CYBER DIPLOMACY IN THE AGE OF TECHNOLOGICAL SOVEREIGNTY: THE UN NORMATIVE FRAMEWORK AND THE STRATEGIC APPROACHES OF THE UNITED STATES, THE EUROPEAN UNION AND JAPAN

Tina ANDOLJŠEK[1], Andrej VASTL[2]
[1] MSc, Ministry of Defence, Republic of Slovenia
andoljsek.tina1@gmail.com (**Corresponding author*)
[2] MSc, Ministry of Education, Science and Youth, Republic of Slovenia

Abstract: Cyber diplomacy is emerging in contemporary international relations as an important field of foreign policy, international security, digital governance and technological sovereignty. The article is based on the assumption that cyber diplomacy is no longer merely a response to individual cyber incidents, but a systemic instrument of state and international action. It analyses the role of the United Nations as a global normative pillar and compares the strategic approaches of the United States, the European Union and Japan. The UN provides a minimum common framework for responsible state behaviour, the United States emphasises strategic competition and digital solidarity, the EU focuses on regulatory power and strategic autonomy, while Japan links cybersecurity, economic security and regional resilience. The central finding is that cyber diplomacy is becoming a permanent capability of contemporary international relations, as it connects norms, security, technology, industrial policy and the resilience of the digital order.
Keywords: cyber diplomacy, cybersecurity, technological sovereignty, United Nations, European Union, United States of America, Japan, international security.

INTRODUCTION

Digitalisation has significantly transformed contemporary international relations. These relations no longer take place only through classical diplomatic channels, international organisations, security alliances, economic agreements and legal regimes, but also through digital and data infrastructures, communication platforms, cybersecurity regimes, technical standards, artificial intelligence and global technological ecosystems. Cyberspace has become a space of cooperation, economic development, political influence, intelligence activity, criminal activity and strategic competition among states.

In this environment, cyber diplomacy is developing. In its broadest sense, it can be understood as the use of diplomatic methods, negotiations, international cooperation and foreign policy instruments to address issues related to cyberspace. Radanliev (2024) defines it as the use of diplomatic techniques and negotiations in international relations when these relate to cyberspace. Similarly, Attatfa, Renaud and De Paoli (2020) emphasise that cyber diplomacy exists when the cyber dimension is the central reason for diplomatic action.

Cyber diplomacy differs from digital diplomacy. Digital diplomacy usually refers to the use of digital tools, social media, online communication and data-based approaches in diplomatic work. Cyber diplomacy, by contrast, concerns the substantive regulation of security, legal, technological, normative and political issues in cyberspace. If digital diplomacy is primarily a channel of diplomatic activity, cyber diplomacy is a field of international governance.

The definitions offered by Radanliev (2024) and Attatfa et al. (2020) describe what cyber diplomacy is, but not how it came to be recognised as a distinct field of diplomatic practice. Barrinha and Renard (2017) address this question directly, describing the emergence of cyber diplomacy as a process of diplomatisation, in which cyber issues move from a purely technical register into the institutional routines of foreign ministries through the parallel dynamics of internal recognition, whereby cyber questions come to be accepted as legitimate objects of diplomatic work, and external positioning, whereby states define themselves in relation to one another on cyber matters. This adds a historical-institutional dimension to the distinctions drawn above and suggests that the boundaries of the field remain subject to ongoing negotiation within national diplomatic services.

A complementary account frames cyber diplomacy not primarily as an institutional process but as a form of systemic governance. Georgescu, Vevera and Cîrnu (2020) argue that the growing interdependence and complexity of cyberspace call for diplomatic mechanisms capable of managing cyberspace as a single interconnected system, rather than addressing isolated incidents or bilateral disputes in sequence. This systemic-governance perspective complements the diplomatisation account of Barrinha and Renard (2017) by shifting attention from how cyber diplomacy became institutionally recognised to how it must be structured in order to govern an inherently complex and interdependent domain.

