CYBER DIPLOMACY AND INTERNATIONAL COOPERATION: BUILDING RESILIENCE IN THE DIGITAL AGE

Carola FREY
Strategic Analysis and Cooperation Department, Euro-Atlantic Resilience Centre
52 Vasile Lascăr Street, District 2, Bucharest, Romania
carola.frey@e-arc.ro

Abstract: In an interconnected and digitized world, cyberattacks represent significant threats to national security and global stability. Governments have recognized the importance of resilience in preventing and mitigating the impact of cyber incidents. Cyber diplomacy has emerged as a critical tool in building international cooperation, preventing cyber threats, and as an important way to build cyber resilience. This article explores the role of cyber diplomacy in resilience building, particularly by international cooperation. The paper also examines the challenges facing cyber diplomacy and proposes strategies for enhancing international collaboration and strengthening resilience. It concludes by highlighting several ways to build resilience through the means of cyber diplomacy and international cooperation.
Keywords: Building resilience, International cooperation, Cybersecurity, Diplomacy, Cyber resilience.

INTRODUCTION

The main research objective of the present paper is to investigate how cyber diplomacy can become a tool for enhancing international collaboration and resilience, as a collective effort on the part of all stakeholders involved in the cyber domain. Cyber diplomacy is understood as the practice of using diplomatic efforts to manage and mitigate cyber threats and improve international cyber relations. The definition used is "cyber diplomacy is the art, the science, and the means by which nations, groups, or individuals conduct their affairs in cyberspace, in ways to safeguard their interests and promote their political, economic, cultural or scientific relations, while maintaining peaceful relationships" (EU Cyber Diplomacy Toolbox, n. d.). The underlying principles can be found in the following paragraph: "Cyber diplomacy involves the use of diplomatic tools and initiatives to achieve objectives in the complex and continuously evolving uncharted territory of cyberspace, as described in the national strategy for cyberspace. States use the shared and accepted rules, protocols, and behaviours, to facilitate interactions between global actors of the public and the private sector" (EU Cyber Diplomacy Toolbox, n. d.).

A review of existing literature on cyber diplomacy was conducted which included authored books, academic articles, government reports and analyses made by tink tanks (necessary to identify key topics and debates in the field). The qualitative method was applied, through content analysis of relevant documents and by observing the interactions of stakeholders involved in cyber diplomacy (case studies analysis), which provided insights into how cooperation and resilience were fostered and maintained.

A BRIEF OVERVIEW: A SNAPSHOT OF THE TOPIC AT HAND

21 years ago, the book „Cyber-diplomacy: Managing Foreign Policy in the Twenty-first Century" focused on exploring how diplomacy was evolving in response to the changes brought about by the new global information order (Potter, 2002). However, at that time, despite efforts to explain or define an emerging concept, a lack of understanding surrounding the idea remained pervasive (even with the Melissa Virus and NASA Cyber Attack as incipient incidents). Over time – not very long, the concept of cyber diplomacy came to existence due to the increasing importance of the internet and digital technologies, in both international relations and day-to-day activities. As states and communities became more interconnected online, it also became obvious that traditional forms of diplomacy were not enough to address the challenges and opportunities presented by cyberspace. And of course, much needed to be done in sight of the long line of cyberattacks that came.

16 years ago, the far-reaching cyberattacks on Estonia left a lasting impression and signalled the start of cyber diplomacy. The attacks on Estonia highlighted the vulnerability of countries to cyberattacks and prompted states to implement cybersecurity measures and international formats of cooperation (the NATO Cooperative Cyber Defence Centre of Excellence, and the International Group of Experts that contributed to the Tallinn Manual on the International Law Applicable to Cyber Warfare). The European Union Agency for Cybersecurity, ENISA, was stablished in 2004. To differentiate between traditional diplomacy and cyber diplomacy is simple: the latter is defined by its focus on the cyber dimension as the primary reason for diplomatic engagement (Attatfa, Renaud & De Paoli, 2020).

