JLP JOURNAL OF LAW AND POLITICS

DOI: https://doi.org//10.69648/QPKO3766
Journal of Law and Politics (JLP), 2025; 6(1): 97-108
jlp.ibupress.com
Online ISSN: 2671-3438

Application: 01.03.2025
Revision: 08.04.2025
Acceptance: 23.04.2025
Publication: 30.04.2025

Buchkovska, K. (2025). Cyber Diplomacy: Securing The (Digital) Future. Journal of Law and Politics, 6(1), 97-108.
https://doi.org//10.69648/QPKO3766

Katerina Buchkovska
International Balkan University, Skopje, North Macedonia
https://orcid.org/0000-0000-0000-0001

We declare no conflicts of interest.

Correspondence concerning this article should be addressed to Katerina Buchkovska, Email: katerina.buchkovska@ibu.edu.mk.

BALKAN JOURNALS

Cyber Diplomacy: Securing The (Digital) Future

Katerina Buchkovska

Abstract

The 21st century has faced a new reality – modern warfare does not occupy only the realms of classical weaponry and armaments. Securing the country`s welfare does not depend solely on traditional diplomacy and robust economic policies. The word 'cyber' opened the door to a new realm of challenges for states in redefining security, diplomacy, and governance in the increasingly interconnected world. The governments have become targets of multiple cyberattacks that have seriously disrupted the normal functioning of institutions and had a great impact on the everyday life of their citizens. It is cyberspace that has become the most critical domain for economic, political, and military activities, thus elevating cybersecurity as an increasingly vital national and international priority.

Cyber diplomacy focuses on the use of diplomatic strategies and negotiations to address and manage issues arising in cyberspace, from protecting critical infrastructure and building resilience to cyber-attacks to establishing international norms in the cyberspace. Despite progress, there is an absence of universally accepted framework for cyberspace governance.

Cyber diplomacy plays vital role in the international relations for securing a peaceful digital future, as states and international organizations work to create cyber policies that promote stability and resilience in cyberspace. As the digital age evolves, cyber diplomacy is becoming international practice in global security positioning itself as an integral part of the foreign policy. It's the place where technology and international relations intersect.

Keywords: cyberspace, cyber diplomacy, security, international relations

Introduction

The 21st century is marked by rapid technological advancements, especially in AI, internet communication, and digital networks. Every day, new technological innovations emerge, reshaping industries, economies, and societies. This accelerated progress increases the level of global interconnectivity, transforming and changing the way individuals, organizations, and nations interact.

However, this rapid evolution also brings about new challenges, particularly in the sphere of security and global stability. As technological solutions advance, so do the threats associated with them. One of the biggest challenges arises in the sphere of digital realm including cyber security risks, misinformation, data privacy concerns and the ethical implications of AI. The dynamic nature of technological progress demands continuous adaptation and vigilance to mitigate emerging risks and ensure that these innovations contribute positively to global development.

One of the main questions is how to safeguard the digital landscape in the global international world? How to secure nations' digital stability and infrastructure and how to encourage responsible behavior among nations throughout the world?

Nowadays, threats are becoming invisible. While traditional warfare and terrorist attacks involve visible, tangible threats, the cyber realm has redefined what may become a threat to national stability and security. It is no longer the tanks, drones, or weapons and ammunition of a foreign intruder. It is not the long-range rockets or any other high-tech weaponry of the 21st century. Instead, what could bring a country to its knees is a single click—one that may in second's compromise its digital systems, cripple its infrastructure, and undermine its national security.

From this point, governments and countries are faced with the new reality. Securing the country`s welfare does not demand solely robust national intelligence, solid economic policies, and educational and health reforms. It also requires engaging efforts to secure the nation`s cyberspace. It demands new perspectives and initiatives in the challenging realm of cyber diplomacy. The governments have become targets of multiple cyberattacks that have seriously disrupted the normal functioning of the state system and had a great impact on the citizens` privacy, everyday life, and safety. While cyber issues were previously treated by states mainly as technical issues and with no real interest, nowadays they have moved to the forefront of their foreign policy agenda. Cyberspace has become the most critical domain for economic, political, and military activities, while cybersecurity has grown into one of the most important priorities among the nations of the modern world.

This article deals with the role of cyber diplomacy in the international society and its impact on the realm of a nation`s security in the digital age. A clear understanding and precise definition of emerging terms such as cybercrime, cyber-attacks, cyber espionage, the Internet of Things, data privacy, and cyber risks are crucial for implementing effective cyber policies and raising awareness about the significance of cyber threats. Nations must invest significant efforts in developing and supporting cyber diplomacy and encourage capacity-building measures in improving nations` cybersecurity skills and strengths through sharing expertise, training, and technology transfer.

