EU Cyber Diplomacy in the Context of Russian Aggression in Ukraine

Oleksandr Korchenko[1,†], Serhii Kondratiuk[1,*,†]

[1] *State University of Information and Communication Technologies, Solomianska 7, 03110 Kyiv, Ukraine*

Abstract

The full-scale Russian invasion of Ukraine has catalyzed a fundamental transformation of security strategies across the Euro-Atlantic region, escalating the use of hybrid threats designed to destabilize Ukraine and the European Union. This paper analyzes the EU's evolving cyber diplomacy in response to this aggression. It posits a central hypothesis: while the EU has achieved significant institutional and regulatory progress in securing critical infrastructure against cyber threats since 2022, its capacity to counter hybrid attacks targeting societal institutions and democratic processes remains underdeveloped, constituting a critical vulnerability. The methodology involves an analysis of the EU's recent legislative frameworks—including the Cyber Resilience Act, the NIS2 Directive, and the Cyber Solidarity Act—and a comparative examination of case studies involving Russian electoral interference in Moldova (2024), Romania (2024–2025), and Poland (2025). The findings reveal a stark asymmetry in the EU's defensive posture, with robust infrastructural defenses contrasting sharply with a vulnerable societal flank. The paper concludes that addressing this imbalance requires a comprehensive, whole-of-society approach, moving beyond technical solutions to build systemic democratic resilience. The EU-Ukraine partnership emerges as a crucial nexus of this new security architecture, where Ukraine's battlefield experience informs and accelerates the development of a more holistic European defense against hybrid warfare.

Keywords

hybrid threats, cyber diplomacy, EU-Ukraine Cyber Dialogue, FIMI, Russian election interference, cyberspace, 2024 Moldova presidential election, 2024-2025 Romania presidential election

1. Introduction

Since the onset of Russia's full-scale invasion of Ukraine, hybrid threats originating from the Kremlin have significantly intensified and continuously evolved, targeting the instability of Ukraine, the European Union and its member states. These threats manifest in an unprecedented volume of cyberattacks on critical infrastructure, heightened activities by Russian intelligence services, attempts to interfere in electoral processes, the dissemination of disinformation, and efforts to undermine trust in democratic institutions.

The Russian aggression has served as a catalyst for a fundamental transformation of security strategies throughout the Euro-Atlantic region. The contemporary conflict increasingly transcends the boundaries of traditional military operations. Hybrid warfare involves the synchronized application of conventional and unconventional instruments of influence to exploit an adversary's weaknesses, operating beyond the scope of direct armed conflict. A key characteristic of this warfare is the deliberate blurring of the line between states of war and peace, which complicates the attribution and identification of informational and cyberattacks.

As noted by Volodymyr Horbulin, former director of Ukraine's National Institute for Strategic Studies, in his seminal work The World Hybrid War: Ukrainian Forefront "the concept of hybrid war has proven to be the most theoretically and practically suitable for defining the specific actions of the Russian Federation, which, by combining military, quasi-military, diplomatic, informational, and economic means, not hesitating to use nuclear blackmail, consistently tries to achieve its own political goals in Ukraine and other parts of the world, which are not fully understood by the international community" [1].

[1] *SMICS'25: Workshop on Cryptology and Data Security, October 16-18, 2025, Lviv, Ukraine*

* Corresponding author.

† These authors contributed equally.

o.korchenko@duikt.edu.ua (O.Korchenko); s.kondratiuk@duikt.edu.ua (S.Kondratiuk)

0000-0003-3376-0631 (O.Korchenko); 0009-0000-2354-8763 (S.Kondratiuk)

Within the academic literature, "cyber diplomacy" is understood as the application of diplomatic techniques and negotiations in international relations that deal with and regulate cyberspace-related issues [2].

One of the earliest definitions was formulated by the U.S. State Department in 2011, stating that cyber diplomacy encompasses “a wide range of U.S. interests in cyberspace. These include not only cyber security and Internet freedom, but also Internet governance, military uses of the Internet, innovation, and economic growth. Cyberspace has also become a foreign policy issue in multilateral fora, in our bilateral relationships, and in our relationships with industry and civil society” [3].

