European Journal of Law and Public Administration
ISSN: 2360-6754 | e-ISSN: 2559-7671
Covered in: Erih Plus; HeinOnline; CEEOL; RePEc; CrossRef; Google Scholar; KVK; WorldCat; ICI Journals Master List - Index Copernicus; EBSCO.

2025, Volume 12, Issue 2, pages: 63-77 | https://doi.org/10.18662/eljpa/12.2/266

The Transformation of Diplomacy in the Digital Age: The Legal Framework, Security Challenges, and the Estonian Model

Marilena-Oana NEDELEA [1]

[1] Lecturer PhD, "Ştefan cel Mare" University of Suceava, Romania; marilena.nedelea@usm.ro; ORCID: https://orcid.org/0000-0001-9478-7673

JEL classification: *K33, K24, K23*

Abstract: *Digital diplomacy today operates within an increasingly well-defined legal framework, resulting from the convergence of global, European, and national regulations. This emerging normative ecosystem is shaping a new branch of international and European law focused on the governance of the digital space. In this context, diplomats are required to develop interdisciplinary skills, combining law, technology, and international relations, as digital diplomacy becomes both a tool for action and an object of negotiation. Although the current legislative framework is in continuous development, the accelerated pace of technological innovation poses major challenges related to the balance between innovation, national security, and the protection of fundamental rights, offering a strategic advantage to states capable of adapting and actively contributing to shaping this field.*

Keywords: *digital diplomacy; legal framework; European Union; Romania; Estonia.*

How to cite: Nedelea, M.-O. (2025). The transformation of diplomacy in the digital age: the legal framework, security challenges, and the estonian model. *European Journal of Law and Public Administration, 12*(2), 63-77. https://doi.org/10.18662/eljpa/12.2/266

©2025 Published by In Manifest Network in partnership with LUMEN Publishing. This is an open access article under the CC BY-NC-ND license http://creativecommons.org/licenses/by-nc-nd/4.0/

Introduction

Digital diplomacy no longer operates outside of clear legal norms. A complex and stratified legislative framework is currently taking shape, generating both opportunities and limitations for the actors involved in diplomatic relations. From the global guidelines promoted through the Global Digital Compact to the detailed regulations of the European Union and national legislative initiatives, such as those adopted in Romania, a new branch of international and European law, centered on the governance of the digital environment, is gradually asserting itself.

For the diplomatic corps, this evolution implies a pressing need to acquire new skills at the confluence of law, technology, and international relations. Diplomats must understand not only the use of digital tools but also the normative architecture that governs them. In this context, digital diplomacy acquires a dual role: an instrument of action and, at the same time, an object of international negotiations.

The current normative framework, however extensive, is only a starting point. The acceleration of technological innovation – from generative artificial intelligence to the development of the metaverse – will continue to exert significant pressure on legislators and diplomats globally. The main challenge of the future lies in maintaining a fine balance between stimulating innovation, guaranteeing national security, and protecting fundamental rights in an increasingly interconnected digital space. States that succeed in understanding, applying, and actively shaping this legal framework will gain a significant strategic advantage in the geopolitical dynamics of the 21st century.

In a world where technology is fundamentally reshaping human interactions, diplomacy, one of the oldest practices of international relations, is no exception. In the context of the accelerated digitalization of international relations, digital diplomacy has become an essential instrument for promoting national interests and managing global challenges.

The evolution of the internet has allowed traditional diplomacy to adopt digital tools. Consequently, digital diplomacy has become a crucial part of public diplomacy and online communication. In an interconnected world, digital tools have become essential for states in achieving their foreign policy objectives.

The digital revolution has fundamentally reconfigured the landscape of international relations, compelling states to adapt their foreign policy instruments and strategies. In this context, digital diplomacy has evolved from a niche concept to a central component of contemporary diplomatic practice. This involves the use of digital platforms and technologies to achieve

diplomatic objectives, from public communication and cultural diplomacy to international negotiations and crisis management. The effectiveness and legitimacy of these actions are, however, intrinsically linked to the existence of a robust and coherent legal framework.