What is Cyber Diplomacy?

Cyberspace has become a major focus of international relations, and most countries have inserted cyber issues into their foreign policies by adopting cyber strategies, harmonizing cyber laws, and redefining the security landscape and protocols. Cyberspace is increasingly becoming serious political space shaped by various interests, policies and strategies. Nowadays, cyberspace is not the domain reserved only for the IT specialists but it has become the central piece of nation`s security strategy.

In this political landscape, cyber diplomacy has become international issue, one that merges the countries' interests and strategies in the sphere of cyber security. Cyber diplomacy may be seen as the new diplomatic field that becomes increasingly demanding at international level due to the fact that it incorporates issues of high importance for each nation.

Understanding the rise of cyber diplomacy is essential for recognizing the efforts, opportunities, and challenges involved in regulating cyberspace. Effective regulation can establish guiding principles, norms, and frameworks for addressing cyber-related issues. Moreover, cyber diplomacy plays a crucial role in shaping responsible state behavior in the digital realm.

In an attempt to give a clear definition of what the term cyber diplomacy means, there are many interpretations and efforts to clarify its function and importance. However, we may define cybersecurity as an application of diplomatic techniques and negotiations in international relations that deal with and regulate cyberspace-related issues (Radanliev, 2024). According to other studies analyzed, cyber diplomacy is defined as a term that incorporates the use of diplomatic tools and mindsets to resolve issues arising from the international cyberspace whereas the

use of cyber tools to promote broader diplomatic agendas as well as the use of diplomatic techniques and mental modes to analyze and manage cyber problems are separate but interdependent activities (Attatfa et al., 2020).

Regardless of the specific definition used, they all share a common concept: cyber diplomacy serves as a vital tool for enhancing cybersecurity, safeguarding national interests, and fostering mutual trust among nations in the digital realm. Its main role is to harmonize the efforts of governments and nations in regulating the norms and guidelines of international cyberspace. Cyber diplomacy aims to assist in dealing with the difficulties and obstacles in the cyber sphere with the clear role to promote responsible behavior, preserve stability in cyberspace, and, most importantly of all, to assist the process of developing national cybersecurity policies.

Cyber diplomacy becomes as indispensable part of the international cooperation. Countries collaborate on developing cyber standards, guidelines and norms in direction of building resilient cyber space and safe digital environment. External attacks and threats combine social engineering tactics with advanced cyber techniques, posing serious political and security risks to a nation's cybersecurity landscape.

Therefore, it is of crucial importance for cyber diplomacy to act proactively in international cyber governance, to coordinate efforts in the creation of cyber laws, agreements, and norms in order to reduce the risks from cyberattacks and cyber terrorism. To do so, cyber diplomacy has to assist the process of confidence-building measures among nations in order to facilitate the process of mutual trust and willingness to support a harmonised and mutually accepted legal framework that will guide the responsible behaviour in cyberspace.

One of the main goals of cyber diplomacy is the identification of cyberattacks. It becomes more and more difficult to identify the attacker due to the advanced hacking technologies and the fact that the cyber-attack might originate from any point on the globe, which makes the process of identifying the perpetrators very difficult and time-consuming. To that end, cyber diplomacy must engage in developing effective mechanisms to combat cyber threats by fostering cooperation not only among states but also involving private corporations. Given the private sector`s crucial role in the cyber realm, its involvement is essential in strengthening the global cybersecurity efforts.

It is very important to mention the interconnection between diplomacy and cyber diplomacy and their complementary role. While diplomacy is defined as the

process of conducting negotiations between representatives of states (Attatfa et al., 2020), addressing many global issues, cyber diplomacy focuses on the use of diplomatic strategies and negotiations in international relations to address and manage issues arising in cyberspace. Cyber diplomacy can be defined as 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 cyberspace (Barrinha & Renard, 2020). While in traditional diplomacy, security risks might involve terrorism, separatist movements, economic destabilization, or pandemic, the cyber diplomacy deals only with vulnerability to cyber threats and cybersecurity.

Terms Connected to Cyber Diplomacy

To better understand the concept of cyber diplomacy, it is useful to define related terms that are commonly associated with it. One of the most frequently used terms in this context is digital diplomacy. Digital diplomacy, also referred to as e-diplomacy, involves the use of modern technologies and social media by diplomats to support and enhance their traditional activities (Manor, 2016). This includes a wide range of diplomatic functions, such as public diplomacy, international negotiations, crisis communication, and consular services. By leveraging digital tools, diplomats can engage more effectively with global audiences, facilitate international cooperation, and respond swiftly to emerging challenges in the digital age (Barrinha & Renard, 2020). In short, digital diplomacy uses technology for diplomatic goals.

