while simultaneously attempting to resolve disputes peacefully and prevent war.

Machiavelli adopts a similar position, stating clearly that diplomats must act as they've been advised, engage in negotiations when necessary, and diligently collect and report information[178].

In Henry Kissinger words: "[…] Negotiation is a process of combining conflicting positions into a common position, under a decision rule of unanimity, a phenomenon in which the outcome is determined by the process"[179]. In other words, it is the act of transforming divergent opinions to agreement.

[178] Meerts, P. (2015). Diplomatic Negotiation Essence and Evolution. The Hague: Clingendael Institute.

[179] Kissinger, H.A. (1969). The Viet Nam Negotiations. [online] www.foreignaffairs.com. Available at: https://www.foreignaffairs.com/articles/asia/1969-01-01/viet-nam-negotiations.

Negotiations will only take place only when the parties realize, in one way or another, that they genuinely need each other. According to the American political scientist I. William Zartman, the timing of negotiations relies on the ripe of the conflict.

In the theory elaborated in the 1980s, Zartman asserts that meaningful talks toward a peace deal are possible once a conflict has matured and reached a "ripe moment"[180].

Although Zartman's thesis refers to the conflict resolution, its core concepts remain adaptable to all kinds of negotiation processes where mediation emerges when the parties recognize a certain amount of mutual reliance and realize they have become trapped in an impasse.
He further clarifies this logic by stating that, "If the parties to a conflict (a) perceive themselves to be in a hurting stalemate and (b) perceive the possibility of a negotiated solution (a way out), the conflict is ripe for resolution". The first condition, the perception of a "hurting stalemate", refers to the idea of a mutually hurting stalemate (MHS), a core concept in ripeness theory. It occurs when all parties realize they've come to a standstill. The second element, "the possibility of a negotiated solution", means that the parties see the potential for resolution through negotiation. Zartman refers to this as a "sense of a way out". Crucially, what matters most is the subjective recognition of stalemate. This means that an MHS cannot arise unless both sides expressly acknowledge it, regardless of how much objective evidence there is about impasse or the high costs of extending the conflict[181].

However, as noted by Sticher in the article "Healing Stalemates: The Role of Ceasefires in Ripening Conflict", the elements at the base of the MHS may dissolve

[180] Zartman, I.William. (2000). Ripeness: The Hurting Stalemate and Beyond. In: D. Druckman and P.C. Stern, eds., International Conflict Resolution After the Cold War. Washington, Dc: National Academy Press.

[181] *Ibidem*

once rounds of negotiation start and hostilities cease, ultimately resulting in the MHS's own dissolution[182]. Zartman introduces the idea of the Mutually Enticing Opportunity (MEO) to mitigate this risk. This gives both parties involved hope throughout the negotiating process. Negotiations are more likely to succeed if the shift from MHS to MEO is handled well. Zartman suggests that the “enticing opportunity” for benefit-seeking parties is the possibility of obtaining something from peace talks, even though he does not explicitly outline the exact requirements for the formation of a MEO. To create such opportunities, political changes must be made to balance the interests of all parties[183].

Nobel Prize recipient Thomas Schelling describes negotiations as mixed-motive situations. In negotiations the different parties are both adversaries and friends. Each is trying to defeat the other but also needs the other to achieve shared goals[184]. On a more practical level, when the parties sit down to discuss an issue, they will each have an idea of how they would like to see the conflict resolved. The preferred outcome of a conflict participant is described in negotiation theory as a party’s ideal point, but almost certainly they will have to compromise and move away from their ideal points to find a solution.

[182] Sticher, V. (2021). Healing Stalemates: The Role of Ceasefires in Ripening Conflict. Ethnopolitics, 21(2), pp.149–162.

[183] Zartman, I.William. (2000). Ripeness: The Hurting Stalemate and Beyond. In: D. Druckman and P.C. Stern, eds., International Conflict Resolution After the Cold War. Washington, Dc: National Academy Press

[184] Schelling, T.C. (1960). The strategy of conflict. New York Oxford University Press.

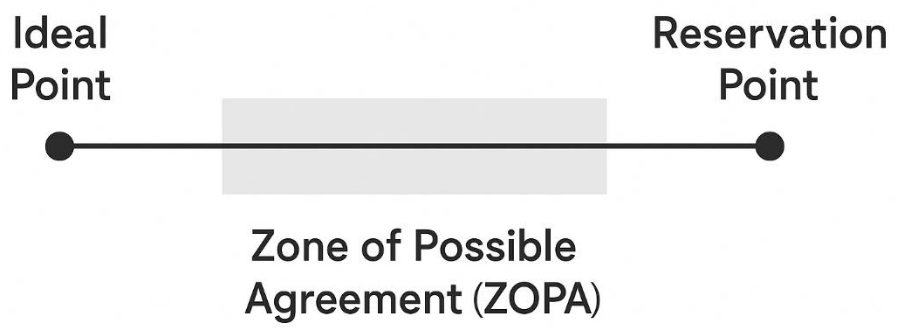


Figure 2: ZOPA illustrated

As illustrated in Figure 2, at the opposite point there is the reservation point, meaning the point where participants no longer see an agreement desirable. The parties are willing to accept solutions on the continuum up to their reservation points[185]. There is an area on the continuum that overlaps for both parties. This overlapping area is known as the zone of possible agreement (ZOPA), and any point in the ZOPA is a workable solution to the problem for both parties[186].

In the zone of possible agreement, any deal would be acceptable, but each party would prefer to have a deal closer to his or her ideal point than further away.

3.1.1 An Overview of Different Negotiation Approaches

In order to achieve an exhausting overview of different negotiation approaches, in 1988, Zartman identified five different levels of analysis, or core approaches. These are the structural, the strategic, the procedural, the behavioral and the integrative approaches[187]. However, it is crucial to acknowledge that in reality, most negotiators employ a combination of them during negotiation rounds.

[185] Raiffa, H., 1982. The Art and Science of Negotiations. Belknap Press of Harvard University Press Cambridge, Mass., USA

[186] Fisher, R. and Ury. W., 1981. Getting to Yes: Negotiating Agreement Without Giving In: Penguin Books. New York, USA.

[187] I. William Zartman (1988). Common elements in the analysis of the negotiation process. Negotiation Journal, [online] 4(1), pp.31–43. Available at: https://link.springer.com/article/10.1007/BF01000902.

The table below summarizes the five negotiation approaches identified by Zartman, highlighting their main focus, assumptions, and limitations.

APPROACH	FOCUS / BASIC FEATURES	ASSUMPTIONS	LIMITATIONS
Structural	Means, positions, and use of power	Win–Lose	Risk of locking into rigid positions; overemphasis on power; reduced chance for mutually beneficial agreements
Strategic (e.g., Game Theory)	Outcomes, rationality, positions	Win–Lose; existence of optimal solutions; rationality of players	Excludes role of power; assumes players are largely undifferentiated apart from their options
Behavioral (e.g., personality traits, diplomatic treatises)	Personality traits, perceptions, expectations	Win–Lose	Overemphasis on positions; limited by subjective perceptions
Procedural (Concession Exchange)	Concessions, reactive moves, positions	Win–Lose; negotiation as learned responses	Emphasis on positions; lack of predictiveness
Integrative (e.g., principled negotiation, process models)	Problem-solving, value creation, communication, relationships, win–win solutions	Win–Win potential	Time-consuming; requires readiness for non-integrative counterparts

Table 4: Zartman Negotiation Approaches

According to Zartman, the different negotiation strategies, each with distinctive advantages and drawbacks, can provide different perspectives on how agreements are reached.

Both the strategic and structural approaches assume win-lose situations, but they focus on distinct aspects. The strategic approach, which uses game theory to explain the connection between process and result – that will be presented in the next section of this chapter – emphasizes rationality and results, presenting negotiators as actors seeking optimal solutions while minimizing the influence of power and individual differences. In contrast, the structural approach emphasizes the role of positions and power, frequently encouraging parties into solid positions. The behavioral and procedural approaches focus on the dynamics of interaction. Although it still relies on hard negotiating positions, the behavioral approach emphasizes how personality, perception, and expectations influence the behavior of the negotiator. According to the procedural one, negotiation is a methodical process in which both parties make compromises while reacting to each other's actions. It uses the economic approach, whereby a range of concessions is analyzed. At a certain moment the costs become too high and the margins disappear, but just before this happens the optimal outcome will be reached, as determined by the balance of costs and benefits. It implies a win-lose scenario in which advancement is reliant on a series of interactions rather than cooperative problem-solving. The main drawback is that it preserves the emphasis on positions while providing little attention to the course of negotiations or the results that will be reached. By emphasizing communication, preparation, alternatives, values, relationships, and information, the integrative approach aims to go beyond positional and adversarial logics. It encourages problem-solving and the development of win-win solutions, providing more opportunities for reciprocal benefits, though at the cost of being time-consuming and reliant on the willingness of all parties to adopt cooperative methods. However, as mentioned beforehand, negotiators rarely follow a single model, and most combine elements of different approaches depending on the context and their counterparts. Zartman himself employs a mixed approach. He characterizes “negotiation as a choice of partners, as an establishment of relations, as a contest of alternatives, as a confrontation of power [...], as a process of elimination, or as problem-solving"[188].

3.2 Strategic Reasoning: Game Theory in cyber-diplomacy

Negotiation is only one of the functions of diplomacy and, in some situations, not the most urgent; in traditional diplomacy via resident missions, neither is it the activity to which most time is now generally devoted. Nevertheless, negotiation remains the most important function of diplomacy. This is, in part, because the diplomatic system now encompasses considerably more than the work of resident missions, and because negotiation becomes more and more its operational focus as we move into the realms of multilateral diplomacy, summitry, and that other growth sector of the world diplomatic system – mediation[189].

When two people enter negotiation, it is problematic to assume that both negotiators will communicate in the same language, belong to the same social group and share the same beliefs and points of view. If a German businessperson negotiates with an Italian, Canadian or Japanese colleague, the two parties' commands of English as means of communication are different, their knowledge and negotiation strategies have been acquired in different schools, their behavior depends on their own cultures and so on.

This complexity results from the interaction of many factors and has been described by the mathematician John von Neumann, who developed the structure of a social game theory in 19281 and, together with Oscar Morgenstern, published "Theory of

[188] Zartman, I.W. (2013). Negotiation: post-modern or eternal? In: A. Colson, D. Druckman and W. Donohue, eds., International Negotiation: Foundations, Models, and Philosophies. Dordrecht: Republic of Letters Publishing BV, pp.209–225.

[189] Berridge, G.R. (2022). Diplomacy: Theory and Practice. Cham, Switzerland: Springer International Publishing.

Games and Economic Behavior", a book on rule-governed behavior in social interactions[190].

Game theory is considered a theory of strategic interaction[191]. It is a theory of rational behavior in social situations in which each player must choose his moves based on what he thinks the other players are likely to do. It helps explaining the strategic interactions between negotiators, illustrating how States anticipate, respond to, and influence each other's moves. Its ultimate goal is to help define players' rational behaviors in real-life economic, political and social situations.
It uses formal mathematical models to describe, recommend or predict the actions parties take in order to maximize their own gains[192]. The rational presupposition can be described as follows: in any negotiation, there must be a rational way to negotiate a conflict, especially when deceptive actions are involved[193]. A conflict can be described as an interactive situation in which several negotiators make decisions and in which the outcome depends on each negotiator's preferences over the set of possible outcomes[194]. A branch of the game theory is the "games of strategy", different from the games of skill or games of chance. Here, the best course of action for each participant depends on what he expects the other participants to do"[195].

[190] Gaffal, M. and Jesús Padilla Gálvez (2023). Negotiation, Game Theory and Language Games. In: Dynamics of Rational Negotiation. pp.11-40.

[191] John Von Neumann and Oskar Morgenstein (1944). Theory of games and economic behaviour. Princeton N.J.: Princeton University Press.

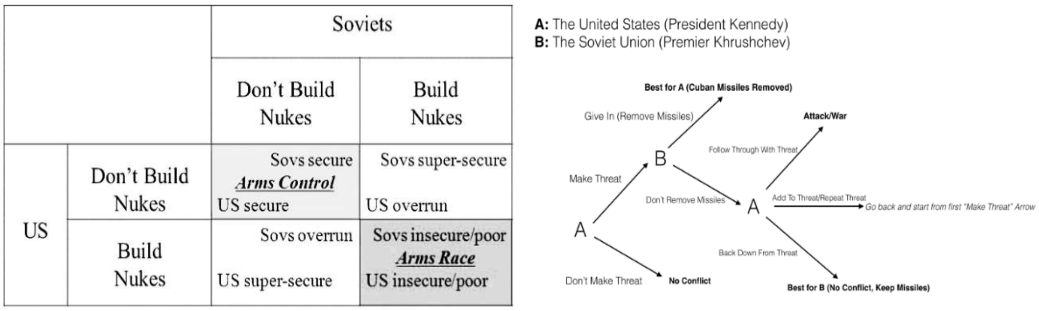
[192] Gaffal, M. and Jesús Padilla Gálvez (2023). Negotiation, Game Theory and Language Games. In: Dynamics of Rational Negotiation. pp.11-40.

[193] Padilla Gálvez (2021, 226–232)

[194] Myerson, R.B. (1997). Game theory: analysis of conflict. Cambridge, Massachusetts: Harvard University Press.

[195] Schelling, T. C., 1960. The Strategy of Conflict, Harvard University Press, Cambridge, MA, USA.

Games are frequently represented as matrixes or trees (in the extensive form of the games) where each player must choose between a finite number of possible “moves”, each with known pay-offs.



		Soviets	
		Don’t Build Nukes	Build Nukes
US	Don’t Build Nukes	Sovs secure ***Arms Control*** US secure	Sovs super-secure US overrun
	Build Nukes	Sovs overrun US super-secure	Sovs insecure/poor ***Arms Race*** US insecure/poor

A: The United States (President Kennedy)
B: The Soviet Union (Premier Khrushchev)

Best for A (Cuban Missiles Removed)
Give In (Remove Missiles)
Attack/War
Follow Through With Threat
B
Make Threat
Don't Remove Missiles
A
Add To Threat/Repeat Threat
Go back and start from first "Make Threat" Arrow
A
Back Down From Threat
Don't Make Threat
No Conflict
Best for B (No Conflict, Keep Missiles)

Figure 3: Cuban Missile Game Matrix (on the left) and Tree (on the right) from Amb. P. Ferrara course on diplomacy and negotiation held in LUISS University (Academic Year 2024/2025)

Ellsberg’s Critical Risk Theory of crisis bargaining[196], introduced for the first time in 1959, like game theory, uses cardinal utility numbers to explain decision-making behavior but introduces the notion that parties use probability estimates when making rational calculations of whether or not to concede, or to stand firm in a crisis negotiation. These probabilities are derived from each player’s calculus of their own critical risk, or the maximum risk of a breakdown in negotiations that the player is willing to tolerate in order to stand firm, combined with each player’s estimation of the level of their opponent’s inherent resolve to stand firm.

