UNIVERSITY OF PIRAEUS

SCHOOL OF ECONOMICS, BUSINESS AND INTERNATIONAL STUDIES

DEPARTMENT OF INTERNATIONAL AND EUROPEAN STUDIES

MSC IN INTERNATIONAL AND EUROPEAN STUDIES

"Cyber diplomacy in times of crisis: The war between Russia and Ukraine"

Leinti Dafni Mitrai

Supervisor: Konstantina E. Botsiou

Scientific Committee:

Petros Liacouras, Professor

Andreas Liaropoulos, Associate Professor

Piraeus, 2026

The intellectual work fulfilled and submitted based on the delivered master thesis is exclusive property of mine personally. Appropriate credit has been given in this diploma thesis regarding any information and material included in it that have been delivered from other sources. I am also fully aware that any misrepresentation in connection with this declaration may at any time result in immediate revocation of the degree title.

Piraeus, February 2026

Leinti Dafni Mitrai

Acknowledgements

I would first like to express my sincere gratitude to Professor Konstantina Botsiou for her valuable guidance and support throughout the development of this thesis. Her academic insight and direction were instrumental in shaping the course of this research. I would also like to thank Professor Andreas Liaropoulos for his constructive feedback and thoughtful comments, which contributed significantly to the improvement and refinement of this work.

My sincere appreciation is further extended to Professor Petros Liacouras, who stood by me throughout the entire duration of my studies. His continuous support and encouragement played an important role in my academic journey.

Special thanks are also due to my family. Words are not sufficient to express my gratitude to my beloved parents, Elmira & Markos, who supported me throughout my studies with constant encouragement, understanding, and unconditional love. I am equally grateful to my sister, Annie, for all her help and for standing by my side during my academic pursuits.

Table of Contents

Contents

Abstract

The emergence of cyber diplomacy has redefined the dynamics of international relations, especially in times of crisis. In the context of the ongoing war between Russia and Ukraine, the digital sphere has become a critical battleground where diplomacy intersects with technology. This paper uses the literature review method to explore the case of the Russo-Ukrainian war and the cyber diplomacy operations that took place. The purpose of the paper is to draw conclusions in relation to cyber diplomacy practices in the context of contemporary international crises. The Russo-Ukrainian war highlighted the dual nature of cyber diplomacy in modern conflicts. Cyberspace tools have facilitated international solidarity, rapid information sharing and resilience building through partnerships such as NATO and EU initiatives to support Ukraine's cybersecurity and counter disinformation. However, challenges such as misinformation and fragmented communication emerged as significant risks. Russia's cyber operations, while disruptive, failed to yield decisive military or political results, revealing the complementary role of digital strategies in warfare. Public-private partnerships, particularly with technology giants, have proved vital. This case study focusing on cyber diplomacy underscores the need for balanced strategies, strong policies and enhanced global cooperation in cyber diplomacy.

Key-Words: *Cyber Diplomacy, Russo-Ukrainian War, International Conflict, Crisis, Cybersecurity*

Introduction

Cyber diplomacy represents a transformative approach to international relations, using digital tools and strategies to address challenges and promote cooperation in cyberspace. As nations become increasingly interconnected, cyberspace has become a critical arena for negotiation, conflict resolution and global governance. Cyberspace diplomacy, therefore, involves efforts to create norms, enhance cyber cooperation and mitigate threats such as cyberattacks, espionage and the spread of disinformation. It serves as a platform for dialogue between states, international organizations and private actors, addressing the complexities of sovereignty, security and ethical behavior in the digital age. By integrating technological expertise with traditional diplomatic practices, cyber diplomacy is not only a tool for conflict prevention, but also a means to promote trust and stability in an ever-evolving digital landscape (Attatfa et al., 2020). The need for successful cyber diplomacy operations and the importance of effective cyber diplomacy is particularly highlighted in the context of contemporary conflict. The Russia-Ukraine conflict exemplifies the growing importance of cyber tools for shaping narratives, promoting alliances and countering disinformation (Marigliano et al., 2024). This paper explores the role of cyber diplomacy in crisis management by examining the case study of the Russo-Ukrainian war. More specifically, the impact of cyber diplomacy on global cooperation, cybersecurity frameworks and the evolving strategies of the international actors involved in this conflict are examined.

Building on the above discussion, this study examines the role and functioning of cyber diplomacy in the context of contemporary international crises through the case of the Russia–Ukraine war. To guide this analysis, the paper addresses three central research questions:

1. What forms of cyber diplomacy were employed by international organizations and private-sector actors during the Russia-Ukraine conflict?
2. How do the strategies and tools of cyber diplomacy differ among NATO, the European Union, the United Nations, and major technology companies?
3. In what ways does cyber diplomacy influence international coordination, cybersecurity resilience, and the mitigation of disinformation during periods of crisis?

These questions structure the investigation and help illuminate the broader implications of cyber diplomacy for global security governance.

As for the structure of this paper, the first section concerns the basic theoretical framework around the concept of cyber diplomacy. The importance of cyber diplomacy in times of crisis is discussed, with reference to cyber warfare and the needs of cybersecurity and cyber deterrence. The theoretical part also includes references to the importance of international law, while the analysis of the challenges and ethical concerns that arise in the context of cyber diplomacy is also included.

Furthermore, the focus is on the impact of cyber diplomacy on international crises. After completing the theoretical part of the paper, the case study is followed, where the focus is on the Russo-Ukrainian war. First, the international and domestic responses to the Russo-Ukrainian war are presented and there is a reference to the role of three international and transnational organizations: the UN, NATO, and the EU. Finally, the literature references to cyber diplomacy operations during this conflict are studied and lessons are drawn for cyber diplomacy practices in the context of contemporary international crises.

1. Theoretical framework and basic concepts

1.1 Definitions and scope of cyber diplomacy

Cyber diplomacy can be simply defined as the use of diplomatic tools and the utilization of a diplomatic mindset through cyberspace to address issues arising from the international use of cyberspace. Essentially, what distinguishes this term from traditional diplomacy is the fact that the cyberspace dimension is the primary focus of diplomatic efforts. In this context, cyber diplomacy incorporates strategies that leverage digital tools to advance diplomatic agendas while addressing the complexities posed by cyber threats and the interconnected nature of today's global landscape (Riordan, 2016).

The study by Attatfa et al. (2020) develops the concept of cyber diplomacy by positioning it as an essential tool in international relations, particularly given the growing importance of cybersecurity and the protection of national interests in cyberspace. This research stresses that cyber diplomacy is not just a technical issue, but instead encompasses a wider range of political, social and strategic challenges. Thus, cyber diplomacy is identified as an adaptive and flexible field that incorporates elements of traditional diplomacy while addressing the unique demands of cyberspace in the modern era. It is also worth noting the interdisciplinary nature and multifaceted characteristics of cyber diplomacy, as it is a field that draws from a variety of fields, including sociology, international law and global politics. This multifaceted approach is necessary due to the evolving landscape of cyber threats, which require nations to collaborate and develop integrated strategies to safeguard their interests in an increasingly digital world.

According to Barrinha & Renard (2017), cyber diplomacy represents an important development in international relations, which arises from the increasing politicization of cyberspace. Initially, cyber issues were considered technical issues, which were mainly managed by engineers and IT specialists. However, as global connectivity expanded, the recognition of cyberspace as a contested political domain led to the involvement of diplomats. This transition marked a shift from treating cyber issues as domestic political problems to recognizing them as critical components of foreign policy. Therefore, Barrinha & Renard (2017) argue that the rise of cyber diplomacy began around the beginning of the 21st century, when major powers began to formulate national cybersecurity strategies, thus framing cyberspace as a strategic asset. In particular, the 2011 United States International Cyberspace Strategy was pivotal, as it explicitly emphasized the role of diplomatic tools in addressing international cyber issues. In addition, the creation of dedicated diplomatic units in State Departments, such as the Office of the U.S. Coordinator for Cyberspace Issues, exemplifies institutional adaptation to this new field. The evolution of cyber diplomacy reflects a broader trend in which states are seeking to establish norms and frameworks for cooperation in cyberspace, bridging national interests

with the dynamics of a global society. This adaptation underscores the necessity of diplomacy to navigate the complexities and challenges posed by cyber interactions on the international stage (Office of the Coordinator for Cyber Issues, 2017).

However, the historical event that is regarded as the birth of cyber diplomacy is the widespread cyber-attack in Estonia in 2007 (Attatfa et al., 2020). This incident serves as an important milestone in the evolution of international relations, particularly in the field of cybersecurity and diplomatic engagement. In April 2007, Estonia faced a series of coordinated cyber-attacks targeting government websites, banks and media outlets. These attacks were prompted by political tensions surrounding the transfer of a Soviet-era war memorial in Tallinn, which caused widespread protests among Estonia's Russian-speaking population. The attacks were unprecedented in scale and intensity, crippling one of the world's most digitally connected nations. They highlighted not only the vulnerabilities of national infrastructures in an increasingly digital landscape, but also the potential of cyber warfare as a tool of geopolitical conflict (Ottis, 2008). This event has raised the awareness of governments worldwide of the need to formulate comprehensive policies to address cybersecurity threats. In response to the attacks, Estonia became a pioneer in cyber defense and cyber diplomacy, supporting international cooperation in cyber security. The event was a catalyst for discussions on the role of state actors in cyber activities and the need for diplomatic frameworks to manage and mitigate cyber threats. Countries recognized that cyberspace could no longer be ignored in foreign policy considerations, leading to the adoption of national cybersecurity strategies that incorporate diplomatic tools (Herzog, 2017).

The Estonian cyber-attacks highlighted the importance of resilience against cyber threats and initiated a change in the way states approached security in the digital domain. This marked the launch of cyber diplomacy as a distinct field, aimed at navigating the complexities of international relations in an era where cyber capabilities can significantly affect power dynamics and national security strategies (Aquino, 2022).

1.2 Basic principles and the mission of cyber diplomacy

The mission of cyber diplomacy is multifaceted and includes efforts to create frameworks for governance, security and cooperation in an increasingly interconnected digital world. At its core, cyber diplomacy seeks to address the complex challenges posed by cyberspace while harnessing its potential for positive international cooperation (Charles, 2024). First and foremost, cyber diplomacy aims to prioritize key areas of focus, such as human rights, international security, cyber governance, cyber-crime prevention, and capacity building. By focusing on these critical issues, diplomats can navigate the vast and fragmented landscape of cyber initiatives and ensure meaningful progress. This requires a forward-looking approach that avoids getting sidetracked by the overwhelming number of cyber activities and events that do

not have meaningful results. Another critical principle of cyber diplomacy is to promote internal coordination and expertise within foreign ministries and government agencies. Diplomats need to develop strong internal frameworks for integrating cyber issues into their broader policy agendas. Establishing specialized units and ensuring the continuing education of diplomats are key steps to maintaining a coherent and unified voice on strategic international cyber issues. Collaboration with national policymakers, the private sector, and academia further enhances the effectiveness of these efforts (Tanczer et al., 2018).

Additionally, as explained in Tiirmaa-Klaar (2013), cyber diplomacy also seeks to address the increasing militarization of cyberspace by promoting idealism and peaceful norms. Over-reliance on security-driven agendas risks creating a vicious cycle of escalating cyber capabilities between nations. Diplomats play a key role in establishing agreements on cyber rules and supporting a less securitized, more collaborative approach to cyber governance. In addition, cyber diplomacy encourages the academic community to contribute to conceptual and analytical understanding of cyber issues. Expanding interdisciplinary studies, particularly in the context of political science and international relations, can provide valuable insights into power dynamics, the privatization of security, and the impact of cyber policies on the multilateral global order. These academic efforts can inform policymakers and shape more comprehensive and effective cyber strategies. Finally, cyber diplomacy aims to create inclusive platforms for dialogue, such as the Global Cyber Conferences (Barman, 2024). These forums bring together diverse stakeholders, including diplomats, industry experts, and policymakers, to align efforts and ensure that cyber issues remain on high-level policy agendas. By facilitating collaboration, cyber diplomacy seeks to harmonize fragmented initiatives and promote a shared vision for a secure and prosperous digital future (Tiirmaa-Klaar, 2013).

Hermawanto & Anggraini (2024) state that measures of transparency, enhancing confidence (which in the context of diplomacy demonstrates goodwill and willingness to cooperate) and building trust play a critical role in the effectiveness and success of the cyber diplomacy mission. Their research highlights the need for strong cybersecurity measures and frameworks that enhance trust and cooperation among nations while emphasizing all of the above parameters. More specifically, transparency is a fundamental element in building trust between states. It is suggested that open communication about cybersecurity policies, intentions and capabilities can significantly mitigate misunderstandings and reduce the likelihood of conflicts arising from misconceptions. By sharing information on cyber threats, response strategies and best practices, countries can create a more secure environment conducive to cooperation. This openness allows states to understand each other's cyber attitudes, enhancing a sense of security and predictability in their interactions. In addition, confidence-building measures can serve as a platform for dialogue on cybersecurity issues. By creating mechanisms for regular communication and information sharing, countries can work together to address common cyber-related challenges. Such collaborative efforts can include joint exercises, joint threat assessments and coordinated responses to cyber incidents. This collaborative approach

not only enhances regional security but also builds mutual trust, which is essential for effective cyber diplomacy (Hermawanto & Anggraini, 2024; Kim, 2014).

However, it is worth noting that the unique characteristics of each country must be taken into account to ensure that these confidence building, trust and transparency measures are relevant and effective. This flexibility allows states to tailor their cybersecurity initiatives according to their specific needs and contexts, thus promoting inclusiveness in the dialogue process (Charles, 2024). Sukumar et al. (2024) explain that this adaptation is crucial because countries have different levels of technological development, distinct political environments, and unique security concerns that affect their approach to cybersecurity. For example, a nation may prioritize certain cyber threats over others based on its strategic interests, necessitating a tailored approach to confidence-building measures that addresses these specific vulnerabilities. Further, when countries feel that their specific situations and concerns are acknowledged, they are more likely to actively engage in negotiations and cooperation efforts. Such participation is vital to creating a comprehensive cybersecurity framework that reflects a multiplicity of perspectives and promotes trust between states. The success of informal institutions and multi-stakeholder initiatives depends on their ability to incorporate the diverse views of participating states, especially in a multipolar world where power dynamics are in constant flux.

However, Broeders et al. (2023) made the apt observation that a delicate balance is required between national security interests and the need for global cooperation in cyber diplomacy. In their research they indirectly highlight that while states are increasingly focusing on securing their national interests through policies to combat cyber terrorism, this is often at the expense of international cooperation and the protection of fundamental human rights. As they analyze, national security frameworks, particularly following major terrorist events, have led to the adoption of broad definitions of cyber terrorism. These definitions have been expanded to include various online activities that pose a threat, effectively blurring the line between legitimate security measures and excessive surveillance. Such measures may violate individual rights, in particular freedom of speech, as states adopt proactive strategies that prioritize security over individual freedoms. Moreover, it is worth noting that authoritarian regimes have exploited the language of counter-terrorism to justify domestic repression, leveraging global narratives to legitimize their actions. This dynamic poses a challenge to liberal democracies defending digital rights, as their engagement in international forums can inadvertently support authoritarian interpretations of security. Thus, the interplay between national legislation and international diplomatic debates, particularly in the context of the United Nations, such as the UN Group of Governmental Experts (UN GGE) and the Open-Ended Working Group (OEWG), reveals the need for precision in language to maintain a human rights-oriented approach that listens to the mission and purpose of international cyber diplomacy.