Cyber norms, on the other hand, may be defined as established principles and rules/ guidelines that regulate government action in cyberspace. Many professional norms in cyberspace might have begun as best practice, and most of them have been written into laws, but not all of them have become legalized (Finnemore, 2017). Cyber norms actually lay the groundwork for collective expectations for state behaviour in cyberspace. They are the solid foundation on which regional and bilateral agreements around state behaviour in cyberspace are built and create a mutually reinforcing set of agreements and expectations.

Cyber terrorism poses a serious threat to disrupt and incapacitate critical national infrastructure through the use of the internet. It is also used as a tool for intimidation of people through dark web or deep net activities. Mainly, it refers to a cyber-attack perpetrated by terrorist groups or individuals with the goal to disrupt,

damage, or threaten critical infrastructure, governments, or societies by intimidation and psychological pressure. These attacks can include hacking, spreading propaganda, disrupting communication networks, or launching cyberattacks on financial, military, or energy systems. Cyber terrorism poses a significant threat as it can cause widespread fear, economic losses, and even physical harm. Given the growing reliance on digital technology, combating cyberterrorism requires enhanced international cooperation among nation-states, intelligence sharing, and the development of robust cybersecurity measures.

Information warfare is a concept where technology is used to influence opinions and perceptions in public. It involves tactics such as cyber-attacks, propaganda, misinformation, disinformation, and psychological operations to influence public opinion, disrupt decision-making, or weaken infrastructure. Governments, military forces, and non-state actors use information warfare to shape opinions, spread false information, and undermine trust in institutions. In the digital age, social media, cyber espionage, and hacking play a crucial role in modern information warfare, making it a critical aspect of national security and global conflicts.

Cyber espionage covers issues of legal principles governing state behavior in cyberspace. It's a type of cyber-attack that hackers use to attack business or government entity. These are usually very expensive and complicated cyber-attacks that use malicious softwares. Cyber espionage is used for gaining strategic advantages over rival entities in the field of politics, economy, business and technological sectors. Cyber espionage is usually initiated by government-based intelligence organization.

Cyber warfare is a concept that is closely related to cyber espionage, but it is not the same. For example, cyber espionage could be used to build the nation state capabilities in the sphere of intelligence as preparation for cyber war. On the other hand, cyber warfare is an attack on government and civilian infrastructure with the goal of disrupting the critical systems and paralyzing the functionality of the state system. Usually, the perpetrator is a nation state, but in some cases, the attacks could be carried out by terrorist organizations or non-state actors. In international cyber legislation, there is still no clear definition of whether a cyber-attack may constitute an act of war. Activities such as espionage, sabotage, electricity disruption, denial of service (DoS), propaganda, or economic disruption are considered cyber warfare.

Cyber Diplomacy in Action, Challenges and Barriers

The growing significance of digital transformation and technologies in geopolitics has elevated cybersecurity to a top priority for governments. States are increasingly focused on strengthening the diplomatic dimension of cybersecurity and are committed to developing robust national and international cyber diplomacy strategies.

Despite the increasing need for cyber diplomacy and cyber diplomats, there remains little substantive comparative research on how states have adapted their governance structures to meet this challenge. According to Barrinha and Renard, "Dozens of ministries have been creating offices exclusively dedicated to cyberspace and appointing 'cyber diplomats'. This move has concentrated more international cyber policy activities in foreign affairs ministries, elevating the issue in government hierarchies and increasing the level of international activity of each state in cyberspace" (Barrinha & Renard, 2020).

The first state to establish such structures was the United States during the term of President Barack Obama through the Office of the Coordinator of Cyber Issues in 2011. The US also pushed other, mainly Western, like-minded states and ROs to act in the cyber domain, including Germany, the EU, Japan, and Australia (Barrinha & Renard, 2020). The Cybersecurity and Infrastructure Security Agency (CISA) was established in 2018. It is a federal agency that functions as a component of the US Department of Homeland Security, dealing with issues of cybersecurity and infrastructure protection across all levels of government. The Agency is coordinating cooperation among US states on cyber programs, cybersecurity, and protection and prevention from cyberattacks. In 2021, during the Biden administration, Congress established the Office of the National Cyber Director (ONCD). This Office advises the President on cybersecurity policy and strategy and is a part of the Executive Office of the President at the White House. The US Cyber Diplomacy Act of 2021 also addresses key aspects of international cyberspace deliberation, and the Bureau of Cyberspace and Digital Policy was created in 2022, along with the appointment of a US Ambassador at Large for Cyberspace and Digital Policy, Nathaniel C. Fick (Bureau of Cyberspace and Digital Policy).