To avoid confusions in the terminology of diplomacy in the digital age British diplomat and researcher Shaun Riordan proposed the following definitional distinction: we should use the term "digital diplomacy" to refer to the use of digital tools and techniques to do diplomacy (including consular diplomacy), and we should use the term "cyber diplomacy" to refer to the use of diplomatic tools, and the diplomatic mindset, to resolve issues arising in cyberspace. According to these definitions, both digital diplomacy and cyber diplomacy can be carried out by state and non-state actors, including companies and NGOs [4].

After February 24, 2022, EU cyber diplomacy is implemented in two main areas. The first is the cyber defense of technical and infrastructure systems and networks that are critical to the functioning of the state. After all, the aggressor actively uses cyberattacks and physical sabotage to destabilize the work of state bodies, banks, energy, communications, transport, etc. The second, equally important, is the social front, where hybrid attacks, such as disinformation, manipulation of public opinion, and interference in electoral processes, are aimed at undermining trust in state institutions and civil society.

This research is guided by a central hypothesis: While the EU has achieved significant institutional and regulatory progress in securing critical infrastructure against cyber threats post-2022, its capacity to counter hybrid attacks targeting societal institutions and democratic processes remains underdeveloped and constitutes a critical vulnerability. This asymmetry has become particularly evident in the context of recent election campaigns in Moldova, Romania, and Poland during 2024 and 2025, which have exposed profound vulnerabilities in this domain.

To achieve the stated objective, this study analyzes recent changes in European cyber diplomacy in response to increasingly aggressive Russian hybrid attacks. It examines the key drivers and features of this process and identifies the political-institutional consequences for ensuring the digital sovereignty of Europe and Ukraine. The research is based on an analysis of new EU and Ukrainian legal regulations in cybersecurity and the works of Ukrainian and European authors studying Russian hybrid threats. The paper is structured as follows: first, an analysis of the EU's legislative and institutional achievements in cybersecurity; second, a detailed examination of the risks and gaps in societal resilience through case studies of recent elections; and finally, a conclusion that synthesizes the findings and their implications.

2. Main

2.1. Fortifying the Foundations: The EU's Push for Digital and Infrastructural Cyber Resilience

In response to the Russian invasion of Ukraine and the proliferation of hybrid threats, EU cybersecurity policy has undergone a significant transformation. Previously oriented primarily toward data protection and economic competition, it is now an integral part of a broader geopolitical strategy that openly identifies Russia as an "existential threat" [5]. This shift is evidenced by an unprecedented level of legislative activity in 2025, aimed at strengthening the collective resilience of the Union against increasingly sophisticated threats.

The rapid succession of major EU cybersecurity laws enacted between December 2024 and June 2025 is not coincidental. This legislative flurry is a direct and urgent response to the escalation of Russian hybrid warfare documented since 2022, demonstrating a powerful causal relationship where Russian aggression has acted as a political catalyst, accelerating and unifying the EU's legislative process in the security domain.

Over the past year, several key documents have entered into force, forming a multi-layered regulatory system for cyber defense:

- Cyber Resilience Act (CRA, December 2024): Building on the 2020 EU Cybersecurity Strategy, the CRA introduces mandatory security requirements for manufacturers and retailers of products with digital components, aiming to secure the entire supply chain from design to maintenance.1
- The Cybersecurity Act Amendment (January 2025): This targeted amendment expands the powers of the EU Agency for Cybersecurity (ENISA) and extends the scope of the European Cybersecurity Certification Framework (ECCF) to include "managed security services".
- Digital Operational Resilience Act (DORA, January 2025): This act addresses a critical gap in EU financial regulation by establishing a comprehensive framework to ensure the digital operational resilience of the financial sector against severe disruptions.
- Cyber Solidarity Act (February 2025): A cornerstone of the EU's collective defense, this act aims to enhance the Union's capacity to detect, prepare for, and respond to cyber threats. It establishes a European Cyber Shield through a network of Security Operations Centres and creates a Cyber Emergency Mechanism, which includes the EU Cybersecurity Reserve.
- EU Cybersecurity Blueprint (June 2025): Adopted by member states, this recommendation from the Council outlines a framework for EU cyber crisis management. It defines the roles of key actors like ENISA and the CSIRTs Network throughout the crisis lifecycle, from preparation to recovery. Henna Virkkunen, Executive Vice-President of the European Commission, emphasized that this blueprint is a "key component of our Union Preparedness Union Strategy" and a "practical tool for Member States and EU bodies to work together" [6].

