ISSN (онлайн): 2663-8959 | ISSN (друк): 2308-6912
УДК 327.82:004.056
DOI: https://doi.org/10.17721/apmv.2026.167.1.53-60

CYBER DIPLOMACY AS AN INSTRUMENT OF COGNITIVE WARFARE IN CYBERSPACE

КІБЕРДИПЛОМАТІЯ ЯК ІНСТРУМЕНТ КОГНІТИВНОЇ ВІЙНИ У КІБЕРПРОСТОРІ

Oleh Kuz
Doctor of Sciences (Philosophy), Professor, Head of the Department of International Relations and Political Philosophy, Educational and Scientific Institute of International Relations, Simon Kuznets Kharkiv National University of Economics,
e-mail: oleh.kuz@hneu.net
ORCID ID: https://orcid.org/0000-0003-1359-2466

Danylo Nepochatov
PhD Student, Department of International Relations and Political Philosophy, Educational and Scientific Institute of International Relations, Simon Kuznets Kharkiv National University of Economics,
e-mail: danylo.nepochatov@hneu.net
ORCID ID: https://orcid.org/0009-0006-5819-5842

Олег Кузь
доктор філософських наук, професор, завідувач кафедри міжнародних відносин і політичної філософії, Навчально-науковий інститут міжнародних відносин, Харківський національний економічний університет імені Семена Кузнеця,
e-mail: oleh.kuz@hneu.net
ORCID ID: https://orcid.org/0000-0003-1359-2466

Данило Непочатов
аспірант кафедри міжнародних відносин і політичної філософії,
Навчально-науковий інститут міжнародних відносин, Харківський національний економічний університет імені Семена Кузнеця,
e-mail: danylo.nepochatov@hneu.net
ORCID ID: https://orcid.org/0009-0006-5819-5842

***Abstract**. This article examines the systemic transformation of cyber diplomacy from a conventional instrument of cyberspace regulation and rule-making into an active mechanism of cognitive warfare. The study investigates how cyberspace has evolved beyond technical and legal domains into a primary theater for meaning-based and narrative confrontation. Methodologically grounded in Alexander Wendt's constructivist paradigm of international relations, the theory of strategic narratives (systemic, identity, and issue-based), and case studies, the authors characterise cyber diplomacy as an instrument of the narrative construction of reality. The research demonstrates that due to institutional stagnation at multilateral platforms like the United Nations (the UN GGE process) and profound value-based divergences between democratic and autocratic regimes, the public attribution of cybercrimes has transitioned from a legal procedure into a strategic weapon of perception management. To illustrate this shift, the paper analyzes the geopolitical discourse surrounding the Volt Typhoon campaign, France's public attribution of decade-long cyber espionage to Russia's APT28, and the Czech Republic's May 2025 standalone attribution of MFA cyberattacks to Chinese-linked groups, which triggered an unprecedented condemnation of China by NATO. It also explores the rise of artificial intelligence and generative 'slopaganda' as force multipliers in manipulating collective consciousness, and details NATO's newly developed cognitive warfare defensive framework (2021-2025). The article concludes with practical recommendations for states, emphasizing the need to institutionalize rapid and persuasive cyber attribution mechanisms while actively building societal cognitive resilience to protect democratic decision-making.*

***Keywords:** cyber diplomacy, cognitive warfare, diplomatic attribution, strategic narratives, international relations, cyberspace, interstate confrontation.*

***Анотація.** У статті досліджено системну трансформацію кібердипломатії з традиційного інструменту регулювання та кодифікації норм відповідальної поведінки держав*