1.3 Mechanisms and frameworks for cyber diplomacy

Bilateral and multilateral cyber agreements, particularly those facilitated by frameworks such as the UN Group of Governmental Experts (GGE) on Cybersecurity, play a critical role in shaping international cyber diplomacy. These agreements are essential for promoting cooperation among states to enhance cybersecurity, mitigate risks and establish norms of cyber conduct. Bilateral agreements involve cooperation between two states on cybersecurity issues, which may include sharing information on threats, developing joint incident response protocols, or establishing points of contact for communication during crises (Hitchens & Gallagher, 2019). Such agreements can enhance trust and cooperation between nations, particularly when dealing with transnational cyber threats, where vulnerabilities in one state can have a cascading effect on other states (Barrinha & Renard, 2017). For example, the 2016 China-Russia Joint Statement highlights bilateral cooperation to combat the misuse of information technologies, emphasizing mutual respect and collective security. Similarly, the US is engaged in bilateral agreements with China to address cybercrime, demonstrating a pragmatic approach to bilateral cooperation to address shared threats. At the same time, the European Union is incorporating bilateral cyber dialogues into its strategic partnerships with nations such as the US, Canada and South Korea. These agreements aim to strengthen cybersecurity, prevent conflicts and align with broader international strategies, such as the 2017 EU Cybersecurity Reforms. By leveraging bilateral frameworks, countries can bypass the inefficiencies of multilateral formats, ensuring tailored responses to cyber threats while promoting stability and trust in the digital realm (Bendiek, 2018).

Multilateral agreements, on the other hand, involve the cooperation of many nations. The GGE is a prime example, bringing together representatives from different countries to discuss and develop rules and confidence-building measures in the field of cybersecurity. Through these discussions, the GGE has produced reports outlining principles for the conduct of states in cyberspace, emphasizing the importance of sovereignty, the applicability of international law, and the necessity of protecting critical infrastructure. These frameworks for cyber diplomacy not only facilitate dialogue, but also help create a common language and understanding around cyber threats and responses. They encourage nations to commit to voluntary rules, enhancing predictability and stability in international relations. Despite the ambiguity of many recommendations, the political commitments made in these forums are important; they create a foundation for accountability and lay the groundwork for future cooperation (Hitchens & Gallagher, 2019).

Furthermore, regional organizations such as NATO, the European Union (EU) and ASEAN are increasingly recognizing the importance of cyber diplomacy in their public diplomacy efforts. Each of these organizations is adopting a unique approach to address the challenges posed by the digital environment and to promote better communication and understanding between their member states and external audiences (Pagovski, 2015):

- NATO has acted proactively to address cyber threats, reflecting its commitment to collective defense in the digital realm. The organization emphasizes the importance of strategic communication and public diplomacy as key tools to enhance its legitimacy and inform the public about its activities. NATO recognizes that effective communication is vital for building trust between its member states and allies. This includes engaging with citizens through social media and digital platforms to promote a better understanding of security issues and NATO's responses to cyber threats.

- The EU, on the other hand, has been slow to formalize its approach to cyber diplomacy. While the EU has developed various strategies to strengthen its digital presence and communication efforts, it has not yet developed a comprehensive public diplomacy strategy specifically for cyber issues. However, the EU is making extensive public diplomacy efforts to influence public opinion and promote understanding of its policies and actions, including those related to cybersecurity. The EU also uses digital communication tools to reach a wider audience, with an emphasis on cooperation and partnership to address global cyber challenges.

- ASEAN's approach to cyber diplomacy is characterized by its focus on regional cooperation and information sharing among member states. Although ASEAN has not explicitly labelled its initiatives as "cyber diplomacy", it recognizes the importance of information management and promoting mutual understanding within the region. This organization aims to create a sense of belonging among its member states and combat the perception that it is a weak regional player. ASEAN has launched several programmes and forums to discuss cybersecurity issues, emphasizing the importance of cooperation and collective responses to cyber threats.

2. Cyber diplomacy in times of crisis

2.1 Cyber warfare, cyber security and cyber deterrence: Why is diplomacy essential

First, it is important to distinguish between the concepts of cyberattacks and isolated incidents of attacks in the cyberspace and cyber warfare, since separating and deepening the understanding of these concepts is vital for clarity in legal, political and operational contexts. In essence, differentiating these terms helps to apply the appropriate legal frameworks, assess severity and intent, and formulate proportionate responses. It also clarifies performance challenges, as cyberattacks can originate from non-state actors, while cyberwarfare usually involves state responsibility and can escalate into broader geopolitical conflicts, thus further contributing to our understanding of the importance and perspective of cyber diplomacy.

According to Davis (2014), a cyberattack is defined as an attempt to damage, disrupt or gain unauthorized access to a computer or a device, computer system or electronic communications network. Cyber warfare, on the other hand, refers to actions undertaken by a nation-state or non-state group to penetrate the computers or networks of another nation with the aim of causing significant damage or disruption. This definition aligns with those of other experts in the field and emphasizes that cyber warfare is usually part of wider conflicts rather than isolated incidents. Cyberattacks can vary in nature and impact. While some may be relatively low risk, others can have profound impacts on national security, affecting critical infrastructure such as energy grids, financial systems and communication networks (Lehto, 2022).

The potential for cyberwarfare is significant, but it is often characterized by uncertainty and temporary effects, as the outcomes of such attacks are not always predictable or catastrophic. Davis (2014) points out that the effectiveness of cyberwarfare is often overestimated, as it is not as destructive as traditional warfare involving physical destruction or territorial gains. However, the risks associated with cyberattacks are real and can cause serious crises between nations. Thus, it is suggested that while deterrence strategies are necessary, they should in fact be part of a broader approach that includes resilience measures and the establishment of international norms to mitigate the risks of cyber conflict.

This observation can be found earlier in the literature, around the beginning of the 21st century, as Lewis (2002), whose study examined the risks associated with cyber terrorism, cyber warfare and their implications for national security and public policy, argues that while the growing reliance on computer networks creates vulnerabilities, the actual threat to critical infrastructure from cyberattacks may be overstated. More specifically, Lewis (2002) argues that many critical infrastructures are resilient and have redundancies that make them less vulnerable

to disruption than is commonly believed. He also points out that historical analyses of infrastructure attacks, such as strategic bombing during World War II, show that societies can be remarkably resilient to attack. For example, despite extensive bombing, German industrial production increased. Cyberattacks, while cheaper and easier to carry out than physical attacks, are less effective and often do not cause lasting physical damage. Of course, this was a view at the beginning of the 21st century, when technology had not evolved at the rapid pace leading to the rapid developments that humanity is experiencing today, so such a view may well be an oversimplification, perhaps even an underestimation of the technological potential for harm today.

This view is also shared by Shackelford (2009), who stresses that cyber-attacks are unlikely to produce the dramatic results desired by terrorists, who usually seek to instill fear and create significant political repercussions. In contrast, cyber terrorism often results in minimal disruption, as critical systems are designed to deal with the usual failures. As Shackelford (2009) explains, unlike traditional acts of terrorism, which can have immediate and visible effects, cyberattacks may lack the immediate visibility needed to create fear in the population. Moreover, the complexity and anonymity of cyberwarfare complicate the attribution of attacks, making it more difficult for terrorists to take responsibility and thus reducing the intended political impact. This means that while cyberattacks may be disruptive, they may fall short of the psychological and political goals typically associated with terrorism.

However, Lewis (2002) had highlighted an important issue, and that is the blurred boundaries between domestic and foreign threats in the context of cyber security, suggesting that national policies need to adapt to these evolving challenges, necessitating international cooperation to better address cyber threats in the modern world. However, in her research O'Connell (2012) highlighted that there is a complex relationship between cybersecurity, cyberwarfare and international law. Interestingly, she disagrees with the militarization of cyber security, arguing instead for a framework that prioritizes law enforcement and international cooperation.

More specifically, O'Connell (2012) notes that the US military has taken a dominant role in cybersecurity, raising concerns about the implications of viewing cyberspace primarily as a battlefield. In her research, she illustrates this point by referring to the development of the US Cyber Command and NATO initiatives following cyber incidents such as the attacks on Estonia in 2007 and during the Georgia-Russia conflict in 2008. These incidents gave rise to the perception that cyber threats are similar to traditional military threats, leading to a tendency to respond with military force. However, O'Connell (2012) critiques this militaristic approach, arguing that most cyber incidents, including piracy and espionage, do not result in the kind of significant harm that would warrant a military response under international law. It is also stressed that the primary cyber threats are often non-state actors engaged in criminal activities rather than state-sponsored warfare. It is therefore sufficient to view cyberspace primarily as an

economic and communications sector to lead to more effective security measures, while focusing on military responses to cyber threats is misguided, as it can lead to a cycle of escalation and further vulnerability. Instead, O'Connell (2012) advocates for legal frameworks governing cyber activities, emphasizing the importance of international law rules relating to economic rights and non-intervention. At the same time, she advocates for the establishment of comprehensive treaties that delineate legal and illegal cyber conduct, similar to existing treaties in other dual-use areas such as chemical and nuclear weapons.

Lancelot's (2020) most recent study outlines several critical aspects regarding the legal focus of cyber warfare, security and diplomacy, highlighting the complexities and challenges that arise in this area. In particular, the following key points are highlighted in his research:

- **Lack of established international laws:** Lancelot's research highlights a major shortcoming in the international legal framework governing cyber warfare. While traditional laws of war, such as Jus ad Bellum and Jus in Bello, exist, their application in cyberspace remains ambiguous. The absence of universally accepted rules of engagement complicates the legality of actions taken during cyber conflicts. This gap can lead to misinterpretations of aggressive acts, particularly when cyber-attacks may come from non-state actors or through anonymous means, making it difficult to assign responsibility and respond to risk.
- **Attribution challenges:** So, one of the central issues in cyber warfare is the attribution challenge, i.e. the process of identifying the source of a cyberattack. Lancelot (2020) argues that without clear attribution, responding to cyberattacks becomes problematic. A nation-state may retaliate based on a perceived threat without definitive evidence of the origin of the attack, which can escalate tensions unnecessarily. This ambiguity can lead to overreactions, where an attack that may not have been hostile is interpreted as an act of war, potentially triggering a massive response and even a military-based reaction.
- **Legal implications of cyber operations:** The Department of Defense has incorporated cyber operations into the Law of War Manual, treating them as legal forms of warfare. This classification implies that the laws governing traditional warfare also apply to cyber operations, particularly with respect to principles such as necessity and proportionality. Lancelot (2020), clearly disagreeing with the above statements, highlights that cyberattacks can actually have real-world consequences, affecting critical infrastructure and civilian populations, which necessitates careful consideration of legal and ethical norms.

In the context of all the above, it follows that cyber diplomacy is becoming a strategic necessity. Given the complexity and the aforementioned cyber challenges, it is argued that cyber diplomacy is essential to manage the risks associated with cyber operations. This form of diplomacy focuses on establishing rules and agreements that govern cyber behavior, with the

aim of mitigating conflicts before they escalate into larger confrontations (White, 2018). Cyber diplomacy involves the collection and dissemination of information in a strategic manner, similar to traditional diplomacy but tailored to the unique challenges of cyberspace (Barrinha & Renard, 2017).

At the same time, it is worth exploring how the fragmented nature of cyberspace challenges traditional notions of sovereignty and international relations, requiring a shift in diplomatic strategies. Eriksson & Giacomello, (2007) disagree with O'Connell's (2012) positions and state that integrating military strategy with cyber diplomacy is vital as states must navigate the anarchic landscape of cyberspace while protecting national interests. This approach recognizes that cyberspace is not a separate entity but is intertwined with broader geopolitical dynamics. In essence, their research argues for the increasing militarization of cyber diplomacy and the growing reliance on a military approach as a necessary practice to address cyber threats. Indeed, they note that while traditional military capabilities have declined since the Cold War, the focus on cyber threats has led to the creation of specialized units and strategies framed by concepts such as cyber warfare, information warfare, and cyber terrorism. Governments worldwide now view information systems as critical vulnerabilities that adversaries can exploit to inflict significant damage, even without conventional military conflict. This shift underscores the centrality of technological developments and intelligence gathering in contemporary security thinking. However, it also reflects the continuation of the traditional military interest in exploiting technological revolutions for strategic advantage, treating cyber capabilities as key tools in the broader context of national defense and security policies.

Generally, this debate is often observed in the literature, with many advocating for militarization and stringent measures and others arguing that this practice is a sure path to escalation and further conflict. Van der Meer's (2015) study also highlights the complex relationship between cyber diplomacy and cyber deterrence, particularly in terms of countering international cyber threats. Cyber deterrence typically refers to a state's efforts to deter cyber aggression through the threat of retaliation, either through cyber assets or other forms of military and economic responses. However, it is argued that while national cyber deterrence policies may appear effective in the short term, they risk leading to an ongoing cyber arms race and an escalation of tensions between states. Instead, cyber diplomacy is presented as a more viable solution for long-term cyber security. It involves diplomatic efforts to establish confidence-building measures and internationally accepted norms regarding state behavior in cyberspace. Van der Meer (2015) argues that although diplomatic approaches may not yield immediate results, they are more promising in promoting a cooperative international environment, thereby reducing the likelihood of misperception and conflict.

2.2 The role of international law in cyber diplomacy in times of crisis

The history of cyber conflicts and cyber warfare has evolved significantly in recent decades, reflecting the growing dependence on digital infrastructure and the increasing complexity of international relations. Therefore, in modern history, there have been several notable incidents of cyber conflict from 1985 to 2013, demonstrating how cyber operations have become an integral part of state and non-state actor strategies. The timeline of cyber conflict begins with early incidents such as the "cuckoo's egg" in 1985, where Markus Hess, a KGB-affiliated hacker, infiltrated US military and research facilities. This marked one of the first cases of state-sponsored cyber espionage, setting the stage for future conflicts. The emergence of worms such as the Morris Worm in 1988 highlighted the vulnerabilities of the nascent internet, affecting a significant portion of connected systems and leading to increased awareness of cybersecurity (Gamero-Garrido, 2014).

As technology evolved, so did the sophistication of cyberattacks. The late 1990s and early 2000s saw an increase in cyber operations linked to geopolitical tensions, such as the Electronic Disturbance Theater's DDoS attacks in support of political causes during the Zapatista uprising. The 1999 Kosovo war further highlighted the intersection of cyber operations and military conflicts, with 'patriot hackers' from different nations launching attacks against rival states (Gamero-Garrido, 2014). Cyberattacks in Estonia in 2007, after a Soviet war memorial was moved, demonstrated just how cyber operations could serve as tools of statecraft, with Russia widely suspected of orchestrating these attacks. Similarly, the Russian-Georgian war in 2008 showed how cyber warfare could complement conventional military operations by disrupting Georgian government and civilian communications (Healey, 2013).

