AGORA International Journal of Juridical Sciences, http://univagora.ro/jour/index.php/aijjs
ISSN 1843-570X, E-ISSN 2067-7677
Vol. 17, No. 2 (2023), pp. 118-125

SECURING THE DIGITAL DIPLOMACY FRONTIER: A GLOBAL PERSPECTIVE IN THE CYBER ERA WITH A FOCUS ON AZERBAIJAN

A. ALIYEVA

Aydan Aliyeva
UNEC Women Researchers Council, Azerbaijan & University of Potsdam, Germany
ORCID ID: https://orcid.org/0009-0000-8252-1931, E-mail: aliyevaaydan1998@gmail.com

Abstract: *The digital age has fundamentally transformed the nature of diplomacy. As countries embrace the opportunities of the digital realm to foster global relationships and promote their interests, they simultaneously confront an array of cyber threats and challenges. The inherent dynamism of this digital transformation challenges the age-old tenets of diplomacy, prompting a re-evaluation of traditional methodologies and strategies. Countries today are presented with a dual-edged sword. On one hand, digital tools serve as potent enablers, facilitating the forging of global relationships, enhancing soft power projection, and promoting nuanced national interests with unparalleled efficiency. Yet, the same arena also poses substantial challenges: cyber threats, misinformation campaigns, and intricate webs of state-backed digital espionage represent just the tip of a vast iceberg of challenges in the cyber domain. This research paper seeks to elucidate the evolving landscape of digital diplomacy, assessing its implications for traditional statecraft and international relations. By examining the dual nature of digitalisation — it's potential for both collaboration and conflict — we aim to provide a comprehensive understanding of the strategies and tactics employed by state actors. This exploration offers insights into the future of diplomacy, advocating for adaptive, resilient, and innovative approaches to navigate the challenges and harness the opportunities of the cyber era.*

Keywords: *Digital diplomacy, cyber threats, digital strategy, cyber-attacks, misinformation campaigns, digital transformation.*

INTRODUCTION

„Without communication, there is no diplomacy"- Christer Jönsson (2016)

In the evolving narrative of international relations, the age-old mechanisms of diplomacy are being transformed by the relentless tide of digitalization. The cyber era, marked by its vast potential and challenges, compels nations to meticulously navigate their diplomatic endeavors, balancing tradition with technological innovation. Globally, the digital frontier offers a platform for enhanced communication, accessibility, and collaboration, obliterating geographical confines and fostering real-time global dialogues. Yet, these opportunities coexist with emerging threats like cyber espionage, state-sponsored attacks, and the pervasive spread of misinformation. How can states and societies cope with these challenges and risks? How can they ensure the security, resilience, and prosperity of their digital domains? This is the main question that this research paper aims to address by exploring the concept and practice of digital diplomacy in the case of Azerbaijan. While this digital shift is universally felt, examining its manifestation in specific geopolitical contexts, such as Azerbaijan, offers deeper insights. Nestled at the crossroads of Eastern Europe and Western Asia, Azerbaijan emerges as a compelling case study in this narrative.

This research paper has three main objectives: first, to provide an overview of the current state of digital diplomacy in the world and its main trends and developments; second, to analyze the cybersecurity policy and digital strategy of Azerbaijan in comparison to other countries and regions; and third, to evaluate the effectiveness and impact of Azerbaijan's digital diplomacy initiatives and practices in terms of its national interests and global influence. To achieve these objectives, this paper will use a mixed-methods approach that combines qualitative data from various sources, such as official documents, media reports, academic articles, online platforms, and surveys. The paper will also use a theoretical framework based on the four modes of digital diplomacy model by Corneliu Bjola and Marcus Holmes (2015), which distinguishes between four modes of digital diplomacy based on the level of engagement and dialogue between actors: broadcasting, listening, networking, and mobilizing. This framework can help us to understand how Azerbaijan uses different digital platforms and strategies to achieve its diplomatic objectives, and how it interacts with different audiences and stakeholders in the cyber domain. This framework can also help us to compare and contrast Azerbaijan's digital diplomacy with other countries and regions, and to identify its strengths and weaknesses.