https://doi.org/10.17721/apmv.2026.167.1.53-60
у кіберпросторі на дієвий механізм ведення когнітивної війни. Кіберпростір концептуалізується не просто як технічне середовище чи сфера правового регулювання, а як первинний театр воєнних дій, де боротьба ведеться за людську свідомість і смисли. Методологічну основу дослідження сформовано на основі конструктивістського підходу Александра Вендта («анархія — це те, що держави з неї роблять»), теорії стратегічних наративів (системних, ідентичнісних та проблемних), а також прикладного аналізу кейсів (case-study). Автори доводять, що в умовах інституційної стагнації на таких міжнародних майданчиках, як ООН, та глибокого ціннісного розколу між демократичними та авторитарними режимами, публічна та дипломатична атрибуція кіберзлочинів перетворилася на потужну зброю управління сприйняттям. Проаналізовано геополітичний дискурс навколо кампанії Volt Typhoon, офіційне звинувачення Францією групи APT28 та Росії у багаторічному шпигунстві, а також безпрецедентну публічну атрибуцію Чехією у травні 2025 року кібератак на своє МЗС китайським хакерам, що призвело до засудження КНР з боку НАТО. Досліджено нові технологічні виклики, зокрема використання генеративного штучного інтелекту та концепт «слопаганди» (slopaganda) як множників сили у маніпулюванні масовою свідомістю. Детально розкрито структуру оборонної концепції НАТО з когнітивної війни (2021-2025) та її три захисні функції, включаючи послаблення спроможностей супротивника, покращення людського та технологічного розуміння й розбудову когнітивної стійкості. Сформульовано рекомендації для держав щодо інституціоналізації швидкої атрибуції кібератак та побудови стійкої ціннісної рамки для захисту democratic decision-making від когнітивних загроз у міжнародній політиці.

Ключові слова: *кібердипломатія, когнітивна війна, дипломатична атрибуція, стратегічні наративи, міжнародні відносини, кіберпростір, міждержавне протиборство.*

Introduction. Cyberspace security has become a crucial priority for states in the twenty-first century. It benefits both governments and their citizens by enabling the development of advanced technologies and digital innovation.

Many scholars conceptualise cyber diplomacy as an instrument for regulating and institutionalising relations among actors in international relations within the diplomatic arena. However, the growing divergence among states regarding the regulation and functioning of cyberspace calls into question the role of cyber diplomacy – particularly amid geopolitical confrontation in cyberspace between a group of states led by Russia and China and Western countries.

Given the inability to resolve conflicts in cyberspace or to reach agreements on its regulation through diplomatic negotiations, states increasingly resort to public cyber attribution – the process of tracing and identifying the perpetrator of a cyberattack or other cyber operation. In the course of attribution investigations, security analysts seek to identify the tactics, techniques, and procedures employed by malicious actors, as well as to determine who is responsible for the attack and why it was carried out. The majority of public accusations have been directed at the Russian Federation and the People's Republic of China.

Holding perpetrators of cybercrime accountable is complicated by the possibility of anonymous interference in a state's cyberspace and the use of proxy hacker groups that may lack an explicit link to the aggressor state. These circumstances compel victim states to engage in narrative communication to present their own version of events and mobilise support from allies. At the same time, states accused of aggression attempt to deny involvement by presenting what they claim is "irrefutable" evidence of their non-participation. Consequently, cyber conflict shifts from the technical domain into a cognitive dimension, where victory depends not on truth or justice, but on the persuasiveness of the narrative.

Thus, the shift of cyber diplomacy from norm development to narrative construction underscores its growing importance as a tool of cognitive confrontation, emphasizing its relevance for international relations and security.

Particular attention is paid to the role of diplomatic attribution as a mechanism of narrative communication aimed at shaping international legitimacy and mobilising allies in the context of interstate confrontation. The article also examines how competition between normative approaches to cyberspace regulation transforms cyber diplomacy from an instrument of institutionalising

cooperation into a component of broader cognitive strategies in contemporary conflicts.

The purpose of the arcticle is to characterise cyber diplomacy as an instrument for the narrative construction of reality by actors in international relations.

Literature Review. Contemporary scholarship demonstrates a shift from the study of cyber norms as a process of rule-making toward the analysis of their ongoing contestation. The origins of these debates are associated with the UN GGE process and the codification efforts of 2015 (United Nations, 2015), as well as with the legal systematisation of the application of international law to cyber operations in the Tallinn Manual 2.0 (Schmitt, 2017). At the same time, recent approaches conceptualise cyber diplomacy as a process of "diplomatization" – can institutional and political arena of contestation in which norms are shaped through struggles over legitimacy and positioning (Barrinha, 2024; Broeders & van den Berg, 2020).