Ellsberg’s Critical Risk Theory helps explain the dynamics of the Cuban Missile Crisis by highlighting how each superpower’s tolerance for risk shaped their decisions.
In October 1962, the Cuban Missile Crisis brought the United States and the Soviet Union to the brink of nuclear war after American reconnaissance revealed Soviet missiles in Cuba. Over thirteen tense days, President Kennedy employed a naval blockade while engaging in secret negotiations with Khrushchev. The crisis was resolved through a combination of firm public posturing and discreet diplomacy:

[196] Ellsberg, D., 1959. The Theory and Practice of Blackmail. Unpublished lecture at the Lowell Institute, Boston. March 1959.

the USSR agreed to remove its missiles from Cuba, and the US pledged not to invade, quietly removing its missiles from Turkey.

During the thirteen-day standoff, both the United States and the Soviet Union initially resisted concessions, pushing the world toward a high probability of nuclear conflict. According to the theory, the U.S. was willing to tolerate a higher critical risk (≈70%) than the Soviets (≈40%), meaning that as the perceived likelihood of war rose, the Soviets reached their threshold first and chose to concede by removing missiles from Cuba. This framework complements the historical narrative: the crisis was resolved not merely through strategic moves or threats, but through the careful calibration of each side's risk tolerance and their reading of the opponent's resolve, showing that negotiation under extreme tension depends as much on risk perception as on material payoffs.

	U.S.S.R. Stands Firm	**U.S.S.R. Concedes**
U.S. Stands Firm	**(–100, –100)** → Nuclear war (breakdown). Outcome depends on which side reaches its *critical risk threshold* first. If both refuse to back down → catastrophic loss for both.	**(+10, –5)** → U.S. victory: Soviet missiles removed from Cuba, but Soviets suffer strategic loss.
U.S. Concedes	**(–5, +10)** → Soviet victory: Missiles remain in Cuba, U.S. avoids war but suffers strategic defeat.	**(+5, +5)** → Compromise: Both sides step back (historically, missiles removed from Cuba in exchange for U.S. missiles in Turkey).

Table 5: Ellsberg Theory applied to the Cuban Missile Crisis

Graham Allison's three models of decision-making further illuminate this outcome. The Rational Actor Model aligns closely with both game theory and critical risk theory, portraying the U.S. and USSR as unitary actors making calculated choices to maximize their strategic objectives. The Organizational Processes Model highlights how standard operating procedures within the military and government agencies—such as naval blockade protocols—shaped the available options and pace of decision-making. The Bureaucratic Politics Model reveals how internal bargaining among political leaders, military officials, and advisors influenced the final course of action, sometimes diverging from purely rational predictions[197].

Viewed together, Ellsberg's focus on calibrated risk tolerance and Allison's emphasis on rational calculation, institutional routines, and political negotiation provide a more comprehensive explanation of how the crisis was managed and ultimately resolved.

By combining these perspectives, the analysis can now move beyond the Cuban Missile Crisis to consider how similar patterns of risk tolerance, strategic calculation, and internal political dynamics might shape decision-making in other international confrontations.

3.2.1 Games' classification

Scholars, in time, have schematized the basic postulates of game theory and modified the way negotiators have to make decisions. They classified games into different categories and described which methods can be applied to solve what ends. These categories include symmetric and asymmetric games, zero-sum and non-zero-sum games, maximin and minimax criteria[198], the Nash equilibrium, cooperative games, non-cooperative games[199], simultaneous and sequential games, perfect information games[200] and many others that are currently being developed.

Cooperative models assume that agents use cooperative mechanisms to make binding commitments outside the specified rules of a game. Cooperative solutions

[197] Allison, G. (2012). The Cuban Missile Crisis at 50: Lessons for U.S. Foreign Policy Today. Foreign Affairs, 91(4), pp.11–16.

[198] Oskar Morgenstern and John Von Neumann (1944). Theory of Games and Economic Behavior (Princeton Classic Editions). Princeton University Press.

[199] Nash, J.F. (1996). Essays on Game Theory. Edward Elgar Publishing

[200] Oskar Morgenstern and John Von Neumann (1944). Theory of Games and Economic Behavior (Princeton Classic Editions). Princeton University Press.

focus on how to allocate the benefits resulting from cooperation. In contrast, non-cooperative models assume that players lack cooperative mechanisms or decide not to apply them. Some non-cooperative models analyze strategic games (including finite games, zero-sum games, matrix games, etc.), extensive games (perfect information games, perfect and imperfect memory games, incomplete information games, etc.) and dynamic games (iterative games, differential games, stochastic games, etc.)[201][202].

A symmetric game is a game in which a negotiator's payoffs for using a particular strategy depends only on the other negotiator's strategy. The game is symmetric if changing the identities of the players does not alter the payoffs of the strategies. Well-known examples of symmetric games are the "prisoner's dilemma", "the game of chicken" and "the stag hunt".

The prisoner's dilemma is frequently used to describe a common negotiation process that might undermine cooperation in international politics[203]. In the classic version of the game, two criminals suspected of a major crime are arrested for a misdemeanor violation. The two criminals are separated and interrogated by the police. Each prisoner is offered a plea deal. The terms of the plea deal are contingent on what each player chooses. Table 6 the illustration of the payoff matrix.

	Player B Cooperates	**Player B Defects**
Player A Cooperates	3, 3	0, 5
Player A Defects	5, 0	1, 1

Table 6: Prisoner's Dilemma – Payoff Matrix

In the numerical payoff matrix, if both players cooperate, they receive a moderate reward (3,3); if both defect, they are worse off (1,1). If one defects while the other cooperates, the defector gains the highest payoff (5) while the cooperator receives

[201] Nash, J.F. (1950). The Bargaining Problem. Econometrica, 18(2), pp.155–162.

[202] Nash, J.F. (1996). Essays on Game Theory. Edward Elgar Publishing

[203] Eatwell, J., Milgate, M. and Newman, P. eds., (1989). Game Theory. London: Palgrave Macmillan UK.

the lowest payoff (0). Despite mutual cooperation being collectively optimal, rational self-interest typically drives both players to defect.

The Cuban crisis explained before in Table 5 can be also interpreted as an example of the game of chicken. The game of chicken describes a simulated conflict in which two participants risk their lives to the limit. The dilemma is best illustrated in a scene of the film “Rebel Without a Cause”, in which two young men race their cars towards a cliff. The first one to jump out of his car loses. In such a dilemma, there are two possible outcomes, depending on the strategy the driver uses, e.g., drive straight ahead or turn or swerve before the precipice[204]. In this case, both the United States and the Soviet Union were facing a critical decision: escalate or de-escalate. Contrary to the prisoner's Dilemma, mutual defection is worse than mutual cooperation, but each player has a dominant strategy to defect. Here, no player has a dominant strategy, and the worst outcome results from mutual escalation – not mutual defection.

Negotiation considered from the point of view of game theory can also be approached in ethical terms. Since games like the prisoner’s dilemma present an apparent conflict between ethics and individual interest, explaining why cooperation is necessary for individual interest is an important component of negotiation. Jean Jacques Rousseau, to solve this “defect”, proposed modifying preferences and thus put forward the following procedure: if the general will could be fulfilled, then all individual wills would have to be brought into conformity with the general will.65 Through this general strategy, a fundamental element on which the social contract is based was developed. This disparity of strategies has been outlined within game theory, as illustrated in the “stag hunt” dilemma, which describes a conflict between individual interests and social cooperation. To illustrate this dilemma, Rousseau described a situation in which two individuals go hunting.

[204] Poundstone, W. (1992). Prisoner’s Dilemma: John Von Neumann, Game Theory and the Puzzle of the Bomb.

	Hunter B: Stag	Hunter B: Hare
Hunter A: Stag	(4, 4)	(0, 3)
Hunter A: Hare	(3, 0)	(3, 3)

Table 7: Stag Hunt Matrix

To hunt a stag, coordination between the two hunters is necessary. If they hunt one stag, they will have enough food for both of them for several weeks (4,4). However, if they wish to satisfy their urgent needs, each hunter may want to hunt a hare instead, as this does not require coordination. As they hunt individually, each of them can eat their hares the same day (3,3). If one hunter tries to cooperate, but the other chooses the safer hare. The stag hunter gets nothing (0), while the hare hunter gets a quick meal (3).

Rousseau pointed to the advantage that cooperation has for each hunter as it facilitates higher profit, even if they had to renounce individual autonomy. In other words, each hunter should separately choose to pursue the more ambitious and rewarding goal, giving up some autonomy in exchange for a higher joint gain. This situation is a model example and an analogy for social cooperation. The problem is that, although both hunters agree to hunt a stag together, there is always a risk that individual interests will overcome the general interest and one or both hunters will end up hunting a hare instead of a stag. Despite this risk, working together within a group of people with the same goals appears to be far more effective than pursuing goals individually[205].

In terms of negotiations, the prisoner's dilemma exemplifies why collaboration frequently fails: parties are afraid of being taken advantage of, so even agreements that benefit both parties may fall through because each actor puts their own interests first in order to avoid being "cheated." The stag hunt, on the other hand, shows how norms and cooperative behavior can develop. Actors are motivated to adhere to common norms and expectations when they understand that coordinating their

[205] Rousseau, J.J. (1762). The Social Contract. Cambridge University Press.

strategies results in greater joint gains. This builds trust and stable norms for future interactions.

In contrast, asymmetric games are those where there is no identical set of strategies for both players, as players develop their strategies in dependence on and in relation to the strategy of the respective other. In zero-sum games, the total benefit for all players in the game, in each combination of strategies, always adds up to zero. Thus, only one player benefits at the expense of all others. The negotiator gains exactly the amount that the opponent loses, which is everything that is at stake. In business, we are often confronted with non-zero-sum games, as some resolutions have net outcomes greater or less than zero. That is, one negotiator's gain does not necessarily correspond to another's loss. For example, a business contract ideally involves a positive-sum outcome, where each opponent ends up in a better position than he or she would have been in if no negotiation had taken place.

The "maximin" and "minimax" criteria State that each negotiator should minimize his maximum loss. The "maximin" criterion is set as follows: negotiator A determines that his minimum possible payoff is the largest possible payoff. Conversely, the "minimax" criterion determines that negotiator B chooses that the maximum payoff of A be as small as possible. Dominant strategy equilibria are fine when they appear in games, but unfortunately, this is rare in real life.

Together, these strategies will constitute a Nash equilibrium if player A's choice is optimal given B's choice, and B's choice is optimal given A's choice. A Nash equilibrium can be interpreted as a pair of expectations about each negotiator's choice such that, when the other reveals his choice, neither will want to alter his action. In this situation, each negotiator knows and has adopted his best strategy, and all know the strategies of the other negotiators. Consequently, each negotiator gains nothing by changing his strategy if the other negotiator maintains his. Thus, each negotiator executes the best “move” he can. This generates a cooperative game between the negotiating parties, which in turn generates contractual compliance[206].

3.2.2 Game theory in cyber-related field

Game theory provides a structured approach for examining strategic decisions in cyber-diplomacy. It helps in planning a strategy for negotiation rounds and explain different actors’ behavior in contexts of cooperation, competition, and confrontation. The theory is also valid when States and diplomats face cyber conflicts. As the Nobel Prize winner Thomas Schelling explained in “The Strategy of Conflict”, many conflicts can be considered as negotiation scenarios that combine opposing and shared interests.

According to this model, a “strategy” is a comprehensive plan which covers all possible scenarios and allows to make predictions. Some cyber interactions are modelled as two-player, zero-sum races – where one actor’s gain is the other’s loss – while others are non-zero-sum, involving trade-offs between mutual restraint and escalation[207].

The Hawk-Dove game is a classic example of a non-zero-sum (anti-coordination) model. It is a simultaneous-move game in which players have complete information of the payoffs and the structure, but they are unaware of the opponent's move.

It was first developed in biology to simulate how two opponents compete over a resource of value (v), where direct confrontation imposes a cost (c).

In the context of cyberspace, a hawkish strategy implies aggression, such as launching cyberattacks or exploiting vulnerabilities to obtain, for instance, intelligence or prepare for further actions, whereas a cooperative strategy emphasizes restraint, focusing on cybersecurity measures to prevent unauthorized

[206] Gaffal, M. and Jesús Padilla Gálvez (2023). Negotiation, Game Theory and Language Games. In: Dynamics of Rational Negotiation. pp.11–40.

[207] Henderson, H. (2021). Cybered Competition, Cooperation, and Conflict in a Game of Imperfect Information. The Cyber Defense Review, 6(3), pp.43–60.

access, protect systems, and defend against specific threats. The following 2x2 matrix summarizes the payoffs:

	Dove (Player 2)	**Hawk (Player 2)**
Dove (Player 1)	v/2, v/2 *(Both share the resource peacefully; each gets half of the value v)*	0, v *(Player 1 plays Dove, Player 2 plays Hawk; Player 1gets nothing, Player 2 takes the full value v)*
Hawk (Player 1)	v, 0 *(Player 1 plays Hawk, Player 2 plays Dove; Player 1 takes full value v, Player 2 gets nothing)*	(v-c)/2, (v-c)/2 *(Both play Hawk; they fight, so each suffers half the conflict cost "c" and splits remaining value)*

Table 8: Hawk–Dove game Matrix

In this matrix, each cell shows the payoff for Player 1 (row) and Player 2 (column), so the first number corresponds to the row player and the second to the column player[208].

Depending on the relationship between the resource value and the cost of conflict, two main forms of the game emerge.

Aggressive play is favored and mutual Hawk can be a Nash equilibrium if the prize value is greater than the cost of conflict (v > c), producing mutually costly outcomes. Although this appears to be similar to mutual defection in the Prisoner's Dilemma, the two games are structurally different; in cyberspace, this explains why offensive actions are common in cyberspace when the potential rewards outweigh the risks.

[208] Wooldridge, M. and Phelps, S. (2013). Game Theory and Evolution. AI and Game Theory | IEEE Computer Society.

On the other hand, when confrontation is more expensive than the gains ($v < c$), the game generates two pure-strategy equilibria – in which one player chooses Hawk and the other Dove – and a symmetric mixed-strategy equilibrium, where each player randomizes and the probability of playing Hawk is $p = v/c$. This scenario, similar to the Chicken game, explains why low-level cyberattacks are frequent while, because of the increased risks, highly destructive attacks are relatively uncommon.

The Hawk-Dove game can also be presented in a sequential form to illustrate deterrence in cyberspace. Although the first mover frequently gains an advantage by committing first in this variant, the second mover is fully aware of the first mover's action. This could result in an equilibrium where Player 1 plays Hawk and Player 2 plays Dove for typical payoff parameters. The outcome might change to mutual restraint, though, if Player 2 can credibly commit to retaliation and signal that commitment (Dove, Dove). This demonstrates how, even in situations where perfect information is unlikely, credible commitment and signaling can strengthen deterrence[209].