The digital revolution has fundamentally reshaped society, and the field of international relations is no exception. Diplomacy, as a central instrument of foreign policy, has had to adapt to an information environment characterized by speed, transparency, and interconnectivity. Thus, the concept of digital diplomacy (also known as e-diplomacy) has emerged and consolidated, which involves the use of the internet, social networks, and other information and communication technologies (ICT) to achieve diplomatic objectives (Verrekia, 2017).

To promote the country's image abroad, the Ministry of Foreign Affairs, together with embassies and consulates, uses digital diplomacy and strategic communication. They distribute public messages and their own content in a coordinated and unified manner, adapting to the international context and respecting the principles of the state's strategic partnerships.

The field of digital diplomacy has long been surrounded by mistrust, mainly due to public concerns about data protection on virtual platforms, skepticism regarding the accuracy of content disseminated through the media, and the perception of reduced credibility generated by the casual tone of communication on social networks. Despite these obstacles, the global health crisis caused by the COVID-19 pandemic and the response measures adopted have highlighted the substantial benefits that modern technologies bring to the social, medical, and protection domains.

Defining key concepts in digital statecraft

Digital Diplomacy refers to the use of digital technologies, particularly social media and other internet-based platforms, as tools to achieve foreign policy objectives. It is the broadest of the four terms and encompasses a wide range of activities, from public diplomacy and strategic communication to online consular services and virtual negotiations. Digital diplomacy is primarily concerned with the how of diplomacy—the use of digital tools to conduct traditional diplomatic functions in a new, digital environment. It focuses on communication, engagement, and influence in the public sphere.

Cyber Diplomacy in contrast, is a more specialized field focused on the what of diplomacy. It deals with the negotiation of norms, rules, and standards for state behavior in cyberspace. Cyber diplomacy addresses the policy and legal aspects of the digital realm, including issues such as

cybersecurity, internet governance, data privacy, and the application of international law to cyberspace. While digital diplomacy uses digital tools to conduct diplomacy, cyber diplomacy makes the digital realm itself the subject of diplomatic negotiation.

Digital Governance is a broader concept that encompasses the frameworks, institutions, and processes that shape the digital world. It is not limited to the actions of states but includes the roles of the private sector, civil society, and the technical community in governing the internet and other digital technologies. Digital governance addresses the development and application of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the internet. It is the system of rules and institutions that govern the digital space.

Digital Statecraft is the most encompassing term, referring to the use of all instruments of national power, including diplomatic, economic, military, and informational, to pursue a state's interests in the digital domain. It goes beyond diplomacy to include intelligence gathering, cyber operations (both defensive and offensive), economic competition, and the promotion of a country's technological model. Digital statecraft is the art and practice of using digital means to achieve strategic objectives in the international arena, and it represents the full integration of digital considerations into a state's foreign and security policy.

The multistratified legal framework of digital diplomacy: from global principles to regional implementation

The complexity of the digital environment, characterized by transboundary scope, powerful non-state actors, and continuously evolving cyber threats, requires a multi-layered approach to regulation. The legislation supporting digital diplomacy is not a monolith, but a mosaic of norms and principles developed at the global, regional (with the European Union as a key actor), and national levels. Understanding this legal ecosystem is essential for any state actor wishing to navigate successfully in the new era of diplomacy.

At the global level, efforts to regulate the digital space are still fragmented, reflecting the diversity of interests and visions of states. However, the awareness of common risks, from cyberattacks to disinformation, has spurred the search for a consensus on fundamental principles. The most ambitious project in this regard is the Global Digital Compact (GDC), initiated under the auspices of the United Nations.

