Cyber Diplomacy: A New Frontier for Global Cooperation in the Digital Age

Ioana-Cristina VASILOIU
Bucharest University of Economic Studies, Romania
ioana.vasiloiu@csie.ase.ro

As the world evolves, becoming increasingly interconnected through digital technologies, there is a growing need for global collaboration in addressing the challenges of cyberspace. Cyber diplomacy, the use of diplomatic means to manage international relations in cyberspace, is emerging as a new field of international relations. With the advancement of cybercrime, cyberspace actors – governments, organizations, corporations, the private sector, and civil society need to collaborate, negotiate and develop cyber capabilities to ensure a safe digital space through cyber diplomacy. The article outlines the current state of cyberspace and critical threats to global security and stability, examining cybercrime, state-sponsored cyberattacks, cyberespionage, cyberterrorism, and trends in cybercrime. It focuses on the concept of cyber diplomacy and its expansion as a field of international relations, noting key developments that have contributed to this aspect. At the same time, the role of cyber diplomacy in shaping global norms, standards, and regulations for cyberspace is mentioned, and the potential advantages of better international cooperation in this field are explored.

Keywords: *Cyber diplomacy, Cyberspace, Cybercrime, Information and Communication Technology, Cyber-attacks*
DOI: 10.24818/issn14531305/27.1.2023.02

1 Introduction

The Internet and digital technologies have changed the world, connecting people and companies across the globe and facilitating the creation of new industries. However, this change has led to the emergence of new threats and challenges to global security and stability. The evolution of cyberspace has led to the development of new forms of conflict, including cyberespionage, cybercrime, and hacktivism (Barrinha & Renard, 2017). And new threats have driven a need to improve international cooperation to manage these challenges and ensure the security and stability of the digital world.

Conventional diplomacy has the role of generating common advantages through dialogue, a role that will translate into the generation of such benefits on the issue of cybersecurity: Internet governance, response to malicious attacks, law enforcement against cybercrimes, critical infrastructures protection etc. To ensure a secure digital space through cyber diplomacy, cyber actors – governments, organizations, corporations, the private sector, and civil society- must collaborate, negotiate and develop cyber capabilities.

This article aims to analyze the current state of cyberspace and critical security threats by examining cybercrime, state-sponsored cyberattacks, cyberespionage, cyberterrorism, and trends in cybercrime.

After establishing the frame of reference, the concept of cyber diplomacy will be discussed, specifying its characteristics. At the same time, the expansion of cyber diplomacy as a field of international relations is also presented, noting the key developments that have contributed to this aspect.

The last chapter highlights the role of cyber diplomacy in shaping international norms, standards, and regulations of cyberspace, the legal frameworks of cyber diplomacy being in full evolution and expansion. Finally, the main conclusions are presented, and specific directions for future scientific research are identified.

2 The current state of cyberspace and critical threats to global security and stability

"Cyberspace is a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies." (Kuehl, 2009). The development of contemporary computing technology has allowed people to enter the brilliant information age, but the internal security deficiencies of computing technology bring uncertain risks and threats. (Wu, 2022) At the same time, the global digital transformation and the expansion of information and communication technology (ICT) have led to increasingly significant use of the Internet (Eriksson and Giacomello, 2022).

So, an accelerated digitization process inevitably brings challenges in terms of cyber security (Fischer-Hübner et al., 2021). As the number of threats increases, fighting cybercrime requires the collective responsibility of society (Ho et al., 2022) and the coordination of forces at the level of individuals, organizations, or states, using the necessary tools to connect better and to create more confidence.

2.1 Cybercrime "consists of criminal acts committed online by using electronic communications networks and information systems" (European Commission, 2007). In 2022, ENISA (European Union Agency for Cybersecurity) described the main threats as ransomware, malware, social engineering, data threats, Denial of Service or Internet availability threats, disinformation, and supply chain attacks.

According to statista.com, by December 2022, 39% of internet users globally have suffered from cybercrime. Most attacks occurred in India – 68%, followed by the United States – 49% and Australia – 40% (figure 1).