Schramm, Alderson, Carlyle, and Dimitrov's paper "*A Game Theoretic Model of Strategic Conflict in Cyberspace*" analyzes cyber conflict using a two-player, zero-sum, non-cooperative game with perfect information.
It emphasizes the trade-off between postponing an attack for greater effectiveness and the possibility that the adversary will find the exploit first. When both players are aware of an exploit, they can either wait or attack, with the following payoffs:

	Player 2: Attack (A)	**Player 2: Wait (W)**
Player 1: Attack (A)	Both attack – both expend munitions; first use captures exploit advantage.	Player 1 attacks and captures the exploit; Player 2 gains nothing.

[209] Henderson, H. (2021). Cybered Competition, Cooperation, and Conflict in a Game of Imperfect Information. The Cyber Defense Review, 6(3), pp.43–60

Player 1: Wait (W)	Player 2 attacks and captures the exploit; Player 1 gains nothing.	Both wait – no one uses the exploit; no payoff occurs.

Table 9: Attack vs. Wait Payoffs Matrix

In this matrix, the first number is Player 1's payoff and the second is Player 2's. Attack is the dominant action once the exploit becomes well-known, so (Attack, Attack) is the model-dependent equilibrium. This is based on the model's assumption that the exploit's full value is obtained by the first one that uses it, making the opponent's weapons essentially useless. This demonstrates that there is no assurance of second-strike capability. The four stages of an exploit's life cycle – Discovery, Development, Employment, and Obsolescence – are also covered by the model. During these stages, exploits are discovered, turned into weapons, used in attacks, and ultimately become outdated. This emphasizes the importance of timing and speed, underscoring the necessity of adaptable command structures in cyberspace.

Game theory models demonstrate the tendency for attacks of different types and the potential for deterrence through calculated threats that involve some degree of uncertainty, demonstrating the pervasive use of cyberspace for strategic objectives.

Because cyber weapons are extremely dynamic and deterrence may be limited in the absence of guaranteed second-strike capabilities, successful cyber operations frequently necessitate quick action. Moreover, the obstacles in attributing attacks make traditional diplomatic attempts to negotiate explicit cyber agreements difficult. But, by correctly employing game theory and facilitating frequent interactions between States, it would be possible also to promote negotiations and foster collaboration.

This might eventually result in the development of norms and "agreed competition", in which mutual trust and persistent limitations would function as de-escalatory mechanisms, thereby lowering conflict and advancing global cybersecurity collaboration.

Foulon and Meibauer, in their article “How cyberspace affects international relations: The promise of structural modifiers”[210], provide an advanced framework for analyzing strategic behavior in cyber-diplomacy and negotiation by presenting cyberspace as a structural modifier. Their approach shows that States' choices regarding, for instance, cooperation and deterrence, are influenced by the systemic characteristics of cyberspace, which affect opportunities, drawbacks, and uncertainties for all actors. This perspective explains why similar cyber actions can result in different outcomes depending on States’ resources, positions and international relations and why traditional game-theoretic concepts must be adapted to the digital domain. By combining structural effects with the logic of strategic interaction, scholars and policymakers can examine behavior, predict reactions, and develop strategies that take into consideration both immediate decisions and the larger systemic context in which they occur.

3.3 Process Observed: Dynamics of Negotiation in Cyber-Diplomacy

Although some negotiations develop a distinctive pattern, according to theoreticians and to practical observations, most negotiations can be broken down into broken down into a number of stages, with distinct purposes.

Confusion may arise in the sequence of events, the process may be fuzzy, the phases may vary in length, or they may overlap or retrace their steps, but looking at the whole sequence the process will result in some similarities. It is mostly evident when dealing with international negotiations, when it is helpful to separate the preliminary phase from the formal event[211].

[210] Foulon, M. and Gustav Meibauer (2024). How Cyberspace Affects International relations: the Promise of Structural Modifiers. Contemporary Security Policy, 45(3), pp.1–33.

[211] Dupont, C., Faure, G. (2013). The Negotiation Process In: A. Colson, D. Druckman and W. Donohue, eds., International Negotiation: Foundations, Models, and Philosophies. Dordrecht: Republic of Letters Publishing BV, pp.67–101.

G. R. Berridge, in his book "*Diplomacy: Theory and Practice*", divides the process of negotiation into four different stages, outlined in the next paragraph[212].

3.3.1 Stages of the Negotiation Process

Prenegotiations, despite their misleading name, are the first stage of negotiations. Also commonly referred to as 'talks about talks', their goal is to establish that substantive negotiations are worth-while, to agree on the agenda and the necessary procedures for tackling it. Usually these discussions are usually informal and well out of the public gaze[213].

As outlined in the opening paragraph of this chapter, parties engaged in a conflict – or, more broadly, in any process requiring an agreement – tend to enter into negotiations once they recognize that further progress is unattainable without a settlement. Zartman conceptualizes this condition as a "mutually hurting stalemate". If, ultimately, the parties next have to acknowledge the possibility that a negotiated settlement may be better than the status quo. This is, perhaps, the true beginning of prenegotiations[214].

Internal stakeholder consultations are crucial to establishing agreement and defining a definitive goal prior to engaging in negotiations. An essential component of the preparation is finding the Best Alternative to a Negotiated Agreement (BATNA), which determines the lowest acceptable result coming from the

[212] Berridge, G.R. (2022). Diplomacy: Theory and Practice. Cham, Switzerland: Springer International Publishing.

[213] *Ibidem*

[214] Berridge, G.R. (2023). Theory and Practice: Negotiations. [online] DiploFoundation. Available at: https://asef.org/wp-content/uploads/2020/10/ModelASEM_Diplo_Negotiations.pdf.

negotiation process. Taking the other party's BATNA into account is equally crucial[215].

If this stage is traversed successfully, it leads to consideration of an agenda, the format of the negotiation process, the venue, the delegations that will represent each side and the timing[216].

Sometimes intermediaries, or track two contact, helps in prenegotiations, if either side is reluctant to start the process, or if there are complexities blocking even the start of formal discussion. The importance of track two diplomacy will be briefly discussed in paragraph 0.

The "around-the-table" stage of negotiations starts when formal discussions begin. The parties' first priority is usually to agree on the broad principles of a settlement, commonly referred to as "guidelines", a "framework for agreement" or simply a "formula". An ideal formula would address all of the main issues at stake, provide a rough gain balance and foresees the possibility of improvement at the details stage the, final stage of a negotiation, where the terms and conditions become definitive and the agreements are ready to be signed and ratified[217].

Phase	**Key Tasks / Focus**	**Notes**
1. Prenegotiations (Talks about Talks)	- Determine if negotiations are worthwhile - Agree on agenda and procedures - Internal stakeholder consultations - Identify BATNA for each side - Use intermediaries/track two contacts if needed	Informal, behind the scenes; sets the stage for formal negotiations
2. "Around-the-Table" Negotiations	- Agree on broad principles of settlement	Formal discussions begin; focuses on overarching

[215] Rana, K.S. (2011). 21st Century Diplomacy: A Practitioner's Guide. Bloomsbury Publishing USA.

[216] *Ibidem*

[217] Berridge, G.R. (2023). Theory and Practice: Negotiations. [online] DiploFoundation. Available at: https://asef.org/wp-content/uploads/2020/10/ModelASEM_Diplo_Negotiations.pdf.

	- Establish “guidelines”, “framework” or “formula” - Address main issues - Ensure rough balance of gains	structure rather than details
3. Details Stage	- Finalize specific terms and conditions - Confirm agreements - Prepare for signing and ratification	Concludes the negotiation process; agreements become definitive

Table 10: Negotiation Stages

3.3.1.1 Track Two Diplomacy

Most international meetings, especially in the diplomatic arenas, are preceded by preliminary contacts, either unofficial or informal. This is sometimes referred to as “Track two” talks[218], as opposed to “Track one” talks, which represent official procedures.

Track two talks start before the formal opening of the negotiations and, sometimes, take on special importance during the course of the negotiations[219] if there is the need to have mediators or advisors for specific matters[220].

Many attempts have been made to define Track Two diplomacy over the years. The challenge is that these processes are rarely the same; they differ depending on the actors involved, moreover academics often disagree on how to categorize these discussions within the larger framework of negotiation. In this study, Track Two will be examined within the prenegotiation stage, given the central role played by

[218] Putnam, R.D. (1988). Diplomacy and Domestic Politics: the Logic of Two-Level Games. International Organization, 42(3), pp.427-460.

[219] Dupont, C., Faure, G. (2013). The Negotiation Process In: A. Colson, D. Druckman and W. Donohue, eds., International Negotiation: Foundations, Models, and Philosophies. Dordrecht: Republic of Letters Publishing BV, pp.67–101.

[220] Berridge, G.R. (2022). Diplomacy: Theory and Practice. Cham, Switzerland: Springer International Publishing.

third parties during this phase[221]. The involvement of private individuals and NGOs was known in the United States as 'citizen diplomacy' until it was christened 'track two' by the American diplomat Joseph Montville in 1981. The practice has increased rapidly over recent decades[222].

Initially, cyber-related track initiatives were innovative and highly interesting because few governments had diplomats with ICT expertise, and few universities or think-tanks produced the interdisciplinary knowledge required to address the complex dimensions of cyberspace; Thanks to these initiatives and conferences, researchers and diplomats were able to share opinions, spread awareness, raise concerns, and clarify perceptions on a broad range of policy, legal and technical issues on the international security agenda, sometimes serving as bridges to more official engagement.

For instance, between 2017 and 2018, the Center for Strategic and International Studies (CSIS) facilitated strategic dialogue between US and Russian experts on the importance of integrating cybersecurity into wider crisis instability scenarios. The dialogue, officially titled "U.S.–Russia strategic dialogue on crisis stability" served as an example of how cyber-related issues are a concrete concern for strategic stability and avoid conflicts. The talks produced a final report which highlighted the need to integrate cybersecurity into broader crisis instability scenarios rather than treating it separately[223].

Due to its tangible and intangible advantages, track two diplomacy is becoming widely used. Building trust between the parties, raising awareness of new issues,

[221] Jones, P.L. and Shultz, G.P. (2015). Track two diplomacy in theory and practice. Stanford, California: Stanford University Press.

[222] Berridge, G.R. (2022). Diplomacy: Theory and Practice. Cham, Switzerland: Springer International Publishing.

[223] Kavanagh, C., Carr, M. and Berglund, N. (2021). Quiet Conversations: Observations from a decade of practice in cyber-related track 1.5 and track 2 diplomacy. [online] EU Cyber Direct. Available at: https://eucyberdirect.eu/research/quiet-conversations-observations-from-a-decade-of-practice-in-cyber-related-track-1-5-and-track-2-diplomacy.

and creating a safer environment for problem-solving are examples of intangible benefits. Although they are more difficult to quantify, tangible results include influencing official policy and diplomacy, adopting norms and standards and advancing multilateral agendas, as well as conducting joint research or sending out operational communiqués[224].

3.4 Conclusion

Negotiation in cyber-diplomacy employs a multi-layered set of formal and informal talks, borrowing from traditional diplomatic practice while adapting to the distinctive challenges of the cyberspace. Each stage – prenegotiations, "around-the-table" negotiations, diplomatic momentum, packaging agreements and the follow up stage – as well as the passage from multi-stakeholder Track Two engagements to Track One State-to-State discussions, provides an inside look into how cyber issues are framed, debated, and settled on the international level.
this complexity is a characteristic of both the negotiations themselves and the academic environment. *Negotiationologists* – researchers who investigate negotiation through an academic lens – inevitably bring their own perspectives to the analysis. Diplomats and practitioners expect to hear from them about the processes of bargaining and their structures as objectively as possible, but, as a constituent part of their culture, academics are influenced by their own background and experience and – often unconsciously – are biased. The approach of an American or European, African or Asian academic will be different, and even these categories are not homogeneous[225].

As in any social science, the problem of objective measurement continues to persists. Although game theory has significantly contributed to our understanding of how negotiations are structured, it cannot capture every dimension of the process. Purely quantitative approaches are incompatible with the nature of negotiation, and

[224] *Ibidem*

[225] Meerts, P. (2015). Diplomatic Negotiation Essence and Evolution. The Hague: Clingendael Institute.

although qualitative methods are crucial, they are vulnerable to subjectivity. The most viable path is therefore pluralistic: studying negotiation from several perspectives to obtain understanding without sacrificing academic rigor. Yet even this approach remains imperfect, constrained by the countless factors that influence negotiation rounds.

This chapter aimed to establish the theoretical framework for comprehending negotiation mechanisms. Because of the anarchy in international relations, State-to-State talks are essential to achieve national goals, avert hostilities, and preserve stability in a globalized world.

4. Cyberwarfare in Ukraine as a Stress Test for Cyber-Diplomacy and Negotiation Mechanisms

Many of the structural factors frequently linked to cyberwarfare are present in the Ukrainian conflict. Each side has advanced knowledge of computer network operations and information technology, and Moscow and Kyiv are fighting a war with significant geopolitical stakes. However, the concept of "cyber war" itself is still up for debate. Academics and professionals are still debating whether cyber operations can accomplish more than just tactical disruption and whether they can yield strategic results on par with traditional military action. The larger normative question of what guidelines should control State conduct in cyberspace in times of peace and armed conflict is also brought up by these discussions. Therefore, the Russo-Ukrainian crisis offers an invaluable case study for investigating the function of cyber operations in modern international security[226].

The ongoing armed conflict in Ukraine presents a complex security challenge due to its use of multidimensional warfare. Cyber activity around Ukraine between 2013 and 2015 demonstrated the growing complexity of warfare. Digital propaganda campaigns, distributed denial-of-service (DDoS) attacks, website vandalism, hacktivist information leaks, and the use of advanced espionage malware were all part of the operations. Even though these operations were intense, they mostly only had the effect of temporarily cutting off communication between Crimea, Donbass, and the rest of Ukraine. Notably, during this early stage, no noteworthy cyberattacks against vital military or civilian infrastructure were reported[227].

After the full-scale Russian invasion in 2022, the situation changed significantly. Cyber operations increasingly targeted civilian infrastructure, according to data gathered by the CyberPeace Institute, a non-governmental organization that records

[226] The NATO Cooperative Cyber Defence Centre of Excellence (2013). Cyber War in Perspective: Russian Aggression against Ukraine.

[227] *Ibidem*

and examines cyber incidents, on its *Platform #Ukraine*[228]. For instance, An attack on a vital energy facility was reported by Ukraine's Computer Emergency Response Team (CERT-UA) in September 2023, signaling a major increase in the scope and purpose of operations[229].