The purpose of this article is to analyse the development of cyber diplomacy as an instrument of contemporary international relations. The research question is: how is cyber diplomacy developing as an instrument of international security, digital governance and technological sovereignty, and what differences can be identified between the approaches of the UN, the United States, the EU and Japan? Methodologically, the article is based on a qualitative comparative analysis of academic literature, strategic documents, legal sources and official policies of the selected actors. The analysis focuses on three dimensions: normative, strategic-security and technological-sovereignty.

CYBER DIPLOMACY, SOVEREIGNTY AND TECHNOLOGICAL POWER

Cyber diplomacy has developed as a response to the transformation of international relations caused by digitalisation, the global interconnection of information systems, the growth of cyber threats and the increasing dependence of states on data, communication and technological infrastructures. While traditional diplomacy was primarily associated with interstate communication, negotiation and the representation of interests, cyber diplomacy transfers these functions into an environment in which the boundaries between internal and external security, the public and private sectors, and technical and political issues are significantly less clear (Attatfa et al., 2020; Radanliev, 2024).

This definition makes it possible to distinguish between traditional, digital and cyber diplomacy. Digital diplomacy refers to the use of digital tools, online platforms, social media and data analytics in the performance of diplomatic tasks (Manor, 2019). Cyber diplomacy, however, is not primarily directed towards the digitalisation of diplomatic communication, but towards the governance of cyberspace as a security, political, legal and technological domain. Digital diplomacy is therefore primarily a method of diplomatic activity, whereas cyber diplomacy is a field of international governance.

Cyber diplomacy has several interrelated dimensions. The normative dimension concerns the development of rules, principles and norms of responsible state behaviour in cyberspace. The strategic-security dimension includes diplomatic coordination of responses to malicious cyber activities, attribution, deterrence, sanctions, crisis communication and the protection of critical infrastructure. The technological-sovereignty dimension covers issues of standards, data infrastructures, cloud services, supply chains, digital sovereignty and dependence on private technology providers (Cici, 2025; Radanliev, 2024).

Cyberspace directly changes the understanding of sovereignty. A state may formally retain legal sovereignty, but its actual capacity for autonomous action is limited if its data, communications, public services, critical infrastructure, cloud services, software and cybersecurity solutions depend on external technology providers, foreign standards or global platforms. It is therefore useful to distinguish between formal sovereignty as the legally recognised authority of the state and functional sovereignty as the actual capacity to ensure the security, resilience and autonomous operation of key systems.

This distinction between formal and functional sovereignty can be linked to the theory of weaponized interdependence developed by Farrell and Newman (2019). States that control the central nodes of global financial, informational or technological networks are able to use this position either to gather information, through what the authors term the panopticon effect, or to deny network access to others, through the chokepoint effect. Applied to cyber diplomacy, this framework clarifies why disputes over technical standards, cloud dependency or telecommunications equipment are not purely economic but also diplomatic in nature, since they concern which states and companies occupy structurally advantageous positions within networks on which other actors depend.

Technical standards play a particularly important role. Standards, protocols, data formats, interoperability requirements, encryption algorithms, certification schemes and security architectures are often presented as technical issues, but they have clear political and geopolitical consequences. They determine which technologies will be used globally, which providers will have an advantage, what level of security will apply, who will control data and how states and companies will be integrated into global digital ecosystems. Standards are therefore not merely technical agreements, but also instruments of structural power (Cici, 2025). The absence of harmonised standards can itself become a source of vulnerability, as illustrated by the construction sector, where the diffusion of cyber-physical systems under the Construction 4.0 paradigm has outpaced the extension of established critical-infrastructure-protection frameworks and standards to construction sites, design data and building-management systems (García de Soto et al., 2022). Distributed-ledger technologies such as blockchain illustrate this dynamic well: although the technology was initially promoted as a means of reducing dependence on centralised intermediaries, early analyses of its adoption in business environments already cautioned that it introduces new questions of trust, governance and organisational adaptation rather than removing dependency altogether (Bucovețchi et al., 2018).