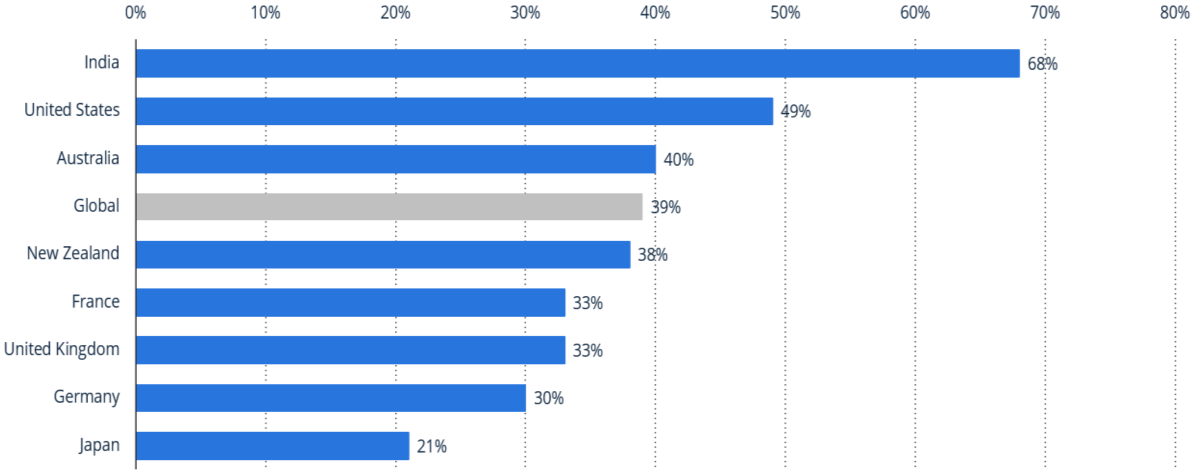

Fig. 1. Percentage of internet users who have ever experienced cybercrime by December 2022, Statista 2022

In Threat Landscape 2022, ENISA defined different types of motivations for cyber-attacks (figure 2):

- Financial: any action through which financial benefits are pursued;
- Geopolitics/Espionage: obtaining information about intellectual property, sensitive data, or classified data (state-sponsored groups);
- Geopolitics/Disruption: any disruptive action done in the name of geopolitics (state-sponsored groups);
- Ideological: any action based on an ideology (example: hacktivism).