Within the report, particular attention has been directed toward Sandworm, a State-sponsored advanced persistent threat (APT) [230] group associated with the Russian Federation’s military intelligence agency. active since at least 2009, the group has caused some of the most damaging cyber events in history, such as the Ukrainian power grid outages in 2015 and the global NotPetya malware in 2017[231]. CERT-UA has also attributed to Sandworm a campaign against eleven Ukrainian telecommunications providers. The threat actor was able to obtain remote control access and search networks for open ports by utilizing previously compromised systems. Once inside, the threat actor was able to remotely access and disrupt the information and communication systems of 11 Ukrainian telecom companies by turning off servers, active networks, and data storage devices. This resulted in

[228] CyberPeace Institute (2023). Cyber Dimensions of the Armed Conflict in Ukraine. [online] CyberPeace Institute. Available at: https://cyberpeaceinstitute.org/wp-content/uploads/2023/12/Cyber-Dimensions_Ukraine-Q3-2023.pdf.

[229] CERT-UA (2023). Кібератака групи UAC-0057 (unc1151) на державні організації України з використанням шкідливої програми MicroBackdoor (CERT-UA#4109). [online] cert.gov.ua. Available at: https://cert.gov.ua/article/5702579.

[230] An advanced persistent threat (APT) is a sophisticated, sustained cyberattack in which an intruder establishes an undetected presence in a network in order to steal sensitive data over a prolonged period of time. An APT attack is carefully planned and designed to infiltrate a specific organization, evade existing security measures and fly under the radar. Executing an APT attack requires a higher degree of customization and sophistication than a traditional attack. Adversaries are typically well-funded, experienced teams of cybercriminals that target high-value organizations.
Baker, K. (2025). What is an Advanced Persistent Threat (APT)? | CrowdStrike. [online] Crowdstrike.com. Available at: https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/advanced-persistent-threat-apt/.

[231] CyberPeace Institute (2023). Cyber Dimensions of the Armed Conflict in Ukraine. [online] CyberPeace Institute.
Available at: https://cyberpeaceinstitute.org/wp-content/uploads/2023/12/Cyber-Dimensions_Ukraine-Q3-2023.pdf.

disruptions in the delivery of services to customers[232]. These operational difficulties serve as an example of how cyber incidents make negotiations more difficult by introducing attribution issues, asymmetrical capabilities, and uncertainty, all of which have an impact on States' willingness and capacity to cooperate or make concessions.

As a stress test, the Ukrainian case demonstrates both the shortcomings of direct negotiation and flexible, integrative solutions achieved through coalition building and multi-stakeholder involvement. In order to comprehend how States manage both competition and cooperation in cyberspace, it emphasizes the significance of looking at a variety of negotiation mechanisms, such as bilateral and multilateral dialogues, cyber confidence-building initiatives, crisis diplomacy, and norm-setting through international organizations.

These circumstances highlight how crucial it is to use negotiation strategies like crisis diplomacy and confidence-building initiatives in order to avoid misunderstandings and control escalation. By framing these mechanisms through negotiation theory, including game-theoretic approaches and multi-party negotiation frameworks, we can evaluate how well these mechanisms manage conflict while fostering cybersecurity cooperation, as well as how States strike a balance between strategic interests and cooperative goals. By framing these mechanisms through negotiation theory, including game-theoretic approaches and multi-party negotiation frameworks, we can evaluate how well these mechanisms manage conflict while fostering cybersecurity cooperation, as well as how States strike a balance between strategic interests and cooperative goals.

4.1 Timeline of cyber-attacks

Since at least 2014, Russia has consistently targeted Ukraine with cyberattacks. Russia's use of cyber operations against Kyiv predates the full-scale invasion of

[232] CERT-UA (2023b). Особливості деструктивних кібератак Sandworm у відношенні українських провайдерів (CERT-UA#7627). [online] cert.gov.ua. Available at: https://cert.gov.ua/article/6123309.

Ukraine on February 24, 2022, having started with the illegal annexation of Crimea in 2014 and intensifying considerably in the months preceding the invasion. Russian cyberattacks have been wide-ranging, from interfering with access to vital services to launching extensive campaigns of disinformation and data theft, including the use of deepfake technologies. Phishing campaigns, distributed denial-of-service attacks, and the use of malicious tools like data-wiper malware, backdoors, surveillance software, and information thieves have also been included in these activities[233].

In an attempt to deflect attention away from the Russian troops' presence in Crimea, Russia launched an eight-minute DDoS cyberattack on March 13, 2014, three days prior to the referendum on the region's status. The attack was intended to disrupt Ukrainian computer networks and communications[234]. The use of cyberattacks as bargaining tools in a larger coercive strategy is also highlighted in this episode. By demonstrating strength and eroding mutual trust, cyberattacks can complicate negotiation dynamics.

A pro-Russian hacktivist group conducted a series of cyberattacks in May 2014, ahead of the Ukrainian presidential elections, in an attempt to rig the results. Targeting the Central Election Commission, the CyberBerkut hackers broke into the network and erased files in an effort to tamper with the election results. The malware was eliminated forty minutes prior to the election (May 25), so the attack was unsuccessful. Nevertheless, the election count was postponed by the hackers[235].

[233] Przetacznik, J. and Tarpova, S. (2022). Russia’s war on Ukraine: Timeline of cyber-attacks. [online] European Parliament. European Parliamentary Research Service. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf.

[234] Clayton, M. (2014). Russia Hammers Ukraine With Massive Cyber-Attack. [online] Business Insider.
Available at: https://www.businessinsider.com/russia-cyberattack-ukraine-2014-3?r=US&IR=T.

[235] Laurens Cerulus (2019). How Ukraine became a test bed for cyberweaponry. [online] POLITICO. Available at: https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/.

On 23 December 2015, another DDoS attack affected call centers and the network of three energy distribution companies. As a result, over 230.000 consumers in western Ukraine experienced power outages ranging from one to six hours. Furthermore, 16 electrical substations' systems were successfully disrupted by the allegedly Russian State-sponsored Sandworm Team[236]. In 2016, a comparable cyberattack took place. A one-hour power outage was caused by disturbances in a Kyiv substation, but the attempt to totally shut down the machinery was unsuccessful[237]. The escalation negotiation dilemma is exemplified by such operations: although cyberattacks can show resolve and capability, they also limit the space for cooperative dialogue by increasing the perceived costs of concession and fostering mistrust.

Cyberattacks against Ukraine had already increased between 2016 and 2021. The most prominent one was the June 2017 release of the NotPetya malware, which is regarded as the most damaging cyberattack in history, through accounting software[238].

At the beginning of 2022, cyberattacks increased dramatically. On January 14, for example, hackers managed to temporarily take over 70 government websites, including those of the Cabinet of Ministers and the Ministries of Defense, Foreign Affairs, Education, and Science. Russia was held accountable by the Ukrainian

[236] Council on Foreign relations (2015). Compromise of a power grid in eastern Ukraine. [online] Council on Foreign Relations. Available at: https://www.cfr.org/cyber-operations/compromise-power-grid-eastern-ukraine.

[237] BBC (2017). Ukraine power cut ‘was cyber-attack’. BBC News. [online] 11 Jan. Available at: https://www.bbc.com/news/technology-38573074.

[238] HYPR (2017). What is NotPetya? 5 Fast Facts to Know About History’s Most Destructive Cyberattack. Security Encyclopedia. [online] www.hypr.com. Available at: https://www.hypr.com/security-encyclopedia/notpetya.

Ministry of Digital Transformation[239]. In mid-February, the HermeticWiper data-wiping malware, which appeared to have some similarities with previous campaigns launched by the Sandworm group[240], was launched against 100 organizations from the financial, IT and aviation sectors[241].

Additionally, independent researchers also discovered a cyber espionage operation called Armageddon that was designed to provide a "military advantage to Russian leadership by targeting Ukrainian government and law enforcement agencies", and included DDoS attacks against Ukrainian and NATO media outlets, and targeted attacks against Ukrainian election commission websites[242].

From the standpoint of negotiation theory, these heightened campaigns highlight the difficulties of negotiating under duress: as hostilities intensify, cyber operations are employed not only tactically but also to mold bargaining positions, demonstrating commitment while limiting the opponent's options.

Concerns regarding harm and effects on the civilian population, as well as the protection of civilians and civilian infrastructure that are vulnerable to both kinetic and cyberattacks, are brought up by the ongoing international armed conflict.

In this war of aggression, the term "cyber war", which describes a strategy of warfare in which both State and non-State actors seek to infiltrate another computer

[239] Catalin Cimpanu (2023). Hackers deface Ukrainian government websites. [online] Therecord.media. Available at: https://therecord.media/hackers-deface-ukrainian-government-websites.

[240] Fendorf, K. and Miller, J. (2022). Tracking Cyber Operations and Actors in the Russia-Ukraine War. [online] Council on Foreign Relations. Available at: https://www.cfr.org/blog/tracking-cyber-operations-and-actors-russia-ukraine-war.

[241] Brumfield, C. (2022). Russia-linked cyberattacks on Ukraine: A timeline. [online] CSO Online. Available at: https://www.csoonline.com/article/571865/a-timeline-of-russian-linked-cyberattacks-on-ukraine.html.

[242] Kostyuk, N. (2015). Ukraine: A Cyber Safe Haven? In: Cyber War in Perspective: Russian Aggression against Ukraine. Tallin: NATO Cooperative Cyber Defence Centre of Excellence. Available at: https://ccdcoe.org/uploads/2018/10/CyberWarinPerspective_full_book.pdf

or network in order to cause harm or disruption, is frequently used. Cyberspace is now a well-established and rapidly evolving area of conflict, despite experts' disagreements regarding the exact scope, significance, and impact of Russian cyberattacks and operations in achieving the nation's strategic objectives[243].

4.2 The engagement of Western Countries

Cyberattacks are now a common occurrence in Vladimir Putin's conflict in Ukraine. Up until 2022, data show that the Russian Federation accounted for the second-largest share of verified State-sponsored cyber operations worldwide, demonstrating its longstanding involvement in counter-State cyber operations[244].

Since the start of the Russian war of aggression in February 2022, the Western nations have greatly increased their cyber assistance to Ukraine. They are determined to keep helping the nation improve its cyber resilience, strengthen communication, and provide support for the prevention, detection, deterrence, and response to cyberthreats, particularly with regard to vital networks and infrastructure.

The European Union agreed to improve exchanges with Ukraine on situational awareness, cyber risk assessment, cyber crisis management, and the use of the EU Cyber-diplomacy Toolbox and its cyber sanctions regime in the wake of Russia's invasion of Ukraine, in a context where the use of cyber operations has enabled and accompanied Russia's war of aggression against Ukraine and continues to affect global stability and security[245].

[243] Madiega, T. (2022). Russia’s war on Ukraine: The digital dimension. [online] European Parliamentary Research Service.
Available at:
https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/729317/EPRS_ATA(2022)729317_EN.pdf.

[244] Council on Foreign Relations (2024). Cyber Operations Tracker. [online] Council on Foreign Relations. Available at: https://www.cfr.org/cyber-operations/.

[245] EU Cyber Direct (2022). Is War in Ukraine the End of Cyber-diplomacy? [online] Available at: https://eucyberdirect.eu/blog/is-war-in-ukraine-the-end-of-cyber-diplomacy.

In an attempt to deter State-backed organizations from attacking Western infrastructure, it has started enforcing sanctions on Russian hackers alongside the US. As part of a larger attempt to persuade Moscow to withdraw from the Ukrainian border, experts advise that sanctions be placed on those responsible for cyberattacks against Ukraine. Heli Tiirmaa-Klaar, the former Estonian ambassador at large for cyber-diplomacy and current head of the Digital Society Institute at the European School of Management and Technology (ESMT) in Berlin, Stated that "If Russia would be hit with major sanctions, the specific entities that were preparing cyberattacks should also feel the impact of those sanctions"[246]. However, the attribution of the actions continues to be the main issue. But these sanctions also point to a larger problem for cyber-diplomacy: clear attribution is necessary for effective negotiation and enforcement, but disagreements over accountability frequently impede diplomatic efforts and make coordinated responses more difficult.

This is a prime example of negotiation under uncertainty from the standpoint of negotiation theory: States must choose between cooperating, deterring, or escalating despite not knowing the other party's actual capabilities or intentions in the absence of trustworthy information about the responsible actors. According to Raiffa's multi-party negotiation framework, this makes it harder to convey credibility, build trust, and enforce agreements[247].

Moreover, practical initiatives have been going on. Following the EU-Ukraine cyber dialogue of June 2021, the European Union Foreign Affairs Council announced on 21 February 2022 that that the EU would take further steps to assist

[246] Laurens Cerulus (2022). Ukraine is getting pummeled with cyberattacks. What's the West to do? [online] POLITICO. Available at: https://www.politico.eu/article/ukraine-russia-cyberattack-west-diplomacy-sanction/.

[247] Merlone, U. and Spilli, G. (2023). Decidere in condizioni di incertezza: dall'approccio normativo alla Negotiation Analysis. Sistemi intelligenti, Rivista quadrimestrale di scienze cognitive e di intelligenza artificiale, (1), pp.9–30.

Ukraine in defending itself against cyberattacks[248]. Dialogues have now arrived at the third edition – the last one was held in July 2024 in Brussels – and another has been already announced and programmed for 2025.

In addition to exchanging technical expertise, the initiative serves as a means of fostering confidence by lowering mistrust and demonstrating a sustained commitment. Additionally, since the results rely on efficient coordination between numerous stakeholders, each with different priorities, dialogues enhance operational resilience and act as a testing ground for negotiation mechanisms, exposing both the potential for multilateral coordination and the ongoing gaps in balancing diverse national interests. However, these mechanisms aid in expanding the potential area of agreement.

This is consistent with the idea that both interests and positions must be taken into consideration for multi-party negotiations to be successful, especially when stakeholders have unequal power or capabilities[249].

Flagship projects, such as "CyberEast" aiming at improving cyber resilience in the Eastern Partnership countries also continued and cyber support efforts have been coordinated with Member States and partners, including through the Tallinn Mechanism[250]. In 2021, EU set up a cyber lab for the Ukrainian Armed Forces, an exercising and researching environment composed of several virtual and physical components. It can be used to represent realistic scenarios for training to advance

[248] Euopean Union External Action Service (2022). Foreign Affairs Council: Press remarks by High Representative Josep Borrell after the meeting. [online] EEAS. Available at: https://www.eeas.europa.eu/eeas/foreign-affairs-council-press-remarks-high-representative-josep-borrell-after-meeting_en.

[249] Pfetsch, F.R. (2011). Power in International Negotiations: Symmetry and Asymmetry. Négociations, 16(2), p.39.