Skipping forward a few years, enough for the technological leap to be more substantial, cyberattacks became an increasingly common threat, affecting individuals, businesses and governments alike. The result was a tendency towards increased international efforts to tackle the emerging attacks, which led to the need of greater cooperation among different countries and organizations. Some examples are represented by the establishment, in 2015, of the Global Forum on Cyber Expertise – GFCE, with the aim to promote international collaboration on cybersecurity issues and to help countries develop their capabilities in this area (Global Forum on Cyber Expertise, 2015) and by the first Global Cybersecurity Index – GCI. The Global Cybersecurity Index is a trusted reference that measures the commitment of countries to cybersecurity at a global level – to raise awareness of the importance and different dimensions of the issue. As cybersecurity has a broad field of application, cutting across many industries and various sectors, each country's level of development or engagement is assessed along five pillars – (i) Legal Measures, (ii) Technical Measures, (iii) Organizational Measures, (iv) Capacity Development, and (v) Cooperation – and then aggregated into an overall score (International Telecommunication Union, n. d.). Also, in 2015, the U.S. – China Cyber Agreement was signed, that aimed at curbing cyber-enabled economic espionage and promoting cooperation on issues related to cybercrime (Renard, 2018). A similar China – Russia cyber agreement was concluded in the same year.

In 2013, the EU issued the Cybersecurity strategy and, in 2015, it issued the Council conclusions on cyber diplomacy. Furthermore, in 2016, EU Global Strategy (EUGS) demonstrated a clear picture of the objectives and requirements of cyber diplomacy. It emphasizes the need to promote responsible state behaviour in cyberspace by adhering to international law and

establishing agreements. In addition, the EUGS aims to establish a system of multilateral digital governance and a global cooperation framework on cybersecurity through partnerships between countries, organizations, the private sector, civil society, and experts who share its ideology (European Union, 2016). Likewise, between 2014 and 2016, NATO formally acknowledged cyberspace as a significant domain of operations (in addition to the established domains of air, land, and sea). This recognition empowered NATO's military leaders with better tools to protect against cyber threats, by leveraging the cyber capabilities of member nations (North Atlantic Treaty Organization, 2014).

The expansion of cyberspace has brought the lawless nature of the Westphalian international state system into a virtual territory, disrupting the existing global order: "the distinctive feature of cyberspace is that it is a notional environment – beyond the jurisdiction of any single nation" (Cole et al., 2009). In addition, in cyberspace, dominance is not established through physical strength, but rather by a combination of psychological manipulation and technological expertise (Lancelot, 2020). Taking into account these considerations, a question arises: how can a way of conduct be established for the cyber domain when there are no established ethical guidelines for conflict, warfare or general conduct? This query is based on the multifaceted nature of cyberspace, which encompasses domestic politics, international relationships, peer-to-peer connections, acts of war, social media networking, digital currencies, and the challenges of jurisdictional matters concerning cybercrime and nation-state interactions. Diplomacy was the age-old method that provided the solution.

Cyber diplomacy was developing into a standard practice as diplomats engaged in bilateral or multilateral talks with both state and non-state actors (leaders of internet companies, technology entrepreneurs, and civil society organizations), in a variety of contexts. The literature available during that time reveals the following definition: "diplomacy in the cyber domain or, in other words, the use of diplomatic resources and the performance of diplomatic functions to secure national interests with regard to the cyberspace" (Barrinha & Renard, 2017). In the article "Cyber-diplomacy: the making of an international society in the digital age", the authors explain that understanding cooperation in cyber diplomacy requires a comprehensive view on the unique characteristics of cyberspace, such as its global nature and contested environment. The text underlines that, despite these complex challenges, diplomacy is necessary in the development of international norms and values in cyberspace, as cooperation in this realm is considered a choice, not a given (Barrinha & Renard, 2017). In 2016, in the book "The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age" the author argues that states began engaging in interactions and negotiations at different levels (bilateral, regional, international) to regulate this new policy domain (Segal, 2016).

Fast forward a bit more and about 3-4 years ago, the creation of multilateral settings could be witnessed, which not only discussed cyber diplomacy, but within which the practical application of it could be observed. During the second edition of the EU Cyber Forum (2020), Josep Borrell (High Representative of the Union for Foreign Affairs) opened the conference by tackling "Cyber diplomacy and shifting geopolitical landscapes" (The European External Action Service, 2020). In 2021, the UN Security Council had a high-level public meeting on cybersecurity (United Nations, 2021) and the event represented "the first time the Council addressed this issue in a formal setting. By then, differences among Council

members – particularly regarding the right of self-defence and the applicability of international humanitarian law in cyberspace – had become evident through several informal Council meetings on cyber during the previous fifteen months" (Security Council Report, 2022).