The Directive on Measures for a High Common Level of Cybersecurity across the Union (NIS2), which entered into force in January 2023 with a final implementation date of 2025, serves as the central legal instrument in this new architecture, replacing the original NIS1 Directive. NIS2 significantly expands the scope of sectors covered, strengthens cybersecurity and risk management requirements, and introduces stricter rules for reporting cyber incidents. By harmonizing requirements and raising the accountability of corporate leadership, the directive establishes a standardized baseline for cybersecurity throughout the EU, with experts noting its potential to significantly enhance the protection of critical infrastructure [7].

Recognizing the necessity of modernizing its legislation for integration into the European cybersecurity space, Ukraine also took a pivotal step by adopting Law No. 11290 on March 27, 2025. This law implements the recommendations of the NIS2 Directive, creating a modern legal foundation for a national cyber incident response system and harmonizing with European norms. Crucially, its adoption was a key condition of the Ukraine Facility Plan, directly linking cybersecurity policy to Ukraine's financial support and European integration process. This demonstrates the EU's use of its regulatory and financial power to bind Ukraine closer, making security harmonization a non-negotiable component of the partnership.

The EU-Ukraine Cyber Dialogue, initiated in June 2021, has substantially strengthened since the start of the full-scale war. In 2025, Kyiv and Brussels agreed to a 4th round of the dialogue, focusing on concrete operational outcomes to bolster Ukraine's cyber resilience and improve bilateral cooperation on threat prevention and response. This collaboration includes flagship projects like EU4Digital's "Cyber East" and coordination with partners through the Tallinn Mechanism [8]. Ukraine's potential access to the EU Cybersecurity Reserve and structured cooperation with ENISA and Europol further institutionalize this partnership.

This deepening relationship marks a significant shift in perception. Ukraine is no longer viewed merely as a recipient of aid but is recognized as an "active contributor and innovative driver" in cybersecurity [9]. Its territory has become a real-world laboratory for hybrid warfare defense, providing invaluable, battle-hardened tactical and strategic intelligence. This creates a new dynamic where the EU provides the regulatory framework and financial support, while Ukraine provides unique experience that shapes and accelerates the evolution of European cyber defense. This symbiotic relationship is evident in the EU Preparedness Union Strategy, which incorporates lessons from Ukrainian responses to major cyberattacks, such as the 2022 attack on Viasat and the 2025 attack on Ukrzaliznytsia (Ukrainian Railways) [10].

2.2. The Unprotected Flank: Hybrid Attacks on EU Societal and Democratic Institutions

Despite substantial progress in fortifying institutional and technical aspects of cybersecurity, hybrid attacks on the EU's societal institutions and civil society continue to pose a significant challenge. These

attacks target not just critical infrastructure but also aim to deepen social conflicts and erode trust in government and democratic processes. In March 2025, the European External Action Service (EEAS) published its 3rd Report on Foreign Information Manipulation and Interference (FIMI) Threats, which Kaja Kallas, High Representative of the Union for Foreign Affairs and Security Policy, noted for its novelty in "exposing the massive digital arsenals specifically created by Russia and China to conduct their FIMI operations" [11]. FIMI is defined by the EEAS not as mere "fake news" but as a strategic, often state-sponsored, effort to manipulate information environments and "undermine the sovereignty of democratic institutions through covert, coercive, or deceptive tactics" [12].

The EU's resilience to hybrid threats is asymmetric. The institutional structure of the EU allows for more rapid and unified action on technical regulations, which often require only a qualified majority vote in the Council. In contrast, issues like FIMI and election interference touch upon sensitive areas of national security and foreign policy, where member states guard their sovereignty and decisions frequently require unanimity. This institutional design creates a structural delay in responding to societal-level hybrid threats compared to technical ones, a vulnerability that adversaries have successfully exploited. The following case studies provide empirical evidence of this asymmetry, demonstrating how adversaries pivot their attacks to less-protected domains.