[250] EEAS Press Team (2024). Ukraine: 3rd Cyber Dialogue with the European Union takes place in Brussels. [online] EEAS. Available at: https://www.eeas.europa.eu/eeas/ukraine-3rd-cyber-dialogue-european-union-takes-place-brussels_en.

the hands-on skills of military cyber defence professionals[251]. A similar initiative was already established at the NATO Summit in Warsaw in July 2016, with the NATO-Ukraine Platform on Countering Hybrid Warfare. The Platform has supported research, training and expert consultations, with a focus on lessons learned, countering disinformation and enhancing resilience[252]. The United States, as well, in July 2022, signed a Memorandum of Cooperation with Ukrainian partners to strengthen collaboration on shared cybersecurity priorities in the areas of information exchanges and sharing of best practices on cyber incidents, critical infrastructure security technical exchanges and cybersecurity training and joint exercises[253].

On 22 August 2025, the Russian Embassy in Malta released a press release on the "*Western Involvement in Cyber Attacks Against the Russian Federation and the Global Risks of Politicizing Cyberspace*". The note explicitly condemned NATO for "actively reforming Ukraine's cyber units", mentioning specific member States, such as the United States, the United Kingdom, Canada, Poland and the Netherlands. Moreover, the US National Security Agency's Directorate of Computer Network Operations and the Department of Defense's Chief Digital and Artificial Intelligence Office were accused of supervising the execution of cyberattacks against Russia, while Poland was retained responsible for the encouraging illegal activity: the award given to the "IT Army of Ukraine" and

[251] Euopean Union External Action Service (2024). Ukraine: EU sets up a cyber lab for the Ukrainian Armed Forces. [online] EEAS. Available at: https://www.eeas.europa.eu/eeas/ukraine-eu-sets-cyber-lab-ukrainian-armed-forces_en.

[252] NATO (2025). Relations with Ukraine. [online] NATO. Available at: https://www.nato.int/cps/en/natohq/topics_37750.htm.

[253] CISA (2022). United States and Ukraine Expand Cooperation on Cybersecurity. [online] www.cisa.gov. Available at: https://www.cisa.gov/news-events/news/united-States-and-ukraine-expand-cooperation-cybersecurity.

Ukraine's Minister of Digital Transformation at the CYBERSEC-2022 conference in Poland was seen as a "blatant example of double standards"[254]

As Ukraine's allies have hastened to develop new means of defense, reconstitution, and deterrence, it has become strikingly clear that "defense [and deterrence] against a military invasion now requires for most countries the ability to disburse and distribute digital operations and data assets across borders and into other countries"[255].

4.3 The engagement of private entities and its advantages

Multiple private companies have played a critical role in helping Ukraine maintain access to cyberspace. In its 2022 report, Microsoft declared that Ukraine was able to withstand a significant percentage of the damaging Russian cyberattacks by combining endpoint protection with cyber threat intelligence[256]. Mykhalio Fedorov, the deputy prime minister and minister of digital transformation for Ukraine, praised Amazon Web Services (AWS) in November 2022 for their assistance in ensuring Ukraine's government continuity during the conflict[257]. Similarly, Cloudflare, a cybersecurity company, expanded its Project Galileo services to important organizations throughout Ukraine. Project Galileo is a comprehensive

[254] Embassy of the Russian Federation to the Republic of Malta (2025). On Western Involvement in Cyber Attacks Against the Russian Federation and the Global Risks of Politicizing Cyberspace - Press Release. [online] Available at: https://malta.mid.ru/en/embassy/press-centre/news/on_western_involvement_in_cyber_attacks_against_the_russian_federation_and_the_global_risks_of_polit/.

[255] Smith, B. (2022). Defending Ukraine: Early Lessons from the Cyber War. [online] Microsoft. Available at: https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/.

[256] Smith, B. (2022). Defending Ukraine: Early Lessons from the Cyber War. [online] Microsoft. Available at: https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/.

[257] Tangalakis-Lippert, K. (2022). Amazon 'saved the Ukrainian government' with suitcase-sized hard drives. [online] Business Insider. Available at: https://www.businessinsider.com/amazon-saved-the-ukrainian-government-with-suitcase-sized-hard-drives-2022-12.

protection program for organizations involved in the arts, human rights, civil society, journalism, and democracy promotion[258]. This effort paralleled Google's Project Shield, which seeks to help at-risk organizations defend against cyber intrusions[259].

Russia has condemned this interaction and accused private companies of supporting Ukraine's cyberattacks. Malicious activity linked to Google Global Cache equipment was discovered in Russia during the "Games of the Future" multisport competition in February 2024. The government condemned publicly the cooperation of Ukrainians with Western companies, asserting that these ones help transforming civilian technologies as weapons in times of conflict[260].

However, the private sector engagement offers operational resilience and provides platforms for information exchange, collaborative training and capacity-building initiative, that complement diplomatic initiatives.

4.4 Legal challenges and normative frameworks

On a legal level, the international armed conflict in Ukraine raises important questions of international law that are also relevant for cyber-diplomacy. These include the conduct of hostilities, international criminal law and State responsibility. Another pressing question concern the regulation of cyber operations by international humanitarian law: cyber operations during armed conflicts must

[258] Prince, M. (2022). Steps we've taken around Cloudflare's services in Ukraine, Belarus, and Russia. [online] The Cloudflare Blog. Available at: https://blog.cloudflare.com/steps-taken-around-cloudflares-services-in-ukraine-belarus-and-russia/.

[259] Greenberg, K. (2023). With political 'hacktivism' on the rise, Google launches Project Shield to fight DDos attacks. [online] TechRepublic. Available at: https://www.techrepublic.com/article/google-launches-project-shield/.

[260] Embassy of the Russian Federation to the Republic of Malta (2025). On Western Involvement in Cyber Attacks Against the Russian Federation and the Global Risks of Politicizing Cyberspace - Press Release. [online] Available at: https://malta.mid.ru/en/embassy/press-centre/news/on_western_involvement_in_cyber_attacks_against_the_russian_federation_and_the_global_risks_of_polit/.

respect its obligations, included those of the Tallinn Manual 2.0 (rules 86–145) and restrictions on targeting civilians and non-military infrastructures[261]. However, in reality, legal interpretation negotiations frequently resemble distributive bargaining, with States promoting stances that safeguard their strategic freedom of action rather than looking for integrative solutions that could benefit both parties[262].

The norms of the framework of responsible State behavior, as laid down in the United Nations Group of Governmental Experts reports of 2015 and 2021 and in the Open-ended Working Group report of 2021, are considered “peacetime norms” and are thus not applicable[263]. States must balance current legal agreements with the pressing demands of conflict, frequently without established mechanisms to mediate disputes over interpretation or enforcement. This discrepancy between normative frameworks and wartime realities exemplifies a fundamental negotiation challenge. Game theory can also be used to examine the problem since States use strategic interactions to strike a balance between immediate military goals and norm compliance, reiterating Schelling's ideas of credible threats and strategic signaling[264].

The UN General Assembly decided in September 2023 to establish a separate "Ad Hoc Committee" to begin negotiations on an international cybercrime convention. Western allies have long advocated for the convention to ensure that human rights obligations are upheld while concentrating exclusively on cybercrime. For their part, States with restrictive digital policies have used language that defends

[261] EU Cyber Direct (2022). Is War in Ukraine the End of Cyber-diplomacy? [online] Available at: https://eucyberdirect.eu/blog/is-war-in-ukraine-the-end-of-cyber-diplomacy.

[262] World Bank (n.d.). Negotiation | Defining Bargaining and Negotiation. [online] The World Bank. Available at: https://assets.publishing.service.gov.uk/media/57a08b4540f0b652dd000bca/Negotiationweb.pdf.

[263] *Ibidem*

[264] Hayati Ünlü (2024). Deterrence in Inter-State Communication: International Signaling Strategies. Erciyes İletişim Dergisi, 11(2), pp.441–459.

repression and surveillance under the pretext of protecting digital "sovereignty" and combatting "extremism" or "harmful information"[265].

The United Nations Convention against Cybercrime was adopted by the UN General Assembly on December 24, 2024, by resolution 79/243[266]. It aims to improve global collaboration in the sharing of electronic evidence related to serious crimes. This Convention, which has nine chapters, provides a comprehensive framework for combating cybercrime while integrating human rights protections. By enhancing global cooperation and modifying conventional investigative techniques for the digital sphere, it tackles both technical and legal issues. With blocs of States pursuing conflicting visions of sovereignty and human rights, the convention process also demonstrates how negotiations can turn into arenas for normative contestation. Zartman refers to this as a "mutually hurting stalemate", where progress only happens when all parties believe that continuing to stand still is more expensive than reaching a compromise.

The Convention has been largely criticized. States seem to be granted excessive powers to collect sensitive and private and personal data without the obligation to comply with the principles of proportionality, necessity and legality, with no human rights safeguards that tackle all these security concerns. Moreover, the Convention gives little attention to the vulnerable individuals, especially women and LGBTQIA+. As mentioned in the *Gender Perspectives* paragraph of this work, cyberspace is inherently a more hostile environment for women than men. According to the report of 2023 by *Derechos Digitales*, developed with the support of the UK government "*Cybercrime laws normally refer to non-gender-specific acts or are designed without due consideration to gender inequalities. Criminal*

[265] Stradner, I. (2023). China and Russia are using the UN to censor the world. [online] The Telegraph. Available at: https://www.telegraph.co.uk/news/2023/09/01/china-xi-jinping-vladimir-putin-united-nations/.

[266] United Nations General Assembly (2024). Resolution 79/243. [online] Un.org. Available at: https://docs.un.org/en/A/RES/79/243.

definitions are drafted in a broad manner and without applying a gender perspective in their formulation and in their implementation. As a result, the impact of the criminalization generated by these laws also has specific effects on gender equality"[267].

The conflict in Ukraine has also demonstrated how underlying geopolitical tensions shape multilateral negotiations, with cyber conventions evolving from purely technical cooperation to arenas where States challenge normative authority and influence. This situation exemplifies the theory of crisis diplomacy, which holds that in order to reach any significant agreement, negotiations must be conducted under conditions of high stakes, low trust, and competing interests[268].

Coordination with private companies and international organizations is necessary as the cyber conflict develops, demonstrating the idea of multi-level negotiations in a complex security environment. This is part of a larger movement in negotiation theory away from State-centric bargaining and toward networked negotiations, in which private actors, international organizations, and States form overlapping negotiation tables with different but related agendas.

When considered collectively, the Ukrainian case demonstrates how coordination between governments, the commercial sector, academic institutions, non-governmental organizations, and international organizations is becoming more and more necessary in the face of cyber conflict. Thus, Ukraine acts as a stress test for cyber-diplomacy, demonstrating how multi-level and multi-track negotiations can shape international cybersecurity cooperation, influence State behavior, and foster trust in highly uncertain environments.

[267] Derechos Digitales (2023). Gender considerations on cybercrime frameworks When Protection Becomes An Excuse For Criminalisation. [online] Available at: https://www.derechosdigitales.org/wp-content/uploads/gender_considerations_on_cybercrime.pdf

[268] Diplo Foundation (2021). Crisis diplomacy. [online] Diplo. Available at: https://www.diplomacy.edu/topics/crisis-diplomacy/.

4.5 Conclusion

The ongoing cyber aspect of the conflict between Russia and Ukraine highlights how international security is changing and how both State and non-State actors are involved in intricate, multifaceted operations. The experience of Ukraine demonstrates that cyber incidents affect strategic calculations, negotiation dynamics, and the more general regulations governing State behavior in cyberspace in addition to being tactical disruptions. Multilateral efforts, private sector involvement, and Western assistance have all been crucial in boosting resilience, promoting information exchange, and broadening the reach of diplomacy beyond conventional State-to-State avenues.

The Ukrainian case illustrates how diplomatic negotiation mechanisms, which range from bilateral and multilateral dialogues to confidence-building measures, crisis diplomacy, and norm-setting processes, are crucial for managing uncertainty, fostering trust, and preventing escalation, according to this thesis, which looks at how diplomatic negotiation mechanisms can mitigate cyber conflicts and improve international cybersecurity cooperation.

The significance of well-planned, inclusive, and multi-level approaches to cyber-diplomacy is underscored by both achievements and constraints, including attribution issues, small-group versus plenary negotiation formats, and normative contestation in international forums.

In the end, the conflict in Ukraine acts as a stress test for international cyber governance. It shows that a combination of multistakeholder engagement, legal and normative clarity, strategic coordination, and flexible negotiation techniques are necessary for successful cyber-diplomacy. States and international organizations can better navigate the new challenges of cyberspace by incorporating lessons learned from this conflict. This will help them balance cooperative objectives with competitive interests and create a more secure and resilient digital domain, which directly answers the main research question of this thesis.

5. Final Conclusion

The purpose of this thesis was to respond to the following research question: How do negotiation mechanisms affect States' attitudes in cyberspace, and how successful are they at resolving disputes and promoting international cybersecurity cooperation?

The study has shown that negotiation mechanisms play a key role in determining State behavior in cyberspace by looking at the development of cyber-diplomacy, the strategic stances of States and international organizations, negotiation theoretical frameworks, and the stress test of the Russo-Ukrainian cyber conflict. They serve as tools for developing collaborative frameworks and promoting global cybersecurity governance in addition to being conflict management tools.

The thesis demonstrated that the "*diplomatization*" of cyberspace has been fueled by historic cyber incidents like Estonia (2007), Georgia (2008), and Stuxnet (2010), as outlined in Chapter 1's historical perspective on cyber-diplomacy. States were encouraged by these crises to create diplomatic tools like new platforms for negotiations and confidence-building measures. The emergence of multistakeholder diplomacy, highlighted by programs such as the Global Commission on the Stability of Cyberspace, has broadened the scope of negotiations beyond States and demonstrated that inclusiveness, transparency, and the incorporation of private actors and civil society are essential for successful diplomacy in cyberspace. These changes show that once cyber incidents showed the dangers of escalation, negotiation mechanisms were no longer an optional option but rather became essential. They also demonstrate how States' perceptions of cyberspace changed from being limited to technical or military issues to acknowledging it as a diplomatic area that calls for organized discussion.

National and international approaches were emphasized in Chapter 2, which demonstrated how the strategic cultures of individual States and the forums in which they participate influence negotiation mechanisms. Russia portrays cyber governance as a security conundrum, while China places more emphasis on cyber sovereignty than the European Union does on rule-based regulation. Multilateral initiatives like the Open-Ended Working Group (OEWG) and the Group of Governmental Experts (GGE), along with OSCE CBMs and NATO frameworks, demonstrate how negotiation creates norms, fosters trust, and deters escalation. These forums, however, are also sites of normative contestation, where divergent perspectives on governance, human rights, and sovereignty make reaching an agreement more difficult. This chapter also demonstrated how gender viewpoints are still underrepresented in many cyber negotiations, underscoring an unsolved issue in creating more inclusive and successful agreements. By requiring opposing viewpoints to coexist within a shared process, negotiation forums serve as stabilizers while also reflecting geopolitical rivalries. The very process of negotiating establishes common expectations that influence State behavior and lessen the possibility of unilateral escalation, even in cases where there is little consensus.