Adopted in September 2024, following a negotiation process involving the 193 member states, the Global Digital Compact represents a milestone in the efforts to establish a global framework for digital governance

(United Nations, 2024). Although it is not a legally binding treaty, the GDC carries significant political weight, outlining a set of principles and commitments intended to guide the actions of states, the private sector, and civil society.

Its central objective is to ensure an "open, free and secure digital future for all," based on respect for human rights, the rule of law, and the principles of the UN Charter.

The EU's digital diplomacy is supported by key legislation such as the Digital Services Act (DSA) (for a safer online space) and policy initiatives like the Digital Europe Programme (2021-2027), aiming to promote EU interests in the global digital sphere, regulate online platforms (what is illegal offline must also be illegal online), and strengthen the Union's strategic autonomy in the face of new technological challenges. The EU Council sets priorities for external digital actions, focusing on cybersecurity, global internet governance, and the promotion of European values.

EU digital diplomacy

In a period characterized by growing geopolitical tensions, the accelerated development of innovative technologies with the potential to reshape the economy and social structures requires the European Union and its members to strengthen their authority and influence in the field of digital administration on an international scale.

It is necessary to develop and implement more robust, strategically oriented, harmonized, and effective European policies and initiatives in the global digital affairs sector.

To elevate EU digital diplomacy to a new dimension, the Union must operate according to a collaborative "United Europe" model, jointly protecting its strategic interests and promoting a humanistic perspective on the digital transformation process. In this regard, it should:

- First, ensure strategic participation in all relevant multilateral forums and protect the current multi-stakeholder model of internet governance.
- Second, ensure the integration of digital diplomacy into the Global Gateway, which represents the EU's "offer" for building secure and trusted connectivity worldwide.
- Finally, consolidate the EU's role in defining the global regulatory framework in the digital field, including by strengthening bilateral and regional digital partnerships and alliances.

The european level: the EU as a digital normative power

The European Union has positioned itself as a global leader in regulating the digital space, adopting a values-based approach that prioritizes fundamental rights, democracy, and the rule of law. This legislative framework, often referred to as the "Brussels effect," not only establishes rules for the single market but, through its scope and requirements, influences standards globally. For member states, this dense normative framework constitutes the main legal basis for exercising digital diplomacy.

The EU's International Digital Strategy (2025)

Adopted in June 2025, this strategy represents the EU's vision for its external action in the digital field (European Commission, 2025). It articulates how the Union will use its diplomatic, economic, and legislative instruments to promote its interests and values in the global digital arena. The strategy focuses on strengthening competitiveness, security, and digital governance, with global partnerships (through Digital Partnerships and Digital Dialogues) and the promotion of a human-centric model of digital transformation as its pillars.

The NIS2 Directive (2022/2555)

The Directive on the security of network and information systems (NIS2) is a central element of the EU's cybersecurity strategy (European Commission, 2023). By extending its scope to 18 critical sectors and imposing stricter risk management and incident reporting obligations, NIS2 strengthens the Union's cyber resilience. For digital diplomacy, the relevance is twofold: on the one hand, it protects the critical infrastructures that support diplomatic activity (communication networks, ministries' information systems); on the other hand, it creates a consolidated cooperation framework at the EU level (through the CSIRT and EU-CyCLONe networks), which can also be projected in relations with external partners.

The AI Act (EU Regulation 2024/1689)

The AI Act is the world's first comprehensive legislation on artificial intelligence (European Commission, 2024). Its innovative, risk-based approach prohibits certain practices considered unacceptable (e.g., social scoring), imposes strict obligations for high-risk systems, and transparency requirements for other systems (e.g., chatbots, deepfakes). The implications for digital diplomacy are vast:

- Establishes a global standard: Like GDPR, the AI Act has the potential to become a de facto global standard, influencing the development and use of AI in other countries.
- Regulates diplomatic tools: The use of AI in diplomacy (e.g., for data analysis, automated communication) will have to comply with these rules.
- Creates a new diplomatic agenda: Promoting ethical and trustworthy AI becomes a foreign policy objective, a subject of negotiation in trade agreements, and a field of cooperation for development.