Moldova (Presidential Election & EU Referendum, 2024–2025). The 2024 elections in Moldova were pivotal for the country's pro-European trajectory under President Maia Sandu. The process was marked by significant external interference, as stated in a joint statement by High Representative Josep Borrell and the European Commission, which noted that the elections occurred in an environment of "concern among stakeholders about illicit foreign interference and active disinformation efforts" attributed to "Russia and its proxies" [13].

Moldova's Intelligence and Security Service (SIS) detailed a multi-faceted campaign coordinated from Moscow, involving fugitive oligarch Ilan Shor. Tactics included large-scale disinformation, voter bribery (over $15 million distributed to approximately 130,000 citizens), the creation of an activist network of 33,000 individuals tasked with persuading voters to oppose EU integration, the involvement of the Orthodox Church in the campaign and cyberattacks on electoral infrastructure [14,15].

Despite these efforts, the pro-EU referendum passed with a razor-thin majority of 50.35%, and Sandu was re-elected in the second round with 55.35% of the vote. However, both victories were secured only by the votes of the Moldovan diaspora in the EU; domestically, Sandu lost the vote, indicating the high effectiveness of the Russian-led destabilization campaign. This case demonstrates the profound vulnerability of a candidate country's population and the decisive role the EU-based diaspora can play as a counterweight.

Romania (Presidential Elections, 2024–2025). Russian interference in Romania's presidential elections had even more dramatic consequences, plunging a NATO and EU member state into a political crisis. The first round of voting in November 2024 produced a sensational result: Călin Georgescu, an obscure, ultra-right, pro-Russian candidate, unexpectedly secured first place. His meteoric rise was fueled by a "perfect storm" of hybrid warfare. In 2024 alone, 34 Russian hybrid attacks against Romania were documented, with over 25,000 TikTok accounts and 5,000 Telegram channels mobilized to support Georgescu [16]. An investigation by Global Witness revealed that during the election period, TikTok's algorithms fed new users three times more far-right content than any other political material [17].

This targeted influence campaign, combined with societal discontent, led to a surge in Georgescu's popularity. In an unprecedented move, the country's Constitutional Court annulled the results of the first round, citing massive foreign interference. The rerun elections in May 2025 were accompanied by an "information and meme war" [18] and saw a massive mobilization of pro-European forces to elect the independent candidate Nicușor Dan over Georgescu's political successor, George Simion. The Romanian case serves as a stark warning of how quickly and effectively social media algorithms can be weaponized to destabilize a core EU and NATO member state.

Poland (Presidential Election, 2025). Even Poland, a key logistical hub for supporting Ukraine and a nation with high awareness of Russian threats, was not immune to hybrid attacks during its 2025 presidential election. The Polish government proactively spent €2 billion to prevent a "Romanian scenario" [19].

Despite these measures, on May 6, 2025, Minister of Digital Affairs Krzysztof Gawkowski stated, "During the current presidential election in Poland, we are facing an unprecedented attempt at interference in the electoral process by Russia". He noted that this interference combined disinformation with hybrid attacks on Polish critical infrastructure, including water companies and thermal power plants, with Russian

involvement in such attacks having more than doubled in that year [20]. Poland's experience demonstrates that even with high alert levels and significant investment, the threat remains potent and highlights the "contagion effect" of the Romanian case, which has become a benchmark scenario for other Eastern Flank nations.

The EU Preparedness Union Strategy, launched on March 26, 2025, represents the EU's strategic answer to the vulnerabilities exposed by these hybrid attacks. The strategy marks a doctrinal shift toward a "whole-of-society" and "all-hazards" approach that moves beyond purely technical solutions [21]. Key actions include promoting population preparedness (e.g., maintaining 72-hour emergency supplies), integrating preparedness into school curricula, strengthening civil-military cooperation, and creating a public-private Preparedness Taskforce. This strategy is the EU's acknowledgment of the resilience asymmetry and its first major attempt to address it systematically.