This dynamic is particularly visible in the role of global technology companies, which operate cloud services, operating systems, communication platforms, social networks, cybersecurity solutions, artificial intelligence models and data services. Cyberspace is also a domain of critical infrastructure vulnerability, since energy, transport, health, finance, telecommunications,

public administration, satellite services and defence systems increasingly depend on digital connectivity and automation. This exposure extends beyond terrestrial systems: the growing dependence of communications, navigation and early-warning capabilities on space infrastructure has itself become a distinct security concern, since disruption of satellite services can cascade into multiple critical sectors simultaneously (Gheorghe et al., 2018). The protection of critical infrastructure is therefore no longer only a national task, but also a diplomatic issue linked to international cooperation, norms of responsible behaviour and joint responses to incidents (United Nations, 2025; U.S. Department of State, 2024). This vulnerability is particularly pronounced in the maritime sector, where advanced persistent threats, hacktivist campaigns and unresolved vulnerabilities in port and vessel systems increasingly threaten the continuity of global trade flows, illustrating how a single critical-infrastructure sub-domain can carry disproportionate diplomatic weight (Badea et al., 2025).

Cyber diplomacy is therefore not merely a response to cyberattacks, but an instrument for shaping the digital order. It enables states, through norms, standards, partnerships, regulation, technology policies and international cooperation, to reduce strategic dependencies, strengthen resilience and increase their capacity to operate in the digital environment. This does not imply complete technological self-sufficiency, but rather the ability to choose among trusted partners, participate in the development of rules, identify technological risks in a timely manner and develop domestic capabilities.

Recent scholarship on organisational resilience adds a further layer to this understanding of functional sovereignty by shifting the unit of analysis from the state to the organisations on which state capacity ultimately depends. Bucovețchi et al. (2025) apply natural language analysis to map the strategic domains and semantic structures through which organisational resilience is conceptualised, identifying artificial intelligence as an emerging enabler of resilience assessment. Building on this, Bucovețchi et al. (2026) model organisational resilience in human-cyber-physical systems characteristic of Industry 5.0, showing how collective decision dynamics and crisis-aware artificial intelligence can be combined in multi-method simulations to anticipate disruption. These findings suggest that the technological-sovereignty dimension of cyber diplomacy cannot be separated from resilience-building at the organisational level, since critical-infrastructure operators and technology providers are themselves complex socio-technical systems whose resilience conditions the functional sovereignty of the states that depend on them.

THE UN AS A GLOBAL NORMATIVE FRAMEWORK

The United Nations has a special role in the development of cyber diplomacy because it represents the broadest and most universal diplomatic forum for discussing the security of information and communication technologies in the context of international security. Its role is not primarily operational, but normative and legitimising: it develops a common language, principles, norms and gradual international consensus on responsible state behaviour in cyberspace (United Nations, 2021, 2025).

Cyber diplomacy within the UN has developed mainly through Groups of Governmental Experts (GGE) and Open-ended Working Groups (OEWG). The GGE represented a narrower expert-diplomatic format, while the OEWG is a broader and more inclusive process open to

all UN Member States. The difference between the two processes reflects the tension between the effectiveness of smaller expert formats and the legitimacy of universal multilateralism (United Nations, 2021, 2025).

The GGE and OEWG processes established the basic framework for responsible state behaviour in cyberspace. This includes the application of international law, voluntary norms of responsible behaviour, confidence-building measures, capacity-building and regular institutional dialogue. One of the most important findings of these processes is the confirmation that international law also applies in cyberspace. This includes the fundamental principles of the UN Charter, especially the sovereign equality of states, the peaceful settlement of disputes, the prohibition of the threat or use of force, and the principle of non-intervention (United Nations, 2021).

Despite this general agreement, open questions remain regarding how individual rules apply in specific cyber circumstances. Particularly challenging issues include sovereignty, due diligence, non-intervention, attribution, proportionality, countermeasures and the threshold for the use of force. The UN therefore has an important role in further developing shared understandings, not necessarily through the immediate adoption of binding rules, but through the gradual development of diplomatic consensus (United Nations, 2025).

