

UDC: 327.8:004.056.5

Nadiia Shmygol¹, Anatolii Antoniuk²

¹ Dr. Sc., professor NU “Zaporizhzhia Polytechnic”

Warsaw University of Technology, Poland

² University Collegium Civitas, Poland

DIGITAL DIPLOMACY AND CYBERSECURITY IN INTERNATIONAL RELATIONS

In the 21st century, digital transformation has reshaped nearly all aspects of international relations, including diplomacy, communication, security, and conflict resolution. One of the most dynamic developments in this context is the rapid growth of digital diplomacy—a strategic use of digital platforms and tools by states to manage foreign policy communication and public engagement online. Alongside it, the field of cybersecurity has emerged as a central concern, dealing with both the technical protection of data systems and the geopolitical implications of cyber threats. Digital diplomacy today encompasses both outward-facing public diplomacy and inward institutional transformation. According to Manor (2023), digital diplomacy enables governments to reach foreign populations directly, bypassing traditional media channels, while also modernizing diplomatic institutions through data analytics and artificial intelligence. Social media platforms like X (formerly Twitter), Facebook, and YouTube have become critical arenas for expressing national positions, shaping international narratives, and influencing public opinion. [1].

However, as governments expand their digital capabilities, they also become more vulnerable to new categories of threats. Cyberattacks on public infrastructure, disinformation campaigns, and the misuse of artificial intelligence are increasingly

common. A 2022 report by the European Union Agency for Cybersecurity (ENISA) notes a sharp rise in politically motivated cyber incidents targeting critical sectors, diplomatic missions, and intergovernmental organizations (ENISA, 2022). To better understand the strategic diversity in digital diplomacy and cybersecurity implementation, Table 1 presents a comparative overview of how three major global actors—the United States, the European Union, and China—approach these domains. [2].

Table 1. Comparative approaches to digital diplomacy and cybersecurity

Parameter	USA	EU	China
Digital diplomacy focus	Public diplomacy, digital innovation	Multilateral coordination, regulatory approach	Controlled communication, state-led tools
Cybersecurity strategy	Public-private partnerships, deterrence	Norm-building, regulatory enforcement	Sovereignty-centered, centralized control
Role of private actors	High (Meta, Google, Microsoft)	Moderate (under regulation, e.g. DSA, DMA)	Low (state dominance)
Legal framework	Fragmented but adaptive (CISA, EO 14028)	Strong, GDPR-based + NIS2	Strict national laws (Cybersecurity Law)

The table highlights key differences in priorities, regulatory philosophies, and institutional arrangements. This comparative analysis illustrates not only the geopolitical fragmentation of the digital space but also the underlying values that shape each region’s digital governance model. By contrasting these approaches, we can better assess how digital diplomacy is influenced by national political systems, legal frameworks, and the involvement of non-state actors. Thus, digital diplomacy is no longer a supplementary instrument but a core pillar of modern foreign policy. It allows for direct global engagement but requires sophisticated risk management to address cyber threats and vulnerabilities.

According to the U.S. State Department (2023), international cooperation on cybersecurity norms and capacity-building in the Global South are now priority areas in digital foreign policy agendas. As Manor (2023) highlights, “the digitalization of diplomacy is not merely a technical shift—it represents a transformation in the way states perceive and enact their roles in global affairs [3].

Digital diplomacy and cybersecurity have become inseperable components of contemporary international relations. States are now required not only to

communicate effectively across digital channels but also to secure those channels against a complex and evolving threat landscape. The comparative analysis shows varying regional approaches: while the U.S. prioritizes public-private cooperation and innovation, the EU leans toward regulatory frameworks, and China maintains strict central control [4].

The future of international cooperation will likely depend on the ability of states to bridge digital divides, build mutual trust in cyberspace, and create interoperable legal and ethical frameworks. The dual challenge of influence and protection in the digital domain marks a fundamental shift in global diplomatic practice, and addressing it will define the stability and security of the international order in years to come.

REFERENCES

1. ENISA. (2022). Threat Landscape 2022: Cybersecurity threats to the EU. European Union Agency for Cybersecurity. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022> (дата звернення: 02.04.2025)
2. European Commission. (2023). Digital Services Act and Digital Markets Act. <https://digital-strategy.ec.europa.eu> (дата звернення: 02.04.2025)
3. Manor, I. (2023). The new public diplomacy in the age of AI: Between innovation and vulnerability. *Journal of Digital Diplomacy*, 5(1), 22–37. <https://doi.org/10.1093/jddplc> (дата звернення: 02.04.2025).
4. U.S. Department of State. (2023). International Cyberspace & Digital Policy Strategy. <https://www.state.gov/international-cyberspace-digital-policy-strategy> (дата звернення: 02.04.2025)