Cyber resilience emerged as a crucial issue that was (and is) consistently addressed at the international level, that went hand-in-hand with cybersecurity. The concept refers to "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks or compromises on systems that use or are enabled by cyber resources" (Petrenko, 2019) and "brings business continuity, information systems security and organizational resilience together. That is to say, the concept describes the ability to continue delivering intended outcomes despite experiencing challenging cyber events, such as cyberattacks, natural disasters or economic slumps" (International Business Machines, n. d.). A definition from the private sector is intentionally utilized. Yet, as per certain authors viewpoint, the concept remains elusive and difficult to implement, despite its theoretical appeal and the desire of some actors to implement it (Dupont, 2019).

A comprehensive insight on cyber resilience can be found in "Making cyber security more resilient: adding social considerations to technological fixes". The article highlights the importance of interdisciplinary research to understand the dynamic and complex interaction between different sub-systems, and suggests that insights from social-ecological resilience research could be helpful in fostering such an approach. The article also emphasizes the need for a public debate on the normative desirability of resilience and cyber resilience, and suggests that society should engage in a transparent negotiation process to facilitate how technologies are used (Dunn Cavelty et al., 2023).

Cyber resilience is further addressed in the paper "Preparing for future cyber crises: lessons from governance of the coronavirus pandemic". In section 2, it is mentioned that "broadly speaking *[cyber resilience]* is a new term that aims to borrow from learning around resilience. It was coined to emphasize the importance of an organizational strategy to be able to prepare, absorb, recover, and adapt from cyber events" (Mott, Nurse & Baker-Beall, 2023). This approach will enable us to comprehend the concept of resilience in the cyber domain in the following section.

THE CHALLENGES FACING CYBER DIPLOMACY

To focus on the subject matter being discussed in this paper, cyber diplomacy can become a tool to bolster resilience. Firstly, cyber diplomacy can be used to create, foster or strengthen international collaboration. One of the most significant challenges is that different states, or other actors with influence, have different perspectives on issues such as cybersecurity, cyber defence, data privacy, and sovereignty (just to name a few). To reconcile different viewpoints, codes of conduct (CoC) for the cyber space were formulated and envisaged. Such CoCs desire to be ethical guidelines that aim to ensure proper behaviour and responsible conduct. In a sense, such codes (whether they are voluntary codes, laws, or regulations) are essential for moulding the expansive realm of the cyber domain. However, in the cyberspace, any code of conduct can be faced with some limitations. They may be hard to enforce, especially if they are voluntary. Not every actor will adhere to the guidelines, and some may engage in unethical behaviour, regardless of the code of conduct. Additionally, the nature of the cyberspace can

make it challenging to enforce these guidelines across different countries with varying laws. Moreover, their effectiveness is dependent on how they are enforced and how well they adapt to new technologies and emerging issues.

Promoting and reinforcing (to some extent) any code of conduct in cyberspace can be done by means of cyber diplomacy and it will comprise a multifaceted approach that will require cooperation between relevant stakeholders. There are a series of strategies that can be put in action, such as:

- the creation of international agreements, treaties or regulations: states can work together to develop and sign treaties and agreements that outline acceptable behaviour and standards in cyberspace. These agreements can include provisions for preventing cyberattacks, protecting critical infrastructure, and respecting privacy.
- the capacity building and technical assistance: developed countries can offer assistance and provide technical expertise to developing countries to help them improve their cybersecurity practices. Developing and implementing cybersecurity policies and procedures, and training personnel in best cybersecurity practices comes as a package deal.
- the cybersecurity awareness and education: diplomatic efforts can focus on raising awareness and educating individuals and organizations on the importance of cybersecurity. This can include public campaigns, workshops, and training programs to promote safe and responsible use of technology.
- the multilateral diplomatic engagement: the emphasis could be on bringing together multiple stakeholders to discuss and address cybersecurity challenges and their willingness to adhere to a specific CoC, tailored to the needs of all sides involved.