Kurawska (2019) emphasises that the Western-centric perspective on the development of international law increasingly encounters resistance from Eastern states. The theory of strategic narratives illustrates how power in cyberspace is exercised through the construction of identities and meanings (Miskimmon et al., 2013). At the practical level, public attribution has become an instrument of strategic communication that states use to signal resolve and mobilise support, balancing deterrence with the risk of escalation (Egloff & Smeets, 2023; IISS, 2025). Debates surrounding the Volt Typhoon case further demonstrate that norm interpretation depends on struggles over narrative credibility (IISS, 2026).

Overall, scholars indicate that cyberspace is increasingly defined not only by legal frameworks but also by communicative narratives and the dynamics of cognitive confrontation in the international arena.

Main results of the research. Traditionally, cyber diplomacy has been understood as a mechanism for regulating international relations in cyberspace through the development of legal instruments, the formulation of norms of responsible state behaviour, and the establishment of multilateral platforms to counter cybercrime and hold perpetrators accountable. In this context, states and international organisations seek to institutionalise rules of conduct in cyberspace. However, despite prolonged negotiation processes, a substantial consensus has yet to be achieved.

Cyber diplomacy is closely intertwined with cybersecurity, yet the two perform distinct functions. Cybersecurity focuses on preventing unauthorised access and hacker attacks on computer systems. It concentrates on the technical aspects of cyberspace governance, whereas cyber diplomacy addresses the political dimension of cyber threats (Radanliev, 2025).

The emergence of cyber diplomacy began with the integration of digital communication tools and the Internet into diplomatic practice. The first recorded use of digital methods in diplomacy was an email sent on February 4, 1994, by Swedish Prime Minister Carl Bildt to U.S. President Bill Clinton. Bildt congratulated Clinton on lifting the embargo against Vietnam and noted that Sweden, as a leading technology nation, considered it appropriate to be among the first to use the Internet for political contacts and global communication (Tom Fletcher, 2016).

The use of social media, online platforms, and digital tools for diplomatic engagement is associated with the phenomenon of "digital diplomacy" or "Diplomacy 2.0," which aims to engage and communicate with international audiences (Radanliev, 2025). Several scholars note that during the 2000s, cyber diplomacy was widely understood as the application of digital tools for diplomatic communication. In 2010, the EastWest Institute emphasised in an analytical report that cyber diplomacy should be regarded as a distinct branch of diplomatic activity designed to address the international dimensions of cyber policy and cybersecurity. The authors stressed the importance of moving beyond a narrow focus on cyber defence or cyber warfare and instead developing diplomatic mechanisms of engagement in cyberspace (Gady & Austin, 2010). Thus, cyber diplomacy increasingly came to be understood as an instrument for developing cyber norms among states to regulate cyberspace.

Accordingly, digital diplomacy concerns the implementation of digital communication tools in diplomatic practice, while cyber diplomacy functions as an instrument for regulating relations in the cyber domain among actors in international relations.

This evolution of cyber diplomacy was significantly influenced by Russia's 2007 cyberattacks against Estonia (Ottis, n.d.). Prior to this event, states and intergovernmental organisations did not

treat cybersecurity and cyberspace as strategically important domains of diplomacy. The Estonian precedent prompted NATO and the European Union to take their first institutional steps. In 2008, the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) was established in Tallinn, while the European Union began developing its own cyber incident response mechanisms, which later materialised in the CSIRT network and the NIS Directive (CCDCOE Centre, 2026).

In recent years, key international actors – particularly the United Nations, the United States, and the European Union – have significantly intensified their cyber diplomatic efforts. The regulation of international relations is impossible without international law. Western states have sought to regulate cyberspace through existing legal frameworks. The first such instrument was the Council of Europe Convention on Cybercrime – the Budapest Convention – adopted in 2001, which became the first universal international legal instrument aimed at combating cybercrime (The Budapest Convention on Cybercrime, 2023). Another important document facilitating the application of international humanitarian law to cyberspace is the Tallinn Manual, which affirms that the fundamental principles governing state conduct during armed conflicts also apply to cyber operations. Consequently, the use of cyber weapons is subject to the same legal restrictions as traditional means of warfare (Schmitt, 2017).