An important element of the UN normative framework is the set of voluntary norms of responsible state behaviour. Their significance does not lie in direct legal coercion, but in shaping expectations, political standards and criteria for assessing responsible behaviour. The protection of critical infrastructure has a special place in this context, since cyber activities targeting energy, health, finance, transport or telecommunications can directly affect public safety and the functioning of the state (United Nations, 2021, 2025).

Confidence-building measures reduce the risk of misperception, incorrect attribution and unintended escalation. They include information exchange, points of contact, transparency of national policies, crisis communication and regular diplomatic consultations. Capacity-building enables states with limited institutional, technical and human resources to participate in global cyber governance. The UN therefore acts as a global normative pillar of cyber diplomacy: it does not directly manage incidents, but establishes a minimum common framework of rules, trust, capabilities and dialogue.

The intergovernmental GGE and OEWG processes do not exhaust the normative development of cyberspace. A parallel multistakeholder track developed alongside them, most visibly through the Paris Call for Trust and Security in Cyberspace, launched by France in November 2018. The Paris Call sets out nine principles for the security of cyberspace and has been endorsed by states, technology companies and civil society organisations, including firms that operate the infrastructure most directly affected by the principles it proposes (France, Ministry for Europe and Foreign Affairs, 2018). Its significance lies less in legal force, which it lacks, than in demonstrating that normative consensus on responsible behaviour in cyberspace is also being built outside the UN's intergovernmental format.

The UN normative framework was extended further in December 2024 with the adoption of the United Nations Convention against Cybercrime, the first binding UN treaty in this domain (United Nations, 2024a). Several states sought unsuccessfully to remove language safeguarding

the Convention from being interpreted as permitting the suppression of human rights or fundamental freedoms, which illustrates that even binding instruments in this field remain sites of normative disagreement rather than settled consensus. A related development followed the Summit of the Future in September 2024, where member states adopted the Pact for the Future together with its annex, the Global Digital Compact, described by the UN as the first comprehensive global framework for digital cooperation, addressing connectivity, online safety and the governance of artificial intelligence alongside more traditional cybersecurity concerns (United Nations, 2024b). Its adoption suggests that the normative agenda long associated with cyber diplomacy is increasingly folded into a broader digital governance agenda.

COMPARATIVE STRATEGIC APPROACHES OF THE UNITED STATES, THE EU AND JAPAN

The United States: Strategic Competition and Digital Solidarity

The United States develops cyber diplomacy as part of a broader cyber and digital foreign policy. Its role derives from a combination of military, intelligence, economic, technological, diplomatic and private-sector power. American technology companies play a key role in global digital infrastructures, cloud services, operating systems, cybersecurity solutions, artificial intelligence and data platforms. U.S. cyber diplomacy therefore rests not only on state capabilities, but also on a wider technological ecosystem (U.S. Department of State, 2024).

In the 2024 *United States International Cyberspace and Digital Policy Strategy*, the United States places cyber and digital policy among the central instruments of foreign policy. The key concept is digital solidarity, which refers to cooperation among states, the private sector and civil society in shaping a secure, open, resilient and rights-respecting digital ecosystem. At the same time, the United States understands cyberspace as an arena of strategic competition between open and authoritarian models of digital governance. Its diplomacy therefore includes strengthening alliances, protecting critical infrastructure, joint responses to ransomware attacks, standardisation, capacity-building for partners and the protection of the open internet (U.S. Department of State, 2024).

This strategy builds on an earlier domestic process, the Cyberspace Solarium Commission, established by Congress in 2018 and reporting in March 2020. The Commission proposed a strategy of layered cyber deterrence, structured around three objectives: shaping the behaviour of other states through partnerships and norms, denying adversaries the benefits of their activity by strengthening resilience and critical-infrastructure protection, and imposing costs on malicious actors through the coordinated use of diplomatic, economic and military instruments (Cyberspace Solarium Commission, 2020). Several of its recommendations were subsequently incorporated into the National Defense Authorization Act, indicating a degree of continuity between domestic strategic planning and the international posture the United States has since adopted.