Examining Azerbaijan's cybersecurity policies, strategic blueprints, and mechanisms for digital engagement provides an in-depth view of the nation's approach to the multifaceted challenges and prospects of the cyber era. Such an exploration not only highlights Azerbaijan's tactics but also sheds light on the broader shifts in global digital diplomacy, emphasizing the pressing need for countries to fortify their digital domains in this interconnected era.

1. GLOBAL SHIFTS AND THE ADVENT OF DIGITAL DIPLOMACY

Digital diplomacy is not a new phenomenon, but rather a continuation and adaptation of traditional diplomacy to the changing technological environment. Diplomacy has always been influenced by the means of communication available at different historical periods, such as letters, telegraphs, telephones, radios, televisions, and satellites.

Globally, the proliferation of digital tools has democratized information dissemination. No longer are diplomatic messages the sole purview of state-controlled media or closed-door meetings. Today, a tweet, a video clip, or a blog post can resonate as powerfully as a formal diplomatic communique, if not more. Such is the power and unpredictability of digital platforms. However, with this new power also comes an array of challenges. Misinformation and disinformation campaigns, threads and cyberattacks can muddy the waters of international discourse, with non-state actors, both benign and malevolent, possessing the tools to shape narratives. The advent of the Internet and digital technologies in the late 20th and early 21st centuries have brought unprecedented changes to the nature and practice of diplomacy, creating new opportunities and challenges for diplomats, states, and non-state actors. An intern posting a photograph on an embassy's social media account, high-level diplomats networking with tech companies in Silicon Valley, and state leaders using „Twitter" to comment on international negotiations are now examples of everyday diplomatic life.

As Corneliu Bjola and Marcus Holmes (2015) argue, digital technologies have enabled a shift from "digital adaptation", which refers to the use of digital tools to support existing diplomatic functions, to "digital adoption", which refers to the creation of new diplomatic

functions that are only possible through digital tools. Therefore, digital diplomacy can be seen as both a continuation and a transformation of traditional diplomacy in the cyber era.

1.1. Unpacking models of digital diplomacy

One of the main concepts and models of digital diplomacy that has been proposed by scholars and practitioners is the four modes of digital diplomacy model by Corneliu Bjola and Marcus Holmes (2015). This model distinguishes between four modes of digital diplomacy based on the level of engagement and dialogue between actors: broadcasting (one-way communication), listening (monitoring and analysis), networking (relationship building), and mobilizing (influencing and persuading). According to this model, each mode of digital diplomacy has its own objectives, tools, strategies, and outcomes, and they can be used separately or in combination depending on the context and the purpose of the diplomatic action. The model also suggests that digital diplomacy is not a static or linear process, but rather a dynamic and interactive one, where actors can switch between different modes depending on the feedback and the results they receive. The model also acknowledges that digital diplomacy is not a monolithic or homogeneous phenomenon, but rather a diverse and heterogeneous one, where different actors have different levels of access, capacity, and influence in the digital domain.

Another model of digital diplomacy is the three levels of digital diplomacy model by Ilan Manor (2019). This model distinguishes between three levels of digital diplomacy based on the degree of innovation and transformation: migration (transferring offline practices to online platforms), adaptation (adapting offline practices to online platforms), and innovation (creating new practices for online platforms). According to this model, each level of digital diplomacy has its own challenges and opportunities, and they can be used to measure the progress and impact of digital diplomacy. The model also argues that digital diplomacy is not only a matter of technology, but also a matter of culture, mindset, and identity.

A third model of digital diplomacy is the three types of media diplomacy model by Eytan Gilboa (2001). This model distinguishes between three types of media diplomacy based on the role of the media in diplomatic processes: public diplomacy (using the media to communicate with foreign publics), media diplomacy (using the media to communicate with foreign officials), and media-broker diplomacy (using the media to facilitate or mediate negotiations). According to this model, each type of media diplomacy has its own advantages and disadvantages, and they can be used to achieve different diplomatic goals. The model also emphasizes the interdependence and interaction between the media and diplomacy in the age of globalization (ibid., 4).