The Digital Services Act (DSA) and the Digital Markets Act (DMA)

This legislative package regulates online platforms. The DSA focuses on combating illegal content and increasing the transparency and accountability of platforms, especially the very large ones (European Commission, 2022). The DMA, on the other hand, targets "gatekeeper" platforms to ensure fair and contestable digital markets. For diplomacy, the DSA is particularly relevant as it provides legal tools to combat disinformation and information manipulation, phenomena that directly affect national security and democratic processes. The obligations of advertising transparency and systemic risk analysis imposed on very large platforms offer states new levers to protect the public information space.

The National Level: The Case of Romania

Romania has aligned with European and international efforts, but has also adopted a proactive approach, being one of the pioneers in the specific regulation of digital diplomacy. The national framework is built around Law no. 58/2023, an innovative normative act.

Law no. 58/2023 on cybersecurity and cyber defense

Adopted in March 2023, this law not only transposes European requirements but also introduces, for the first time at the international level, two key concepts: "cyber diplomacy" and "cyber hygiene" (Ministerul Cercetării, Inovării şi Digitalizării, 2023).

Cyber diplomacy is explicitly defined as "the diplomatic activity through which the foreign policy and security interests of Romania are promoted, within bilateral and multilateral formats of dialogue and negotiation on topics relevant to the field of cybersecurity." This definition legally anchors the activity of digital diplomacy in the mandate of the Ministry of Foreign Affairs and other relevant institutions, providing a clear legal basis for:

- Participation in international negotiations on cybersecurity topics.
- Promoting Romania's position within international organizations (UN, NATO, EU, OSCE).
- Developing bilateral partnerships in the digital field.

Cyber hygiene is defined as a "set of routine measures applied regularly by individuals and legal entities that have the role of reducing their exposure to the risks posed by cyber threats." The inclusion of this concept in the law and the plan to integrate it into the educational system and the administration has an indirect but significant impact on diplomacy. A higher level of awareness and cyber resilience throughout society contributes to strengthening national security, a fundamental objective of foreign policy.

The law also establishes the role of the National Cyber Security Directorate (DNSC) as the national authority and point of contact in cooperation mechanisms, thus strengthening the institutional architecture necessary for effective digital diplomacy.

Analysis and synthesis: the common pillars of legislation

The analysis of the legislative framework at the three levels – international, European, and national – reveals a set of common pillars that structure digital governance and, implicitly, the legal foundations of digital diplomacy. These reflect an emerging consensus on the essential elements for a stable and predictable digital space.

Common Pillar	International Level (GDC)	European Level (EU)	National Level (Romania)
Cybersecurity	Ensuring a stable and secure internet	NIS2 Directive, Cyber Resilience Act	Law 58/2023, Cybersecurity Strategy
Protection of Fundamental Rights	Respect for human rights online	GDPR, AI Act (risks to rights), DSA (freedom of expression)	Law 58/2023 (guarantees against abuse)
Digital Governance	Governance of data and AI	DSA, DMA, AI Act	Law 58/2023 (institutional framework)

Security challenges

The transition to digital diplomacy, while offering significant advantages in terms of efficiency and reach, also introduces a new spectrum of complex and persistent security challenges. The very infrastructure that

enables modern diplomatic engagement has become a contested domain, where state and non-state actors vie for influence, information, and strategic advantage. Navigating this environment requires a profound understanding of the multifaceted threats that define the digital age.