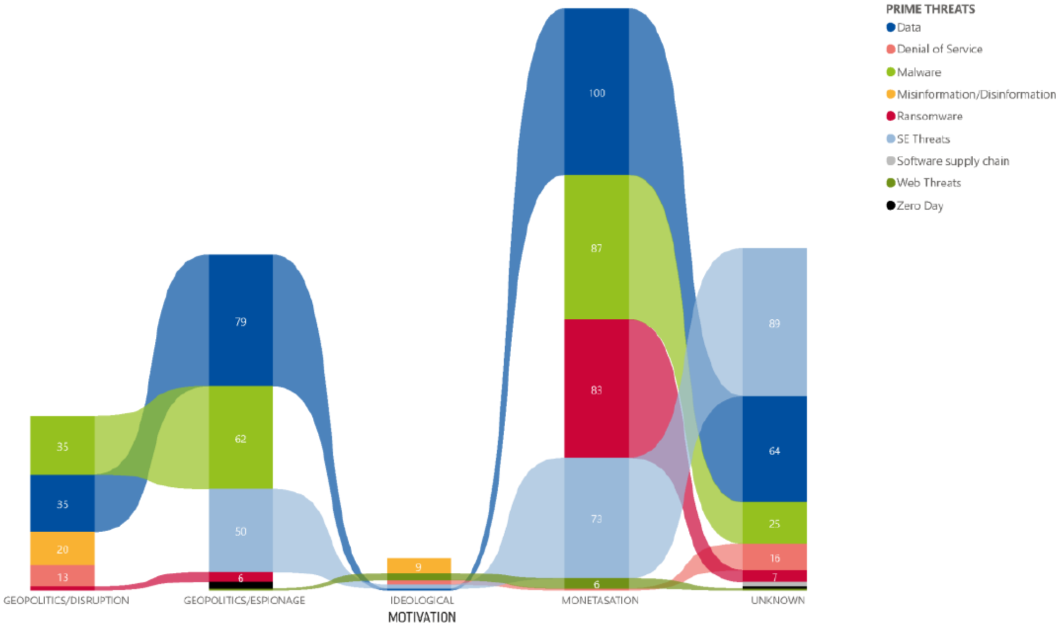

Fig. 2. Motivations for cyber-attacks by threat, ENISA 2022

Regarding the cost of cybercrime globally, for the year 2022, it has been estimated at $8.4 trillion. Considering the growth rate of cyber-attacks, for 2023, the cost is estimated at 11.5 trillion dollars, and in 2027 it will reach 23.84 trillion, an amount three times higher than in 2022 (figure 3).

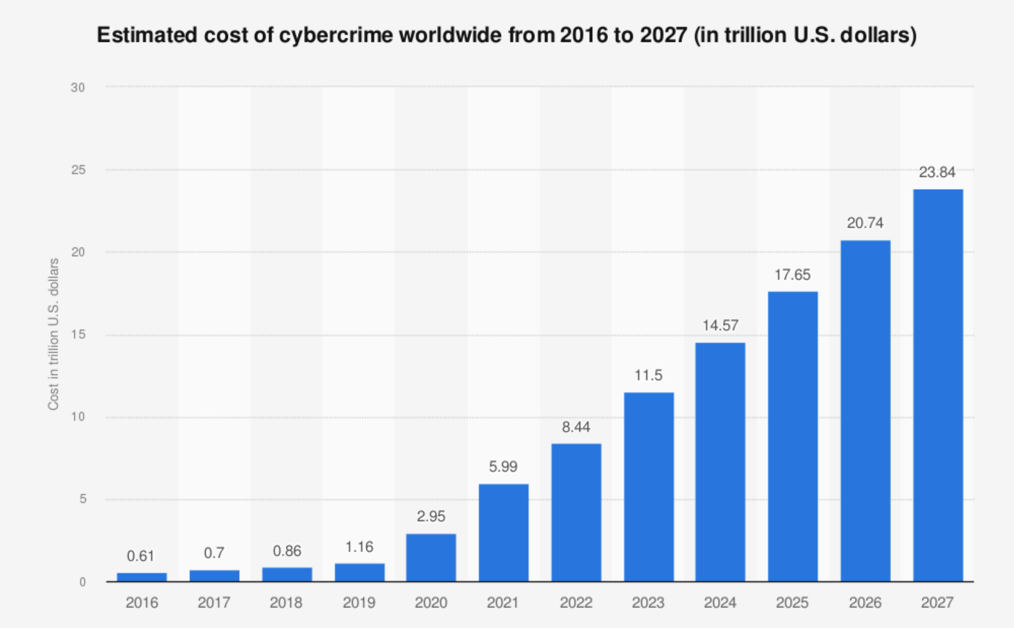

Fig. 3. Estimated costs of cybercrime globally 2016-2027, Statista, 2022

2.2 State-sponsored cyber-attacks are conducted to extract classified information, disrupt critical infrastructure, jam military systems, and shake the foundations of other countries' democracies through propaganda or disinformation (Osawa, 2017). In a 2017 study, Osawa distinguishes five types of these attacks:

- Cyber espionage: obtaining confidential, secret, or intellectual property information;

- Cyber sabotage: temporarily paralyzing servers or the network through a massive volume of data traffic;
- Cyber subversion: disrupting the function of the computer network, including critical infrastructure, by deleting or manipulating data;
- Propaganda/Cyber Manipulation: undermining or manipulating public opinion through cyber media propaganda or fake news;
- Military Cyber Attack (Hybrid Cyber Warfare): Disruption or destruction of military cyber assets or critical infrastructure.