Historically, diplomatic engagements were primarily physical, but the emergence of online platforms has dramatically reshaped how nations interact. Digital diplomacy or also so called e-diplomacy has emerged as a prominent instrument of statecraft, especially evident in the nuanced situations that have marked recent global affairs. During the 2020 COVID-19 pandemic, as face-to-face diplomatic encounters came to a halt, online platforms became the fulcrum of international communication and cooperation (cf. Naylor, 2023: 1). The World Health Organization adeptly used these tools to circulate indispensable health advisories globally.

„The most effective diplomacy doesn't take place in the formal meeting itself. It's what's happening on the margins. It's what happens in the corridors."- Dr. Tristen Naylor (2023)

However, this digital space was simultaneously contested, with some countries manipulating it to disseminate misleading information or further political agendas about the pandemic. Earlier, during the Ukraine conflict of 2014-2015, digital spaces became battlegrounds for information warfare and cyberattacks. Russia's orchestrated misinformation campaign aimed to validate its annexation of Crimea and involvement in Eastern Ukraine. Conversely, Ukraine turned to social media to rally domestic and international support (*The Diplomacy Network*, 2023). A further testament to the power of digital diplomacy was seen in the 2015 Iran Nuclear Deal negotiations.

Platforms like „Twitter" or also for instance „Zoom"-Rooms (Calls and Videocalls) were no longer mere communication tools but became instrumental in shaping diplomatic outcomes. Both US Secretary of State John Kerry and Iranian Foreign Minister Javad Zarif took to „Twitter" to engage directly, bridging diplomatic divides and simultaneously communicating the accord's nuances to a global audience (Manor, 2019: 3-5).

However, while the proliferation of digital platforms offers transformative avenues for diplomatic discourse and statecraft, it also opens up a Pandora's box of security vulnerabilities. The same online spaces that can be harnessed for fruitful online dialogue and collaboration also expose states to a spectrum of cyber threats that can compromise national security and destabilize diplomatic relations.

1.2. Cyberdiplomacy: cyberattacks in diplomatic relations

Before explaining what 'cyber diplomacy' means, is cruical to define the two terms that compose it: 'diplomacy' and 'cybersecurity'. Diplomacy pertains to the strategic efforts by representatives to further the objectives of the states or entities they champion, leveraging methods such as advocacy, dialogue, and mediation. On the other hand, cybersecurity encompasses the protective strategies employed by individuals and entities to safeguard both their physical resources, like infrastructure and personnel, and intangible assets, such as data, expertise, service provision capabilities, influence, or intellectual capital. With our lives becoming more intertwined with the digital integration, the need for stringent cybersecurity measures is more imperative than ever (Hartmann, 2023).

Such measures are not merely about safeguarding physical assets like infrastructure but also extend to protecting intangible resources, including data, service capabilities, and intellectual capital. Yet, as we emphasize on the importance of cybersecurity, we must acknowledge the vulnerabilities it aims to address.

Delving into the world of cyberattacks in diplomatic relations reveals a stark manifestation of the vulnerabilities inherent in our increasingly digitized global landscape. Cyberattacks in diplomatic relations are malicious activities that use information and communication technologies (ICTs) to target or disrupt the political, economic, or security interests of another state or entity. Cyberattacks can have various objectives, such as espionage, sabotage, coercion, or influence. Cyberattacks can also have various effects, such as damaging critical infrastructures, stealing sensitive data, disrupting public services, or undermining trust and confidence.

Cyberattacks in diplomatic relations pose significant challenges and risks for the international community, as they can escalate tensions, undermine stability, and violate international law and norms. Therefore, "cyber diplomacy" is a very important field of diplomacy that aims to prevent and respond to cyberattacks, and to promote responsible state behaviour in cyberspace. Cyber diplomacy involves various actors, such as states, international organisations, private sector, civil society, and academia. Cyber diplomacy also involves various tools and instruments, such as dialogue, cooperation, capacity building, norms, confidence building measures, attribution, and cyber sanctions regime (Ivan, 2019: 3).