Overall, promoting and reinforcing a code of conduct in cyberspace through cyber diplomacy requires a collaborative, multilateral approach that prioritizes cooperation and education.

Regarding resilience, the challenge is to build a recovery mechanism against dangerous cyber incidents, which can take many forms, including hacking, cybercrime, and cyber warfare. Cyber diplomacy can strengthen resilience in several ways. Firstly, by promoting international cooperation, it can foster collaboration between stakeholders and create a common approach in dealing with challenges and threats posed by cyberattacks. Thus, in the case of states, they can better respond to cyberattacks and mitigate the risks and impacts of potential incidents, ultimately ensuring greater stability and security in the digital sphere.

Secondly, through cyber diplomacy, shared norms and standards for responsible cyber behaviour can be developed, such as mutual assistance in the event of a cyberattack and respect for the privacy and security of cyberspace. Thirdly, cyber diplomacy can support the building of technical expertise and capacity in countries to respond to cyberattacks, including improving computer and network security, incident response mechanisms and increasing cybersecurity awareness. Lastly, using the resources of cyber diplomacy, advancements in international law could lead to the creation of a legal framework (on the long term).

To get the edge on addressing cyberattacks and to strengthen resilience, an important approach is to foster constructive, ongoing relationships between the public and private sectors. Cyber

diplomacy could represent the binder. A public-private partnership can help drive innovation in cybersecurity and promote more effective cooperation in addressing cyber incidents, as it enhances the sharing of expertise and best practices.

Cyber diplomacy faces several challenges that can hinder its effectiveness in addressing cyber threats and promoting international cooperation. They can be seen in Table 1.

Table 1. Challenges and solutions in cyber diplomacy

	Challenge	Solutions
1.	Divergent perspectives: diverse perspectives among states and other influential actors regarding cybersecurity, cyber defence, data privacy, and sovereignty.	1. Creating a platform for discussions and negotiations, so as to identify a common ground and reach compromises; 2. Establishing common goals: Underlining the importance of shared goals and objectives can help bridge the gap between different perspectives. By focusing on overarching goals such as ensuring cybersecurity, protecting critical infrastructure, and protecting privacy, stakeholders can find common ground and work toward mutually beneficial outcomes; 3. Enhancing cyber awareness and education.
2.	Partial enforcement: Enforcing codes of conduct and international agreements in cyberspace can be challenging, especially when they are voluntary. Not all actors may adhere to the guidelines, and some may engage in unethical behaviour, despite the established norms.	1. Implementing accountability mechanisms – essential to enforce codes of conduct and agreements (monitoring, verification, and reporting mechanisms); 2. Enhancing cybersecurity capabilities; 3. Promoting awareness and norm internalization; 4. Strengthening international legal frameworks.
3.	National legal frameworks: Due to the existence of different legal systems and national laws across countries, enforcing guidelines and regulations consistently across borders becomes challenging, as different countries may have varying levels of cybersecurity regulations and enforcement capabilities.	1. Enhanced international cooperation (forums, platforms for dialogue and information sharing); 2. Mutual Legal Assistance Treaties (MLATs); 3. Regional harmonization aligning legal frameworks to ensure consistent approaches to cybercrime, data protection, and other relevant aspects of cybersecurity. 4. Private-public partnerships.
4.	Emerging technologies	1. Monitoring and analysis in order to create updates and assessments on the potential implications and associated risks; 2. Flexibility and adaptability: Embrace a flexible and adaptable approach to cyber diplomacy, acknowledging that the cyber landscape evolves rapidly. This includes regularly updating and revising existing frameworks, codes of conduct, and international agreements to incorporate new technological developments and emerging issues.

STRATEGIES FOR ENHANCING INTERNATIONAL COLLABORATION AND STRENGTHENING RESILIENCE

Resilience is a critical component of individual, national and international strength. Cyber threats have become one of the most significant challenges to resilience. Cyberattacks can paralyze critical infrastructure, disrupt trade and economy, and cause massive damage and loss of life. The rise of new technologies and global connectivity makes cyber threats increasingly complex and difficult to address for any nation or organization. Thus, building resilience requires collaboration and dialogue between nations to develop effective cybersecurity policies and strategies. In addition, there is a need for foreign policy institutions to establish and enhance their functions towards cybersecurity. These institutions can contribute to the development of a secure cyber ecosystem and encourage international cooperation in cybersecurity, while offering a united front to protect against cyber threats.