The European Union: Regulatory Power and Strategic Autonomy

The European Union develops a different model of cyber diplomacy. Its power derives primarily from regulatory capacity, the internal market, legal harmonisation, the Common Foreign and Security Policy, and the gradual formation of strategic autonomy. Since the EU is not a classical state but a multi-level political and legal system, cyber diplomacy is

shaped through coordination between EU institutions and Member States. This is particularly important in attribution, sanctions and foreign policy responses, where the national competences of Member States remain significant.

The basic instrument of European cyber diplomacy is the framework for a joint EU diplomatic response to malicious cyber activities, known as the Cyber Diplomacy Toolbox. The Council of the EU established it in 2017, while the revised implementing guidelines of 2023 emphasise coordinated strategies towards persistent cyber actors, attribution, strategic communication and links with other EU crisis and hybrid instruments (Council of the European Union, 2017, 2023). The EU has also developed a regime of restrictive measures against cyberattacks, which may include asset freezes and travel bans for responsible individuals or entities (Council of the European Union, 2024).

European cyber diplomacy is closely linked to the internal regulatory framework. The NIS2 Directive establishes measures for a high common level of cybersecurity across the Union and expands obligations for essential and important entities (European Union, 2022). The Cyber Resilience Act sets horizontal security requirements for products with digital elements, while the Artificial Intelligence Act establishes rules for the safe and trustworthy use of artificial intelligence (European Union, 2024a, 2024b). The European model therefore confirms that cyber diplomacy is also conducted through regulation, standards and market conditions that have effects beyond the borders of the EU. This regulatory expansion increasingly extends to the space domain: Georgescu, Cotroneo and Dinu (2025) show that the EU's approach to protecting critical space infrastructure evolved rapidly between 2020 and 2024, as the 2022 Strategic Compass and the 2023 EU Space Strategy for Security and Defence reframed space from a primarily scientific and civilian domain into one central to European security and defence, extending the logic of critical-infrastructure resilience into orbit.

The Cyber Diplomacy Toolbox was first applied in practice on 30 July 2020, when the Council adopted its first sanctions under the framework against six individuals and three entities located in Russia, China and North Korea, in connection with the WannaCry and NotPetya attacks, the Operation Cloud Hopper campaign, and the attempted attack against the Organisation for the Prohibition of Chemical Weapons (Council of the European Union, 2020). The measures, comprising asset freezes and travel bans, were presented as distinct from the political act of attribution, which the Council treats as a sovereign decision left to individual Member States. The regulatory dimension of this model can be situated within the theory of the Brussels effect, developed by Bradford (2020), which explains how EU regulation shapes global markets even without direct coercion, as multinational companies adjust their products and practices to EU standards in order to retain access to its internal market. Read alongside the instruments discussed above, this suggests that the EU's model of cyber diplomacy operates as much through market-driven diffusion of its own legal standards as through diplomatic bargaining.

Japan: Economic Security, Resilience and Indo-Pacific Cooperation

Japan places cyber diplomacy within a broader framework of national security, economic security, critical infrastructure resilience and regional cooperation in the Indo-Pacific. Its approach is linked to the security alliance with the United States, dialogue with the EU and cooperation with ASEAN countries. Japan does not act as a global platform power

in the American sense, nor as a regulatory power in the European sense, but as a highly technologically developed state that uses cyber diplomacy to strengthen resilience, supply chain security and regional stability (Ministry of Foreign Affairs of Japan, 2025a, 2026).

A distinctive feature of the Japanese model is the link between cybersecurity and economic-industrial policy. The strategy for the vitalisation of Japan's cybersecurity industry emphasises that excessive dependence on foreign solutions may constitute a strategic vulnerability. Japan therefore strengthens its domestic industry, human capital development, critical infrastructure protection and international cooperation in building partner capacities (Ministry of Economy, Trade and Industry, 2025a, 2025b). Its model confirms that cyber diplomacy is not only a normative or crisis-response field, but also an instrument of economic security and technological resilience.