One of the most direct threats is the proliferation of **cyberattacks and espionage** targeting diplomatic missions and critical national infrastructure. Diplomatic networks, which carry sensitive political, economic, and security information, are high-value targets for intelligence gathering. Hostile actors employ sophisticated techniques, from phishing and malware to zero-day exploits, to infiltrate these networks, steal classified data, and monitor confidential communications. The 2007 cyberattacks on Estonia, which temporarily crippled the nation's digital infrastructure, served as a stark wake-up call, demonstrating the vulnerability of even the most advanced digital societies and underscoring the potential for cyber incidents to escalate into major diplomatic crises (NATO Cooperative Cyber Defence Centre of Excellence, 2025). These attacks are no longer isolated incidents but part of a persistent, low-intensity conflict in cyberspace.

Another significant challenge is the weaponization of information through **disinformation and foreign information manipulation**. Digital platforms and social media have become fertile ground for the dissemination of false or misleading narratives designed to sow discord, polarize societies, undermine trust in democratic institutions, and disrupt foreign policy objectives. These campaigns can be used to influence elections, shape public perception during a crisis, or discredit a state's international standing. As the European Union's Digital Services Act (DSA) acknowledges, combating this phenomenon requires a robust regulatory framework that holds platforms accountable, but the speed, scale, and sophistication of disinformation campaigns present a continuous challenge for diplomats who must work to counter false narratives and protect the integrity of the public information space (European Commission, 2022).

The increasing reliance on data-driven tools in diplomacy raises critical issues of **data security and privacy**. Diplomatic services handle vast amounts of data, including the personal information of citizens abroad requiring consular assistance. Ensuring the confidentiality, integrity, and availability of this data is paramount. A significant data breach can not only have severe operational consequences but also erode the trust between citizens and the state. While regulations like the GDPR provide a strong foundation for data protection, the transnational nature of diplomatic activity creates complex jurisdictional challenges and requires constant vigilance to safeguard sensitive information against an ever-evolving threat landscape.

Furthermore, the issue of **attribution** poses a fundamental problem for diplomatic response in the event of a cyber incident. The technical difficulty of definitively and publicly identifying the perpetrator of a cyberattack allows state and non-state actors to operate with a degree of plausible deniability. This ambiguity complicates the formulation of a proportional response, whether through sanctions, legal measures, or other diplomatic tools. The lack of a universally accepted mechanism for attribution hinders the development of clear norms of state behavior and the enforcement of international law in cyberspace, creating a permissive environment for malicious activity.

Finally, the rapid advancement of emerging technologies, particularly in the field of **Artificial Intelligence (AI)**, introduces a new frontier of security risks. While AI offers promising tools for data analysis and predictive modeling in diplomacy, it also presents new vectors for attack. AI-powered malware, the use of deepfakes to create convincing but fabricated video or audio for disinformation campaigns, and the potential development of autonomous cyber weapons represent a significant escalation of the threat. The AI Act in the European Union is a pioneering effort to regulate these risks, but the global technological arms race means that diplomats will be in a constant struggle to keep pace with innovations that could destabilize the digital environment (European Commission, 2024).

The Estonian Model: a pioneer of digital diplomacy

Estonia is widely recognized as a global leader in digital governance and, by extension, in digital diplomacy. Its success is not accidental but the result of a long-term strategic vision, a solid legal framework, and a culture of innovation. The Estonian model offers valuable lessons for any state wishing to maximize the opportunities of the digital age.

The foundations of the estonian model

Estonia's digital transformation began in the 1990s, with the launch of the "Tiigrihüpe" (Tiger Leap) project, which focused on developing internet infrastructure and digital literacy. This was followed by the creation of a robust legal framework, including the Electronic Identification and Digital Signature Act (2000), which gave legal value to digital identity and signatures.

The cornerstone of the Estonian system is the X-Road, a secure data exchange layer that allows public and private institutions to interact and exchange information in a standardized and secure manner. This interoperability is essential for the provision of integrated digital public services.