In response to these evolving threats, nations have begun to adopt cyber diplomacy as a means of managing conflict in the digital domain. Cyberspace diplomacy involves negotiations and dialogues aimed at establishing rules and agreements governing state behavior in cyberspace. For example, initiatives such as the Paris Call for Trust and Security in Cyberspace[1], launched in 2018, seek to promote international cooperation to address malicious cyber activities and promote stability (Bechara & Schuch, 2021). According to Libicki (2012), the role of cyber diplomacy becomes particularly critical during times of crises, as the threat of cyber escalation can lead to real-world consequences. Cyber incidents can easily misinterpret intentions and lead to retaliation, making diplomatic channels essential for de-escalation. Establishing clear communication and understanding between states can help mitigate the risks associated with cyber conflicts.

As the landscape of international relations continues to evolve, the importance of cybersecurity and cyber diplomacy will increase. The complexity of cyber threats necessitates cooperation between states, the private sector and civil society to create a secure and stable

[1] https://pariscall.international/en/

cyberspace. Thus, the history of cyber conflict is not just a chronicle of attacks and defenses, it is also a narrative of how states navigate the challenges presented by digital warfare through diplomacy and cooperation. In this context, the importance of the role of international law is also highlighted. Chatterjee & Lefcovitch (2016) acknowledge that international law plays a key role in shaping the dynamics of cyber diplomacy, particularly as nations grapple with the challenges posed by cyber threats and the need for cooperative frameworks to address them. Indeed, the growing reliance on digital infrastructure has transformed the landscape of international relations, necessitating a corresponding evolution of the legal frameworks governing the conduct of states in cyberspace. Thus, several key aspects of this relationship between international law and cyber diplomacy are highlighted.

To begin with, it is worth emphasizing that at the heart of cyber diplomacy is the recognition that cyber threats are transnational in nature. Cybercrimes, such as piracy and cyberespionage, often transcend national borders, making it imperative that states cooperate to develop effective responses (Buchan, 2015). International law serves as a fundamental tool to facilitate this cooperation, providing a legal framework through which states can negotiate treaties and agreements aimed at enhancing cybersecurity and preventing cyberwarfare (Roscini, 2014). For example, the adoption of binding international conventions could help to classify certain cyber activities, such as cyber terrorism and attacks on critical infrastructure, as international crimes, thus promoting a collective response from the global community (Chatterjee & Lefcovitch, 2016).

International organizations, such as the International Telecommunication Union (ITU), play a critical role in setting norms and standards for cybersecurity on a global scale. In particular, the ITU has been involved in creating frameworks for international cooperation in cybersecurity since its establishment in 1865. By promoting partnerships between states, the ITU aims to build alliances that can comprehensively address the challenges posed by cyber threats. This effort is aligned with the broader goal of international law to promote peace and security on the global stage (Schia, 2016). Furthermore, the need for legal harmonization among jurisdictions to effectively combat cybercrime should be emphasized. The establishment of common legal standards and frameworks can enhance the ability of states to work together to address cybersecurity issues. The Global Cybersecurity Agenda (GCA), launched by the ITU in 2007, underlines the importance of harmonizing cybercrime legislation between Member States. By promoting a unified approach to legal standards, the GCA facilitates international cooperation and enhances the effectiveness of collective responses to cyber threats (Clough, 2014).

Therefore, the role of international law in cyber diplomacy is multifaceted and essential for navigating the complex landscape of cybersecurity. As cyber threats become more sophisticated and pervasive, the need for a strong international legal framework to govern the behavior of states in cyberspace is more critical than ever (Buçaj & Idrizaj, 2024).

By promoting cooperation, clarifying the responsibility of states, and promoting legal harmonization, international law can help create a safer digital environment. The evolution of cyber diplomacy will depend on the willingness of states to engage in meaningful dialogue and cooperation within established legal frameworks, paving the way for a more secure and cooperative international community in the face of evolving cyber threats.

An important concluding reference within the legal dimension of cyber diplomacy is the Tallinn Manual 2.0. Even though it does not represent binding international law and lacks formal endorsement by states, it constitutes the most comprehensive and influential attempt to clarify how existing legal norms apply to cyber operations. The Manual elaborates on key principles such as sovereignty violations, due diligence obligations, state responsibility for cyber activities, and the legal thresholds for use of force and armed attack. In practice, and particularly in the absence of a cyber-specific international treaty, the Tallinn Manual 2.0 serves as the primary legal compass for policymakers, militaries, and international organizations. Its significance lies not in its formal legal authority but in its role as the only coherent doctrinal framework for interpreting state behavior in cyberspace, thereby shaping expectations and informing diplomatic negotiations (Schmitt, 2017).

2.3 Russia as a Cyber Anti-Diplomacy Actor

Russia's behavior during the Russo-Ukrainian war demonstrates a systematic pattern of cyber anti-diplomacy, defined as the strategic use of cyber capabilities not to foster cooperation, de-escalation, or norm-building, but rather to undermine dialogue, disrupt institutional frameworks, and weaken the credibility of multilateral actors (Allahverdiyeva, 2024). Whereas cyber diplomacy aims to promote stability, confidence-building measures, and transparency, Russia frequently adopts the opposite approach, giving emphasis on exploiting cyber tools to create ambiguity, obstruct accountability, and challenge the foundations of the rules-based international order (Barrinha & Renard, 2017). This anti-diplomatic posture is consistent with the Russian doctrine of information confrontation, which perceives the information domain as an arena of constant strategic struggle rather than a space suitable for cooperative security governance (Giles, 2016).

During the Russia-Ukraine conflict, Moscow employed cyber operations not only as tactical instruments but also as mechanisms to contest Western cyber norms. The spread of disinformation, coordinated cyberattacks against Ukrainian infrastructure, and efforts to destabilize public opinion across Europe and North America illustrate how Russia uses digital means to erode trust between allies and to weaken institutional cohesion (Mueller et al., 2023). Moreover, Russia systematically rejects attribution findings from international organizations such as NATO, the EU, and the UN, thereby frustrating any attempt to establish shared investigative procedures or common legal understandings. This persistent denialism constitutes

a deliberate anti-diplomatic strategy, as it obstructs the formation of collective responses and undermines deterrence frameworks (Bendiek, 2018).

A central issue in evaluating Russia's cyber conduct lies in the legal ambiguity surrounding cyber operations. Although no binding international treaty specifically regulates cyber warfare, the Tallinn Manual 2.0 on the International Law, applicable to Cyber Operations remains the most authoritative guide for interpreting how existing international law applies in cyberspace (Roscini, 2014). While not an official legal instrument, it provides detailed clarifications on sovereignty, due diligence, state responsibility, and the thresholds of use of force and armed attack in cyberspace. In the context of the Russo-Ukrainian war, many of Russia's actions, such as targeting civilian infrastructure or interfering with critical financial networks, fall within areas explicitly examined by the Tallinn Manual, even if attribution challenges often prevent formal legal condemnation. The Manual's emphasis on state accountability, proportionality, and precaution highlights the degree to which Russia's cyber behavior contradicts emerging legal expectations (Davis, 2014).

Furthermore, Russia positions itself as an opponent of Western-led norm-building initiatives. Within UN processes such as the Open-Ended Working Group (OEWG) or the Group of Governmental Experts (GGE), Russia advocates for an alternative model of international information security, emphasizing state control, digital sovereignty, and restrictions on information flows (Buchan, 2015). This model clashes fundamentally with the openness and multistakeholder governance promoted by Western states (Pawlak, 2024). Russia's proposed norms, often supported by authoritarian regimes, reflect an anti-diplomatic strategy seeking to reshape the global cyber governance landscape in ways that legitimize domestic information control while constraining Western influence (Catanzariti, 2024). Ultimately, Russia's cyber anti-diplomacy undermines the prospects for cooperative governance in cyberspace. By weaponizing ambiguity, rejecting shared legal interpretations, and promoting alternative authoritarian-leaning information norms, Russia acts not merely as a cyber aggressor but as a normative disruptor. This behavior complicates crisis management during conflicts such as the Russia-Ukraine war, making cyber diplomacy both more necessary and more challenging (Fasinu et al, 2024).

3. Challenges, ethical concerns and implications of cyber diplomacy in times of crisis

3.1 Ethical considerations for cyber diplomacy operations

By examining the literature, various ethical implications of cybersecurity in the context of cyber diplomacy emerge, particularly in terms of the evolving landscape of technology and international relations. As cyber diplomacy becomes increasingly critical to securing information and infrastructure, ethical considerations must be at the forefront of discussions regarding its implementation and governance. According to Radanliev (2024), a primary ethical implication concerns the balance between national security and individual privacy rights. As governments strengthen their cybersecurity measures and tend to form their diplomatic parts into the cyberspace to protect against threats, they often resort to surveillance techniques that may violate privacy. This raises ethical questions about the extent to which individuals should be monitored for the sake of national security. While it is necessary to protect citizens from cyber threats, the methods used should not violate fundamental human rights. Striking a balance between these competing interests requires careful deliberation and adherence to ethical standards that prioritize civil liberties alongside security needs.

Another ethical concern arises from the use of Artificial Intelligence (AI) in cybersecurity and in the context of engaging cyber diplomacy. AI has the potential to significantly improve threat detection and response capabilities and this is not a matter in dispute. However, it also presents ethical dilemmas, particularly with regard to bias and transparency in decision-making. AI systems may inadvertently perpetuate biases in training data, leading to discriminatory practices that disproportionately affect certain groups. In addition, the opacity of AI algorithms can impede accountability, making it difficult to ascertain how decisions are made during cyber diplomacy operations. This challenge is serious given the importance of accountability in diplomatic practices in cyberspace. Therefore, ethical frameworks must guide the development and deployment of AI in cybersecurity and cyber diplomacy operations to ensure fairness, accountability and transparency (Radanliev (2024).

The ethical implications of cybersecurity and cyber diplomacy clearly extend to the realm of international relations, where state-sponsored cyber operations can blur the lines between warlike and peaceful acts. Cyber warfare poses significant ethical challenges, particularly in terms of justifying aggressive cyber actions against foreign entities. Such actions can lead to unintended consequences, including harm to civilians and disruption of infrastructure. Ethical considerations should guide nations in their cyber strategies to prevent escalation and ensure that responses to cyber threats do not violate international humanitarian laws or cause conflict (Tsotniashvili, 2024).

The ethical implications of cybersecurity also include the need for cooperation and information sharing among nations to effectively combat cyber threats. Countries must navigate the complexities of national sovereignty while promoting international cooperation to address global cyber challenges. Ethical considerations should guide diplomatic discussions to ensure that agreements respect the rights and interests of all parties involved, promoting a collaborative approach to cybersecurity that transcends geopolitical tensions (Radanliev, 2024). However, as Allahverdiyeva (2024) discusses in her study, the challenges and related ethical considerations in the context of cyber diplomacy arise almost entirely because of digitization, although speaking of cyber diplomacy, digitization is a prerequisite. In detail, her study explores how digitization has revolutionized diplomacy, presenting opportunities and challenges for the field. The focus of the discussion is on the transformation from traditional practices to virtual diplomacy, emphasizing how the internet and digital tools have reshaped communication, transparency and engagement in international relations.

Allahverdiyeva (2024) underlines that digital technologies enhance diplomatic effectiveness by enabling direct and immediate communication across geographical borders. This development has significantly increased the speed and quality of information exchange, promoting improved cooperation, transparency and public participation. Social media platforms allow diplomats to communicate directly with global audiences, promoting participation and understanding of foreign policy decisions. In addition, digital tools facilitate multilateral dialogue, enabling rapid coalition building to address global challenges such as climate change and cybersecurity. However, in the same context, ethical and practical challenges introduced by digitalization are also noted. The proliferation of digital tools intensifies competition between nations for technological dominance, increasing conflicts and rivalries. Cybersecurity is emerging as a critical concern, with cyber-attacks posing a threat to diplomatic institutions and sensitive communications. Issues such as data privacy and the spread of disinformation require diplomats to navigate a more complex and uncertain environment, balancing technological advances with security measures whilst in a certain field of a global competition for technological dominance.

Thus, ethical considerations discussed in the literature in the context of cyber diplomacy include the responsibility to ensure transparency without compromising sensitive information. While digital platforms make diplomacy more accessible, they also expose processes to public scrutiny, requiring diplomats to balance openness with confidentiality. The rise of disinformation campaigns further complicates this balance, as the integrity of diplomatic communications must be preserved to maintain trust and credibility. Moreover, the ethical use of digital tools for public engagement requires careful management to avoid manipulation or exploitation of the public. All of the above require clear ethical guidelines and safety and security measures, as alternatively automation through modern AI tools, instead of becoming a useful tool to promote collaboration and support, can become a serious risk. Besides, it is only through proper ethical practice that diplomatic operations can take on the proactive nature of

their effectiveness, demonstrating flexibility, adaptability and long-term focus on the security horizon (Stoltz, 2024).

3.2 Challenges in terms of attribution and accountability in the context of cyber diplomacy

Some of the most important challenges of cyber diplomacy relate to those strategies related to accountability and responsibility in the field. In the cyber domain, anonymity allows states or actors to conduct covert operations, making it difficult to determine who is responsible for cyber incidents. This anonymity may serve strategic purposes, such as avoiding escalation of conflict or shielding donors from public scrutiny. However, advances in performance technologies and the broader involvement of governments and the private sector in identifying perpetrators have reduced the effectiveness of reasonable denial. Public attribution of cyber incidents has both advantages and risks. On the one hand, revealing the perpetrator behind a cyberattack can act as a deterrent, signaling to other states that similar actions will not go unnoticed. Public attribution weighs on reputation, especially when many states condemn the act, and can enhance global cybersecurity by encouraging international cooperation. On the other hand, public attribution of cyber incidents could trigger retaliation or escalate tensions, especially if no decisive action is taken after attribution, which could encourage attackers. The literature also notes that while cyber operations are often considered less escalatory than conventional or nuclear attacks, public attributions must be managed carefully. If states fail to respond adequately after naming an actor, this can undermine the credibility of deterrence. For example, the limited responses to incidents such as the 2014 Sony hack or the 2016 DNC hack suggest that public attribution alone is not sufficient to deter future hostile activities, highlighting the complexity of maintaining accountability in cyberspace (Lee, 2023).

As explained in detail in Pawlak (2024), accountability and the responsibility of attribution are significant challenges in cyber diplomacy due to the complex interdependencies and the current geopolitical landscape. The primary issue is the state-centric view of accountability, which traditionally limits accountability to government actions and excludes the roles of the private sector and civil society in cyber governance. This narrow focus on state actions leads to a lack of comprehensive accountability mechanisms, particularly for malicious behavior carried out by non-state actors such as private companies and individuals. Accountability further complicates this picture, as it involves identifying the specific actors behind cyber incidents, a process rife with uncertainty and often influenced by political motivations or party agendas. States are reluctant to share information related to cyberattacks, which can hinder the attribution process and raise doubts about the credibility of governments' claims about cyber incidents. Moreover, requiring absolute certainty in attribution may prevent timely responses and ultimately discourage accountability.