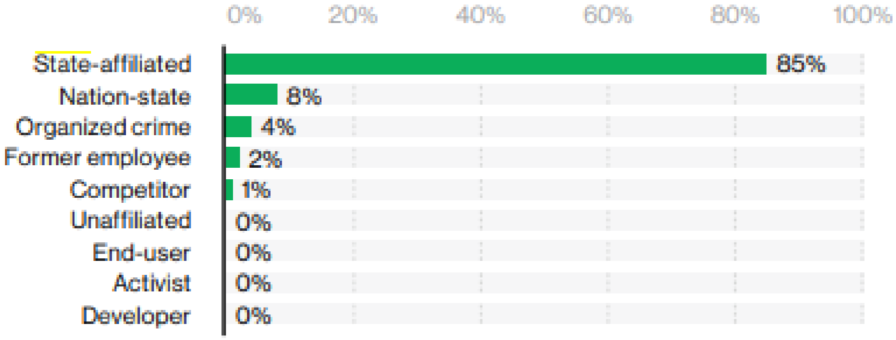

Fig. 4. Actors Involved in Cyber Espionage, Verizon 2020

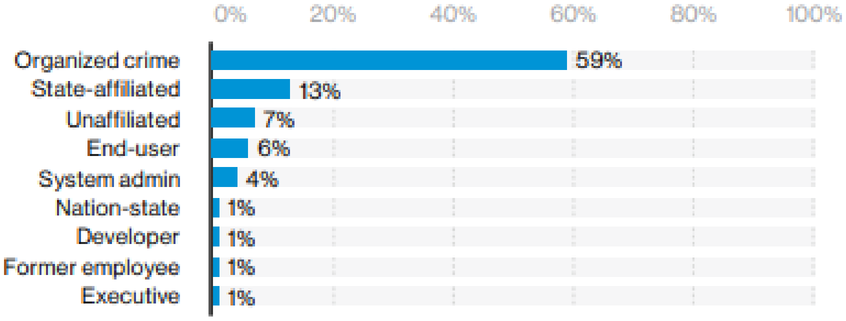

Fig. 5. Actors Involved in Cyber Attacks, Verizon 2020

A study conducted by Verizon between 2014 and 2020 confirms what also emerges from the abovementioned ENISA report: state-sponsored groups are the most critical actors in cyber espionage (figures 4, 5).

2.3 Cyber espionage, according to Freet and Agrawal (2017), is the act of obtaining personal/sensitive information or intellectual property from individuals without their knowledge or consent.

In 2020, the same Verizon produced a report on this topic, in which the percentage of compromise on different types of data was analyzed: credentials were compromised by a percentage of 56%, secret - 49%, internal - 12%, classified - 7%, banking, source code and digital certificates – 6% (figure 6).

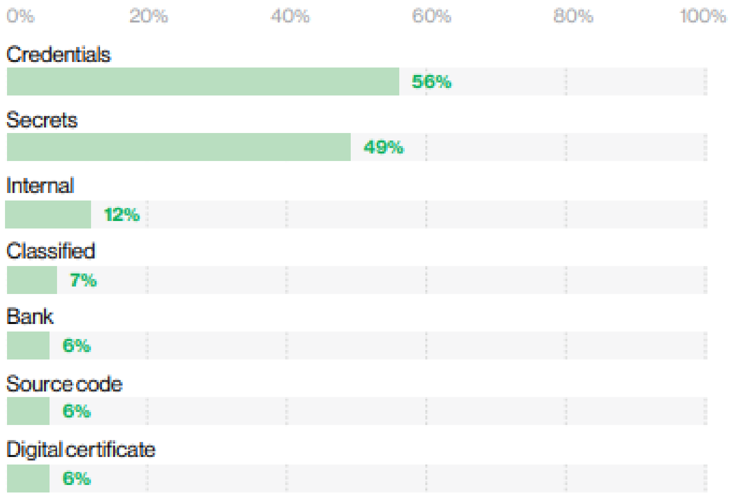

Fig. 6. The percentage of compromise on different types of data, Verizon 2020

Another important study that needs to be mentioned is the 2022 study by Härting et al., which found that employees are the main gateway to industrial espionage. So awareness through professional training is essential. Another conclusion of the study was that management must be informed about the importance of security measures in IT in order to apply the necessary actions.