On the other hand, Russia and the People's Republic of China advocate a different vision of cyberspace governance. In 1998, the Russian Federation initiated a United Nations General Assembly resolution on "developments in the field of information and telecommunications in the context of international security" (UN, 1998), linking ICTs to threats to international peace and emphasising the risk of an "information arms race." From the outset, the Russian approach favoured the creation of a specific international treaty on information security grounded in a strict interpretation of sovereignty.

China, in parallel with Russia, has advanced the concept of "cyber sovereignty," which combines a normative dimension (the right of states to determine their own model of internet governance) with a material dimension (data localisation and infrastructure control). At the international level, Beijing supports an intergovernmental governance model and criticises the multistakeholder approach as a form of concealed hegemony (Hung, 2025).

At first glance, the primary obstacle to consensus is the fundamental divergence in legal approaches to cyberspace governance. However, behind this legal debate lies a deeper political and value-based conflict. Proponents of applying existing international law seek to preserve the openness, interoperability, and global character of cyberspace, whereas advocates of a separate regulatory regime aim to institutionalise control, fragmentation, and informational sovereignty.

Although the United Nations was expected to serve as the principal diplomatic arena for resolving disputes in cyberspace, it has struggled to fulfil this role effectively. The first Group of Governmental Experts (GGE) failed to produce a consensus report due to disagreements among the UN Security Council's permanent members. The fourth GGE (2014–2015) succeeded in formulating a package of eleven voluntary norms of responsible state behaviour, including the prohibition of attacks on critical infrastructure, protection of supply chains, the inviolability of CERT/CSIRT entities, and respect for human rights (UN GGE, 2015).

Simultaneously, in 2011 and 2015, Russia, China, and their Shanghai Cooperation Organisation partners promoted an International Code of Conduct for Information Security, which institutionalised the principle of "cyber sovereignty." Western states rejected this initiative as legitimising censorship. The fifth GGE (2016–2017) reached an impasse. In 2018, Russia initiated the Open-Ended Working Group (OEWG), which adopted a consensus report in 2021 reaffirming previously agreed norms and subsequently replaced the GGE as the primary institutional platform. In December 2024, the UN General Assembly adopted a new Convention against Cybercrime – the first global treaty in this field since the Budapest Convention (United Nations Convention against Cybercrime, 2024).

Nevertheless, the confrontation between the West and the Russia–China bloc does not fully capture the architecture of contemporary cyberspace competition. Countries of the Global South– such as India, Brazil, South Africa, and ASEAN member states–have emerged as influential actors. Romanian scholar Daria-Elena Popescu (2025) argues that this group increasingly articulates a position of "digital non-alignment."

The roots of digital non-alignment can be traced back to the Cold War and to countries like India's reluctance to become entangled in superpower rivalry. Today's cyberspace confrontation has

revived this logic. States in the Global South are hesitant to fully embrace the Western multistakeholder model, as they perceive risks to their own security. However, they also remain cautious of the rigid digital authoritarianism promoted by Moscow and Beijing. For these states, the priority is to develop their own technological capacities while preserving sovereignty without becoming isolated from the global economy.

Accordingly, the struggle for their support has become a central task of cyber diplomacy. Legitimacy will ultimately belong to the actor whose strategic narrative of cyberspace governance proves more inclusive and adaptable.

Researcher Xymena Kurowska argues that contemporary cyber norm politics is at a deadlock because the strategic construction of norms by a Western-led "like-minded" coalition is increasingly perceived as lacking legitimacy and provokes normative resistance (Kurowska, 2019). Without incorporating alternative narratives into the rule-making process, even formally agreed documents risk remaining fragile compromises rather than foundations of a stable cyber order.