Digital diplomacy in action

Estonia has used its technological advance to project its influence on the international stage. Its digital diplomacy is based on several pillars:

- Promoting the digital society model: Estonia actively promotes its model of e-governance, offering expertise and solutions to other countries. This has become a brand for the country and an effective tool of soft power.
- Cybersecurity expertise: Following the 2007 cyberattacks, Estonia has become a leading voice in international debates on cybersecurity. It hosts the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn and has been a firm advocate for the application of international law in cyberspace.
- e-Residency: Launched in 2014, the e-Residency program allows foreign citizens to obtain a digital identity issued by the Estonian state, with which they can set up and manage a company in the EU online. The program is a unique example of "virtual" diplomacy, attracting talent and investment and creating a global community of "e-Estonians."

Lessons from the estonian model

The Estonian model demonstrates that a small state can become a major player in the digital age through a clear vision, consistent investments, and a favorable legal framework. The key lessons are:

- The importance of a long-term strategy: Digital transformation is a marathon, not a sprint.
- The need for a robust legal framework: Trust in digital services is based on clear and predictable rules.
- Interoperability is key: Isolated systems cannot provide integrated and efficient services.
- Public-private partnership: Collaboration between the state and the private sector is essential for innovation.
- Digital diplomacy as a soft power tool: Technological expertise can be a valuable diplomatic asset.

"We are not just digitizing old processes, we are rethinking them to meet people's needs in difficult times," said Enel Pungas, head of the Population Facts Department at the Estonian Ministry of the Interior, referring to the digitization of the divorce process.

Critical analysis of the estonian model: transferability, costs, and geopolitical tensions

Although the Estonian model of digital diplomacy is often presented as a benchmark of success, a deeper scientific analysis requires a critical evaluation of its limits and challenges. This section aims to interrogate the model's transferability, examine its costs and externalities, and analyze the geopolitical tensions inherent in promoting a national digital model as a soft power tool.

The limits of transferability: a sui generis model?

The digital success of Estonia is the result of a unique set of historical, political, and social circumstances, which raise questions about its replicability in other national contexts. Several factors contribute to the sui generis character of the Estonian model:

Small Population and Cultural Homogeneity: With a population of approximately 1.3 million, Estonia has benefited from a small scale that has facilitated the rapid and coordinated implementation of digital reforms. In states with large and diverse populations, the logistical, administrative, and cultural challenges are exponentially greater.

High Level of Social Trust: Estonian society is characterized by a high level of trust in public institutions, an essential factor for the widespread adoption of digital services, including electronic voting and digital identity. Replicating this model in states with low levels of social trust and political polarization is problematic.

The Post-Soviet Context and the Opportunity of a Digital Greenfield: The absence of legacy administrative systems allowed Estonia to build a modern digital infrastructure from scratch, a "greenfield" advantage that few states have. Many countries face the challenge of modernizing old and fragmented IT systems, a costly and complex process.

Costs, externalities, and internal challenges

Beyond the image of success, the Estonian model also involves a series of costs, risks, and negative externalities that are often overlooked:

Security Risks and Vulnerabilities: Data centralization and dependence on digital infrastructure create significant vulnerabilities to cyberattacks, as demonstrated by the 2007 attack. Although Estonia has developed top expertise in cybersecurity, the risk of a paralyzing attack remains a constant threat.

Digital Exclusion: Although Estonia has a high internet penetration rate, there are still vulnerable groups (the elderly, low-income individuals, linguistic minorities) who risk being excluded from the digital society. Ensuring universal access and digital skills for all citizens is an ongoing challenge.

Risks Associated with e-Residency: The e-Residency program, although innovative, has been criticized for its potential to facilitate tax evasion, money laundering, and other illicit activities. Although Estonian authorities have implemented verification and control measures, the risk of misuse of the platform persists.

Geopolitical tensions and the limits of digital soft power

The active promotion of the digital model as a soft power tool places Estonia at the center of geopolitical tensions and raises questions about the sustainability of this strategy:

Dependence on External Technologies: Although Estonia has a vibrant IT sector, its digital development is largely based on technologies and platforms developed by multinational companies, especially from the United States. This technological dependence can create strategic vulnerabilities and limit Estonia's decision-making autonomy.