2.4 Cyberterrorism can have the same results and use the same methods as regular cyber-attacks, but the motivation differs. In the case of terrorist attacks, it is desired to destabilize some institutions or some countries or intimidate the population (Jerman-Blazic & Klobucar, 2016). Kijewski et al., in 2016, identified three forms of activities that may fall under the scope of cyber terrorism:

- Terrorist cyber-attacks, which have political-ideological, ethnic, and/or religious motivation and for which electronic means are used with the aim of committing attacks that can cause tremendous damage, endangering the security of the state;
- Cyber terrorism carried out by terrorists, from the deformation of websites to the disruption of the functionality of certain services and infrastructures, aiming to disrupt society's organization;
- The use of the Internet by terrorists for propaganda, indoctrination, radicalization, financing, planning, communication, and recruitment.

2.5 Trends in cybercrime. Koops, in 2016, discussed six significant trends in cybercrime:

- **The Internet as the Infrastructure of Everything** – after communications, media and entertainment, today, even education, work, healthcare, and transportation, all sectors of society need the Internet to facilitate daily processes, leaving society vulnerable to cyber attacks.
- **Autonomic Technologies** – ICT exists in any technological application, including bio-, nano-, neuro-, and robo- type applications. Thus, ICT vulnerabilities or those caused by ICT become threats to all applications that both individuals and organizations use.
- **Datafication of Everything** – almost anything can be translated and reduced to data. Datafication refers to the fact that there are vast amounts of information about individuals and organizations that can not only be mined for profit but can be abused for criminal or terrorist purposes. In addition, there are new risks of statistical or algorithm-based decisions, decisions that no human can understand the rationale for.
- **The Onlife World** – people move in physical space and in cyberspace at the same time. This is a simple example of the merging of online and offline life, described by the term onlife. The

emergence of such a society has crucial implications for how people behave and interact and also for how they are vulnerable to cybercrime.

- **The Transformation of Crime and Terrorism** – as society transforms into an onlife one, there are critical implications for how cybercrime and terrorism are carried out. Offline crime policies and measures must also consider digital technologies, as can happen in cyberspace, where the physical component of threats must be taken into account.
- **The Fourth Generation of Cybercrime: Attacks on IoT and IoP** – the forms of attacks on the Internet of Things (IoT) and the Internet of People (IoP) will be approximately the same as the known ones (hacking, data interference, interference with system, interception of communications), but the impact will be different. It is difficult to estimate the degree of fear that may be induced by attacks on vehicles, pacemakers, or bionic limbs, as these would directly affect people's physical security.

To develop collective cybersecurity, like-minded countries must strengthen information protection through partnerships, training programs, awareness campaigns, exchange of best practices, and international agreements.

3 The concept of cyber diplomacy and its extension as a field of international relations

According to the previous chapter, crime, espionage, sabotage, subversion, propaganda, and military attack have become cybernetic today, and all these topics are the field on which political battles are fought, this field being represented by cyberspace. Since this space was politicized, the appearance of diplomats was needed. Thus, although it was initially an area only for technical discussions between ICT specialists, the role of diplomacy in cyberspace is indisputable and is always present in the media (Barrinha & Renard, 2017).

3.1 Cyber diplomacy concept

Cyber diplomacy can be seen as a symptom of more extensive changes in the evolving methods of diplomacy (Potter, 2002). Given traditional diplomacy's role in generating common advantages through dialogue, cyber diplomacy involves using diplomatic tools to resolve conflict situations that arise in cyberspace (cybersecurity, cybercrime, and cyberterrorism). (Pierini, 2016)

Cyber diplomacy can be described as the latest stage, a particularly important stage, of the progressive change in the role of diplomacy in the digital age (Barrinha & Renard, 2017). Georgescu (2022) defined this new type of diplomacy as a natural tool for the coordination and collective action of sovereign actors with at least partially divergent interests.