Cyber diplomacy, through international cooperation, can help build resilience in several ways. Firstly, it allows nations to share knowledge and experience on best practices and lessons learned. By working together, nations can leverage each other's expertise to build more robust systems and develop response plans for cyber incidents.

Secondly, international cooperation enables states to engage in joint exercises and simulations to test and refine their response capabilities. By practicing response scenarios with multiple stakeholders involved (through a whole-of-society approach), nations can identify weaknesses and enhance their resilience against potential threats.

Thirdly, through cooperation and diplomatic channels, states and organizations can facilitate the development of common standards and regulations for cybersecurity. Such standards can help harmonize regulations across jurisdictions and enhance interoperability between national systems, promoting resilience across borders.

Lastly, cyber diplomacy is a way through which states can build trust and confidence. Trust is essential to enable information-sharing and coordinated action in response to cyber incidents. With trust established, nations can collaborate effectively to build resilience against cyber threats.

CONCLUSION

As technologies advance and new cyber threats emerge, the need for effective cyber diplomacy will increase. By adapting to evolving challenges, embracing new technologies, and fostering ongoing cooperation, cyber diplomacy can continue to play a key role in securing the digital domain.

Moreover, the multifaceted approach of cyber diplomacy, which includes international agreements, capacity building, cybersecurity awareness, and multilateral engagement, provides a comprehensive framework for addressing cyber threats and building resilience. The establishment of international treaties and agreements provides a basis for defining acceptable behaviour and standards in cyberspace, promoting responsible actions, and protecting critical infrastructure. Capacity-building and technical assistance initiatives enable countries to improve their cybersecurity practices, strengthen incident response mechanisms, and raise awareness of cyber risks.

In addition, cyber diplomacy's emphasis on cybersecurity awareness and education is critical to fostering a cyber resilient society. By raising awareness among individuals and organizations about the importance of cybersecurity, promoting the safe and responsible use of technology, and offering training programs, cyber diplomacy can contribute to attain the objective of a more informed and prepared population.

Multilateral diplomatic engagement plays a critical role in the effectiveness of cyber diplomacy. By bringing together diverse stakeholders, including governments, private sector entities, and civil society organizations, to discuss and address cybersecurity challenges, a collaborative approach can be fostered. This collaborative spirit encourages cooperation, knowledge sharing, and the development of tailored codes of conduct that address the needs and perspectives of all stakeholders.

Ultimately, the evolution of cyber diplomacy reflects its growing recognition as a critical component of global governance in the digital age. As cyber threats continue to evolve, cyber diplomacy must adapt and evolve with them. By continuously refining strategies, fostering international cooperation, and harnessing the power of public-private partnerships, cyber diplomacy can effectively respond to cyber incidents, mitigate risks, and promote a resilient cyber landscape.

Building resilience requires collaboration and dialogue among nations, supported by foreign policy institutions that focus also on cybersecurity. Cyber diplomacy plays a crucial role in this process. It enables the sharing of knowledge and best practices, facilitates joint exercises to improve response capabilities, promotes the development of common cybersecurity standards and regulations, and fosters trust and confidence among states. By leveraging these strategies, nations can enhance resilience and effectively combat cyber threats.

REFERENCE LIST

Attatfa, A., Renaud, K. & De Paoli, S. (2020) Cyber Diplomacy: A Systematic Literature Review. *Procedia Computer Science*. 176, 60-69. doi: 10.1016/j.procs.2020.08.007.

Barrinha, A. & Renard, T. (2017) Cyber-diplomacy: the making of an international society in the digital age. *Global Affairs*. 3(4-5), 353-364. doi: 10.1080/23340460.2017.1414924.

Cole, A., Drew, P., McLaughlin, R. & Mandsager, D. (2009) *Sanremo Handbook of Rules of Engagement*. Sanremo, Italy, International Institute of Humanitarian Law.