Illustrating the gravity of this cyber-centric landscape are incidents like the 2020 SolarWinds attack, which saw the US pointing fingers at Russia, resulting in consequential sanctions. In 2017, over 150 countries and entities grappled with the ramifications of the WannaCry ransomware, with countries like the UK and US holding North Korea responsible (ibid., 7; *Net Politics*, 2019). Germany too has been on the receiving end, attributing cyber offensives against its parliament in both 2015 and 2020 to Russian hacker factions, a move that led to the expulsion of Russian diplomats. 2020 also spotlighted cyber tensions between India and China, with the former suspecting that cyberattacks on its power grids were inextricably linked to their border skirmishes (*The Diplomat*, 2021).

Adding to the series of cyber-centric geopolitical events, the 2020 Karabakh conflict between Armenia and Azerbaijan provides another illustrative example. Alongside the on-the-ground altercations over the contested Karabakh region, both nations encountered significant challenges on the cyber front. This ranged from intensified campaigns on social media platforms to orchestrated Distributed Denial of Service (DDoS) attacks, leading to disruptions and outages on official portals (*External Cyberattacks During Second Karabakh War Mainly Focused on Azerbaijan's Central Bank – CERT*, 2021; Spînu, 2021: 5). Personal data, often of military personnel or public figures, became a valuable target, resulting in numerous high-profile breaches and subsequent leaks. The conflict's digital dimension also witnessed the symbolic defacement of websites and more covert operations suggestive of cyber espionage, targeting critical infrastructures and communication channels. Such episodes from the Karabakh War II serve as an emphatic testament to the evolving nature of conflicts, underscoring the dual theaters of physical and cyber warfare in modern geopolitics.

2. AZERBAIJAN'S CYBER STRATEGY IN A GLOBAL CONTEXT

A recent study by the A recent study by the Asian Development Bank illuminates Azerbaijan's strategic approach towards bolstering its security and cybersecurity. Spanning from 2019 to 2022, Azerbaijan's strategy is driven by the imperative need to escalate the country's cybersecurity fortifications and mitigate potential threats to its information systems (Yoon, 2019: 19-20; Mehdiyev, 2021: 2-8, 23). The strategy was developed based on the need to increase the level of national cybersecurity in Azerbaijan and reduce threats to information systems. The strategy has following objectives: to improve the legal framework for cybersecurity; to enhance the institutional capacity for cybersecurity; to develop human resources for cybersecurity; and to raise awareness and cooperation on cybersecurity (Yoon, 2019: 20).

However, it's not merely about building an internal strategy. The Cybil Portal's report accentuates that Azerbaijan's cybersecurity tactics resonate with international standards and esteemed practices like the Budapest Convention on Cybercrime and the Global Cybersecurity Index. Yet, it's crucial to acknowledge the existing challenges. The report brings to light certain areas and specific vulnerabilities identified during the ongoing Karabakh conflict that need further attention, including the establishment of a national cyber incident response team, a comprehensive data protection legislation, clarity in inter-agency roles, and a consistent assessment mechanism (Spînu, 2021: 5, 7-10).

Shifting the lens to digital development, DataReportal's research (2022) showcases Azerbaijan's commendable advancements. The country boasts impressive metrics: 82% internet penetration, 116% mobile penetration, 50% social media usage, and a thriving 28% e-commerce engagement among its citizens. Azerbaijan's proactive measures to catalyze its digital transformation journey are evident. These include the inauguration of a national e-government portal, the development of a digital trade nucleus, the foundation of a high-tech park, and a palpable support system for emerging startups and innovative ventures. Furthermore, Azerbaijan is actively participating in various regional digital connectivity initiatives and campaigns.

As reported by Trend News Agency, Azerbaijan is actively formulating an all-encompassing strategy that covers diverse areas of digitalization, spanning big data, artificial intelligence, the Internet of Things, and digital marketing. The country's objective is to launch this advanced digital economy strategy by 2024 (Gasimov, 2023).

3. GLOBAL FUTURE OF E-DIPLOMACY AND DIGITALISATION

As more nations recognize the transformative power of digital tools, the global diplomatic community is poised for a shift towards a more interconnected, transparent, and efficient mode of operations. E-diplomacy isn't just about integrating technology into diplomacy; it's about reimagining the very essence of diplomatic engagements in the digital era.