Kumar (2022) states that cyber diplomacy, through negotiations, helps to avoid the escalation of a conflict and reduces the gaps between nations during a cyber war or during the conduct of cyber-attacks. At the same time, it defines the term as an infusion of modern technology and conventional diplomacy, thus appearing as a suitable tool for the future.

Barrinha and Renard (2017) state that cyber diplomacy can be implemented in whole or in part by diplomats, in bilateral formats or multilateral forums. In addition to conventional diplomacy, cyber diplomacy also involves non-state actors, leaders of Internet companies, ICT entrepreneurs, or civil society representatives.

Riordan (2019) argues that it is not enough for an international actor to rely only on technical solutions to solve the problems of governance, security, crime, and espionage that arise in cyberspace, and cyber diplomacy is needed to complement them. Moreover, cyber diplomacy must introduce norms and rules through which cyberspace acquires a degree of stability and predictability.

In cyberspace, diplomacy is a strategic function that manages risk by solving the problem of attributing or disclosing a cyber-attack, much like a detective tactfully solving a crime (Lancelot, 2020).

Tiirmaa-Klaar (2013) lists five areas that should be prioritized for cyber diplomacy: human rights, international security, internet governance, cybercrime, and capacity building. And Areng (2013) argues that there is a need to share best practices between governments and capacity building in less capable countries to facilitate and increase the speed of crisis response, encouraging national and multinational exercises to test and identify gaps.

Based on the studies mentioned above, three key characteristics of cyber diplomacy can be determined:

a. Existence of multiple stakeholders, not just governments, even though they are responsible for developing and implementing policies related to cyber security. The issue of cyberspace also involves international organizations that promote cooperation in this field (the United Nations, the Organization for Security and Cooperation in Europe, the International Telecommunication Union), the private sector that owns critical infrastructure, non-governmental organizations that support human rights, the academic environment that is involved in research and civil society.
b. Promoting the development of a legal framework by facilitating international agreements, encouraging responsible behavior in cyberspace, highlighting existing risks, promoting dialogue and cooperation, building trust and addressing cybercrime, investigating and prosecuting criminals.
c. Capacity building, aiming to support countries in developing the technical and institutional capacities needed to address cybersecurity challenges through training and education, technical assistance, information sharing, and international cooperation.

3.2 The expansion of cyber diplomacy as a domain of international relations

Cyber diplomacy, referring to cyberspace that requires technical knowledge, is considered by Barrinha and Renard (2017) to be a peripheral issue in the international relations literature. Mannes and Valeriano (2016) note that cyber actions are becoming part of the normal process of constructing threats in international relations. Thus, it is acceptable for an incident in cyberspace to be responded to through physical, conventional space, abandoning the barriers between the hypothetical and the abstract, as the cyber world imposes costs on the physical world.

Among the key developments that have contributed to the expansion of cyber diplomacy as a field of international relations are UN initiatives addressing issues related to cyber security (Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security).

The emergence of cyber diplomats and entities dedicated to cyber diplomacy within ministries of foreign affairs is another argument for the inclusion in the field of international relations. There are many countries with officials responsible for this area. Although the exact names and duties vary from country to country, they aim to promote the interests of the country they represent in cyberspace. Such countries include the United States of America, France, Germany, Australia, Israel, Japan, South Korea, Singapore, Estonia, Canada, etc. Moreover, states collaborate on cybersecurity issues through the Budapest Convention and other norms that will be discussed in the next chapter.

4 The role of cyber diplomacy in shaping international norms, standards, and regulations of cyberspace

Cyberspace and the digital domain offer new opportunities and challenges for customary international norms (Polanski, 2017). The answer to these challenges is cyber diplomacy, through activities ranging from bilateral dialogues to negotiating international agreements and standards.

Ziolkowski (2013) states that the general principles of international law can be derived, inter alia, from general considerations, legal logic, legal relations in general, international relations, or a particular treaty regime. Pirker (2013) notes that while several international law prescriptions are pertinent to sovereignty and territorial integrity in cyberspace, their exact content remains to be specified by future state practice and, perhaps, jurisprudence. The emerging dilemma can be described as follows: the imposition of requirements must be avoided. Adopting a laissez-faire approach by loosely interpreting the obligations of states could leave other states without an adequate legal remedy under international law against impermissible interference with their sovereignty and territorial integrity.