Of course, the voluntary nature of existing rules and the absence of binding international law on cyber conduct exacerbate these challenges (Tiirmaa-Klaar, 2013). This is why the importance of having ethical guidelines and clearer guidance based on international law and rules was emphasized as a matter of critical importance earlier. Indeed, many countries, especially those in the Global South, may lack the necessary capacities to engage in accountability, further widening the accountability gap. Ultimately, the intertwining of accountability and attribution, combined with the political sensitivities surrounding state behavior in cyberspace, creates a significant barrier to effective cyber diplomacy and the creation of strong accountability mechanisms (Pawlak, 2024).

3.3 Legal and political gaps in cyber diplomacy practices

The challenges and ethical concerns surrounding the activities of cyber diplomacy highlight the existence of serious legal and policy gaps in this field. First, according to Tiirmaa-Klaar (2013), the lack of structured international coordination and oversight mechanisms in cybersecurity capacity building is evident. Current efforts are numerous but fragmented, which underscores the need for a global accountability system to streamline these activities and ensure effectiveness. Informal collaborative networks, such as the Meridian process and FIRST, are effective but are limited by their focus on specific stakeholders, such as government representatives or technical experts, leaving broader international policy coordination unaddressed. Second, human rights issues in cyberspace remain a significant challenge. Many regimes use information and communication technology (ICT) to suppress dissent, censor content and monitor opposition. While frameworks such as the UN Human Rights Council Resolution and EU strategies promote online freedoms, gaps in implementation and enforcement remain. These observations link to cyber diplomacy in the following way: they highlight the need for international cooperation to address cybersecurity challenges. The lack of coordination in cybersecurity capacity building underscores the role of cyber diplomacy in promoting global cooperation, aligning efforts, and rationalizing resources. Similarly, the reliance on informal networks points to the need for cyber diplomacy to create formal, multilateral mechanisms to manage crises and build trust between nations. These efforts enhance global cyber resilience and ensure a unified approach to addressing cybersecurity threats.

In addition, Internet governance disputes reflect a political divide. Divisions between countries that support multi-stakeholder models, such as the US and the EU, and those that favor government-controlled frameworks hinder global consensus. These disagreements risk fragmenting the internet and compromising the protection of fundamental rights (Catanzariti, 2024). Finally, the lack of awareness and resources among developing countries to address cyber threats exacerbates disparities in cybersecurity and the prospects for cooperation in diplomatic operations (Maina, 2024). Development assistance and capacity building programmes are not

sufficiently coordinated, leaving many states vulnerable. Bridging these gaps requires enhanced international cooperation, integrating security and human rights considerations into broader cyber diplomacy strategies.

Psaila (2021) in her official study for Diplo Foundation (a non-profit organization in the field of diplomacy and digital policy) refers to the disadvantaged position of some states in the context of cyber diplomacy. She explains that small and developing countries face several significant challenges in cyber diplomacy, mainly due to limited human and financial resources. These nations often prioritize immediate economic and development needs over cyber issues, which are considered less critical. Consequently, this leads to a lack of expertise and knowledge in cybersecurity and cyber diplomacy, hindering effective participation in international discussions and negotiations. The lack of trained diplomats equipped to handle cyber issues further exacerbates this situation, resulting in these countries being underrepresented in global cyber policy dialogues.

Moreover, the political dimension plays a critical role in shaping a country's engagement in cyber diplomacy. If cyber issues are not prioritized at the political level, the necessary capacity building efforts to address these issues are often neglected. This creates a vicious cycle where low prioritization leads to insufficient capacity, which in turn perpetuates a lack of engagement in the field of cyber diplomacy. This situation highlights important legal and political gaps in the field of cyber diplomacy. Small and developing countries may lack the legal frameworks needed to effectively address cyber threats, making them vulnerable to cyber incidents. Furthermore, their limited participation in international legal discussions contributes to their lack of representation in the setting of rules and standards governing state behavior in cyberspace. As a result, the absence of a strong cyber diplomacy framework leaves these countries at a disadvantage, unable to adequately protect their national interests in an increasingly interconnected digital landscape (Psaila, 2021).

3.4 Lessons learnt from the dimensions of cyber diplomacy

By examining the aspects of diplomatic practices in cyberspace so far, important lessons can be learned which in turn can guide future practices and inform the effectiveness of cyber diplomacy operations. In detail, Sotiriu (2015) reports the following:

- Digital diplomacy as change management: Digital diplomacy is not just a tool for public diplomacy, but also serves as a mechanism for managing change in the international system. The importance of adapting to technological developments and understanding the impact of these changes on diplomatic practices is highlighted.

- Endogenous vs. exogenous changes: Two main sources of change are highlighted in Sotiriu (2015): incremental, step by step changes that occur through everyday diplomatic practices and exogenous shocks, massive shifts resulting from major events. Effective digital diplomacy must recognize and adapt to both types of change in order to manage relationships and responses appropriately.

- Data overload and data analysis challenges: With the vast amounts of data generated through digital platforms, there is the challenge of 'data suffocation'. Diplomats need to develop sophisticated methods to effectively analyze this data to derive relevant information for decision making.

- The importance of human interaction: While technology facilitates the collection and sharing of data, the nuances of personal interactions, such as understanding intentions and building trust between two parties, remain difficult to replicate in a digital environment, where there is no personal interaction and face-to-face communication. This underlines the need for a balanced approach that integrates both digital tools and traditional face-to-face diplomacy.

- Public engagement: Digital diplomacy has broadened the scope of who can engage in diplomatic processes, moving beyond interactions between states to include public opinion and grassroots movements, which use collective action. This shift necessitates a deep understanding of how public sentiment can influence international relations, since it can dramatically change the way in which cyber diplomacy engages the public in such affairs.

- Security vs. engagement: Despite the potential benefits of digital diplomacy, there is often a tension between the ideals of open engagement and the reality of national security concerns. This complexity must be carefully managed to ensure that digital initiatives do not compromise sensitive diplomatic objectives.

So, summarizing the lessons learnt from cyber diplomacy, one can understand that there is an increased need for adaptability, for integrating appropriate data analysis practices always in combination with human interaction and for recognizing the broader implications of collaboration with various stakeholders in the digital realm. These observations are useful because they can shape contemporary diplomatic practices and can be particularly helpful in times of crisis. Other researchers have also reached these observations. For example, Rashica (2018) identifies in the rapid development of information and communication technologies (ICTs) the challenges that arise for cyber diplomacy in practice, as diplomatic teams have to adapt quickly to new tools and platforms. The integration of social media, for example, has transformed traditional diplomatic interactions, promoting greater transparency and direct

engagement with global audiences. Furthermore, Rashica (2018) discusses benefits and risks: she explains that while cyber diplomacy offers significant benefits, such as improved communication and reduced costs, it also presents risks, particularly through the threats of piracy and disinformation that can undermine diplomatic efforts and national security. Therefore, countries must invest in strong cybersecurity measures and diplomatic training to effectively navigate this complex landscape.

Admittedly, the emergence of a digital public sphere underlines the importance of managing the narratives and perceptions of the public. Diplomats must recognize that their interactions and messaging can have far-reaching consequences and that public discourse is often influenced by social media. This requires a strategic approach to content creation and distribution, ensuring that messages resonate with targeted audiences while maintaining ethical standards (Shvelidze et al., 2024). Finally, the lessons learned from cyber diplomacy highlight the need for cooperation among international actors. Indeed, transnational and international cooperation is an issue that arises frequently, so it is a matter of major importance that cannot be overemphasized. As digital platforms facilitate interaction between states, non-state actors and civil society, a multilateral approach is essential to address common challenges and seize the opportunities presented by the digital age. This collaborative framework will be vital for the future of international relations in an increasingly interconnected world (ud din Bhat, 2023).

3.5 Impact of cyber diplomacy on potential international crises

Fasinu et al. (2024) explain that cyber diplomacy significantly affects communication in crisis situations, as it shapes the ways in which governments and diplomats interact with both domestic and international stakeholders. Their research highlights that during crises, social media platforms such as Twitter and Facebook facilitate the rapid distribution of information, allowing governments to communicate directly with citizens and effectively counter misinformation. This immediacy can enhance transparency and build public trust, as officials can provide timely updates and clarify rumors. However, the study also identifies challenges associated with the impact of cyber diplomacy in times of crisis. More specifically, the rapid pace of social media news dissemination can lead to the rapid spread of misinformation, which can exacerbate tensions and confuse the public. This underscores the dual-edged nature of digital tools in diplomacy, where their potential to facilitate transparency and trust can quickly transform into a liability if mismanaged, as the rapid dissemination of information also amplifies the risks of misinformation and public confusion. Moreover, reliance on digital platforms risks undermining traditional diplomatic channels, potentially leading to a fragmented communications landscape. Based on these findings, Fasinu et al. (2024) suggest that while cyber diplomacy offers opportunities for enhanced engagement and accountability, it also requires the development of strategic communication guidelines to manage the unique

challenges posed by the digital environment, particularly during crises. Balancing the benefits and risks of digital tools is therefore vital for effective crisis communication in diplomacy.

According to Radanliev (2024), the impact of cyber diplomacy in times of crisis can indeed be multifaceted, and this is clear if one focuses on promoting international cooperation, enhancing trust and facilitating effective incident response. During crises such as cyber-attacks or data breaches, cyber diplomacy plays a critical role in creating channels of communication between nations, enabling the rapid exchange of information and intelligence about threats. This rapid communication can help mitigate misunderstandings and prevent tensions from escalating, as timely information about cyber incidents can clarify intentions and responsibilities. Radanliev (2024) adds to the positive impact of cyber diplomacy that it promotes confidence-building measures, which are necessary to reduce suspicion between states. These measures can include joint cyber exercises, common cybersecurity policies and direct lines of communication, which enhance transparency and foster an environment of cooperation, as stated earlier. Furthermore, cyber diplomacy encourages public-private partnerships, enabling cooperation between governments and private sector actors to enhance cyber defense. By sharing resources and expertise, nations can improve their collective resilience against cyber threats. In addition, effective cyber diplomacy can help develop international norms and standards that guide states' cyber behavior, reinforcing a unified approach to crisis management. This cooperative framework is the most important form of cyber diplomacy's impact, as it ultimately contributes to global stability in times of crisis.

4. Case study:
Cyber diplomacy in the war between Russia and Ukraine

4.1 The Role of International Organizations and Their Digital Interventions in the Russo-Ukrainian War

The war between Russia and Ukraine, which escalated dramatically following the Russian invasion in February 2022, constitutes one of the most characteristic examples of contemporary conflict in which hostilities are not confined to the conventional military domain. Beyond land, naval, and air operations, the war unfolded in parallel within cyberspace, which emerged as a critical and autonomous field of confrontation. Cyberattacks against critical infrastructure, large-scale disinformation campaigns, influence operations conducted through digital platforms and efforts to strengthen the digital resilience of the Ukrainian state formed integral components of the overall war strategy (Darmayadi et al, 2024).

Within this context, cyberspace did not function merely as a supplementary tool, but as a parallel front where state functionality, social cohesion, and the international image of the parties involved were at stake. Russia employed cyber operations and systematic disinformation with the aim of destabilizing Ukraine, undermining trust in state institutions, and shaping favorable narratives both domestically and internationally. Conversely, Ukraine faced the urgent need to ensure the continuity of state governance, protect its digital infrastructure, and communicate its position effectively to the international community. In this setting, concepts such as cyber operations, countering digital disinformation, and digital resilience acquired central importance (Mueller et al, 2023).

The scale and intensity of digital threats made it evident that Ukraine could not respond effectively relying solely on national resources. Cyberattacks, the technical complexity of threats and the rapid dissemination of disinformation exceeded the capacities of a state already under immense military and economic pressure. That’s why international organizations emerged as pivotal actors in this case study, functioning as force multipliers and stabilizing agents in the digital domain (Moustakis et al, 2025).

International organizations contributed in distinct yet complementary ways. They provided technical and operational support to enhance cybersecurity, reinforced the institutional resilience of the Ukrainian state under wartime conditions and contributed to narrative coordination and norm-setting regarding responsible behavior in cyberspace. At the same time, they operated as platforms for the international legitimation of Ukraine’s position, strengthening its diplomatic leverage in the digital sector (Darmayadi et al, 2024).

Within the framework of this chapter, the case study explicitly focuses on the role of specific international organizations and actors that played a very important role in the digital dimensions of the Russo-Ukrainian war. In particular, the analysis examines NATO, the European Union, the United Nations and also the private-sector technology actors, such as Microsoft, Amazon, Google, Meta, and Twitter. The selection of these actors is not arbitrary but reflects the distinct nature of their contributions and the complementarity of their interventions in the digital battlefield (Carrapico & Farrand, 2024).

This section does not aim to provide a general or theoretical institutional overview of these organizations. Instead, the analysis is strictly focused on concrete digital interventions directly linked to the Russo-Ukrainian war. In the case of NATO, attention is directed toward its role in strengthening Ukraine's cyber defense, transferring expertise and operating as a framework for strategic coordination against Russian cyber threats. With regard to the European Union, the analysis focuses on policy and operational initiatives aimed at supporting Ukraine's digital resilience, as well as on regulatory and counter-disinformation measures within and beyond European borders (Gao et al, 2024).

In addition, for the United Nations, the analysis examines its role as a forum for international legitimation, dialogue, and norm-setting in cyberspace, along with its interventions in areas such as information protection, human rights, and digital security in conditions of armed conflict. Very important can be considered the examination of private technology companies centers on their practical digital interventions, including the provision of cloud infrastructure, the protection of government networks, the limitation of Russian disinformation and content governance on social media platforms (Danylenko & Patsyora, 2024).

In this way, this section functions as a very important analytical framework for examining the role of international organizations and private actors in the digital dimension of the war between Russia and Ukraine. Finally, in this section the specific digital interventions of each digital organization are examined systematically and comparatively within the context of the war.

4.1.1 NATO

The international reaction to the Russo-Ukrainian war highlighted the limitations of existing crisis prevention and resolution mechanisms. Many international actors stress the need for civilian approaches to conflict resolution, focusing on national resilience, international cooperation and countering disinformation. Ukraine has worked extensively to strengthen its ties with global partners, in particular NATO, while intensifying its use of modern technologies and communication strategies to counter Russian aggression (Kostyrev, 2023). Thus, NATO has played a critical role in supporting Ukraine and adapting its strategies to counter modern hybrid threats such as cyber-attacks and disinformation. The Alliance strengthened collective defense capabilities by increasing troop readiness and deploying additional forces to member states close to the conflict zone. Importantly, NATO has also condemned Russia's actions as

violations of international law and stressed the importance of maintaining global order (Donaldson, 2017). According to Danylenko & Patsyora (2024), NATO's support to Ukraine includes financial assistance, military training and assistance in equipping Ukrainian forces. It also counters Russian propaganda through public communication, media cooperation and advanced cybersecurity measures. By strengthening its communication strategy, NATO aims to provide accurate information, counter disinformation and strengthen international solidarity against Russian aggression. This multifaceted response underscores NATO's role in safeguarding regional and international security in the face of evolving threats.