The economic-security orientation of Japanese cyber diplomacy was reinforced by the National Security Strategy adopted by the Cabinet in December 2022, which introduced the concept of active cyber defence, understood as a whole-of-government capability to detect and respond to cyber threats before damage occurs, departing from Japan's previously more passive defensive posture (Cabinet Secretariat of Japan, 2022). The Strategy is closely linked to the Act on the Promotion of Economic Security through Integrated Implementation of Economic Measures, adopted in 2022, which identifies critical-infrastructure operators subject to enhanced reporting obligations across fifteen sectors including finance, energy, transport and telecommunications (Government of Japan, 2022). This combination of strategic and legislative measures illustrates that Japan's cyber diplomacy rests on domestic institutional reform as much as on external partnership.

DISCUSSION

The comparison of the UN, the United States, the EU and Japan shows that cyber diplomacy does not follow a single model. The UN develops it primarily as a global normative framework, the United States as an instrument of strategic competition and digital solidarity, the EU as a combination of regulatory power, joint diplomatic response and strategic autonomy, and Japan as part of broader economic-security resilience. What all approaches have in common is the recognition that cyberspace is no longer merely a technical environment, but a space of political influence, legal regulation, economic dependence and strategic competition.

Cyber diplomacy is therefore developing at three levels. The first is the normative level, where principles of responsible state behaviour, the application of international law, confidence-building measures and minimum standards of stability are shaped. The second is the strategic-security level, where states and regional organisations use cyber diplomacy for deterrence, attribution, sanctions, the protection of critical infrastructure and responses to malicious activities. The third is the technological-sovereignty level, where cyber diplomacy is linked to standards, industrial policy, digital platforms, artificial intelligence, cloud services and supply chains.

It follows that cyber diplomacy is no longer only reactive, but is becoming preventive and structural. Reactive diplomacy deals with incident response, public attribution, diplomatic protests and sanctions. Preventive diplomacy reduces risks through norms, trust, information exchange and crisis communication channels. Structural diplomacy shapes the technological

environment: standards, rules, data flows, supply chains and institutional mechanisms that determine the future digital order.

The role of the private sector is particularly important. In all analysed models, it is evident that states cannot effectively conduct cyber diplomacy without cooperation with technology companies, cloud service providers, critical infrastructure operators, industry and research institutions. This raises questions of responsibility, oversight and sovereignty, since global technology companies influence the digital autonomy of states through standards, platforms and security practices.

This comparison can be extended by distinguishing two structural mechanisms through which non-military power operates across the cases examined: a coercive mechanism, described by weaponized interdependence, through which control over network chokepoints is used to gather information or restrict access (Farrell & Newman, 2019), and a regulatory mechanism, described by the Brussels effect, through which standard-setting diffuses through markets rather than compulsion (Bradford, 2020). The American model relies more heavily on the former, the European model on the latter, while Japan combines elements of both within a smaller, regionally bounded framework. This transatlantic dynamic is also visible in the governance of artificial intelligence: Georgescu (2022) shows that despite the EU's more prescriptive regulatory posture and the United States' greater reliance on voluntary frameworks and private-sector standards, both sides have progressively converged around shared principles of trustworthy and secure AI, indicating that technological-sovereignty diplomacy can produce soft convergence even without a binding treaty framework. The tension between multilateral and multistakeholder tracks, visible in the coexistence of the UN's intergovernmental processes with the Paris Call and in the contested negotiation of the UN Convention against Cybercrime, further indicates that the normative level of cyber diplomacy is not converging on a single institutional format (France, Ministry for Europe and Foreign Affairs, 2018; United Nations, 2024a).

CONCLUSION

Cyber diplomacy has evolved from a specialised response to the security challenges of the digital environment into one of the central fields of contemporary international relations. The article has shown that it combines normative, preventive, strategic, technological-sovereignty and developmental functions. Its value lies not only in responding to cyber threats, but in its capacity to connect diplomacy, law, security, technology, the economy and resilience.

In this context, the UN provides a universal normative framework, the United States strategic leadership and coalition power, the EU regulatory influence and a legal framework, and Japan a connection between regional security and economic-technological resilience. These models differ, but together they confirm that cyber diplomacy is becoming a permanent component of the international order.