From a theoretical perspective, the shift from legal regulation to narrative confrontation is best explained through the constructivist paradigm of international relations. Unlike neorealism or neoliberalism, which prioritise material factors, Alexander Wendt argues that socially shared ideas and knowledge shape the international system. According to Wendt's well-known thesis, "anarchy is what states make of it" (Mengshu, 2020). Under such conditions, the dynamics of international relations depend on which shared ideas states can institutionalise. Consequently, the actor that dominates the narrative surrounding a cyber incident gains the power to construct the very nature of international cybersecurity and to define roles such as "victim," "aggressor," or "ally" for other actors.

A fundamental challenge of the cyber diplomatic process lies in the attribution of cyberattacks – the process of identifying individuals, criminal groups, or state actors responsible for conducting a cyber operation. Technical uncertainty, evidentiary ambiguity, anonymity, and the use of proxy actors make attribution one of the most complex issues in cybersecurity (Rogndokken et al., 2025). In such circumstances, establishing the factual truth of aggression often becomes secondary to the struggle over defining "what happened," "who is the aggressor," and "what response is legitimate."

These political realities reshape the understanding of cyber diplomacy – from a diplomatic strategy for resolving cyberspace-related issues into an increasingly explicit arena of narrative contestation. States seek not only to prove technical responsibility for an incident, but also to consolidate their version of events through diplomatic attribution publicly. Attribution processes may last for years, and for both accusing and accused states, it is crucial to present their own "story" and persuade others of its credibility.

On the political stage, adversaries construct strategic narratives. According to Alister Miskimmon and Ben O'Loughlin (2017), strategic narratives are a means by which political actors attempt to shape a shared understanding of the past, present, and future of international politics in order to influence the behaviour of domestic and international audiences. The authors distinguish three types of narratives: systemic (about the international order), identity (about who the actors are), and issue narratives (about specific policy questions). Publicly assigning responsibility for a cyberattack thus becomes an instrument of cognitive influence aimed at shaping international perception, legitimising countermeasures, and consolidating allies.

As a result, in contemporary interstate confrontation, diplomatic attribution increasingly transforms into a tool of perception management through which strategic narratives are constructed. The primary objective is no longer solely to hold perpetrators legally accountable for cybercrime, but rather to shape target audiences' consciousness and convince partners of one's legitimacy. Diplomacy thereby shifts from a mechanism of compromise-seeking to a strategic arena of cognitive warfare, where new rules of dominance are formed.

The concept of cognitive warfare is not new. In the fifth century BCE, Sun Tzu described methods of warfare, stating: "If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained, you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle" (Giles, 2013). This emphasis on managing perception and information as a condition of victory remains highly relevant in today's cyberspace.

Contemporary scholars define cognitive warfare as a concept whereby one state seeks to

influence another through manipulation aimed at weakening, subordinating, or even destroying it. This includes psychological tactics, information manipulation, and cognitive strategies designed to influence the emotions, beliefs, perceptions, and behaviour of individuals, groups, or entire populations. In this context, cyber diplomatic attribution functions as one of the mechanisms for achieving these objectives in the international arena.

NATO has taken the threat of cognitive warfare seriously. In 2020, NATO's Innovation Hub, under Allied Command Transformation, launched research into cognitive warfare as a new form of conflict. It proposed the recognition of a sixth operational domain–the "Human Domain" (Cognitive Warfare, 2025). In June 2021, France hosted NATO's first scientific meeting dedicated to cognitive warfare. Researchers and practitioners have since noted the gradual institutionalisation of cognitive warfare as a field of study. NATO experts conceptualise cognitive warfare as a dimension of confrontation that integrates psychological operations, influence operations, and cyber tools, complemented by advances in psychological science. It emerges at the intersection of two previously relatively autonomous domains: on the one hand, PSYOPS and mechanisms of "soft power," and on the other, cyber operations targeting or degrading information infrastructure (Claverie & Cluzel, 2021). This intersection creates an interdisciplinary framework for analysing how technology affects human perception, behaviour, and political agency.

From the perspective of cognitive confrontation, the case of the Chinese-linked hacking group Volt Typhoon is illustrative. In May 2023, Microsoft released a report alleging a direct connection between Volt Typhoon and the People's Republic of China (Microsoft Threat, 2023). In 2024, official Beijing responded by asserting that Volt Typhoon was an international ransomware group and that U.S. accusations of links to the Chinese government were unfounded (Bruss, 2026).