During the Russia-Ukraine war, international organizations went beyond strategic statements and traditional support, implementing specific digital interventions to strengthen Ukraine's defense and counter Russian cyber operations. NATO, in addition to military and diplomatic assistance, activated the NATO Cyber Rapid Reaction Team, a specialized unit designed to provide immediate support during critical cyber incidents (Kostyrev, 2023). This team was instrumental in analyzing threats, coordinating responses, and assisting Ukrainian systems in real time. NATO also provided Ukrainian organizations with access to the Malware Information Sharing Platform (MISP), facilitating timely identification of malware and coordination between multiple CERTs (Computer Emergency Response Teams) (Danylenko & Patsyora, 2024).

Technical training was systematically provided to Ukrainian CERTs, and exercises such as "Cyber Coalition" strengthened government networks and critical infrastructure through attack simulations and resilience testing. NATO also promoted knowledge-sharing initiatives.

In this way Ukrainian networks are connected with the Alliance's threat monitoring and detection systems, enhancing real-time response capabilities and ensuring interoperability of cyber defense measures (Mueller et al., 2023). These interventions are in line with broader developments in modern warfare, where AI-assisted threat detection and autonomous defensive systems are increasingly integrated into cyber operations (Moustakis et al, 2025).

Beyond its traditional military and political commitments, NATO expanded its digital intervention toolkit to address the escalating cyber dimension of the Russia-Ukraine war. The Alliance intensified its support for Ukraine by reinforcing the protection of critical digital infrastructure and enhancing operational readiness against hybrid threats. Through the NATO Communications and Information Agency (NCIA), specialized technical assistance was delivered to improve the security of governmental networks, support incident-response capabilities, and integrate advanced cyber-defense technologies across Ukrainian systems. NATO also strengthened its strategic communication and counter-disinformation capacities, deploying digital monitoring tools, supporting real-time threat-analysis platforms, and enhancing cooperation with Ukrainian institutions to track and counter Russian information operations. These initiatives were complemented by NATO's StratCom Centre of Excellence,

which provided research, analytical assessments, and training on narrative warfare, digital manipulation techniques, and resilience against coordinated propaganda campaigns (Danylenko & Patsyora, 2024).

Additionally, the Alliance broadened its use of public-private cybersecurity partnerships**,** embedding industry expertise into cyber-defense missions and enabling rapid information sharing through mechanisms such as the NATO Industry Cyber Partnership (NICP)**.** This collaboration helped accelerate the detection of malware, improve cyber-forensics capabilities, and facilitate the deployment of cutting-edge defensive tools, including AI-supported threat-monitoring systems. Joint cyber exercises and simulations further enhanced interoperability and crisis-response preparedness, ensuring that Ukraine's cyber-defense posture aligned with NATO's broader strategic framework. Overall, these NATO-driven digital interventions underscore the central role of cyber diplomacy in contemporary conflict management. By combining robust defense mechanisms, technical expertise, multi-stakeholder cooperation, and advanced technologies, NATO has positioned itself as a critical actor in supporting national resilience, strengthening collective security, and coordinating international responses to hybrid aggression throughout the Russia-Ukraine war (Moustakis et al, 2025).

Beyond its established cyber assistance mechanisms, NATO implemented additional specialized interventions aimed at enhancing Ukraine's national cyber resilience. Through the NATO Defence Innovation Accelerator for the North Atlantic (DIANA), the Alliance supported Ukrainian institutions in testing emerging defensive technologies, including secure communication tools, AI-enabled intrusion-detection systems, and satellite-based cyber-monitoring platforms war (Moustakis et al, 2025). NATO also expanded the "Federated Mission Networking" initiative to Ukraine, enabling secure information exchange with Allied forces and providing a resilient digital backbone for situational awareness. Moreover, the Cooperative Cyber Defence Centre of Excellence (CCDCOE) integrated Ukrainian analysts into advanced cyber-forensics programmes, enabling joint investigations and threat-pattern mapping of Russian GRU-based operations. NATO's Technical Arrangements Framework further allowed Ukrainian agencies to access specialised encryption suites and post-incident recovery tools, accelerating system restoration after critical intrusions. Collectively, these measures strengthened Ukraine's operational coherence, digital sovereignty, and interoperability with Euro-Atlantic cyber-defence networks war (Moustakis et al, 2025).

In addition to the already established mechanisms of cyber assistance and strategic communication, NATO's engagement in the Russia-Ukraine war illustrates a broader shift toward institutionalized digital crisis management. The conflict accelerated the Alliance's transition from reactive cyber defense to proactive digital deterrence, where early warning systems, predictive analytics and coordinated information-sharing architectures play a very important role. NATO's ability to integrate cyber intelligence from multiple Allied states allowed for near real-time situational awareness, enabling faster identification of coordinated

cyber campaigns attributed to Russian state and proxy actors. This enhanced intelligence fusion proved critical in mitigating large-scale attacks on Ukrainian energy grids, telecommunications networks, and public administration platforms (Kostyrev, 2023).

Furthermore, NATO placed particular emphasis on strengthening Ukraine's societal resilience through digital literacy and information integrity initiatives. Recognizing that cyber operations and disinformation campaigns aim not only at technical disruption but also at eroding public trust, the Alliance supported programs focused on media literacy, open-source intelligence (OSINT) analysis, and fact-checking infrastructures. These initiatives empowered Ukrainian civil society actors, journalists, and local authorities to detect manipulated narratives and respond swiftly to coordinated influence operations. By supporting decentralized information verification networks, NATO contributed to limiting the psychological and political impact of Russian hybrid tactics (Danylenko & Patsyora, 2024).

In addition, the Alliance actively promoted adherence to international law, including the applicability of international humanitarian law and norms of responsible state behavior in cyberspace. Through policy dialogues and expert consultations, NATO supported Ukraine in documenting cyber incidents, attributing responsibility, and preserving digital evidence for future legal and accountability processes. This normative approach reinforced Ukraine's position in international forums and contributed to shaping a broader consensus on cyber accountability during armed conflict (Kostyrev, 2023). NATO's digital interventions also extended to the protection of electoral systems and democratic institutions. As Russia sought to exploit political vulnerabilities through cyber-enabled interference, NATO-assisted risk assessments and penetration testing helped safeguard voter registries, digital identification systems, and election-related communication platforms. These measures were designed not only to prevent direct manipulation but also to preserve public confidence in democratic processes during wartime conditions (Danylenko & Patsyora, 2024).

Overall, NATO's digital interventions in the Russia-Ukraine war demonstrate a comprehensive approach that transcends traditional military assistance. By combining cyber defense, strategic communication, legal norm-building, societal resilience and technological innovation, NATO has contributed significantly to Ukraine's ability to withstand sustained hybrid aggression. This case underscores the growing centrality of digital power and cyber diplomacy in contemporary international security, presenting in this way NATO as an important actor in shaping the future architecture of conflict management in the digital age (Moustakis et al, 2025).

4.1.2 EU

The EU has developed a broader framework of diplomatic policies on crisis management and the use of soft power to address security concerns arising from the conflict, especially after Russia's annexation of Crimea in 2014 and the subsequent invasion in 2022. In detail, the EU

has stressed the importance of supporting Ukraine's sovereignty and territorial integrity through various measures, including humanitarian and military assistance. In essence, the EU's approach includes strengthening cooperation with Ukraine in the field of cybersecurity, as cyber threats are an important aspect of modern warfare, particularly in the Russian-Ukrainian context. Furthermore, the EU's commitment to human rights and democracy, as well as its strategic responses to Russian aggression, suggest that cyber diplomacy will play a critical role in maintaining both defensive and offensive cyber capabilities during the ongoing conflict (Aydemir & Güner, 2023).

According to Carrapico & Farrand (2024), the EU's diplomatic role in this war focuses on leveraging Europe's cybersecurity policy framework to counter external threats and promote strategic autonomy.

Through deepening regulation and rule extraction, the EU has focused on establishing strong cybersecurity standards based on European values, with the aim of mitigating vulnerabilities and claiming global leadership. This approach reflects a mix of economic and security objectives, with an emphasis on digital sovereignty. In response to Russia's actions, EU cyber diplomacy has sought to strengthen domestic resilience and influence international norms, positioning the Union as an active rule-maker amidst evolving global challenges. So, the EU's response to the Russia-Ukraine war can be inferred through its focus on regulatory deepening and cybersecurity norm exporting. By strengthening its cybersecurity frameworks, the EU addresses external threats and promotes digital sovereignty to counteract vulnerabilities exposed by conflicts like the war. These measures aim to secure critical infrastructure and assert global leadership, ensuring resilience in a world marked by complex, evolving security challenges (Carrapico & Farrand (2024).

The European Union focused on cyber resilience and the protection of critical digital infrastructure, recognizing that modern conflicts extend well beyond kinetic operations into cyberspace. In response to the Russia-Ukraine war, the EU deployed the EU Cyber Rapid Response Team (CRRT), integrating specialists from Lithuania and Estonia who provided on-the-ground technical assistance to Ukrainian authorities. The CRRT's role included rapid threat assessment, incident response coordination, and supporting Ukrainian CERTs in mitigating the impact of cyberattacks on governmental networks and essential services (Carrapico & Farrand, 2024). In addition to personnel support, the EU allocated €10 million in emergency funding to reinforce cybersecurity capabilities. This funding enabled Ukraine to strengthen its IT infrastructure, implement protective measures, and increase system redundancy against disruptive cyber campaigns. To safeguard critical state data, Ukrainian governmental databases were transferred to secure European cloud infrastructures, ensuring continuity of essential operations even under intense cyber pressure. These measures illustrate a proactive approach to data sovereignty and resilience, reinforcing Ukraine's operational stability during periods of heightened threat (Gruszczak & Kaempf, 2023).

Beyond technical support, the EU focused on countering disinformation and hybrid threats, which were integral to Russia's asymmetric strategy. Using the EUvsDisinfo platform, European actors monitored and analyzed propaganda narratives, identifying misinformation and providing reliable alternatives to both Ukrainian citizens and the international community. This integration of cyber and informational efforts highlights the EU's recognition that digital security is inseparable from strategic communication and public trust (EUvsDisinfo, 2025). Through the European Union Agency for Cybersecurity (ENISA), the EU provided extensive training programs for Ukrainian cyber teams, emphasizing best practices, incident response protocols, and adoption of common security standards across governmental networks. These initiatives foster interoperability with European partners and strengthen regional cybersecurity norms, demonstrating how cyber diplomacy combines technical, regulatory, and strategic measures. By leveraging expertise, infrastructure, and policy tools, the EU's digital interventions exemplify a comprehensive approach to supporting resilience, maintaining operational continuity, and enhancing international coordination in modern conflict settings (Gruszczak & Kaempf, 2023).

The EU deepened its digital engagement through the Cybersecurity Blueprint Implementation Mechanism, which provided Ukraine with crisis-response protocols aligned with the NIS2 Directive, ensuring standardisation across energy, healthcare, and transport sectors. Moreover, the EU Cybersecurity Competence Centre facilitated access to cutting-edge research infrastructure, enabling Ukrainian analysts to utilise quantum-resistant cryptography and big-data threat-intelligence platforms. The Digital Europe Programme financed cross-border cyber-range exercises simulating large-scale Russian hybrid operations, improving Ukrainian agencies' readiness for coordinated cyber-physical attacks. Additionally, the European Digital Media Observatory (EDMO) collaborated with Ukrainian fact-checking networks to analyse synthetic media, detect coordinated inauthentic behaviour, and train journalists on adversarial information techniques. The EU Satellite Centre (SatCen) provided geospatial intelligence to support attribution of cyber-enabled kinetic strikes. These interventions demonstrate the EU's multi-layered approach that merges regulatory, technical, and informational resilience in times of conflict (Carrapico & Farrand, 2024).

In addition, the European Union has increasingly framed its cyber engagement in the Russia-Ukraine war as part of a broader strategy of strategic autonomy and normative power projection. The conflict accelerated the EU's ambition to act not merely as a regulatory actor, but as a security provider capable of responding to high-intensity hybrid threats (Gruszczak & Kaempf, 2023).

By integrating cyber defense into the Common Security and Defence Policy (CSDP), the EU strengthened the linkage between digital resilience and geopolitical stability, reinforcing its role as a credible actor in crisis management beyond its borders. A significant dimension of the EU's digital intervention has been its emphasis on public-private cooperation in

cybersecurity. Recognizing that much of the critical digital infrastructure is owned or operated by private entities, the EU facilitated structured information-sharing mechanisms between Ukrainian authorities, European technology firms, cloud-service providers, and cybersecurity vendors. These partnerships enabled rapid patch deployment, malware analysis, and coordinated responses to ransomware and distributed denial-of-service (DDoS) attacks targeting Ukrainian institutions. Such collaboration reflects the EU's market-driven yet security-oriented approach to cyber diplomacy, where economic actors are embedded within strategic resilience frameworks (Gruszczak & Kaempf, 2023).

Furthermore, the EU gave emphasis on capacity-building and long-term institutional reform. Rather than focusing solely on immediate crisis response, European initiatives aimed to align Ukraine's cybersecurity governance with EU acquis and best practices. Support for legislative harmonization, risk-management frameworks, and oversight mechanisms contributed to the gradual institutionalization of cyber resilience within Ukrainian public administration. This alignment not only enhanced Ukraine's defensive posture during the war but also facilitated its broader European integration trajectory (Carrapico & Farrand, 2024). The EU also expanded its efforts in cyber attribution and accountability. Through joint analytical platforms and intelligence coordination, European institutions supported Ukraine in identifying patterns of state-sponsored cyber operations and linking them to broader military and information campaigns. This capacity to attribute cyber incidents strengthened the EU's diplomatic leverage, enabling coordinated sanctions, public condemnation, and norm-enforcement measures at the international level (Gruszczak & Kaempf, 2023).

Overall, the EU's response to the Russia-Ukraine war illustrates an integrated model of cyber diplomacy that combines regulatory power, operational support, market coordination, and normative influence. By addressing cyber threats as both technical and political challenges, the EU has contributed to strengthening Ukraine's resilience while simultaneously reinforcing its own strategic position in global cybersecurity governance. This approach underscores the evolving role of the European Union as a hybrid security actor in contemporary conflicts, where digital domains are central to both defense and diplomacy (Carrapico & Farrand, 2024).

4.1.3 UN

The United Nations occupies a distinct position in the Russia-Ukraine war, operating within a complex institutional and political environment shaped by competing state interests and structural constraints. Unlike NATO and the European Union, the UN's role is primarily normative and diplomatic, focusing on conflict prevention, international law, and humanitarian protection. Despite limitations stemming from the Security Council's power dynamics, this global organization has sought to adapt its tools to the digital dimension of the conflict. Through cyber governance initiatives, humanitarian technologies, and norm-setting processes, the UN

has attempted to address emerging cyber and hybrid threats while upholding principles of sovereignty, human rights, and international stability (Schmitt, 2017).