The future development of cyber diplomacy will depend on the ability of states and international organisations to move beyond a narrow understanding of cybersecurity as a technical issue. In the digital age, the most successful actors will be those capable of connecting foreign policy action, science, industry, regulation, the private sector, critical infrastructure protection and the development of trusted technological capabilities.

The adoption of the Global Digital Compact alongside the Pact for the Future in 2024 suggests a further direction for this development: the gradual absorption of cyber-diplomatic questions into a wider digital governance agenda that also encompasses connectivity, online safety and artificial intelligence (United Nations, 2024b). If Barrinha and Renard (2017) are correct that cyber diplomacy emerged through a still-unsettled process of diplomatisation, this broadening of scope may represent a new phase of that process, in which the field's institutional boundaries continue to shift rather than stabilise around a fixed definition.

REFERENCES

Attatfa, A., Renaud, K., & De Paoli, S. (2020). Cyber diplomacy: A systematic literature review. Procedia Computer Science, 176, 60–69. https://doi.org/10.1016/j.procs.2020.08.007

Badea, M., Bucovețchi, O., Gheorghe, A.V., Hnatiuc, M., & Raicu, G. (2025). Maritime industry cybersecurity threats in 2025: Advanced persistent threats (APTs), hacktivism and vulnerabilities. Logistics, 9(4), 178. https://doi.org/10.3390/logistics9040178

Barrinha, A., & Renard, T. (2017). Cyber-diplomacy: The making of an international society in the digital age. Global Affairs, 3(4–5), 353–364. https://doi.org/10.1080/23340460.2017.1414924

Bradford, A. (2020). The Brussels effect: How the European Union rules the world. Oxford University Press.

Bucovețchi, O., Badea, D., & Stanciu, R. (2018). Blockchain technology - a new approach in business environment. Proceedings of the Annual Session of Scientific Papers "IMT Oradea 2018", XVII(XXVII), 245-248.

Bucovețchi, O., Voipan, A.E., Voipan, D., & Stanciu, R.D. (2025). Redefining organizational resilience and success: A natural language analysis of strategic domains, semantics, and AI opportunities. Systems, 13(11), 999. https://doi.org/10.3390/systems13110999

Bucovețchi, O., Voipan, A.E., Voipan, D., Georgescu, A., & Dobrescu, R.M. (2026). Modeling organizational resilience in human-cyber-physical systems (Industry 5.0) through collective dynamics, decision scenarios and crisis-aware AI: A multi-method simulation approach. Applied Sciences, 16(1), 292. https://doi.org/10.3390/app16010292

Cabinet Secretariat of Japan. (2022). National security strategy of Japan. https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-e.pdf

Cici, A. (2025). Diplomacija digitalne suverenosti: strukturni izzivi za majhne države v tehnološki dobi. IFIMES. https://www.ifimes.org/sl/raziskave/diplomacija-digitalne-suverenosti-strukturni-izzivi-za-majhne-drzave-v-tehnoloski-dobi/5695

Council of the European Union. (2017). Council conclusions on a framework for a joint EU diplomatic response to malicious cyber activities ("Cyber Diplomacy Toolbox") (Doc. 9916/17). https://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf

Council of the European Union. (2023). Revised implementing guidelines of the Cyber Diplomacy Toolbox (Doc. 10289/23). https://data.consilium.europa.eu/doc/document/ST-10289-2023-INIT/en/pdf

Council of the European Union. (2020). Council Decision (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States. Official Journal of the European Union, L 246. https://eur-lex.europa.eu/eli/dec/2020/1127/oj/eng

Council of the European Union. (2024). Sanctions against cyber-attacks. https://www.consilium.europa.eu/en/policies/sanctions-against-cyber-attacks/

Cyberspace Solarium Commission. (2020). Final report. https://www.solarium.gov/report

European Union. (2022). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union. Official Journal of the European Union. https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

European Union. (2024a). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence. Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

European Union. (2024b). Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements. Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng

France, Ministry for Europe and Foreign Affairs. (2018). Paris Call for Trust and Security in Cyberspace. https://pariscall.international/en/