So, being a relatively new field, the legal frameworks of cyber diplomacy are evolving and expanding. Considering the fact that international law is fragmented, with different interpretations of the current norms regarding the cyber issue, new legal instruments are needed to address the emerging challenges.

Cîrnu and Vasiloiu (2022) provide an overview of legislative instruments on cyber diplomacy worldwide, classifying the universal instruments (the instruments of the North Atlantic Treaty Organization, the Budapest Convention on Cybercrime, and the Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security), regional (ASEAN Cyber Security Cooperation Strategy, Organization of American States - Declaration on Strengthening Cyber Security in the Americas, Cyber Diplomacy in the European Union) and local, exploring legal frameworks in different countries (United States of America, Russia, China, Australia, Singapore, Korea, South Africa). These tools cover topics such as cybercrime, data protection, online freedom of expression, and cybersecurity.

The Cyber Diplomacy Act (US, 2021) addresses key moments in international cyberspace regulation, from the United States International Strategy for Cyberspace (May 16, 2011), to the report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security - GGE (June 24, 2013), the international code of conduct for information security proposed by China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan (January 2015), GGE Consensus Report (July 22, 2015), United States-China Commitment (September 25, 2015), G20 Antalya Summit (November 15-16, 2015), Department of State International Cyberspace Policy Strategy (March 2016), the recommendation from the Commission on Enhancing National Cybersecurity to appoint a US Cyber Security Ambassador (December 1, 2016) to the 2017 G7 Declaration on Responsible State Behavior in Cyberspace (April 11, 2017).

5 Conclusions

The emergence of cyberspace has created new challenges and opportunities for the international community. While cyberspace has the potential to bring an evolution in the global economy, it also presents new risks and challenges to international security and stability. To address these challenges, the field of cyber diplomacy has emerged as a crucial tool for managing cyberspace.

This paper established the framework of reference by analyzing cyberspace, from cybercrime (main threats, motivations, costs at the global level), the five types of state-sponsored cyberattacks, cyberespionage, cyberterrorism, and the three forms of activities that may fall under it, as well as trends in cybercrime.

The article went on to explore the concept of cyber diplomacy and its three key characteristics, as well as its expansion as a field of international relations, noting key developments that have contributed to this aspect.

The last chapter highlighted the role of cyber diplomacy in shaping the norms, standards, and international regulations of cyberspace, the legal frameworks of cyber diplomacy being in full evolution and expansion, specifying the critical moments of the international law of cyberspace.

Cyber diplomacy is a critical tool for managing the risks and opportunities associated with cyberspace. Even though the challenges in this environment are significant, the rewards of better international cooperation are substantial. Policymakers must prioritize international collaboration and work together to develop common cyber standards and norms to promote a more stable, more secure, and more predictable global cyber environment.

The study will continue with an analysis of the evolution of cyber diplomacy, how it has developed, and how it merges with diplomatic practices. The results will be published in a new research paper. Both studies will be used to create a framework (policies, training programs, skills development) for realizing diplomatic objectives while collecting relevant information from sources available in the public space (OSINT).

References

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

[2] C.E. Cîrnu and I.C. Vasiloiu, *Exploring the legislative dimension of cyber diplomacy worldwide: universal, regional, and local instruments*. Editura ICI, 2022.

[3] J. Eriksson and G. Giacomello., "Cyberspace in Space: Fragmentation, Vulnerability, and Uncertainty," 2022 [online] Available at: https://www.researchgate.net/publication/357934889_Cyberspace_in_Space_Fragmentation_Vulnerability_and_Uncertainty.

[4] European Commission, "home-affairs.ec.europa.eu. (n.d.). Cybercrime," [online] Available at: https://home-affairs.ec.europa.eu/cybercrime_en [Accessed 12 Jan. 2023].