Within this context, the UN's engagement with the cyber dimension of the conflict reflects an effort to reconcile its traditional peacekeeping mandate with the realities of digitally mediated warfare. Rather than direct operational intervention, the organization has emphasized compliance mechanisms, multilateral dialogue, and the development of shared norms governing state behaviour in cyberspace. These initiatives seek to reduce escalation risks, protect civilian infrastructures, and ensure accountability in an environment where cyber operations increasingly intersect with humanitarian and human-rights concerns. As such, the UN's approach highlights both the potential and the limitations of cyber diplomacy within a highly polarized international system (Mukarzel, 2023). Mukarzel (2023) states that the UN's efforts in the Russia-Ukraine war are focused on promoting peace through compliance mechanisms and using their diplomatic influence. Key UN actions include:

- supporting the Minsk agreement
- the deployment of peacekeeping and monitoring missions for the observance of ceasefires
- encouraging dialogue.

UN Security Council Resolution 2202 also emphasized Ukraine's sovereignty and political settlement, reinforcing global diplomatic efforts. However, significant challenges, such as geopolitical tensions, ceasefire violations and Russia's dual role as a party to the conflict and a veto-wielding Security Council member, limited the UN's ability to mediate effectively. These obstacles highlight the complexity of cyber diplomacy in this conflict. Despite institutional constraints caused by Russia's position in the Security Council, the United Nations advanced several digital, and in many cases governance-oriented initiatives. First, the UN promoted resolutions emphasizing the protection of digital sovereignty, framing cyberspace as a domain where state rights and obligations under international law must be upheld. Within the Open-Ended Working Group (OEWG), the UN coordinated technical working groups to strengthen global cyber norms, facilitating dialogue on responsible state behavior in cyberspace and encouraging multilateral confidence-building measures. The UN also advocated for treating severe cyberattacks as potential threats to international peace and security, consistent with principles outlined in the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Additionally, UN humanitarian agencies activated networks for technological and communications support, ensuring secure channels for humanitarian operations, crisis reporting, and the protection of sensitive humanitarian data (Schmitt, 2017).

While limited by political constraints, the UN implemented several specialised digital initiatives focused on governance, humanitarian protection, and cyber-norm development. Through the International Telecommunication Union (ITU), the UN coordinated emergency

restoration missions to stabilise telecommunications infrastructure damaged by cyberattacks and kinetic strikes, deploying mobile network-recovery units and secure emergency communication nodes. The UN Office for Disarmament Affairs (UNODA) facilitated expert dialogues on de-escalation mechanisms, producing technical guidelines on preventing misinterpretation of cyber incidents during armed conflict (Schmitt,2017). The UN Development Programme (UNDP) launched digital-governance resilience projects helping Ukrainian public institutions implement secure data-management frameworks for essential services. Additionally, the UN Human Rights Monitoring Mission used encrypted reporting systems and secure-data routing networks to document cyber-enabled human-rights violations, including online intimidation and targeting of journalists (Schmitt,2017).

These initiatives highlight the UN's role in fostering responsible digital conduct and safeguarding humanitarian operations in hybrid conflict environments (Schmitt, 2017).

4.1.4 Private Sector Actors (Big Tech Companies)

The private sector became a decisive pillar of Ukraine's cyber resilience. The war confirmed that in the digital era, state survival partly depends on partnerships with technology companies-actors whose capabilities often exceed those of governments. Microsoft reported blocking over 200 cyberattacks conducted by Russian GRU-affiliated actors and migrated key Ukrainian government databases to the Azure cloud, ensuring continuity of governance even if physical infrastructure were destroyed (Erendor, 2025). Amazon Web Services (AWS) supported Ukraine by creating secure backups of critical state archives, including historical and bureaucratic records, stored in protected European data centers. This action prevented the potential loss of millions of documents during targeted Russian strikes on state IT systems. Google deployed Project Shield, providing robust DDoS protection to Ukrainian ministries and independent media outlets. The Google Threat Analysis Group additionally exposed large-scale phishing campaigns aimed at Ukrainian and European leadership. Meta and Twitter (pre-2023 policy changes) significantly reduced the reach of Russian automated propaganda networks, removing bot accounts and content farms linked to coordinated influence operations. Their interventions aligned with the findings from EUvsDisinfo (2025), which documented large-scale Russian disinformation efforts presenting fabricated narratives as legitimate news.

These actions occurred alongside the growing militarization of emerging technologies-such as AI-assisted targeting, autonomous threat detection, and augmented reality-based command systems, demonstrating the blurred lines between civilian and military digital infrastructures in modern conflict (Moustakis et al., 2025). Together, the UN and major technology companies constituted a multi-level cyber diplomatic ecosystem that strengthened Ukraine's digital resilience. Their interventions reinforced international norms, countered disinformation, and showcased how cyber diplomacy increasingly relies on hybrid networks of states, international institutions, and private actors. This reflects the future trajectory of conflict,

where kinetic, informational, and digital warfare evolves in tandem with technological innovation (Erendor, 2025).

Beyond these core contributions, private technology companies expanded their operational involvement through advanced cyber-defense, threat-intelligence, and infrastructure-protection measures tailored specifically to wartime conditions. Microsoft's Digital Security Unit supported Ukrainian institutions by deploying real-time threat-hunting teams, enhancing endpoint security with behavioral analytics, and conducting coordinated global takedowns of GRU-linked command-and-control servers. Amazon Web Services introduced automated resilience architectures, enabling rapid failover for essential government platforms and providing quantum-safe encryption prototypes to protect sensitive state records. Google's Mandiant division supplied continuous incident-response coverage and mapped Russian intrusion clusters through forensic reconstruction of attack vectors and malware-lineage tracing. Meta developed advanced detection models identifying coordinated inauthentic behaviour through cross-platform metadata correlation. Twitter (pre-2023) reinforced governmental communications by elevating verified emergency channels and mitigating impersonation efforts targeting Ukrainian officials (Erendor, 2025).

Collectively, these targeted interventions demonstrate how private actors now function as essential cyber-diplomatic agents, providing capabilities and resilience levels previously attainable only by state intelligence structures. In addition, private sector actors played a crucial role in fostering collaboration and knowledge transfer between Ukrainian agencies and international partners. Through joint cyber exercises, threat intelligence sharing platforms, and public-private partnerships, technology companies facilitated the rapid dissemination of best practices in incident response, network hardening, and AI-driven threat detection. These efforts not only strengthened Ukraine's immediate cyber defenses but also contributed to building sustainable institutional capacities. That's why, by integrating corporate expertise into national security frameworks, private actors effectively became strategic partners in cyber diplomacy, demonstrating that resilient governance in the digital age increasingly relies on multi-stakeholder cooperation across public, private, and international domains (Erendror, 2025).

In this way it can be understood that key factor contributing to Ukraine's resilience in cyberspace appears to be the involvement of major American technology companies (Big Tech). These private actors are reshaping the balance of power in the digital domain, as governments increasingly rely on companies whose cyber capabilities are now comparable to, or even exceed, their own. The long-term implications of this commercial dimension of national cybersecurity remain uncertain. Nevertheless, its significance is expected to grow as technologies such as artificial intelligence, quantum computing, and semiconductor manufacturing open new opportunities for emerging actors to assert influence in the cybersecurity arena. Finally, it can be mentioned that further research is needed to fully understand these developments in this modern war (Bassett, 2024).

4.2 Cyber diplomacy and asymmetric strategies in the Russo-Ukrainian war: Lessons and implications for modern warfare

During the Russo-Ukrainian war, especially after Russia's invasion of Ukraine in February 2022, cyber diplomacy emerged as a critical component of the conflict. In this context, various nations and organizations, as presented above, engaged in cyber diplomacy to strengthen Ukraine's defense and counter Russian aggression, utilizing cyber media to influence international relations and conduct strategic communications to shape public perception and policy. An important aspect of cyber diplomacy has been the creation of public-private partnerships to enhance Ukraine's cybersecurity capabilities. The US government, along with private sector entities, provided critical support by sharing information and offering technical assistance. Companies such as Microsoft and Amazon played a key role, providing information on cyber threats and backing up critical data. For example, Microsoft reported helping Ukraine withstand a high rate of catastrophic cyberattacks through endpoint protection measures (Smith, 2022; Tangalakis-Lippert, 2022).

Mueller et al. (2023) explain that international organizations, such as NATO and the European Union, have increased their cyber defense commitments to Ukraine. NATO accepted Ukraine as a contributing participant in its collaborative center of excellence for cyber defense, facilitating knowledge sharing and cooperation to strengthen Ukraine's cybersecurity framework. This cooperation was essential for the development of a national cyber strategy that prepared Ukrainian networks for anticipated cyber-attacks. However, another important dimension of cyber diplomacy involved countering Russian disinformation campaigns. Various governments and organizations worked to expose and counter disinformation spread by Russia, which was trying to undermine support for Ukraine. This was evident in efforts to create narratives framing Russia as a victim of Western aggression, often disseminated through social media platforms. According to Mueller et al. (2023), the global response to cyberattacks and the narrative from Russia included diplomatic efforts to unify international positions against such disinformation actions. Countries coordinated sanctions and public condemnations of Russia's aggressive cyber tactics, putting pressure on Moscow to rethink its strategies.

Marigliano et al. (2024) in their study highlight the ongoing battle between the disinformation campaigns conducted by the Russian state and the counter-narratives developed by Ukraine and its supporters. They also agree that the role of social media has been a critical battleground for controlling narratives and public perception during the Russia-Ukraine conflict. Russia's disinformation strategy often portrays itself as a victim of Western aggression, utilizing platforms such as Twitter to reinforce these narratives through automated bots and trolls. In the context of cyber diplomacy, they also suggest that governments and organizations should be actively involved in countering disinformation by promoting real narratives and strengthening international solidarity. As they explain, this involves not only sharing accurate information, but also understanding the psychological bases of belief and perception that make disinformation

effective. The emergence of social cybersecurity as a field reflects this need, focusing on the interplay between technology and human behavior to safeguard democratic values and political processes. By confronting the complexities of information warfare, stakeholders can work towards a more resilient digital environment that addresses adversarial narratives and supports democratic dialogue. Thus, effective cyber diplomacy requires strategic communication and collective action to mitigate the effects of disinformation campaigns; this has become clear in this contemporary Russia-Ukraine conflict.

An interesting observation is that Russia's cyber operations during the Russo-Ukrainian war showed a distinct pattern compared to its previous conflicts, particularly in terms of severity, targeting and overall effectiveness. Historically, Russian cyber campaigns have focused on espionage, disruption, and information warfare, as seen in previous confrontations with countries such as Estonia and Georgia (Lilly, 2022). However, the conflict in Ukraine revealed a change in both the nature and execution of these operations. In terms of severity, the data collected showed that the cyber incidents attributed to Russia during the Russo-Ukrainian war did not escalate to the levels of devastating cyberattacks, at least to the lengths that analysts expected prior to the invasion. The empirical analysis identified 47 publicly attributed cyber incidents from November 2021 to May 2022 that were characterized primarily by disruptive operations rather than serious degradation of critical infrastructure. The most severe attacks were classified at level 5 on a scale of 0 to 10, indicating a significant but not catastrophic impact (Mueller et al., 2023).

Furthermore, the targeting of Russian cyber operations showed continuity with previous behaviors, focusing primarily on private non-state actors rather than military targets (Morin, 2022). Indeed, Mueller et al. (2023) in their related analysis show that approximately 59.6% of incidents targeted private entities, while only 8.5% were directed at government military actors. This suggests that, despite the intense military context of the Russo-Ukrainian war, Russia's cyber efforts have remained more aligned with harassment and information operations than with seeking to achieve decisive military results through cyber means, a practice Moscow has adopted in recent years as part of its exercise of power (Giles, 2016). Moreover, the overall effectiveness of Russian cyber operations appeared limited, in sharp contrast to previous expectations of a 'surge' strategy that would exploit cyber capabilities for rapid military advantage (Valaitytė, 2024). Analysts of the Russian-Ukrainian war noted that despite an increase in the frequency of cyber intrusions, there was no corresponding increase in severity or shift in targeting patterns. This suggests that Russia has struggled to effectively integrate its cyber capabilities with conventional military operations, leading to a protracted conflict without the expected cyber advantage (Mueller et al., 2023).

According to Forsström (2023), the Russo-Ukrainian war revealed crucial aspects of cyber diplomacy and military strategies. Russia used indirect and asymmetric methods, including advanced cyber tools, to influence the conflict. Despite struggling with inferior

satellite support compared to NATO, Russia's anti-space capabilities, electronic warfare (EW) and cyber operations are designed to disrupt adversary systems and level the operational playing field. These tools have proven instrumental in creating strategic vulnerabilities for Ukraine and its allies, demonstrating the importance of cyber assets in modern conflicts. The war has also highlighted the challenges in managing escalation due to the unpredictability of indirect strategies, which can have serious consequences for both sides. Russia's approach combined the use of economic, information and military tools to create asymmetric advantages, leaving weaker adversaries in a precarious position. Moreover, this conflict underscored the need for integrated, multi-sectoral defense systems among nations that share borders with Russia to deter aggression. In addition, the Russo-Ukrainian war underscored the strategic role of unmanned aerial vehicles (UAVs) and loitering munitions, which, while effective in certain scenarios, are dependent on an adversary's air defense capabilities. Thus, this present conflict has demonstrated that modern warfare is a blend of traditional military operations and advanced cyber, electronic and information strategies, shaping the future of international security dynamics.

4.3 Comparative Analysis of Cyber Diplomacy Strategies

The Russo-Ukrainian war illustrated that cyber diplomacy is not a monolithic sphere but a constellation of strategic approaches that mirror the institutional identities, technological capacities, and geopolitical objectives of the actors involved. NATO, the European Union, the United Nations, and major private-sector technology companies all played decisive yet distinct roles in the cyber dimension of the conflict. These differences highlight how cyber power operates across multiple layers- military, regulatory, legal, and technological- confirming broader scholarly analyses on the co-evolution of warfare and digital transformation (Moustakis, German & Liaropoulos, 2025; Gruszczak & Kaempf, 2023).

NATO embodies a military-operational model of cyber diplomacy, grounded in its collective defense mandate and shaped by the recognition that contemporary conflict increasingly merges kinetic operations with cyber and informational tools. The Alliance’s deployment of cyber rapid reaction teams, enhanced intelligence sharing, and continuous support to Ukrainian cyber defense structures demonstrated NATO’s emphasis on actionable operational capabilities rather than norm entrepreneurship. This model reflects an understanding that AI-enabled systems, autonomous threat detection, and real-time cyber situational awareness now form integral components of modern military planning (Moustakis et al., 2025). Erendor (2025) similarly emphasizes that autonomous defensive systems and AI-supported cyber monitoring constitute key force multipliers in hybrid environments, a dynamic evident in NATO’s assistance to Ukraine. NATO’s actions also implicitly align with the legal framework articulated in the Tallinn Manual 2.0, which affirms state obligations in responding to hostile

cyber operations, particularly those affecting critical infrastructure. Nonetheless, NATO's cyber diplomacy remains fundamentally operational rather than regulatory or legalistic.