Analysis of the pro-EU electoral victories in Moldova and Romania suggests they would have been unlikely without significant EU engagement. This engagement went beyond traditional diplomacy and included mobilizing the decisive diaspora vote, providing European grants to support independent media, funding pro-democratic NGOs, issuing prompt public condemnations of interference by EU leaders, and leveraging the influence of EU structural funds. These actions can be interpreted as the EU developing its own implicit doctrine of "counter-hybrid influence." While Russia's goal is destabilization, the EU's is stabilization and the protection of a pro-European trajectory. The methods, however, are converging in the gray zone of political influence, suggesting that defending against hybrid warfare may compel liberal democracies to adopt more proactive influence operations of their own.

3. Conclusions

The escalation of Russian hybrid attacks has served as a catalyst for fundamental changes in European security strategies. The analysis indicates that the EU and Ukraine have made significant progress in building a collective, proactive architecture for the cybersecurity of critical infrastructure. This success is reflected in legislative harmonization (NIS2 and Law No. 11290), the institutionalization of cooperation (EU-Ukraine Cyber Dialogue, ENISA), and the integration of Ukraine's unique experience into the European security community.

However, this progress is asymmetric. While the EU's technical and infrastructural defenses are strengthening, hybrid attacks aimed at undermining societal and democratic resilience remain a serious and insufficiently regulated problem. Recent elections on the EU's eastern flank—in Moldova, Romania, and Poland—demonstrate that adversaries are successfully shifting their focus to the societal front, where existing legal and institutional mechanisms have proven inadequate. The Russian interference documented in these cases utilized a wide range of hybrid tactics, from mass disinformation and illicit financing to the exploitation of social media algorithms, particularly TikTok in Romania.

The case of Romania stands as a watershed moment, proving that a NATO country's democratic process can be derailed to the point of requiring annulment—a theoretical threat that has now become a demonstrated capability of adversaries. While pro-European outcomes were ultimately secured in Moldova and Romania, this was often due to reactive and extraordinary measures, including the decisive mobilization of diaspora communities and the EU's own use of hybrid influence mechanisms.

The EU's policy response is evolving, characterized by unprecedented political and legislative activity aimed at enhancing collective resilience. The EU Preparedness Union Strategy is a critical document in this regard, introducing a common framework for crisis response and seeking to reduce vulnerabilities across all sectors of society. This legislative shift is a direct consequence of the new geopolitical realities that have forced the EU to move from reactive to proactive crisis management.

The future security of Europe will depend on its ability to apply the same level of strategic focus and political will to the defense of its democracy and civil society as it has to the protection of its critical infrastructure. The deep synergy between Ukraine and the EU in cybersecurity offers a promising model, but the challenge now is to make this cooperation truly comprehensive, extending its reach to all fronts of modern hybrid warfare, from the server rack to the ballot box.

Declaration on Generative AI

During the preparation of this work, the authors used ChatGPT to: translate certain text fragments into English, perform grammar and spelling checks, and paraphrase or reword content. After using these tools, the authors carefully reviewed and edited the content as needed and take full responsibility for the publication's content.

References

[1]. Global Hybrid Warfare: The Ukrainian Front: Monograph / Edited by V.P. Gorbulin. Kyiv: NISD, 2017. P. 15. [in Ukrainian].

[2]. 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, DOI: 10.1080/23742917.2024.2312671

[3]. International Cyber Diplomacy: Promoting Openness, Security and Prosperity in a Networked World. Bureau of Public Affairs. July 14, 2011. Retrieved September 9, 2025 from: https://2009-2017.state.gov/r/pa/pl/168689.htm

[4]. Riordan S. Cyber Diplomacy vs. Digital Diplomacy: A Terminological Distinction. USC Center on Public Diplomacy. May 12, 2016. Retrieved September 9, 2025 from: https://uscpublicdiplomacy.org/blog/cyber-diplomacy-vs-digital-diplomacy-terminological-distinction

[5]. Necva Tastan Sevinc. Russia is an existential threat to Europe: Macron. Anadolu Ajansı. 07.03.2025. Retrieved September 8, 2025 from: https://www.aa.com.tr/en/europe/russia-is-an-existential-threat-to-europe-macron/3502464

[6]. New Cyber Blueprint to Scale Up the EU Cybersecurity Crisis. ENISA. Press Release. Jun 06,2025. - https://www.enisa.europa.eu/news/new-cyber-blueprint-to-scale-up-the-eu-cybersecurity-crisis-management

[7]. Chub D. A fresh look at information security from the EU, or how NIS 2 counters modern threats. 05.05.2025. Retrieved September 8, 2025 from: https://my-itspecialist.com/nis2-kiberbezpeka-yes-2025 [in Ukrainian].