In Europe, awareness of cybersecurity has grown significantly, with all 27 EU member states now having developed their own cyber strategies and ten of them (Denmark, Sweden, Finland, Estonia, Netherlands, Germany, Poland, Czech Republic, France and Spain) have appointed cyber ambassadors, envoys and representatives (Latici, 2020).

In addition, The European Union Agency for Network and Information Security (ENISA) is critical component of the EU cybersecurity infrastructure and it serves as network and information security agency with the main goal to assist the EU member countries and EU institutions in harmonization of cyber legislation, creating shared standards and norms important for cybersecurity activities. One of the main goals of the Agency is to protect the EU's digital and critical infrastructure by building cybersecurity resilience and promoting collaboration among the member countries. Furthermore, the EU has established the Cyber Diplomacy Toolbox as part of its Common Foreign and Security Policy (CFSP) to provide a coordinated diplomatic response to malicious cyber activities. This framework includes a range of measures, from political dialogues and diplomatic engagement to sanctions, aimed at strengthening cybersecurity and deterring cyber threats.

However, besides all of these efforts in the cyber field, cyber diplomacy is confronted with numerous roadblocks and challenges on the path to secure and safe cyberspace. One of those challenges is the difficulty of tracking cyberattacks. Having into consideration the international character of cyber threats, the attack may originate from any geographical point in the world. This makes the prosecution of the perpetrators a very difficult task.

Another significant challenge to cyber diplomacy is the absence of unified international legislation. Defining the term cyber-attack has many different interpretations in many national strategies and legislations. This is a serious burden to the process of coordination and cooperation among countries. The international legal framework for cybersecurity is not unified and is continually changing. In addition to this, many countries have different national interests and priorities, and balancing the national security priorities and international cooperation might become a troublesome process. Given that cyberattacks may be state-sponsored, they have the potential to escalate conflicts and increase mistrust among nations.

While the US, EU countries, Japan, Australia, Canada, and the United Kingdom have invested substantial resources in building cybersecurity resilience, many developing countries face challenges due to a lack of resources, guidance, and infrastructure to address cybersecurity effectively. Bridging this gap and providing support to developing countries through assistance from more developed nations is essential for effectively addressing international cyber threats.

Besides many multinational initiatives and cyber agencies, there are many obstacles on the road to successful cyber diplomacy. Cyber risks and threats are becoming

increasingly dynamic, making the prevention of cyberattacks an ongoing challenge for cyber diplomats. Building on existing institutions and creating a more complex global cooperation framework in the domain of cyberspace is essential in building coherent and strong cyber diplomacy.

Regular cooperation on cyber issues among countries is an important factor in developing partnerships in cyberspace. Building trust among governments is critical for lowering the risks of future cyber threats and attacks. In case of cyber emergencies, countries should establish direct contact channels and an information exchange system that would improve the capacities for adequate cyber response. Joint cyber exercises, capacity-building measures, and technical cooperation on issues of cybersecurity are essential elements in developing a crisis management system among governments. This will enable authorities to manage cyber crises more effectively, minimizing potential damage and preventing escalation.

Another significant challenge to cyber diplomacy is the rise of artificial intelligence and the emergence of new technologies such as blockchain and the Internet of Things (IoT).

The integration of AI into cybersecurity has profound implications for cyber diplomacy. Governments must address critical issues such as AI ethics in cybersecurity and the development of guidelines and procedures for its responsible use in cyber operations. However, despite the risks, AI, when properly used, can greatly benefit cyber diplomacy. It can analyze vast amounts of data, enhance threat detection, and improve the identification and prevention of cyberattacks.

IoT security is becoming an increasingly complex challenge as IoT devices and networks operate globally, transcending national borders. The expanding connectivity of devices increases the attack surface, making systems more vulnerable to cyber threats. Therefore, cyber diplomacy must prioritize international cooperation to develop unified cybersecurity standards and safeguard IoT systems (Lu, 2023).

On the other hand, blockchain technology operates as a decentralized system, ensuring secure and transparent transactions without the need for a central authority. Beyond its association with cryptocurrencies, blockchain has the potential to benefit various sectors, including optimizing international trade and assisting governments in areas such as secure data management, digital identity verification, and transparent supply chain tracking (Tripathi et al., 2023).