Chapter 3's analysis of the theoretical frameworks made clear how negotiation works in real-world situations. Game theory in conjunction with traditional diplomatic ideas demonstrated why, in anarchic international systems, cooperation is frequently brittle but essential. Models like the stag hunt and prisoner's dilemma showed that although mistrust can erode agreements, a common understanding of interdependence offers incentives for collaboration. Using expert discussions between the United States and Russia as an example, the chapter also demonstrated the value of Track II diplomacy and informal communication in mending rifts when formal negotiations stall. The chapter came to the conclusion that multi-level negotiation mechanisms that combine State-led (Track I) efforts with multi-stakeholder and informal channels are the most successful in cyberspace. The results imply that maintaining open communication, rephrasing incentives, and letting trust grow gradually are more effective strategies in cyberspace than drafting quick, legally binding agreements. Therefore, negotiation functions as an ongoing adaptation process as opposed to a one-time settlement event.

Chapter 4 illustrated how negotiation mechanisms are put to the test in situations of geopolitical rivalry and ongoing conflict using the Russo-Ukrainian conflict as a case study. In addition to serving as tactical instruments, cyber operations during the conflict had an impact on multilateral negotiations and diplomatic signaling. Negotiations between Western nations, private businesses, and international organizations transcended conventional diplomacy and reflected the new reality of multi-level, multi-actor cyber-diplomacy. The case also revealed the limitations of negotiation, as progress toward legally binding agreements was slowed by attribution issues, divergent narratives, and geopolitical divisions. However, the Ukrainian experience demonstrated that negotiation mechanisms—whether through legal frameworks, crisis diplomacy, or confidence-building—remain crucial for preventing escalation and fortifying long-term cooperation, even during times of crisis. Negotiation does not vanish during times of war; rather, it adjusts to the new circumstances, as the Ukrainian case illustrates. Mechanisms like CBMs, informal discussions, and private-sector involvement remain essential barriers against unchecked escalation even in the face of fierce geopolitical competition.

This thesis emphasizes for academics the importance of connecting negotiation theory and international relations when studying cyberspace. Future studies should look into how power dynamics in cyber negotiations may change as a result of emerging technologies like artificial intelligence and quantum computing, as well as how underrepresented and developing nations' perspectives can be better incorporated into international cyber-diplomacy.

Three key conclusions can be drawn from this thesis's findings when combined. First, by defining expectations, lowering mistrust, and providing alternatives to unilateral action, negotiation mechanisms have a substantial impact on State attitudes in cyberspace. Second, they continue to be the most effective means of preventing escalation and encouraging responsible State behavior, even though their ability to manage conflicts is frequently limited by power politics and normative divides. Third, the development of cyber-diplomacy emphasizes that inclusiveness – including nations, academia, and civil society – as well as flexibility in the face of swiftly shifting geopolitical and technological environments are necessary for successful negotiation.

To sum up, negotiation mechanisms shape States' attitudes in cyberspace by redefining competition as manageable cooperation, fostering dialogue where mistrust predominates, and maintaining open lines of communication even in times of crisis. Building trust, lowering the risk of escalation, and laying the groundwork for long-term international cybersecurity cooperation are what make them effective rather than achieving quick and legally binding settlements. A stable and secure digital order must be built on the foundation of negotiation mechanisms, even though cyber-diplomacy is still a developing field.

Glossary

Chapter 1

Cyberspace: The interdependent network of information-technology infrastructures, including the Internet, telecom networks, computer systems, and embedded controllers.

Cyber-diplomacy: The use of diplomatic tools and thinking to manage, govern, and negotiate issues arising in cyberspace (norms, security, cooperation).

Cybersecurity: Technical, organizational and policy measures aimed at protecting networks, systems and data from unauthorized access, damage or disruption.

Digital diplomacy / E-diplomacy: Use of digital tools (social media, virtual meetings, online platforms) to conduct diplomatic outreach and communications.

Confidence-Building Measures (CBMs): Voluntary transparency and communication procedures designed to reduce mistrust, prevent escalation and improve predictability between States in cyberspace.

Multistakeholderism: An approach to governance that includes States, private sector, academia and civil society as co-participants in policymaking.

Group of Governmental Experts (GGE): A UN expert forum historically used to discuss norms, international law and responsible State behaviour in cyberspace.

Open-Ended Working Group (OEWG): A UN plenary format for broader participation of UN member States (and inputs from non-State actors) on cyber norms and rules.

Tech or Digital Ambassador (TechPlomacy): A diplomatic post created to engage with global tech firms and stakeholders and to promote national tech priorities abroad.

Global Commission on the Stability of Cyberspace (GCSC): A multistakeholder commission that proposes norms and policies aimed at improving global cyber stability.

Chapter 2

National cyber posture / strategy: A country's mix of legal, political, technical and (sometimes) military measures defining how it manages cyberspace risks and advances interests.

Digital sovereignty: A policy orientation emphasizing a State's authority to regulate data, infrastructure and digital activity within its territory.

EU cyber-diplomacy toolbox / mechanisms: The set of EU policies, coordination tools and frameworks used to project the EU's external cyber policy and crisis response.

Bureau of Cyberspace and Digital Policy (CDP): The U.S. diplomatic bureau that consolidates U.S. international engagement on cyberspace and digital policy.

Budapest Convention: The Council of Europe treaty that harmonizes legislation and cooperation on cybercrime and cross-border investigations.

NATO information-sharing / resilience initiatives: Alliance mechanisms for sharing cyber threat intelligence, conducting exercises and strengthening collective resilience.

Public-private partnership: Cooperative arrangements between governments and private sector actors to share information, expertise and capabilities in cybersecurity.

Digital authoritarianism: Use of digital tools and policies by States to surveil, control and repress populations online (contrasted with liberal/rights-based approaches).

Chapter 3

Prenegotiations ("talks about talks"): Informal preliminary discussions to agree whether to negotiate, set the agenda and determine procedures.

"Around-the-table" negotiations: The formal negotiation phase focused on agreeing broad principles and a framework for settlement.

Details stage / finalization: The phase where specific terms, verification and ratification processes are finalized and commitments are made binding.

BATNA (Best Alternative to a Negotiated Agreement): The fallback option a party will pursue if negotiations fail; central to bargaining power.

Track-Two / Track-1.5 diplomacy: Informal expert, academic or NGO dialogues (Track-Two) and hybrid unofficial/official formats (Track-1.5) used to build ideas and trust.

Distributive bargaining: A negotiation approach that treats outcomes as a fixed pie where one party's gain is another's loss (zero-sum).

Integrative bargaining: A negotiation approach that seeks value creation and mutually beneficial trade-offs (win-win opportunities).

Game theory (strategic reasoning): Formal models (matrices, extensive trees) representing strategic choices, payoffs and interdependence among negotiators.

Ellsberg's Critical Risk Theory: A crisis bargaining model that explains decisions by reference to each actor's tolerance for breakdown risk and estimates of the opponent's resolve.

Chapter 4

Advanced Persistent Threat (APT): A highly capable, sustained and stealthy intrusion campaign aimed at long-term access, espionage or disruption.

Phishing: A method where attackers send fake emails or messages pretending to be trustworthy sources, tricking people into giving away sensitive information like passwords or credit card numbers.

Distributed Denial-of-Service (DDoS) Attack: An attack that overwhelms a website or server with too much traffic from many sources, causing it to slow down or crash so real users can't access it.

Data-Wiper Malware: Malicious software designed to permanently delete or corrupt files on a system, often used to cause damage or erase evidence of other attacks.

Backdoor: A hidden way for attackers to access a system without permission, often installed secretly to allow remote control or data theft.

Surveillance Software: Software used to secretly monitor a user's activity – like tracking keystrokes, recording screens, or turning on cameras – often for spying or data collection.

Information Stealer (Infostealer): Malware that quietly collects private data such as login credentials, browser cookies, and banking info, then sends it to the attacker.

NotPetya: A destructive 2017 malware campaign (disguised as ransomware) that caused widespread damage in Ukraine and internationally.

Sandworm: A State-linked APT group associated with destructive operations against Ukrainian infrastructure and high-profile incidents.

Bibliography

Allison, G. (2012). The Cuban Missile Crisis at 50: Lessons for U.S. Foreign Policy Today. *Foreign Affairs*, 91(4), pp.11–16.

and, E. (2024). *Browse Issue | Asian Research Policy : KISTEP Korea Institute of S&T Evaluation and Planning*. [online] KISTEP Korea Institute of S&T Evaluation and Planning. Available at: https://www.kistep.re.kr/arpIssue.es?act=content_view&list_no=225&act=content_view&mid=a20802000000.

Annegret Bendiek (2024). *The EU as a Force for Peace in International Cyber Diplomacy*. [online] Stiftung Wissenschaft und Politik (SWP). Available at: https://www.swp-berlin.org/publikation/the-eu-as-a-force-for-peace-in-international-cyber-diplomacy.

Attatfa, A., Renaud, K. and Paoli, S.D. (2020). Cyber diplomacy: A systematic literature review. *Procedia Computer Science*, 176.

Baker, K. (2025). *What is an Advanced Persistent Threat (APT)? | CrowdStrike*. [online] Crowdstrike.com. Available at: https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/advanced-persistent-threat-apt/.

Barmpaliou, N. and Pawlak, P. (2025). *Between ambition and pragmatism: The future of cyber capacity-building in a fragmented world*. [online] European Union Institute for Security Studies. Available at: https://www.iss.europa.eu/publications/reports/between-ambition-and-pragmatism-future-cyber-capacity-building-fragmented.

Barrinha, A. (2024a). Cyber-diplomacy: The Emergence of a Transient Field. *The Hague Journal of Diplomacy*, 19(3), pp.1–28.

Barrinha, A. (2024b). Cyber-diplomacy: The Emergence of a Transient Field. *The Hague Journal of Diplomacy*.

Barrinha, A. and Renard, T. (2017). Cyber-diplomacy: the making of an international society in the digital age. *Global Affairs*, 3(4-5), pp.353–364.

BBC (2017). Ukraine power cut 'was cyber-attack'. *BBC News*. [online] 11 Jan. Available at: https://www.bbc.com/news/technology-38573074.

Bendiek, A. (2018). *The EU as a force for peace in international cyber diplomacy*. Berlin: Stiftung Wissenschaft und Politik (SWP) | German Institute for International and Security Affairs.

Berridge, G.R. (2022). *Diplomacy*. Cham, Switzerland: Springer International Publishing. doi:https://doi.org/10.1007/978-3-030-85931-2.

Berridge, G.R. (2023). *Theory and Practice: Negotiations*. [online] DiploFoundation. Available at: https://asef.org/wp-content/uploads/2020/10/ModelASEM_Diplo_Negotiations.pdf.

Betz, D. and Stevens, T. (2017). *Cyberspace and the State*. 1st ed. Routledge. doi:https://doi.org/10.4324/9781351224543.

Boella, G. and Van Der Torre, L. (2007). *Power in Norm Negotiation*.

Borg Psaila, S. (2021). *Improving the practice of cyber diplomacy: A gap analysis of training, tools, and other resources*. DiploFoundation. Commisioned by the Global Forum on Cyber Expertise (GFCE) .

Bozhkov, N. (2020). *China's Cyber Diplomacy: A Primer :: EU Cyber Direct*. [online] eucyberdirect.eu. Available at: https://eucyberdirect.eu/research/chinas-cyber-diplomacy-a-primer.

Brumfield, C. (2022). *Russia-linked cyberattacks on Ukraine: A timeline*. [online] CSO Online. Available at: https://www.csoonline.com/article/571865/a-timeline-of-russian-linked-cyberattacks-on-ukraine.html.

Buck, S.J. (1998). *The Global Commons*. Routledge.

Carpini, L. (2021). *Diplomazia cyber*. [online] Agenda Digitale. Available at: https://www.agendadigitale.eu/sicurezza/diplomazia-cibernetica-carpini-maeci-sfide-e-obiettivi-della-farnesina-sullo-scacchiere-globale/.

Catalin Cimpanu (2023). *Hackers deface Ukrainian government websites*. [online] Therecord.media. Available at: https://therecord.media/hackers-deface-ukrainian-government-websites.

CERT-UA (2023a). *Кібератака групи UAC-0057 (unc1151) на державні організації України з використанням шкідливої програми MicroBackdoor (CERT-UA#4109)*. [online] cert.gov.ua. Available at: https://cert.gov.ua/article/5702579.

CERT-UA (2023b). *Особливості деструктивних кібератак Sandworm у відношенні українських провайдерів (CERT-UA#7627)*. [online] cert.gov.ua. Available at: https://cert.gov.ua/article/6123309.

Cheney, C. (2022). *Why more lower-income nations are engaging in tech diplomacy*. [online] Devex. Available at: https://www.devex.com/news/why-more-lower-income-nations-are-engaging-in-tech-diplomacy-104006.

CISA (2022). *United States and Ukraine Expand Cooperation on Cybersecurity*. [online] www.cisa.gov. Available at: https://www.cisa.gov/news-events/news/united-states-and-ukraine-expand-cooperation-cybersecurity.

CISA. (2009). *Cyberspace Policy Review*.

Clayton, M. (2014). *Russia Hammers Ukraine With Massive Cyber-Attack*. [online] Business Insider. Available at: https://www.businessinsider.com/russia-cyberattack-ukraine-2014-3?r=US&IR=T.

Correia, M. (2024). *Securing cyberspace : threats and challenges to NATO*. [online] Repositorio.ucp.pt. Available at: https://repositorio.ucp.pt/entities/publication/d68f6efe-0e0a-4b02-b3a6-d10d7bdee695.

Council Conclusions on Cyber Diplomacy. (2015). [online] Council of the European Union. Available at: https://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf.

Council of Europe (2014). *Budapest Convention and Related Standards*. [online] Council of Europe. Available at: https://www.coe.int/en/web/cybercrime/the-budapest-convention.

Council on Foreign Relations (2024). *Cyber Operations Tracker*. [online] Council on Foreign Relations. Available at: https://www.cfr.org/cyber-operations/.

Council on Foreign relations (2015). *Compromise of a power grid in eastern Ukraine*. [online] Council on Foreign Relations. Available at: https://www.cfr.org/cyber-operations/compromise-power-grid-eastern-ukraine.

Cyber Diplomacy Toolbox (n.d.). *Cyber Diplomacy in the USA*. [online] Available at: https://www.cyber-diplomacy-toolbox.com/Cyber_Diplomacy_USA.html.

Cyber Security Strategy of the United Kingdom safety, security and resilience in cyber space. (2009). London: Cabinet Office.

CyberPeace Institute (2023). *Cyber Dimensions of the Armed Conflict in Ukraine*. [online] CyberPeace Institute. Available at: https://cyberpeaceinstitute.org/wp-content/uploads/2023/12/Cyber-Dimensions_Ukraine-Q3-2023.pdf.