[8]. The third round of the Ukraine-EU Cyber Dialogue took place in Brussels. Joint press release. July 16, 2024. Retrieved September 9, 2025 from: https://mfa.gov.ua/news/tretij-raund-kiberdialogu-ukrayina-yes-vidbuvsya-u-bryusseli [in Ukrainian].

[9]. Cyber resilience and international cooperation: Andriy Nadzhos participated in the Kyiv Cybersecurity Forum. Ministry of Culture and Strategic Communications of Ukraine. 13.03.2025. - https://mcsc.gov.ua/news/kiberstijkist-ta-mizhnarodna-spivpraczya-andrij-nadzhos-vzyav-uchast-u-kyyivskomu-forumi-z-kiberbezpeky/ [in Ukrainian].

[10]. Reznikova, O., and K. Voitovskyi. Strategy for ensuring EU preparedness to respond to new threats. Opportunities for Ukraine. Center for Security Studies, NISD. 19.05.2025. https://niss.gov.ua/sites/default/files/2025-05/az_pidgotovlenist_es_19052025.pdf [in Ukrainian].

[11]. 3rd EEAS Report on Foreign Information Manipulation and Interference Threats Exposing the architecture of FIMI operations. European External Action Service (EEAS). March 2025. Retrieved from: https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf

[12]. Proto L., Lamoso-González P., Bouza García L. The EU's FIMI Turn: How the European Union External Action Service Reframed the Disinformation Fight. 28 May 2025. P.4. Retrieved from: https://www.cogitatiopress.com/mediaandcommunication/article/view/9474

[13]. Moldova: Joint Statement by High Representative Josep Borrell and the European Commission on the Presidential Election and the Constitutional Referendum. 21.10.2024. Retrieved September 9, 2025 from: https://www.eeas.europa.eu/eeas/moldova-joint-statement-high-representative-josep-borrell-and-european-commission-presidential_en

[14]. Ntousas V., Pleșca L. Russian Meddling in Moldova. German Marshall Fund of the United States. October 18, 2024. Retrieved September 9, 2025 from: https://www.gmfus.org/news/russian-meddling-moldova;

[15]. Šlerka J. Intelligence Report Exposes Russian Meddling in Moldova's EU Vote. - VSquare. 2025-01-17. Retrieved September 9, 2025 from: https://vsquare.org/intelligence-report-russian-meddling-in-moldova-eu-referendum-sis-ilian-sor

[16]. Marcu-Andrei Solomon. Hybrid warfare through disinformation: the case of Romania's presidential election. Friends of Europe. 10 Jul 2025. Retrieved from: https://www.friendsofeurope.org/insights/critical-thinking-hybrid-warfare-through-disinformation-the-recent-case-of-romania

[17]. TikTok algorithm continues to push multiple times more far-right content to users ahead of Romanian election. Global Witness Investigation. 15 May 2025. Retrieved from: https://globalwitness.org/en/campaigns/digital-threats/tiktok-algorithm-continues-to-push-multiple-times-more-far-right-content-to-users-ahead-of-romanian-election/

[18]. Expert Comment: Which urgent tech lessons must the EU take from Romania's election? University of Oxford. News, 22 May 2025. Retrieved from: https://www.ox.ac.uk/news/2025-05-22-expert-comment-which-urgent-tech-lessons-must-eu-take-romania-s-election

[19]. Lasica J. Can Poland's cyber umbrella stop digital election meddling? Monocle: Affairs, April 23, 2025. Retrieved from: https://monocle.com/affairs/poland-cyber-umbrella-elections/

[20]. Badohal K. Poland says Russia is trying to interfere in presidential election. Reuters. May 6, 2025. Retrieved from: https://www.reuters.com/world/europe/poland-says-russia-is-trying-interfere-presidential-election-2025-05-06/

[21]. EU Preparedness Union Strategy to prevent and react to emerging threats and crises. PreventionWeb. 27 March 2025. https://www.preventionweb.net/news/eu-preparedness-union-strategy-prevent-and-react-emerging-threats-and-crises