Rivalry with Alternative Models: The Estonian model, based on transparency, democracy, and the rule of law, is in direct competition with alternative models of digital governance, such as the one promoted by China, which prioritizes state control and mass surveillance. This confrontation of models is taking place globally and has major geopolitical implications.

Instrumentalization as a Geopolitical Target: By positioning itself as a digital leader and an active member of NATO and the EU, Estonia becomes a prime target for hostile state actors, especially the Russian Federation. Cyberattacks and disinformation campaigns are not only technical threats but also instruments of geopolitical pressure designed to undermine the credibility of the Estonian model.

In conclusion, although the Estonian model of digital diplomacy offers valuable lessons, a critical approach is essential to understand its limits and to avoid uncritical replication. A thorough analysis of the specific context, costs, and geopolitical tensions is indispensable for any state that wishes to draw inspiration from the Estonian experience to build its own digital strategy.

Conclusions

The digital revolution has irreversibly transformed the practice of diplomacy, creating a new field of action with its own rules, opportunities, and risks. The legal framework for digital diplomacy is in a continuous process of construction, at the intersection of international, European, and national law. This emerging normative ecosystem provides diplomats with the necessary tools to act in the digital space, but also imposes limits on them, in a constant search for a balance between innovation, security, and fundamental rights.

The analysis of the legislative framework at the global, European, and national levels reveals a growing convergence on a set of common principles: the need to ensure cybersecurity, the obligation to protect fundamental rights online, and the importance of a clear governance of digital platforms and technologies. The European Union has established itself as a normative power in this field, with its legislation (GDPR, DSA, AI Act, NIS2) setting global standards. Romania, through Law 58/2023, has positioned itself as a pioneer by explicitly regulating cyber diplomacy and cyber hygiene.

The Estonian model demonstrates that a strategic approach, based on a solid legal framework and a culture of innovation, can transform a small state into a digital leader. The lessons learned from Estonia – the importance of a long-term strategy, interoperability, and the use of technology as a soft power tool – are valuable for any country that wants to navigate successfully in the new geopolitical context.

For the diplomatic corps, the challenge is twofold. On the one hand, diplomats must develop new interdisciplinary skills to understand and use digital tools and the legal framework that governs them. On the other hand, they must be able to negotiate and promote their country's interests in an increasingly complex digital arena. Digital diplomacy is no longer an option, but a necessity for any state that wants to remain relevant in the 21st century.

Use of AI tools statement

No AI-assisted technologies were used in the writing, editing, or data analysis for this manuscript. All work is original and completed solely by the listed author.

References

European Commission. (2022). The digital services act. https://digital-strategy.ec.europa.eu/en/policies/digital-services-act

European Commission. (2023). NIS2 directive. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

European Commission. (2024). AI act. https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

European Commission. (2025). The international digital strategy for the European Union. https://digital-strategy.ec.europa.eu/en/policies/international-digital-strategy

Ministerul Cercetării, Inovării şi Digitalizării. (2023, 1 Martie). *România este printre primele state din lume care reglementează diplomația și igiena cibernetică într-o lege*. https://www.research.gov.ro/romania-este-printre-primele-state-din-lume-care-reglementeaza-diplomatia-si-igiena-cibernetica-intr-o-lege-9531/

NATO Cooperative Cyber Defence Centre of Excellence (n.d.). *The 2007 Cyber Attacks on Estonia.* https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf

POEU (2016, April 27). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)https://op.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/

United Nations. (2024). Global digital compact. https://www.un.org/global-digital-compact/en

Verrekia, B. (2017). *Digital diplomacy and its effect on international relations*. Independent Study Project (ISP) Collection. https://digitalcollections.sit.edu/isp_collection/2596/