Dunn Cavelty, M., Eriksen, C. & Scharte, B. (2023) Making cyber security more resilient: adding social considerations to technological fixes. *Journal of Risk Research*. doi: 10.1080/13669877.2023.2208146.

Dupont, B. (2019) The Cyber-Resilience of Financial Institutions: Significance and Applicability. *Journal of Cybersecurity*. 5(1), tyz013. doi: 10.1093/cybsec/tyz013.

EU Cyber Diplomacy Toolbox. (n. d.) *What is cyber diplomacy?*. https://www.cyber-diplomacy-toolbox.com/Cyber_Diplomacy.html [Accessed 19th June 2023].

European Union. (2016) *Shared Vision, Common Action: A Stronger Europe*. https://op.europa.eu/en/publication-detail/-/publication/3eaae2cf-9ac5-11e6-868c-01aa75ed71a1 [Accessed 19th June 2023].

Global Forum on Cyber Expertise. (16 April 2015) *The Hague Declaration on the GFCE. Launch of the Global Forum on Cyber Expertise*. https://thegfce.org/wp-content/uploads/2020/04/the-hague-declaration-on-the-gfce.pdf [Accessed 19th June 2023].

International Business Machines. (n. d.) *Cyber resilience defined*. https://www.ibm.com/topics/cyber-resilience [Accessed 19th June 2023].

International Telecommunication Union. (n. d.) The Global Cybersecurity Index (GCI). https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx [Accessed 19th June 2023].

Lancelot, J. F. (2020) Cyber-diplomacy: cyberwarfare and the rules of engagement. *Journal of Cyber Security Technology*. 4(4), 240-254. doi: 10.1080/23742917.2020.1798155.

Mott, G., Nurse, J. R. C. & Baker-Beall, C. (2023) Preparing for future cyber crises: lessons from governance of the coronavirus pandemic. *Policy Design and Practice*. 6(2), 160-181. doi: 10.1080/25741292.2023.2205764.

North Atlantic Treaty Organization. (2014) *Wales Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales*. https://www.europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede240914walessummit_/sede240914walessummit_en.pdf [Accessed 19th June 2023].

Petrenko, S. (2019) *Cyber Resilience, River Publishers Series in Security and Digital Forensics*. ⁋ Nordjylland, Denmark, River Publishers.

Potter, E. H. (ed.). (2002) *Cyber-Diplomacy: Managing Foreign Policy in the Twenty-first Century*. Montreal, McGill-Queen's University Press.

Renard, T. (2018) EU cyber partnerships: assessing the EU strategic partnerships with third countries in the cyber domain. *European Politics and Society*. 19(3), 321-337. doi: 10.1080/23745118.2018.1430720.

Security Council Report. (31 January 2022) *In Hindsight: The Security Council and Cyber Threats, an Update*. https://www.securitycouncilreport.org/monthly-forecast/2022-02/in-hindsight-the-security-council-and-cyber-threats-an-update.php [Accessed 19th June 2023].

Segal, A. (2016) *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*. New York, PublicAffairs.

The European External Action Service. (14 September 2020) *Cyber diplomacy and shifting geopolitical landscapes*. https://www.eeas.europa.eu/eeas/cyber-diplomacy-and-shifting-geopolitical-landscapes_en [Accessed 19th June 2023].

United Nations. (29 June 2021) *'Explosive' Growth of Digital Technologies Creating New Potential for Conflict, Disarmament Chief Tells Security Council in First-Ever Debate on Cyberthreats*. https://press.un.org/en/2021/sc14563.doc.htm [Accessed 19th June 2023].

Carola FREY

Is an expert with deep knowledge and hands-on experience within the Strategic Analysis and Cooperation Department of the Euro-Atlantic Resilience Centre. She specializes in conflict analysis, futures studies, and emerging and disruptive technologies.

She has solid experience in the government sector, with previous employment in the Romanian Ministry of Defence, Ministry of Foreign Affairs, and Ministry of Research, Innovation and Digitalization. In addition, Carola Frey has been active in academia since 2014, publishing numerous articles and participating in national and international conferences and workshops. From 2021, she is a PhD Candidate with a thesis that aims to investigate China's foreign policy in the new world order using futures studies methods.

Carola is part of the Community of Interest Emerging and Disruptive Technologies.