[5] European Union Agency for Cybersecurity (ENISA) *ENISA Threat Landscape 2022*. [online] ENISA. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022.

[6] S. Fischer-Hübner, C. Alcaraz, A. Ferreira, C. Fernandez-Gago, J. Lopez, E. Markatos, L. Islami and M. Akil, "Stakeholder perspectives and requirements on cybersecurity in Europe," *Journal of Information Security and Applications*, [online] 61, 2021, p.102916. Available at: https://www.sciencedirect.com/science/article/pii/S2214212621001381#.

[7] D. Freet and R. Agrawal. Cyber Espionage. *Encyclopedia of Big Data*, 2017, pp.1–5.

[8] A. Georgescu, "Cyber Diplomacy in the Governance of Emerging AI Technologies - A Transatlantic Example," International Journal of Cyber Diplomacy, 3, 2022, pp.13–22.

[9] B. Jerman-Blažič and T. Klobučar, "Towards the Development of a Research Agenda for Cybercrime and Cyberterrorism – Identifying the Technical Challenges and Missing Solutions," Advanced Sciences and Technologies for Security Applications, 2016, pp.157–174.

[10] P. Kijewski, P. Jaroszewski, J.A. Urbanowicz and J. Armin, The Never-Ending Game of Cyberattack Attribution. *Advanced Sciences and Technologies for Security Applications*, 2016, pp.175–192.

[11] B.J. Koops, "Megatrends and Grand Challenges of Cybercrime and Cyberterrorism Policy and Research," Advanced Sciences and Technologies for Security Applications, 2016, pp.3–15.

[12] D.T. Kuehl, "From cyberspace to cyberpower: Defining the problem," Cyberpower and national security, 30, 2009.

[13] A. Kumar, "Cyber Diplomacy - The Concept, Evolution and its Applicability," International Journal of Cyber Diplomacy, 3, 2022, pp.23–32.

[14] A. Liina, *Peacetime Regime for State Activities in Cyberspace,* NATO CCD COE Publications, 2013.

[15] R. Maness and B. Valeriano, "The Impact of Cyber Conflict on International Interactions," Armed Forces & Society,

[online], 2015, 42(2). Available at: https://www.researchgate.net/publication/277583804_The_Impact_of_Cyber_Conflict_on_International_Interactions.

[16] J. Osawa, "The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem?," Asia-Pacific Review, 24(2), 2017, pp.113–131.

[17] G. Pierini, *Cyber security meets diplomacy: the EU-NATO cooperation and the Italian case*. 2016, [online] Available at: https://tesi.luiss.it/20167/1/627242_PIERINI_GABRIELE.pdf.

[18] P.P. Polański, "Cyberspace: A new branch of international customary law?," Computer Law & Security Review, 33(3), 2017, pp.371–381.

[19] E.H. Potter, *Cyber-Diplomacy: Managing Foreign Policy in the Twenty-First Century*, McGill-Queen's Press – MQUP, 2002.

[20] S. Riordan, *Cyberdiplomacy: Managing Security and Governance Online*, John Wiley & Sons, 2019.

[21] Verizon Business. *2020 Cyber-Espionage Report (CER)*, 2021 [online] Available at: https://www.verizon.com/business/resources/reports/cyber-espionage-report/.

[22] J. Wu. "Cyberspace Endogenous Safety and Security," *Engineering*, 15, 2022.

[23] www.statista.com. (n.d.). *Statista - The Statistics Portal for Market Data, Market Research and Market Studies*. [online] Available at: https://statista.com

Ioana-Cristina VASILOIU is a PhD Student at the Bucharest University of Economic Studies in the field of Economic Informatics. She graduated with a master's degree in International Economic Diplomacy from the Faculty of International Business and Economics of the same university. She also benefited from an ERASMUS+ scholarship, which allowed her to study in Poland. She is a graduate of the Faculty of International Business and Economics. Currently, she works for the National Institute for Research and Development in Informatics - ICI Bucharest, where she is involved in research on various topics, from cyber security and cyber diplomacy to high performance computing.