The European Union, by contrast, adopts a regulatory, institutional, and financial approach to cyber diplomacy. The EU's strategic identity as a normative power shapes a model that emphasizes digital sovereignty, democratic resilience, and long-term capacity-building. Through mechanisms such as ENISA, the Cybersecurity Act, the NIS2 Directive, and the coordinated cyber rapid response teams, the EU supported Ukraine by strengthening both digital governance structures and administrative cyber readiness. Importantly, the EU also played a critical role in combating Russian information manipulation. EUvsDisinfo (2025) documented extensive disinformation campaigns designed to invert facts and fabricate alternative realities, highlighting the need for cyber diplomacy that integrates information integrity alongside cybersecurity. This reveals the EU's distinct model, based on regulation-driven, institutionally anchored, and deeply intertwined with information-space governance.

The United Nations adopts a third, equally important yet fundamentally different model grounded in legal-political cyber diplomacy. Lacking the operational capacities of NATO or the EU, the UN focuses on norm development, legal interpretation, and global consensus-building. Through the Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG), the UN reaffirmed that existing international law applies fully to cyberspace, consistent with the framework elaborated in the Tallinn Manual 2.0. The UN's approach seeks to prevent escalation by promoting predictability and accountability in state cyber behavior. However, structural constraints, especially Russia's Security Council veto, limited its effectiveness during the war. This dynamic is consistent with broader academic assessments that cyber governance requires multilateral frameworks but is hampered by geopolitical fragmentation. Thus, the UN's cyber diplomacy is characterized by legal norm-building, political dialogue, and sovereignty protection, rather than technical defense (Moustakis et al., 2025).

In addition, the private sector represents a unique model of cyber diplomacy rooted in technological capability and infrastructural dominance. Technology companies possess tools unavailable to states, including global cloud infrastructures, proprietary AI-driven monitoring systems, and real-time threat intelligence networks. Microsoft's disruption of more than 200 GRU-associated cyberattacks, AWS's backup of Ukrainian government archives across secure European cloud nodes, and Google's deployment of Project Shield to prevent large-scale DDoS attacks exemplify how private actors delivered frontline cyber defense at a scale unmatched by public institutions. Meta and Twitter (pre-2023) significantly curtailed Russian automated propaganda networks, aligning with the findings of EUvsDisinfo (2025) regarding industrial-scale manipulation efforts. These interventions reflect broader scholarly analyses on the digitization of the battlefield, where AI, autonomous systems, and augmented reality, enabled infrastructure are reshaping both warfighting and state. The private sector therefore constitutes

a technically indispensable actor whose cyber diplomacy is rapid, global, and innovation-driven resilience (Gruszczak & Kaempf, 2023).

We can understand that the four models, NATO's operational defense, the EU's regulatory and institutional power, the UN's legal-political norm-setting, and the private sector's technological enablement, form a multi-layered cyber diplomatic ecosystem.

Comparative Table: Cyber Diplomacy Strategies

Actor	Core Strategy	Primary Tools	Strengths	Limitations
NATO	Military–operational cyber defense	Rapid Reaction Teams, cyber exercises, threat intelligence	Strong operational capacity; integration with kinetic defense; AI-enabled systems	Limited regulatory and legal mandate
European Union	Normative power & institutional cyber resilience	Regulations (NIS2), ENISA, funding, cloud relocation, counter-disinformation	Strong regulatory influence; long-term capacity-building; digital sovereignty framework	Slower decision-making; limited military role
United Nations	Legal-political multilateral diplomacy	GGE, OEWG, sovereignty norms, confidence-building measures	Norm creation; legitimacy; alignment with Tallinn Manual 2.0	No operational cyber defense; geopolitical constraints
Private Sector	Technical cyber defense & cloud infrastructure	Threat intelligence, cloud backups, DDoS protection, disinformation moderation	Unique technological tools; global infrastructure; rapid response	No formal diplomatic mandate; profit-driven constraints

The Russo-Ukrainian war made clear that no single actor can address the complexity of cyber conflict alone. Instead, modern cyber diplomacy emerges from the intersection of military capability, regulatory governance, international law, and advanced private-sector technology, an evolution consistent with the trajectory of warfare and technological transformation outlined (Moustakis et al. 2025).

4.4 Attribution problem

One of the most persistent and complex challenges in analysing cyber diplomacy during the Russo-Ukrainian war is the attribution problem, which concerns the difficulty of determining, with sufficient technical and political certainty, who is responsible for a cyber operation (Kostyrev, 2023).

Attribution is central to understanding how international organizations such as NATO, the EU and the UN formulate responses, impose consequences, and coordinate collective defence measures. Unlike kinetic attacks, cyber operations are executed through layers of obfuscation, including proxy networks, compromised devices, spoofed IP addresses, and malware designed to mimic the signatures of other threat actors. As a result, even technologically advanced states often struggle to achieve definitive attribution without access to classified intelligence, satellite data, or cross-border investigative capacities (Lin, 2018).

During the Russo-Ukrainian war, Russia's operational doctrine deliberately leveraged ambiguity as a strategic asset. Russian-affiliated advanced persistent threat (APT) groups, such as Sandworm, Fancy Bear (APT28) and Gamaredon, frequently used infrastructures in third countries, deploying false flags and reusing code fragments observed in non-Russian threat clusters. These tactics were designed not only to complicate attribution but also to undermine the credibility of Western intelligence assessments. Because attribution requires a combination of technical forensics, behavioural analysis and geopolitical context evaluation, Russia's ability to blur these indicators hindered rapid and unified responses by international actors. NATO, for instance, must reach political consensus among its members before issuing attribution statements- a process that inherently slows its reaction, especially when evidence cannot be shared publicly due to intelligence sensitivities (Danylenko & Patsyora, 2024)..

The EU faced parallel constraints. Although institutions like ENISA and the EU Intelligence and Situation Centre contributed to forensic evaluations, the Union lacked a centralised political mandate capable of delivering swift, binding attribution. The Cyber Diplomacy Toolbox, established in 2017, provides a framework for joint attribution, yet its implementation depends on voluntary consensus among Member States. In the context of the Russia-Ukraine war, this meant that responses to Russian cyber incidents-ranging from DDoS attacks to destructive wiper malware-sometimes appeared fragmented or delayed. This diffusion of responsibility created opportunities for Russia to deny involvement, frame cyber incidents as internal Ukrainian failures, and foster confusion within the European information space (Valeriano et al, 2018).

For the UN, attribution challenges were even more pronounced. Russia's status as a permanent Security Council member limits the organisation's ability to attribute cyber aggression formally, as any resolution or investigative mandate could be vetoed. Consequently, UN mechanisms remained largely restricted to humanitarian and normative frameworks,

avoiding direct technical accusations that could escalate diplomatic tensions. The lack of universally accepted international rules for cyber attribution-despite attempts by the UN Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG)-further constrained the UN's capacity to address the full spectrum of Russian hybrid tactics (Danylenko & Patsyora, 2024).

Furthermore, the attribution problem affects disinformation ecosystems, which rely heavily on deniable, decentralised content distribution. Meta, Twitter, and Google reported that many Russian influence operations were executed through seemingly unrelated third-party digital marketing networks, bot clusters hosted outside Russia, or compromised private accounts, making attribution of psychological operations even more challenging. The blurred lines between state-sponsored propaganda, freelance cyber-criminal activity, and ideologically motivated troll communities illustrate how attribution extends far beyond malware analysis into the sociotechnical dynamics of online influence (Rid, 2015). Ultimately, the Russo-Ukrainian war demonstrates that attribution remains both a technical challenge and a political battlefield. Inadequate attribution prevents timely countermeasures, enables adversaries to exploit legal grey zones, and undermines collective defence frameworks. As cyber operations grow more complex, international organisations face increasing pressure to develop shared forensic standards, improve intelligence-sharing protocols, and design escalation-aware response mechanisms that do not rely solely on absolute attribution certainty. Finally, it can be mentioned that the war thus highlights the urgent need for global governance models capable of addressing ambiguous, hybrid cyber threats without allowing strategic deniability to paralyse decision-making (Mueller et al., 2023).

5. Conclusions

This study examined the evolving role of cyber diplomacy in times of crisis through a combined theoretical and empirical analysis focusing on the war between Russia and Ukraine as a defining case of contemporary digital conflict. The central objective was to understand how cyber diplomacy operates under conditions of high- intensity geopolitical confrontation and to assess the strategies implemented by international organizations and private actors within a hybrid warfare environment. By integrating theoretical debates on norm- building, deterrence, international law, accountability and governance gaps with a detailed case study, this research provides a structured and evidence-based understanding of cyber diplomacy as both a strategic practice and a governance challenge.

The theoretical part of the paper demonstrated that cyber diplomacy has transitioned from a peripheral diplomatic activity into a core component of international security governance. Literature consistently highlights that cyberspace has become a politicized and contested domain where sovereignty, power projection, and legitimacy are negotiated. Unlike traditional diplomacy, cyber diplomacy operates in an environment characterized by technological acceleration, attribution ambiguity, private sector dominance, and fragmented legal regulation. While mechanisms such as confidence- building measures, transparency initiatives, and multilateral dialogue aim to reduce tensions, the absence of binding and universally accepted international norms leaves cyberspace structurally unstable. The debates surrounding militarization versus cooperation, deterrence versus resilience, and sovereignty versus multistakeholder governance reveal that cyber diplomacy functions within an inherently contested global order.

Against this theoretical background, the case study of the Russo - Ukrainian war provided empirical confirmation of the central argument of this study: cyber diplomacy is not an auxiliary dimension of conflict management but a strategic pillar in contemporary warfare. The war demonstrated that digital infrastructure information integrity and network resilience are as critical as territorial defense. Cyber operations, disinformation campaigns, digital infrastructure protection, and strategic communication were not secondary phenomena but integrated elements of the broader war strategy. The analysis focused on four pillars of intervention: NATO, the European Union, the United Nations, and private sector technology companies. Through comparative examination this study identified distinct models of cyber diplomacy that coexisted and interacted within the same conflict environment.

The first research question asked what forms of cyber diplomacy were employed by international organizations and private sector actors during the Russia- Ukraine conflict. The findings show that cyber diplomacy manifested in four primary forms. First operational cyber defense and rapid incident response mechanisms were activated to protect Ukrainian infrastructure. Second regulatory and institutional resilience strategies were deployed to secure governance continuity and data protection. Third normative and diplomatic efforts sought to preserve dialogue and reinforce responsible state behavior in cyberspace. Fourth infrastructural

and technological interventions by private companies ensured continuity of state functionality and mitigated cyber disruption. These forms of engagement illustrate that cyber diplomacy is multidimensional, combining security, governance, norm-setting, and technological capabilities.

The second research question examined how the strategies and tools differed among NATO, the European Union, the United Nations, and major technology companies. The comparative analysis reveals four distinct strategic models. NATO implemented a security-centered model of cyber diplomacy. Its strategy was anchored in collective defense, deterrence signaling, interoperability, intelligence sharing, and rapid cyber response. Through cyber rapid reaction teams, joint exercises, malware information-sharing platforms, and strategic communication initiatives, NATO reinforced Ukraine's defensive capacity and integrated its cyber resilience within broader Euro-Atlantic security architecture. NATO's model reflects what may be described as defensive-operational cyber diplomacy, where digital resilience is embedded within a deterrence framework. The European Union adopted a regulatory- resilience model of cyber diplomacy. Rather than focusing primarily on deterrence, the EU emphasized digital sovereignty, institutional capacity building, critical infrastructure protection, and norm exporting. By deploying Cyber Rapid Response Teams strengthening ENISA cooperation, facilitating cloud migration of Ukrainian governmental data, and coordinating counter-disinformation initiatives, the EU demonstrated a governance-driven approach. This model illustrates regulatory cyber diplomacy grounded in standards, harmonization, and long-term structural resilience. The United Nations operated through a normative-deliberative model. Although structurally constrained by geopolitical divisions, the UN maintained dialogue platforms and preserved discussions on responsible state behavior in cyberspace. Its contribution was not operational but normative. It functioned as a legitimate arena preventing total breakdown of diplomatic engagement. This model may be described as procedural cyber diplomacy, where the emphasis lies on dialogue maintenance rather than enforcement. The private sector finally, embodied an infrastructural- operational model of cyber diplomacy. Technology companies ensured continuity of Ukrainian governance through secure cloud infrastructure, real-time threat intelligence, malware detection, and platform moderation. The relocation of critical data to resilient cloud systems and the deployment of rapid security updates significantly reduced vulnerability to both kinetic and cyber-attacks. This reveals that contemporary cyber diplomacy cannot be understood through a purely state-centric lens. Corporate actors constitute essential strategic partners in digital crisis management.

The third research question addressed how cyber diplomacy influenced international coordination, cybersecurity resilience, and the mitigation of disinformation. The case study demonstrates that coordinated cyber diplomacy strengthened Ukraine‘s resilience in three decisive ways. First it prevented systemic digital collapse. Despite sustained Russian cyber pressure Ukrainian governance systems remained functional. Second it limited the strategic impact of disinformation campaigns through coordinated counter-narrative mechanisms and platform governance. Third it reinforced alliance cohesion and prevented fragmentation of

Western support structures. In this sense cyber diplomacy acted as a stabilizing multiplier reinforcing both technical and political resilience.

The comparative analysis also demonstrates that Russian cyber operations while disruptive failed to achieve decisive strategic outcomes. Cyber-attacks and information warfare generated pressure but did not collapse Ukrainian governance nor fracture Western unity. This confirms a critical theoretical insight: cyber power functions primarily as a complementary instrument of warfare rather than a decisive substitute for conventional force. The case study thus challenges alarmist narratives that portray cyber operations as inherently decisive weapons. Instead, it shows that their impact depends heavily on the resilience and coordination of the defending side.

From this analysis several lessons emerge for the future of cyber diplomacy. First resilience outweighs retaliation in the cyber domain. The capacity to absorb attacks and rapidly recover proved more effective than escalation-based deterrence. Ukraine's digital survival was not the result of counterattacks alone, but of distributed resilience supported by multilevel cooperation. Second, public- private interdependence is structurally embedded in modern sovereignty. Digital sovereignty no longer implies self-sufficiency. The war revealed that state continuity increasingly depends on privately owned technological infrastructure. Cyber diplomacy must therefore institutionalize structured cooperation with technology companies rather than treat them as auxiliary actors. Third strategic communication and information integrity constitute core security domains. Disinformation is not merely a communication issue but a strategic weapon targeting social cohesion. Cyber diplomacy must therefore integrate narrative governance and digital literacy into security frameworks. Fourth the attribution problem continues to undermine accountability. Even with improved forensic capabilities, political consensus on collective response remains fragile. Without clearer enforcement mechanisms, deterrence credibility remains limited. Fifth the absence of a binding global cyber governance framework remains the most significant structural weakness. Competing models of digital sovereignty and geopolitical polarization hinder consensus. The case study demonstrates that crisis coordination is possible, but long-term normative consolidation remains elusive.