With artificial intelligence, big data analytics, and blockchain technologies making inroads into this realm, there's an increasing opportunity to harness these advancements for peacekeeping, international collaborations, and global policymaking. Moreover, social media channels are playing pivotal roles in shaping public opinion, making them invaluable tools for soft diplomacy and public diplomacy initiatives. This paradigm shift warrants exploration, and to that end, a journal article by Hedling and Bremberg serves as a seminal piece. In their analysis, they present a practice-based exploration of digital diplomacy. Central to their discourse is the transformative influence of digital technologies, highlighting three dimensions: the reshaping of space, or 'spatiality'; how tangible 'materiality' elements influence diplomatic practices; and the shift in the perception of time, or 'temporality' (Hedling & Bremberg, 2021: 1596-1598).

Building on this foundational understanding, a subsequent layer of analysis comes from Kürzdörfer and her team. Their policy brief examines the European Union's recent digital regulation endeavors. By introducing the Digital Services Act (DSA) and Digital Markets Act (DMA), the EU aims not only to counteract the weaponization of digital interdependence but also to enhance the robustness of its digital ecosystem. Such moves could potentially amplify

the EU's values and norms on the global digital stage (*Digital Transformation Lab (DIGITRAL): Digital Diplomacy and Statecraft*, 2021-2024).

The global future of e-diplomacy is not just a mere extension of traditional diplomacy but a profound evolution. It demands that nations not only adapt to the changing technological landscape but also embrace the ethos of digital age diplomacy—openness, inclusivity, and collaboration—in all spheres of their lives.

CONCLUSIONS

The digital age has brought about transformative shifts in how nations engage with each other, and the domain of diplomacy has not been immune to these changes. Digital diplomacy, or e-diplomacy, stands at the crossroads of traditional statecraft and modern technology. The recent cyber-centric geopolitical events, such as those witnessed during the Karabakh conflict between Armenia and Azerbaijan, emphasize the growing significance of the cyber dimension in international relations.

Azerbaijan, in its journey of digital evolution, has recognized the imperatives of cybersecurity and digital diplomacy. Its strategic alignment with international standards and ambitious plans for the future, such as the upcoming comprehensive digital economy strategy, highlights the nation's commitment to staying abreast with global best practices. Furthermore, the insights from esteemed researchers and global organizations underscore the broader shifts in digital diplomacy and the opportunities and challenges it presents.

The European Union's endeavors, like the introduction of the Digital Services Act (DSA) and the Digital Markets Act (DMA), indicate a global trend towards safeguarding digital ecosystems and promoting values and norms in the digital sphere (Steffens & Müller, 2023; Mschmitz, 2022;).

In this ever-evolving landscape, world must continue to adapt, innovate, and collaborate. The future of e-diplomacy isn't merely an extension of traditional diplomacy but a profound digital evolution and digitalisation. It calls upon countries to not only adapt to technological advancements but also uphold the values of inclusivity and collaboration in the digital era. As we forge ahead in the cyber age, it is crucial for nations worldwide to grasp the potential of digital diplomacy in shaping a connected, inclusive, and resilient global community.

REFERENCES

1. Bjola, C., & Manor, I. (2022). The rise of hybrid diplomacy: from digital adaptation to digital adoption. International Affairs, 98(2), 471–491. https://doi.org/10.1093/ia/iiac005
2. Dayeh, Anas. (2023, May 29). Diplomacy in the Digital Age: The rise, impact, and future of digital diplomacy. The Oxford Student.
3. Digital Diplomacy | EEAS. (n.d.). https://www.eeas.europa.eu/eeas/digital-diplomacy_en
4. Digital Transformation Lab (DIGITRAL): Digital diplomacy and statecraft. (2021-2024). https://www.giga-hamburg.de/de/forschung-und-transfer/projekte/digital-diplomacy-and-statecraft
5. External cyberattacks during Second Karabakh War mainly focused on Azerbaijan's Central Bank – CERT. (2021, December 9). Azernews.Az. https://www.azernews.az/business/186732.html
6. Feldstein, S. (2021, July 21). Digital technology's evolving role in politics, protest and repression. United States Institute of Peace.