Derechos Digitales (2023). *Gender considerations on cybercrime frameworks WHEN PROTECTION BECOMES AN EXCUSE FOR CRIMINALISATION*. [online] Available at: https://www.derechosdigitales.org/wp-content/uploads/gender_considerations_on_cybercrime.pdf [Accessed 14 Sep. 2025].

Diplo Foundation (2021). *Crisis diplomacy*. [online] Diplo. Available at: https://www.diplomacy.edu/topics/crisis-diplomacy/.

Duguin, S. and Pavlova, P. (2023). *The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict*. Brussels: European Parliament.

Eatwell, J., Milgate, M. and Newman, P. eds., (1989). *Game Theory*. London: Palgrave Macmillan UK. doi:https://doi.org/10.1007/978-1-349-20181-5.

EEAS (n.d.). *EU-China 2020 Strategic Agenda for Cooperation*. [online] Available at: https://www.eeas.europa.eu/sites/default/files/20131123.pdf.

EEAS Press Team (2022). *European Union and NATO hold the first Structured Dialogue on Cyber*. [online] EEAS. Available at: https://www.eeas.europa.eu/eeas/european-union-and-nato-hold-first-structured-dialogue-cyber-0_en.

EEAS Press Team (2024). *Ukraine: 3rd Cyber Dialogue with the European Union takes place in Brussels*. [online] EEAS. Available at: https://www.eeas.europa.eu/eeas/ukraine-3rd-cyber-dialogue-european-union-takes-place-brussels_en.

Embassy of the Russian Federation to the Republic of Malta (2025). *On Western Involvement in Cyber Attacks Against the Russian Federation and the Global Risks of Politicizing Cyberspace - Press Release*. [online] Available at: https://malta.mid.ru/en/embassy/press-centre/news/on_western_involvement_in_cyber_attacks_against_the_russian_federation_and_the_global_risks_of_polit/.

Erzse, A. and Garson, M. (2022). *A Leaders' Guide to Building a Tech- Forward Foreign Policy*. London: Tony Blair Institute for Global Change.

EU Cyber Direct (2022). *Is War in Ukraine the End of Cyber Diplomacy?* [online] Available at: https://eucyberdirect.eu/blog/is-war-in-ukraine-the-end-of-cyber-diplomacy.

Euopean Union External Action Service (2024). *Foreign Affairs Council: Press remarks by High Representative Josep Borrell after the meeting*. [online] EEAS.

Available at: https://www.eeas.europa.eu/eeas/foreign-affairs-council-press-remarks-high-representative-josep-borrell-after-meeting_en.

Euopean Union External Action Service (2024). *Ukraine: EU sets up a cyber lab for the Ukrainian Armed Forces*. [online] EEAS. Available at: https://www.eeas.europa.eu/eeas/ukraine-eu-sets-cyber-lab-ukrainian-armed-forces_en.

EUR-Lex (2019). *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).* [online] Europa.eu. Available at: https://eur-lex.europa.eu/eli/reg/2019/881/.

European Commission (2024). *EU Cyber Resilience Act | Shaping Europe's digital future*. [online] digital-strategy.ec.europa.eu. Available at: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act.

European Commission (2025). *The EU Cyber Solidarity Act | Shaping Europe's digital future*. [online] Available at: https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity.

European Commission. (2020). *The EU's Cybersecurity Strategy for the Digital Decade | Shaping Europe's digital future*. [online] Available at: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0.

European Union (2020). *Shared Vision, Common Action: A Stronger Europe A Global Strategy for the European Union's Foreign And Security Policy.* [online] Europa.eu. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020JC0018.

Fendorf, K. and Miller, J. (2022). *Tracking Cyber Operations and Actors in the Russia-Ukraine War*. [online] Council on Foreign Relations. Available at: https://www.cfr.org/blog/tracking-cyber-operations-and-actors-russia-ukraine-war.

Foulon, M. and Gustav Meibauer (2024). How Cyberspace Affects International relations: the Promise of Structural Modifiers. *Contemporary Security Policy*, 45(3), pp.1–33. doi:https://doi.org/10.1080/13523260.2024.2365062.

Gady, F.-S. and Austin, G. (2010a). *Russia, The United States, And Cyber Diplomacy Opening the Doors*. New York: EastWest Institute.

Gady, F.-S. and Austin, G. (2010b). *Russia, The United States, And Cyber Diplomacy Opening the Doors*. [online] Available at: https://www.files.ethz.ch/isn/121211/USRussiaCyber_WEB.pdf.

Gaffal, M. and Jesús Padilla Gálvez (2023). Negotiation, Game Theory and Language Games. In: *Dynamics of Rational Negotiation*. pp.11–40. doi:https://doi.org/10.1007/978-3-031-49051-4_2.

Geoff Berridge (2015). *Diplomacy Theory and Practice*. Basingstoke, Palgrave Macmillan.

Giles, K. and Hagestad II, W. (2013). Divided by a Common language: Cyber Definitions in Chinese, Russian and English. In: *5th International Conference on Cyber Conflict*. Tallinn: NATO CCD COE Publications.

Global Commission on the Stability of Cyberspace (2019). *The Global Commission on the Stability of Cyberspace: Promoting stability in cyberspace to build peace and prosperity* . [online] Available at: https://cyberstability.org.

Global Commission on the Stability of Cyberspace (GCSC) (2019). *ADVANCING CYBERSTABILITY FINAL REPORT GLOBAL COMMISSION ON THE STABILITY OF CYBERSPACE*. [online] Available at: https://hcss.nl/wp-content/uploads/2019/11/GCSC-Final-Report-November-2019.pdf.

Government of Canada (2010). *Canada's Cyber Security Strategy: for a Stronger and More Prosperous Canada*.

Greenberg, K. (2023). *With political 'hacktivism' on the rise, Google launches Project Shield to fight DDos attacks*. [online] TechRepublic. Available at: https://www.techrepublic.com/article/google-launches-project-shield/.

Guterres, A. (2023). *A New Agenda for Peace*. [online] Available at: https://www.un.org/sites/un2.un.org/files/our-common-agenda-policy-brief-new-agenda-for-peace-en.pdf.

Hansel, M. (2023). Great power narratives on the challenges of cyber norm building. *Policy Design and Practice*, pp.1–16. doi:https://doi.org/10.1080/25741292.2023.2175995.

Hayati Ünlü (2024). Deterrence in Inter-State Communication: International Signaling Strategies. *Erciyes İletişim Dergisi*, 11(2), pp.441–459.

Henderson, H. (2021). Cybered Competition, Cooperation, and Conflict in a Game of Imperfect Information. *The Cyber Defense Review*, 6(3), pp.43–60. doi:https://doi.org/10.2307/48631154.

Herrero, Á. (2025). *The future of global security and why cyber diplomacy matters* . [online] Diplo. Available at: https://www.diplomacy.edu/blog/the-future-of-global-security-and-why-cyber-diplomacy-matters/ [Accessed 20 Jul. 2025].

Höne, K. (2022). *What is Tech Diplomacy?* Heinrich-Böll-Stiftung.

HYPR (2017). *What is NotPetya? 5 Fast Facts | Security Encyclopedia*. [online] www.hypr.com. Available at: https://www.hypr.com/security-encyclopedia/notpetya.

I William Zartmann (2001). *Preventive negotiation : avoiding conflict escalation*. Lanham, Md.: Rowman & Littlefield.

I. William Zartman (1988). Common elements in the analysis of the negotiation process. *Negotiation Journal*, [online] 4(1), pp.31–43. Available at: https://link.springer.com/article/10.1007/BF01000902.

Implementing Guidelines of the Cyber Diplomacy Toolbox. (2023). [online] pp.14–15. Available at: https://data.consilium.europa.eu/doc/document/ST-10289-2023-INIT/en/pdf.

Ioana-Cristina Vasiloiu (2023). Cyber Diplomacy: A New Frontier for Global Cooperation in the Digital Age. *Informatica Economica*, 27(1), pp.41–50.

ITU (2021). *Guide to Developing a National Cybersecurity Strategy 2nd Edition | Strategic Engagement in Cybersecurity Guide to Developing a National Cybersecurity Strategy*.

Jacobsen, J.T. (2024). Commitment and compromise in Danish cyber and tech diplomacy. *International Affairs*, 100(6), pp.2361–2378.

Johansmeyer, T., Mott, G. and Nurse, J. R. C. (2024) 'Cyber Strategy in Practice: The Evolution of US, Russian and Ukrainian National Cyber Security Strategies through the Experience of War', *The RUSI Journal*, 169(3), pp. 40–51.

John Von Neumann and Oskar Morgenstein (1944). *Theory of games and economic behaviour*. Princeton N.J.: Princeton University Press.

Johnstone, I., Sukumar, A. and Trachtman, J. (2023a). *Building cybersecurity through multistakeholder diplomacy: Politics, processes, and prospects*.

Johnstone, I., Sukumar, A. and Trachtman, J. (2023b). *Building cybersecurity through multistakeholder diplomacy: Politics, processes, and prospects*.

Jones, P.L. and Shultz, G.P. (2015). *Track two diplomacy in theory and practice*. Stanford, California: Stanford University Press.

Kasper, A., Osula, A.-M. and Molnár, A. (2021). EU cybersecurity and cyber diplomacy. In: *Revista de Internet, Derecho Y Politica*. Universitat Oberta de Catalunya.

Kavanagh, C., Carr, M. and Berglund, N. (2021). *Quiet Conversations: Observations from a decade of practice in cyber-related track 1.5 and track 2 diplomacy*. [online] *EU Cyber Direct*. Available at:

https://eucyberdirect.eu/research/quiet-conversations-observations-from-a-decade-of-practice-in-cyber-related-track-1-5-and-track-2-diplomacy.

Keohane, R.O. and Nye, J.S. (2012). *Power and interdependence, 4th ed.* Glenview, IL: Pearson Education, Inc.

Kerry, C. (2017). *The Cyber Diplomacy Act of 2017: Giving Cyber the Importance It Needs at the State Department*. [online] Lawfare. Available at: https://www.lawfaremedia.org/article/cyber-diplomacy-act-2017-giving-cyber-importance-it-needs-state-department [Accessed 27 Jul. 2025].

Kissinger, H.A. (1969). *The Viet Nam Negotiations*. [online] www.foreignaffairs.com. Available at: https://www.foreignaffairs.com/articles/asia/1969-01-01/viet-nam-negotiations.

Kostyuk, N. (2015). Ukraine: A Cyber Safe Haven? In: *Cyber War in Perspective: Russian Aggression against Ukraine*. Tallin: NATO Cooperative Cyber Defence Centre of Excellence.

Kurbalija, J. (2016). *An Introduction to INTERNET GOVERNANCE 7th edition*. [online] Available at: https://www.diplomacy.edu/wp-content/uploads/2021/12/AnIntroductiontoIG_7th-edition.pdf.

Laurens Cerulus (2019). *How Ukraine became a test bed for cyberweaponry*. [online] POLITICO. Available at: https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/.

Laurens Cerulus (2022). *Ukraine is getting pummeled with cyberattacks. What’s the West to do?* [online] POLITICO. Available at: https://www.politico.eu/article/ukraine-russia-cyberattack-west-diplomacy-sanction/.

Le Blanc, M. and Salvi, A. (2024). European Cyber Policy and Cyber Diplomacy. In: A. Salvi, H. Tiirmaa-Klaar and J.A. Lewis, eds., *A Handbook for the Practice of Cyber Diplomacy*. Luxembourg: Publications Office of the European Union, pp.58–70.

Lee, G. and Ayhan, K. (2015). Why Do We Need Non-state Actors in Public Diplomacy?: Theoretical Discussion of Relational, Networked and Collaborative Public Diplomacy. *Journal of International and Area Studies*, 22(1), pp.57–77.

Liliya Khasanova (2023). *Multilateral Cyber Negotiations and Gender Mainstreaming: A Complicated Relationship - Women In International Security*. [online] Women In International Security. Available at: https://wiisglobal.org/multilateral-cyber-negotiations-and-gender-mainstreaming-a-complicated-relationship/.

Madiega, T. (2022). *Russia's war on Ukraine: The digital dimension*. [online] European Parliamentary Research Service. Available at: https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/729317/EPRS_ATA(2022)729317_EN.pdf.

Martino, L. (2021). *Le iniziative diplomatiche per il cyberspazio: punti di forza e di debolezza. IAI Istituto Affari Internazionali*. Rome: IAI.

Maurer, T. (2011). *Cyber norm emergence at the United Nations - An Analysis of the Activities at the UN Regarding Cyber-security*. Cambridge: Belfer Center for Science and International Affairs - Harvard Kennedy School.

Meerts, P. (2015). *Diplomatic Negotiation Essence and Evolution*. The Hague: Clingendael Institute.

Merlone, U. and Spilli, G. (2023). Decidere in condizioni di incertezza: dall'approccio normativo alla Negotiation Analysis. *Sistemi intelligenti, Rivista quadrimestrale di scienze cognitive e di intelligenza artificiale*, (1), pp.9–30.

Metzl, J.F. (2001). Network Diplomacy. *Georgetown Journal of International Affairs*, 2(1), pp.77–87.

Meyer, P. (2012). Diplomatic Alternatives to Cyber-Warfare. *The RUSI Journal*, 157(1), pp.14–19.

Microsoft Netherlands (2018). *The Need for Digital Peace at the Peace Palace, The Hague*. [online] YouTube. Available at: https://www.youtube.com/watch?v=rMXJMMcHjYs [Accessed 23 Jun. 2025].

Mihai Sebastian Chihaia and Rempala, J. (2023). Cyber Diplomacy. *Springer eBooks*, pp.260–264.

Miller, K., Shires, J. and Tropina, T. (2021). Gender Approaches to Cybersecurity. *unidir.org*. [online] Available at: https://unidir.org/publication/gender-approaches-to-cybersecurity/.

MR. S. SHESTAKOV (2010). *STATEMENT BY MR. S. SHESTAKOV, REPRESENTATIVE OF THE RUSSIAN FEDERATION, AT THE JOINT MEETING OF THE OSCE FORUM FOR SECURITY CO-OPERATION AND THE OSCE PERMANENT COUNCIL*. [online] Available at: https://www.osce.org/files/f/documents/f/9/68693.pdf.

Myerson, R.B. (1997). *Game theory : analysis of conflict*. Cambridge, Massachusetts: Harvard University Press.

Nash, J.F. (1950). The Bargaining Problem. *Econometrica*, 18(2), pp.155–162. doi:https://doi.org/10.2307/1907266.

Nash, J.F. (1996). *Essays on Game Theory*. Edward Elgar Publishing.

NATO (2024). *Cyber defence*. [online] NATO. Available at: https://www.nato.int/cps/en/natohq/topics_78170.htm.

NATO (2025). *Relations with Ukraine*. [online] NATO. Available at: https://www.nato.int/cps/en/natohq/topics_37750.htm.