The broader implication of this research concerns the future of cyber diplomacy in an unstable international system. The digital domain is evolving rapidly through artificial intelligence integration, automated cyber operations, quantum encryption developments, and expanded attack surfaces. Simultaneously, geopolitical fragmentation is intensifying. In such an environment, cyber diplomacy faces a dual responsibility: managing immediate crises while contributing to long-term governance stabilization.

Yet a profound structural dilemma persists. Cyberspace lacks satisfactory, enforceable, and universally accepted governance architecture. Unlike traditional domains such as maritime or airspace governance, cyberspace is decentralized, largely privately controlled, and technologically fluid. The absence of binding treaties and effective enforcement mechanisms creates a condition of permanent normative uncertainty. Cyber diplomacy must therefore

operate within an environment where rules are contested and legitimacy is continuously renegotiated.

The Russia-Ukraine war illustrates both the strengths and the fragilities of cyber diplomacy. It demonstrates that coordinated digital intervention can sustain governance continuity, reinforce alliances, and mitigate hybrid aggression. At the same time, it reveals that cyber governance remains incomplete and politically fragmented. The effectiveness of cyber diplomacy depends less on technological superiority and more on cooperative architecture, trust networks, and resilience frameworks.

Ultimately cyber diplomacy has become indispensable to contemporary crisis management. However, its long-term sustainability depends on whether the international community can transcend fragmented and reactive approaches. Without progress toward clearer norms, structured public-private cooperation, and inclusive governance mechanisms, cyberspace risks remaining a domain of perpetual instability. In an era where geopolitical volatility converges with technological acceleration, the future of cyber diplomacy will determine not only digital security but the broader stability of the international order.

References

Allahverdiyeva, N. (2024). Virtual Diplomacy: Digital Communication and Security in International Relations. *Baku State University.* http://dx.doi.org/10.13140/RG.2.2.28227.41767

Aquino, S. B. (2022). Shifting from Kinetic to Cyber: A Cyber Diplomacy Literature Review. *International Journal of Cyber Diplomacy*, *3*, 3-11.

Attatfa, A., Renaud, K., & De Paoli, S. (2020). Cyber diplomacy: A systematic literature review. *Procedia computer science*, *176*, 60-69.

Aydemir, E., & Güner, O. (2023). Crisis Management Policies Concerning the Russo-Ukrainian War in the European Union's Security and Defence Approach: Soft Power and EUAM. *Sosyal Mucit Academic Review*, *4*(2), 189-205.

Barman, C. (2024). Digital diplomacy: the influence of digital platforms on global diplomacy and foreign policy. *Peer-Reviewed, Multidisciplinary & Multilingual Journal*, *3*(1), 61-78.

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

Bassett, L. (2024). Silicon Shadow: The Influence of Big Tech in Russo-Ukrainian Cyber Warfare. *Cambridge Journal of Political Affairs*. 5(1), 70-116

Bechara, F. R., & Schuch, S. B. (2021). Cybersecurity and global regulatory challenges. *Journal of Financial Crime*, *28*(2), 359-374.

Bendiek, A. (2018). The EU as a force for peace in international cyber diplomacy. SSOAR. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-57428-2

Broeders, D., Cristiano, F., & Weggemans, D. (2023). Too close for comfort: cyber terrorism and information security across national policies and international diplomacy. *Studies in Conflict & Terrorism*, *46*(12), 2426-2453.

Buçaj, E., & Idrizaj, K. (2024). The need for cybercrime regulation on a global scale by the international law and cyber convention. *Multidisciplinary Reviews*, *8*(1), 2025024.

Buchan, R. (2015). Cyber espionage and international law. In *Research handbook on international law and cyberspace* (pp. 168-189). Edward Elgar Publishing.

Carrapico, H., & Farrand, B. (2024). Cybersecurity Trends in the European Union: Regulatory Mercantilism and the Digitalisation of Geopolitics. *JCMS: Journal of Common Market Studies*.

Catanzariti, M. (2024). *Disconnecting sovereignty: how data fragmentation reshapes the law* (Vol. 65). Springer Nature.

Charles, J. (2024). *Rethinking diplomacy: how small states can leverage new media for the conduct of diplomacy in the digital age* (Master's thesis, University of Malta).

Chatterjee, C., & Lefcovitch, A. (2016). Cyber security, diplomacy and international law. *Amicus Curiae*, *108*, 2.

Clough, J. (2014). A world of difference: The Budapest convention on Cybercrime and the challenges of Harmonisation. *Monash University Law Review*, *40*(3), 698-736.

Danylenko, S., & Patsyora, Z. (2024). NATO's communication strategies in the context of the russian-ukrainian war. *Actual Problems of International Relations*, *1*(158), 36-42.

Darmayadi, A., Surya, A., & Soares, J. R. (2024). The role of international organizations in handling the humanitarian crisis as a impact of the Russian – Ukrainian war. *Proceeding of International Conference on Business, Economics, Social Sciences, and Humanities*, *7*, 335-347

Davis, P. K. (2014). Deterrence, influence, cyber-attack, and cyberwar. *NYUJ Int'l L. & Pol.*, *47*, 327.

Donaldson, R. H. (2017). The Role of NATO enlargement in the Ukraine crisis. *The soviet and post-soviet review*, *44*(1), 32-52.

Erendor, M. (2025). *Autonomous Weapons Systems and the Future of Warfare. Cybersecurity in the Age of Artificial Intelligence and Autonomous Weapons*. London, UK. CRC Press, Taylor & Francis Group

Eriksson, J., & Giacomello, G. (Eds.). (2007). *International relations and security in the digital age* (Vol. 52). London: Routledge.

EUvsDisinfo. (2025). *Fake fact-checking: when facts are fiction and falsehoods are facts*. https://euvsdisinfo.eu/fake-fact-checking-when-facts-are-fiction-and-falsehoods-are-facts/

Fasinu, E. S., Olaniyan, B. J. T., & Afolaranmi, A. O. (2024). Digital diplomacy in the age of social media: challenges and opportunities for crisis communication. *African Journal of Social Sciences and Humanities Research, 7*(3), 24- 38.

Forsström, P. (2023). Russia's war on Ukraine: strategic and operational designs and implementation. *National Defence University Department of Warfare Series 2: Research Reports No. 29.* https://www.doria.fi/bitstream/handle/10024/187854/Russia%20Seminar%20publication_2023_web_v2(1).pdf?sequence=3

Gamero-Garrido, A. (2014). Cyber conflicts in international relations: Framework and case studies. *Available at SSRN 2427993*.

Gao J X. (2024). Practices and Lessons from Russian Enhancement of Technological Sovereignty Under the Background of Major Country Technological Competition[J*J. Russian, East European, and Central Asian Studies*, 2024(1): 93-114+165

Giles, K. (2016). Russia's 'new'tools for confronting the West: Continuity and innovation in Moscow's exercise of power. *Russia and Eurasia Programme.*

Gruszczak, A. & Kaempf, S. (2023). *Digitizing the battlefield: Augmented and virtual reality applications in warfare*. London, UK. Routledge Handbook of the Future of Warfare

Healey, J. A (2013). Fierce Domain: Conflict in Cyberspace, 1986 to 2012. *Atlantic Council. Cyber Conflict Studies Association.*

Hermawanto, A., & Anggraini, M. (2024). Strengthening Confidence, Security Building Measures (CSBMs) In Southeast Asia: ASEAN in the Post COVID-19 Era. *SINERGI: Journal of Strategic Studies & International Affairs*, *4*(1), 85-98.

Herzog, S. (2017). Ten years after the Estonian cyberattacks: Defense and adaptation in the age of digital insecurity. *Geo. J. Int'l Aff.*, *18*, 67.

Hitchens, T., & Gallagher, N. W. (2019). Building confidence in the Cybersphere: a path to multilateral progress. *Journal of Cyber Policy*, *4*(1), 4-21.

Kim, S. (2014). Cyber security and middle power diplomacy: A network perspective. *The Korean Journal of International Studies*, *12*(2), 323-352.

Kostyrev, A.G. (2023). NATO-Ukraine Strategic Communications: Theory and Practice. *Hileya: Scientific Bulletin/Gileya*.

Lancelot, J. F. (2020). Cyber-diplomacy: cyberwarfare and the rules of engagement. *Journal of Cyber Security Technology*, *4*(4), 240-254.

Lee, H. (2023). Public attribution in the US government: Implications for diplomacy and norms in cyberspace. *Policy Design and Practice*, *6*(2), 198-216.

Lehto, M. (2022). Cyber-attacks against critical infrastructure. In *Cyber security: Critical infrastructure protection* (pp. 3-42). Cham: Springer International Publishing.

Lin, H. (2016). Attribution of Malicious Cyber Incidents: From Soup to Nuts (September 2, 2016). *Columbia Journal of International Affairs, Forthcoming*, Hoover Institution Aegis Paper Series on National Security, Technology, and Law, (2016)

Lewis, J. A. (2002). *Assessing the risks of cyber terrorism, cyber war and other cyber threats* (p. 12). Washington, DC: Center for Strategic & International Studies.

Libicki, M. C. (2012). *Crisis and escalation in cyberspace*. Rand Corporation.

Lilly, B. (2022). *Russian Information Warfare: Assault on Democracies in the Cyber Wild West*. Naval Institute Press.

Maina, C. (2024). Challenges and Opportunities of Digital Diplomacy and Cyberwarfare in Kenya. *Journal of International Relations*, *4*(1), 46-56.

Marigliano, R., Ng, L. H. X., & Carley, K. M. (2024). Analyzing digital propaganda and conflict rhetoric: a study on Russia's bot-driven campaigns and counter-narratives during the Ukraine crisis. *Social Network Analysis and Mining*, *14*(1), 170.

Morin, B. (2022). *Russian Information and Influence Operations: Putin's regime survival tools*. [Master's Thesis, Royal Military College of Canada]

Moustakis, F. German, T. & and Liaropoulos, A. (2025). *Fighting for influence: The promise of Artificial Intelligence*. The Co-evolution of Warfare and Technology, London, UK. Routledge

Mueller, G. B., Jensen, B., Valeriano, B., Maness, R. C., & Macias, J. M. (2023). Cyber Operations during the Russo-Ukrainian War. *Center for Strategic Int. Studies, Washington, DC, USA*.

Mukarzel, R. (2023). *The Russo-Ukrainian war and its transformative impact on European security dynamics: shifting power, emerging challenges, and future implications* (Doctoral dissertation, Notre Dame University-Louaize).

O'Connell, M. E. (2012). Cyber security without cyber war. *Journal of Conflict and Security Law*, *17*(2), 187-209.

Office of the Coordinator for Cyber Issues (2017). https://www.State.gov/s/cyberissues/

Ottis, R. (2008, July). Analysis of the 2007 cyberattacks against Estonia from the information warfare perspective. In *Proceedings of the 7th European Conference on Information Warfare* (p. 163). Reading, MA: Academic Publishing Limited.

Pagovski, Z. Z. (2015). Public Diplomacy of Multilateral Organizations: The Cases of NATO, EU, and ASEAN. *USC Center for Public Diplomacy (CPD)*.

Pawlak, P. (2024). Accountability in cyberspace: the Holy Grail of cyber stability?. *EU Cyber Direct, Policy Brief, 2024, [EU Institute for Security Studies], [Carnegie Endowment for International Peace], [Leiden University]*

Psaila, S. B. (2021, December). *Improving the practice of cyber diplomacy*. DiploFoundation 2021.

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*, 1-51.

Rashica, V. (2018). The benefits and risks of digital diplomacy. *Seeu Review*, *13*(1), 75-89.

Rid, T. (2015). Attributing Cyber Attacks. *Journal of Strategic Studies*, 38(1-2), 4–37

Riordan, S. (2016). Cyber diplomacy vs. digital diplomacy: a terminological distinction. USC CPD Blog (May 12). http://uscpublicdiplomacy.org/blog/cyber-diplomacy-vs-digital-diplomacy-terminological-distinction

Roscini, M. (2014). *Cyber operations and the use of force in international law*. Oxford University Press, USA.

Schia, N. N. (2016). Teach a person how to surf: Cyber security as development assistance. *Norwegian Institute of International Affairs.*

Shackelford, S. J. (2009). From nuclear war to net war: analogizing cyber-attacks in international law. *Berkeley J. Int'l Law*, *27*, 192.

Shvelidze, L., Karavaieva, T., & Tomchakovska, Y. (2024). The Influence of Communicative Strategies in Social Media Discourse on the Development of Communication Conflicts. *International Journal of Religion*, *5*(5), 368-378.

Smith, B. (2022, June 22). *Defending Ukraine: Early Lessons from the Cyber War.* Microsoft, https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-fromthe-cyber-war/

Schmitt M. N. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd ed. Cambridge University Press

Sotiriu, S. (2015). Digital diplomacy: Between promises and reality. In *Digital Diplomacy* (pp. 33-51). Routledge.

Stoltz, M. (2024). Artificial Intelligence in Cybersecurity: Building Resilient Cyber Diplomacy Frameworks. *arXiv preprint arXiv:2411.13585*.

Sukumar, A., Broeders, D., & Kello, M. (2024). The pervasive informality of the international cybersecurity regime: Geopolitics, non-state actors and diplomacy. *Contemporary*

Security Policy, *45*(1), 7-44. Tanczer, L. M., Brass, I., & Carr, M. (2018). CSIRT s and global cybersecurity: How technical experts support science diplomacy. *Global policy*, *9*, 60-66.

Tangalakis-Lippert, K. (2022, December 18). Amazon helped the Ukrainian government and economy using suitcase-sized hard drives brought in over the Polish border: 'You can't take out the cloud with a cruise missile'. *Business Insider.* https://www.businessinsider.com/amazon-saved-the-ukrainian-government-with-suitcase-sized-hard-drives-2022-12

Tiirmaa-Klaar, H. (2013). Cyber diplomacy: Agenda, challenges and mission. *Peacetime Regime for State Activities in Cyberspace*, 509-531.

Tsotniashvili, Z. (2024). Defining the Rules of Engagement: Legal and Ethical Standards in Cyber Conflict. *Journal of Digital Sociohumanities*, *1*(2), 119-132.

ud din Bhat, M. (2023). The Changing Face of International Relations: Adapting to Global Governance Challenges. *Journal of Science & Technology (JST)*, *8*(11), 26-36.

Valaitytė, D. (2024). *Russia's overbalanced behaviour in its full-scale invasion of Ukraine* [Doctoral dissertation, Vytauto Didžiojo Universitetas].

Valeriano, B., Jensen, B., & Maness, R. (2018). *Cyber Strategy: The Evolving Character of Power and Coercion*. Marine Corps UniversityNaval Postgraduate School

Van der Meer, S. (2015). Enhancing international cyber security: A key role for diplomacy. *Security and Human Rights*, *26*(2-4), 193-205.

White, S.P. (2018). Understanding cyberwarfare: lessons from the Russia-Georgia War. *West Point, New York: Modern War Institute at West Point, 20th March,* 1–28.