This case demonstrates that justice and the technical aspects of attribution may become secondary to the more persuasive effort to construct, disseminate, and prevail through competing narratives in cognitive confrontation.

Columbia University researcher Virpratap Vikram Singh offers a similar assessment. According to him, France deliberately issued its first direct public attribution, linking a decade of malicious cyber activity to the APT28 group and Russia, to raise public awareness in French society about broader Russian threats. In May 2025, the Czech Republic publicly attributed cyber espionage activities within its Ministry of Foreign Affairs to a Chinese-linked group. This marked Prague's first standalone public attribution against China. The disclosure aimed to inform the public about threats emanating from China while simultaneously demonstrating determination to counter them. It quickly generated statements of support, including an unprecedented condemnation of China by NATO (Virpratap, 2026).

Conclusions. This article has examined cyber diplomacy as a potential instrument of cognitive confrontation among states in cyberspace and compared this perspective with the conventional understanding of cyber diplomacy. The study demonstrates that the inability to regulate cyberspace effectively through international platforms such as the United Nations contributes to growing tensions among states – tensions that diplomacy is not always capable of resolving. Under such conditions, public attribution of cybercrime and the construction of reality through narrative become more significant than achieving consensus or ensuring justice. Consequently, cyber attribution becomes an important political act that shapes international perceptions and mobilises allies.

The analysis of several cyber incident cases, including Volt Typhoon, supports this argument and illustrates that the struggle concerns not only the establishment of responsibility, but also the right to define the interpretation of reality itself.

Cyber diplomacy is transforming an instrument of institutional cooperation into a mechanism of strategic communication. On the one hand, this shift enables states to articulate their own interpretation of events through narrative framing and to strengthen their positions on the international stage. On the other hand, it reveals that achieving justice and mutual understanding among international actors in cyberspace currently appears increasingly unrealistic.

For states to effectively employ all dimensions of cyber diplomacy, they should:

1. Institutionalise attribution mechanisms. States must learn not only to respond technically to cyber threats, but also to expose aggressors rapidly and convincingly. This requires coordination among government bodies, intelligence agencies, and diplomatic institutions. Attribution should

become a systematic instrument of deterrence and international signalling.

2. Enhance societal resilience to cognitive threats. Cyber diplomacy increasingly operates within a cognitive dimension where perception management is central. It is essential not only to counter disinformation campaigns but also to build a coherent, value-based narrative framework actively. This will reduce the influence of adversarial actors on state institutions and consolidate society in the face of cyber threats.

3. Develop multilateral cyber alliances. Given the stagnation of the UN framework and the growing divergence between democratic and authoritarian approaches to cyberspace governance, greater emphasis should be placed on forming coalitions of like-minded states. Joint and coordinated attribution of cyber incidents – such as solidarity statements by NATO or EU member states – significantly enhances the legitimacy of the narrative advanced. Such collective action generates stronger political and reputational pressure on violator states than isolated démarches.

4. Engage non-state actors in the cyber diplomatic process. Technology companies such as Microsoft, Google, and others often possess greater resources and expertise than many states. They are frequently the first to detect cyber threats and to develop defensive measures. Public–private partnerships could substantially strengthen interstate alliances and help build robust cyber defence systems equipped with advanced detection mechanisms for cybercriminal activity.

Funding: *no external funding.*

Conflict of Interest: *the authors declare no conflict of interest regarding the publication of this article.*

Data Availability Statement: *not applicable*

References

Bruss, J. (2026). Volt Typhoon's long shadow. IISS. https://www.iiss.org/online-analysis/cyber-power-matrix/2026/01/volt-typhoons-long-shadow/

CCDCOE Centre. (2026). About us. https://ccdcoe.org/about-us/

Claverie, B., & du Cluzel, F. (2021). Cognitive warfare: The advent of the concept of "cognitics" in the field of warfare. NATO Innovation Hub. https://www.innovationhub-act.org/sites/default/files/2021-01/Cognitive%20Warfare.pdf