https://www.usip.org/publications/2021/07/digital-technologys-evolving-role-politics-protest-and-repression
7. Gasimov, K. (2023, September 21). *Azerbaijan announces dates for digital economy strategy adoption*. Trend.Az. https://en.trend.az/business/economy/3800773.html
8. Gilboa, E. (2001). Diplomacy in the media age: Three models of uses and effects. Diplomacy & Statecraft, 12(2), 1–28. https://doi.org/10.1080/09592290108406201
9. Hartmann, F. (2023, April 6). EU Cyber Diplomacy 101. Eipa. https://www.eipa.eu/blog/eu-cyber-diplomacy-101/
10. Hedling, E., & Bremberg, N. (2021). Practice Approaches to the Digital Transformations of Diplomacy: Toward a New Research Agenda. International Studies Review, 23(4), 1595-1618. https://doi.org/10.1093/isr/viab027
11. Holmes, M., & Bjola, C. (2015, March 19). Digital Diplomacy: theory and practice. Routledge & CRC Press. https://www.routledge.com/Digital-Diplomacy-Theory-and-Practice/Bjola-Holmes/p/book/9781138843820
12. Ivan, P. (2019, March 18). Responding to cyberattacks: Prospects for the EU Cyber Diplomacy Toolbox. https://epc.eu/en/publications/Responding-to-cyberattacks-EU-Cyber-Diplomacy-Toolbox~218414
13. Jönsson, C. (2016). Diplomacy, communication and signaling. Lund University Publications. https://lup.lub.lu.se/search/publication/314d79ad-dabd-413c-9d9e-716c1562d3ac
14. Kemp, S. (2022, February 15). Digital 2022: Azerbaijan — DataReportal – Global Digital Insights. DataReportal – Global Digital Insights. https://datareportal.com/reports/digital-2022-azerbaijan
15. Mehdiyev, E. (2021, May 21). Security sector reform in Azerbaijan: key milestones and lessons learned | DCAF – Geneva Centre for Security Sector Governance. https://www.dcaf.ch/security-sector-reform-azerbaijan-key-milestones-and-lessons-learned
16. Manor, I. (2019). The digitalization of public diplomacy. In *Palgrave Macmillan series in global public diplomacy*. https://doi.org/10.1007/978-3-030-04405-3
17. Mschmitz. (2022, February 10). *The Digital Services Act (DSA) and the Digital Markets Act (DMA)*. Global & European Dynamics. https://globaleurope.eu/europes-future/the-digital-services-act-dsa-and-the-digital-markets-act-dma/
18. Naylor, T. (2023, October 10). *COVID-19's impact on global statecraft | Research for the World | LSE Research*. LSE Research for the World. https://www.lse.ac.uk/research/research-for-the-world/politics/diplomacy-at-a-distance-covid-19s-impact-on-global-statecraft
19. Net Politics, G. B. F. N. (2019, April 2). Global consequences of escalating U.S.-Russia cyber conflict. Council on Foreign Relations.
20. Spînu, N. (2021, November 1). Azerbaijan Cybersecurity Governance Assessment | DCAF – Geneva Centre for Security Sector Governance.
21. Steffens, A., & Müller, C. (2023, March 10). Digital Services Act (DSA) und Digital Markets Act (DMA). *KPMG*. https://kpmg.com/de/de/home/themen/2023/03/digital-services-act-dsa-und-digital-markets-act-dma-neue-umfangreiche-compliance-anforderungen.html
22. Sun, Cathy., I.F.U.D.O.G.(2020, January 31). Social Media and The New Age of Diplomacy.
23. The Diplomat.(2021,March 12). China's dangerous step toward cyber conflict.
24. The Diplomacy Network.(2023,Feburary 6). The Digital Diplomacy Revolution: How Technology is Transforming International Relations.
25. Yoon,S.(2019,Janaury31). Azerbaijan: Country Digital Development Overview.