García de Soto, B., Georgescu, A., Mantha, B., Turk, Ž., Maciel, A., & Sonkor, M.S. (2022). Construction cybersecurity and critical infrastructure protection: New horizons for Construction 4.0. Journal of Information Technology in Construction, 27, 571-594. https://doi.org/10.36680/j.itcon.2022.028

Gheorghe, A.V., Georgescu, A., Bucovețchi, O., Lazar, M., & Scarlat, C. (2018). New dimensions for a challenging security environment: Growing exposure to critical space infrastructure disruption risk. International Journal of Disaster Risk Science, 9, 555-560. https://doi.org/10.1007/s13753-018-0197-2

Georgescu, A. (2022). Cyber diplomacy in the governance of emerging AI technologies - A transatlantic example. International Journal of Cyber Diplomacy, 3, 13-22. https://doi.org/10.54852/ijcd.v3y202202

Georgescu, A., Cotroneo, C., & Dinu, A. (2025). The European Union and the protection of critical space infrastructure from cyber-threats: A strategic approach? Proceedings of the European Conference on Cyber Warfare and Security, 24(1). https://doi.org/10.34190/eccws.24.1.3576

Georgescu, A., Vevera, V., & Cîrnu, C.E. (2020). The diplomacy of systemic governance in cyberspace. International Journal of Cyber Diplomacy, 1, 79-88.

Government of Japan. (2022). Act on the promotion of economic security through integrated implementation of economic measures. https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/index_e.html

Manor, I. (2019). The digitalization of public diplomacy. Palgrave Macmillan. https://doi.org/10.1007/978-3-030-04405-3

Ministry of Economy, Trade and Industry. (2025a). "Strategy for vitalization of the cybersecurity industry" compiled. https://www.meti.go.jp/english/press/2025/0305_002.html

Ministry of Economy, Trade and Industry. (2025b). Study group for promoting the development of cybersecurity talent compiles and announces its final report. https://www.meti.go.jp/english/press/2025/0514_002.html

Ministry of Foreign Affairs of Japan. (2025a). Diplomatic Bluebook 2025: Global security. https://www.mofa.go.jp/policy/other/bluebook/2025/en_html/chapter3/c030103.html

Ministry of Foreign Affairs of Japan. (2026). Cybersecurity. https://www.mofa.go.jp/policy/page18e_000015.html

Radanliev, P. (2024). Cyber diplomacy: Defining the opportunities for cybersecurity and risks from artificial intelligence, IoT, blockchains, and quantum computing. Journal of Cyber Security Technology. https://doi.org/10.1080/23742917.2024.2312671

United Nations. (2021). Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security: Note by the Secretary-General (A/76/135). United Nations General Assembly. https://digitallibrary.un.org/record/3934214

United Nations. (2024a). United Nations Convention against Cybercrime (General Assembly Resolution 79/243). https://www.unodc.org/unodc/en/cybercrime/convention/home.html

United Nations. (2024b). Pact for the Future, Global Digital Compact and Declaration on Future Generations (General Assembly Resolution A/RES/79/1). https://www.un.org/en/summit-of-the-future/global-digital-compact

United Nations. (2025). Developments in the field of information and telecommunications in the context of international security: Report of the Secretary-General (A/80/257). United Nations General Assembly. https://digitallibrary.un.org/record/4087789

U.S. Department of State. (2024). United States international cyberspace and digital policy strategy. https://www.state.gov/wp-content/uploads/2024/07/United-States-International-Cyberspace-and-Digital-Strategy-FINAL-2024-05-15_508v03-Section-508-Accessible-7.18.2024.pdf



Tina ANDOLJŠEK is a legal professional from the Ministry of Defence of Republic of Slovenia. She is active in both domestic and international legal environments, particularly at the European level. In addition to the legal field, she is engaged in higher education.



Andrej VASTL is the Acting Director-General of the Directorate for Science at the Ministry of Education, Science and Youth of the Republic of Slovenia. He is an expert in security, crisis management, and digital transformation, with extensive experience in national security, regulatory affairs, and the implementation of advanced technologies in decision-making processes.



This is an open access article distributed under the terms and conditions of the
Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.