Cybil Portal. (n.d.). The Budapest Convention on Cybercrime: Benefits and impact in practice. Retrieved February 27, 2026, from https://cybilportal.org/publications/the-budapest-convention-on-cybercrime-benefits-and-impact-in-practice/

Fletcher, T. (2016). Naked diplomacy: Power and statecraft in the digital age. HarperCollins. https://tomfletcher.global/publications/details/6

Gady, F.-S., & Austin, G. (2010). Russia, the United States, and cyber diplomacy. EastWest Institute. https://www.files.ethz.ch/isn/124603/russia_usa_cyber_diplomacy.pdf

Hung, H. T. (2025). Exploring China's cyber sovereignty concept and artificial intelligence governance model: A machine learning approach. Journal of Computational Social Science, 8(1), 24. https://doi.org/10.1007/s42001-024-00346-8

Institute for National Strategic Studies. (2026). Cognitive warfare 2026: NATO's chief scientist report as sentinel call for operational readiness. https://inss.ndu.edu/Media/News/Article/4371195/cognitive-warfare-2026-natos-chief-scientist-report-as-sentinel-call-for-operat/

Kurowska, X. (2019). When one door closes, another one opens: The ways and byways of denied access, or a Central European liberal in fieldwork failure. Journal of Narrative Politics, 5(2), 101–114. https://jnp.journals.yorku.ca/index.php/default/article/view/101

Mengshu, Z. (2020, May 19). A brief overview of Alexander Wendt's constructivism. E-International Relations. https://www.e-ir.info/2020/05/19/a-brief-overview-of-alexander-wendts-constructivism/

Microsoft Threat Intelligence. (2023, May 24). Volt Typhoon targets US critical infrastructure with living-off-the-land techniques. Microsoft Security Blog. https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/

Miskimmon, A., & O'Loughlin, B. (2017). Russia's narratives of global order: Great power legacies in a polycentric world. Politics and Governance, 5(3), 111–120. https://doi.org/10.17645/pag.v5i3.961

Ottis, R. (2008). Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective. Cooperative Cyber Defence Centre of Excellence (CCDCOE). https://ccdcoe.org/uploads/2018/10/Ottis2008_EstoniaCyberAttacks.pdf

Popescu, D.-E. (2025). Cyberdiplomacy and the new digital non-alignment in the Global South: India as a case study of technological sovereignty in the age of AI. International Journal of Cyber Diplomacy, 6, 39–59. https://doi.org/10.54852/ijcd.v6y202503

Radanliev, P. (2025). Cyber diplomacy: Defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing. Journal of Cyber Security Technology, 9(1), 28–78. https://doi.org/10.1080/23742917.2024.2312671

Rogndokken, M. R., Delport, P. M. J., & van Niekerk, J. (2025). Facilitating informed cyberattack attributions: The PACT model. Procedia Computer Science, 263, 399–409. https://doi.org/10.1016/j.procs.2025.07.049

Schmitt, M. N. (Ed.). (2017). Tallinn Manual 2.0 on the international law applicable to cyber operations (2nd ed.). Cambridge University Press. https://doi.org/10.1017/9781316822524

Sun Tzu. (2013). The art of war (L. Giles, Trans.). Routledge. https://doi.org/10.4324/9781315030081

United Nations. (1998, September 23). Letter dated 23 September 1998 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General (A/53/425). UN Digital Library. https://digitallibrary.un.org/record/261158

United Nations Group of Governmental Experts (UN GGE). (2015). Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174). United Nations. https://digitallibrary.un.org/record/799853

United Nations Office on Drugs and Crime (UNODC). (2024). United Nations Convention against Cybercrime. https://www.unodc.org/unodc/en/cybercrime/convention/home.html

Virpratap, V. S. (2026). Reframing cyber attribution. IISS. https://www.iiss.org/online-analysis/charting-cyberspace/2025/12/reframing-cyber-attribution/

Received: 20.01.26 / Revised: 14.02.26 / Accepted: 18.03.26 / Published: 30.06.26