Conclusion

The global digital transformation is continuing to reshape the lives of people, businesses, and institutions. The rise of Artificial Intelligence has a very strong impact on many economic, political, and security issues. Digitalization creates a more connected and globalized world, creating more opportunities for open markets, innovation, and prosperity. It actually increases the quality of life for everyone.

As the world becomes more dependent on cyberspace, the number of malicious cyber activities has grown. Cyber-attacks have become more and more severe over time, more complex and sophisticated. There is an increase in cyber incidents and attacks on critical infrastructure, democratic institutions, media, and businesses. Cyber-attacks do happen, and they pose a significant threat to political stability, economic development, and democratic processes. The war in Ukraine and the usage of high-technology cyber weapons have just accelerated the need for a more complex and careful approach in cybersecurity.

Therefore, states and governments are focusing their efforts on creating a safe and secure cyberspace to protect national interests and priorities. Nations are committed to working more closely to develop unified principles and standards, ensuring responsible state behavior. This is where cyber diplomacy becomes crucial, as it plays a key role in addressing the complexities of the digital environment and ensuring international collaboration in cyberspace.

Cyber diplomacy complements traditional diplomacy and is key to uniting nations in strengthening cyber resilience. All states and non-state organizations play critical role in advancing cyber diplomacy and strengthening its role in the process of development unified cyber legislation. Countries should strengthen cooperation in threat intelligence sharing, cybersecurity awareness, and joint cyber prevention measures. Cyber laws and international conventions establish norms and procedures that help safeguard data privacy, protect digital rights, and uphold cybersecurity standards.

Governments, international organizations, and NGO`s should amplify their efforts to support effective national policies and raise civil society awareness concerning the importance of cyber threats. Cyber capacity building and cybersecurity training are essential for strengthening the capabilities of both governments and the private sector.

Cyber diplomacy plays a crucial role in defining the government's incident response strategy and cyber crisis management systems. It is an essential prerequisite in building rapid detection, solid defense, protection, and prevention from future cyberattacks and incidents. The security of cyberspace presents a top national strategic priority. Only by creating secure cyber systems, the use of the internet and opportunities of the new modern technologies can be maximized and beneficial for all.

Cyber diplomacy remains a developing and evolving field, but given the increasing significance of cybersecurity as a rapidly growing domain, it is becoming a key priority in foreign policy. Strengthening cyber diplomacy is essential for fostering international peace, enhancing mutual trust, and promoting cooperation among nations in cyberspace.

References

Attatfa, A., Renaud, K., & De Paoli, S. (2020). Cyber diplomacy: A systematic literature review. *Procedia Computer Science, 176*, 60–90. https://doi.org/10.1016/j.procs.2020.08.007

Barrinha, A., & Renard, T. (2020). *The emergence of cyber diplomacy in an increasingly post-liberal cyberspace.* Council on Foreign Relations. https://www.cfr.org/blog/emergence-cyber-diplomacy-increasingly-post-liberal-cyberspace

Bureau of Cyberspace and Digital Policy. (n.d.). *U.S. Department of State*. https://www.state.gov/bureaus-offices/deputy-secretary-of-state/bureau-of-cyberspace-and-digital-policy/

Finnemore, M. (2017, November 30). Cybersecurity and the concepts of norms. *Carnegie Endowment for International Peace*. https://carnegieendowment.org/research/2017/11/cybersecurity-and-the-concept-of-norms?lang=en

Latici, T. (2020, May). *Understanding the EU's approach to cyber diplomacy and cyber defence* (Briefing No. 651937). European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651937/EPRS_BRI(2020)651937_EN.pdf

Lu, Y. (2023, November). Security and privacy of Internet of Things: A review of challenges and solutions. *Journal of Cybersecurity and Mobility*.

Manor, I. (2016). What is digital diplomacy and how it is practised around the world? A brief introduction. *The Diplomatist Magazine, 2016 Annual Review*, 36. http://www.diplomatist.com/dipoannual2016/index.html?pageNumber=36

Paulus, A. (2024). *Building bridges in cyber diplomacy*. Springer Cham.

Radanliev, P. (2024, February 5). Cyber diplomacy: Defining the opportunities for cybersecurity and risks from artificial intelligence, IoT, blockchains and quantum computing. *Journal of Cybersecurity Technology*. https://www.tandfonline.com/journals/tsec20

Tripathi, G., Abdul Ahad, M., & Casalino, G. (2023). A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges. *Decision Analytical Journal, 9*.