Neumann, I.B. (2017). *At Home with the Diplomats Inside a European Foreign Ministry*. Cornell University Press.

Ning, H. and Meihui, X. (2024). *The Transformation of China's S&T Diplomacy*. Korea Institute of S&T Evaluation and Planning.

Office of the Danish Tech Ambassador (2021). *Tech Diplomatic Results (2021-2023)*. [online] Ministry of Foreign Affairs of Denmark. Available at: https://techamb.um.dk/impact/tech-diplomatic-results.

Office of the Danish Tech Ambassador (n.d.). *The TechPlomacy Approach*. [online] Ministry of Foreign Affairs of Denmark . Available at: https://techamb.um.dk/the-techplomacy-approach.

Office, A. (2025). *Cyber Diplomacy: The Bureau of Cyberspace and Digital Policy's Efforts to Advance U.S. Interests*. [online] Gao.gov. Available at: https://www.gao.gov/products/gao-25-108445 [Accessed 27 Jul. 2025].

Office, U.S.G.A. (2024). *Cyber Diplomacy: State's Efforts Aim to Support U.S. Interests and Elevate Priorities | U.S. GAO*. [online] www.gao.gov. Available at: https://www.gao.gov/products/gao-24-105563.

OSCE (2024). *Promoting greater engagement in international cyber diplomacy negotiations*. [online] Osce.org. Available at: https://www.osce.org/cyber-ict-security/579961.

OSCE (2025). *Permanent Council Decision No. 1039*. [online] Osce.org. Available at: https://www.osce.org/pc/90169 [Accessed 30 Jul. 2025].

Oskar Morgenstern and John Von Neumann (1944). *Theory of Games and Economic Behavior (Princeton Classic Editions)*. Princeton University Press.

Paganini, P. (2022). *Non State Actors in Cyberspace: an Attempt to a Taxonomic classification, role, Impact and Relations with a State's socio- Economic Structure*. Università degli Studi di Firenze: Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali (CCSSII).

Painter, C. (2018). *Diplomacy in Cyberspace*. [online] afsa.org. Available at: https://afsa.org/diplomacy-cyberspace.

Pawlak, P. (2016). Confidence-Building Measures in Cyberspace: Current Debates and Trends Confidence-Building Measures in Cyberspace: Current

Debates and Trends. In: H. Rõigas and A.-M. Osula , eds., *International Cyber Norms Legal, Policy & Industry Perspectives*. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, pp.129–153.

Pfetsch, F.R. (2011). Power in International Negotiations: Symmetry and Asymmetry. *Négociations*, 16(2), p.39.

Poast, P. (2013). Issue linkage and international cooperation: An empirical investigation. *Conflict Management and Peace Science*, 30(3), pp.286–303.

Popescu, N., Secrieru, S., Alatalu, S., Borogan, I., Chernenko, E., Herpig, S., Jonsson, O., Kurowska, X., Limnell, J., Pawlak, P., Pernik, P., Reinhold, T., Reshetnikov, A., Soldatov, A. and Vilmer, J.-B. (2018). *Hacks, leaks and disruptions Russian cyber strategies EDITED BY Chaillot Papers*. [online] Available at: https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf.

Poundstone , W. (1992). *Prisoner's Dilemma: John Von Neumann, Game Theory and the Puzzle of the Bomb*.

Prince, M. (2022). *Steps we've taken around Cloudflare's services in Ukraine, Belarus, and Russia*. [online] The Cloudflare Blog. Available at: https://blog.cloudflare.com/steps-taken-around-cloudflares-services-in-ukraine-belarus-and-russia/.

Przetacznik, J. and Tarpova, S. (2022). *Russia's war on Ukraine: Timeline of cyber-attacks*. [online] *European Parliament*. European Parliamentary Research Service. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf.

Putnam, R.D. (1988). Diplomacy and Domestic Politics: the Logic of Two-Level Games. *International Organization*, 42(3), pp.427–460.

Qian, X. (2019). Cyberspace Security and U.S.-China Relations. *Proceedings of the 2019 International Conference on Artificial Intelligence and Computer Science*.

Radanliev, P. (2024). Cyber diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing. *Journal of Cyber Security Technology*, [online] pp.1–51. doi:https://doi.org/10.1080/23742917.2024.2312671.

Rana, K.S. (2011). *21st Century Diplomacy: A Practitioner's Guide*. Bloomsbury Publishing USA.

Reed, J. (2024). *State department international cyberspace digital policy strategy*. IBM.

Riordan, S. (2019). *Cyberdiplomacy: Managing Security and Governance Onlines*. Cambridge: Polity Press, 2019.

Rousseau, J.J. (1762). *The Social Contract*. Cambridge University Press.

royalsociety.org. (2010). *The Royal Society*. [online] Available at: https://royalsociety.org/-/media/policy/publications/2010/4294969468.pdf.

Ruhl, C., Hollis, D., Hoffman, W. and Maurer, T. (2020a). *Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Pro cesses at a Crossroads*.

Ruhl, C., Maurer, T., Hoffman, W. and Hollis, D.B. (2020b). Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads. Washigton DC: Carnegie Endowment for International Peace.

Saaida, M. (2024). The Influence of Non-State Actors on International Relations. *Department of International Relations and Diplomacy, Faculty of Administration Sciences and Informatics, Al-Istiqlal University, Jericho – Palestine.*, 1(1), pp.1–3.

Salvi, A., Tiirmaa-Klaar, H. and Lewis, J. (2025). *A Handbook for the Practice of Cyber Diplomacy*. Luxembourg: EU Institute for Security Studies.

Satariano, A. (2019). The World’s First Ambassador to the Tech Industry (Published 2019). *The New York Times*. [online] 3 Sep. Available at: https://www.nytimes.com/2019/09/03/technology/denmark-tech-ambassador.html.

Sayles, B. (2021). *Throwback Attack: How NotPetya Ransomware Took Down Maersk - Control Engineering*. [online] Control Engineering. Available at: https://www.controleng.com/throwback-attack-how-notpetya-accidentally-took-down-global-shipping-giant-maersk/.

Schaffer, A. (2022). It’s a big day at the State Department for U.S. cyberdiplomacy. *Washington Post*. [online] Available at: https://www.washingtonpost.com/politics/2022/04/04/its-big-day-state-department-us-cyberdiplomacy/.

Schandorf, S.O. (2024). Power Relations and Maritime Justice: An Exploration of UNCLOS Negotiations. *Ocean and Society*, 1(Article 8791).

Schelling, T.C. (1960). *The strategy of conflict*. New York Oxford University Press.

Scholte, J. (2020). *Multistakeholderism: Filling the Global Governance Gap?* School of Global Studies University of Gothenburg.

Schramm, H.C., Alderson, D.L., Carlyle, W.M. and Dimitrov, N.B. (2014). A Game Theoretic Model of Strategic Conflict in Cyberspace. *Military Operations Research*, 19(1), pp.5–17.

Segal, A. (2018). *When China Rules the Web*. [online] Foreign Affairs. Available at: https://www.foreignaffairs.com/china/when-china-rules-web.

Segal, A. (2020). *China’s Alternative Cyber Governance Regime Hearing on A ‘China Model?’ Beijing’s Promotion of Alternative Global Norms and Standards*. [online] Available at: https://www.uscc.gov/sites/default/files/testimonies/March%2013%20Hearing_Panel%203_Adam%20Segal%20CFR.pdf.

Shaping Europe’s digital future. (2025a). *Commission launches new cybersecurity blueprint to enhance EU cyber crisis coordination*. [online] Available at: https://digital-strategy.ec.europa.eu/en/news/commission-launches-new-cybersecurity-blueprint-enhance-eu-cyber-crisis-coordination.

Shaping Europe’s digital future. (2025b). *Cyber Blueprint - Draft Council Recommendation*. [online] Available at: https://digital-strategy.ec.europa.eu/en/library/cyber-blueprint-draft-council-recommendation.

Shared Vision, Common Action: A Stronger Europe A Global Strategy for the European Union’s Foreign And Security Policy. (2016). Available at: https://eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf.

Smith, B. (2022). *Defending Ukraine: Early Lessons from the Cyber War*. [online] Microsoft. Available at: https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/.

Sticher, V. (2021). Healing Stalemates: The Role of Ceasefires in Ripening Conflict. *Ethnopolitics*, 21(2), pp.149–162. doi:https://doi.org/10.1080/17449057.2022.2004776.

Stradner, I. (2023). *China and Russia are using the UN to censor the world*. [online] The Telegraph. Available at: https://www.telegraph.co.uk/news/2023/09/01/china-xi-jinping-vladimir-putin-united-nations/.

Sukumar, A. (2023). *Building an International Cybersecurity Regime: Multistakeholder Diplomacy*. Edward Elgar Publishing.

Sukumar, A., Broeders, D. and Kello, M. (2024). The pervasive informality of the international cybersecurity regime: Geopolitics, non-state actors and diplomacy. *Contemporary Security Policy*, 45(1), pp.7–44.

Sustainability Directory (2025). *Cyber Diplomacy Strategies*. [online] Available at: https://pollution.sustainability-directory.com/term/cyber-diplomacy-strategies/.

Tangalakis-Lippert, K. (2022). *Amazon 'saved the Ukrainian government' with suitcase-sized hard drives*. [online] Business Insider. Available at: https://www.businessinsider.com/amazon-saved-the-ukrainian-government-with-suitcase-sized-hard-drives-2022-12.

The Hague Centre for Strategic Studies (2021). *Global Commission on the Stability of Cyberspace*. [online] HCSS. Available at: https://hcss.nl/global-commission-on-the-stability-of-cyberspace-homepage/.

The NATO Cooperative Cyber Defence Centre of Excellence (2013). *Cyber War in Perspective: Russian Aggression against Ukraine*.

Tiirmaa-Klaar, H. (2021). *The Evolution of the UN Group of Governmental Experts on Cyber Issues From a Marginal Group to a Major International Security Norm-Setting Body Heli Tiirmaa-Klaar Ambassador for Cyber Diplomacy, Estonian Ministry of Foreign Affairs Cyberstability Paper Series New Conditions and Constellations in Cyber*. [online] Available at: https://hcss.nl/wp-content/uploads/2021/12/Klaar.pdf.

U.S Congress (2021). *117th Congress (2021-2022): Cyber Diplomacy Act of 2021*. [online] Congress.gov. Available at: https://www.congress.gov/bill/117th-congress/house-bill/1251/text.

U.S. Department of State (2024). *United States International Cyberspace & Digital Policy Strategy - United States Department of State*. [online] United States Department of State. Available at: https://2021-2025.state.gov/united-states-international-cyberspace-and-digital-policy-strategy/.

U.S. Department of State. (2017). *Office of the Coordinator for Cyber Issues*. [online] Available at: https://2009-2017.state.gov/s/cyberissues/index.htm [Accessed 2 May 2025].

U.S. Department of State. (2022). *DENMARK – Summit for Democracy*. [online] Available at: https://www.state.gov/wp-content/uploads/2022/02/DENMARK-Summit-for-Democracy-Written-Statement-Accessible.pdf.

U.S. Government Accountability Office. (2025). *GAO-25-108445, CYBER DIPLOMACY: The Bureau of Cyberspace and Digital Policy's Efforts to Advance U.S. Interests*. [online] Available at: https://files.gao.gov/reports/GAO-25-108445/index.html#_ftn3.

UN General Assembly (2025). *Resolution Adopted By The General Assembly: Developments in the field of information and telecommunications in the context of international security*. [online] Un.org. Available at: https://docs.un.org/en/A/RES/53/70.

UN Secretary-General and UN Group (2013). *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. [online] United Nations Digital Library System. Available at: https://digitallibrary.un.org/record/753055?v=pdf.

UN Secretary-General and UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2015). Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. *digitallibrary.un.org*. [online] Available at: https://digitallibrary.un.org/record/799853?v=pdf.

UN Women Headquarters Office (2022). *Feminist Foreign Policies: An Introduction*. [online] New York: United Nations Entity for Gender Equality and the Empowerment of Women . Available at: https://www.unwomen.org/sites/default/files/2022-09/Brief-Feminist-foreign-policies-en.pdf.

Understanding the EU's approach to cyber diplomacy and cyber defence. (2020). [online] European Parliament. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651937/EPRS_BRI(2020)651937_EN.pdf.

United Nations General Assembly (2024). *Resolution 79/243*. [online] Un.org. Available at: https://docs.un.org/en/A/RES/79/243.

United Nations. Office for Disarmament Affairs. (n.d.). *Military Confidence-Building Measures – UNODA.*

United States Department of State. (n.d.). *Key Topics Bureau of Cyberspace and Digital Policy*.

Urlacher, B.R. (2015). *International Relations as Negotiation*. Routledge.

US Congress (2025). *U.S. Cyber Diplomacy in an Era of Growing Threats*. [online] Congress of the United States . Available at: https://www.congress.gov/event/115th-congress/house-event/106830/text [Accessed 27 Jul. 2025].

Wooldridge, M. and Phelps, S. (2013). *Game Theory and Evolution*. AI and Game Theory | IEEE Computer Society.

World Bank (n.d.). *Negotiation | Defining Bargaining and Negotiation*. [online] The World Bank. Available at: https://assets.publishing.service.gov.uk/media/57a08b4540f0b652dd000bca/Negotiationweb.pdf.

www.cyber-diplomacy-toolbox.com. (n.d.). *The EU Cyber Diplomacy Toolbox*. [online] Available at: https://www.cyber-diplomacy-toolbox.com/.

Zartman, I.W. (2013). Negotiation: post-modern or eternal? In: A. Colson , D. Druckman and W. Donohue, eds., *International Negotiation: Foundations, Models, and Philosophies*. Dordrecht: Republic of Letters Publishing BV, pp.209–225.

Zartman, I.William. (2000). Ripeness: The Hurting Stalemate and Beyond. In: D. Druckman and P.C. Stern, eds., *International Conflict Resolution After the Cold War*. Washington, Dc: National Academy Press.

Zwarts, H., Du Toit, J. and Von Solms, B. (2022). A Cyber-Diplomacy and Cybersecurity Awareness Framework (CDAF) for Developing Countries. *European Conference on Cyber Warfare and Security*, 21(1), pp.341–349.

Acknowledgments

It is with sincere appreciation that I acknowledge the guidance and support I have received during the course of my research and the writing of this thesis.

I wish to express my profound gratitude to Ambassador Pasquale Ferrara, my supervisor, for his invaluable guidance and constant support throughout this work.

I am also indebted to Professor Antonio Giordano for his insightful contributions and for the encouragement he has provided to my academic development.

In particular, I am deeply grateful to Professor Enzo Maria Le Fevre, whose continuous support and inestimable comments have accompanied me throughout this entire journey, significantly enriching the quality of my research.

To all those who have contributed, directly or indirectly, to the realization of this work, I extend my deepest gratitude.