Connections: The Quarterly Journal
ISSN 1812-1098, e-ISSN 1812-2973

Roland Kelemen, *Connections QJ* 22, no. 2 (2023): 75-90
https://doi.org/10.11610/Connections.22.2.55

Research Article

The Impact of the Russian-Ukrainian Hybrid War on the European Union's Cybersecurity Policies and Regulations

Roland Kelemen

Széchenyi István University, https://www.uni.sze.hu/

Abstract: While Russia transitioned from hybrid to conventional warfare in Ukraine, NATO recognized cyberspace as another domain where allied response can be invoked. The European Union also decided to enhance the cybersecurity capabilities of the organization and its member states, making social resilience a priority area. It is recognized that the security of cyberspace and related systems is not just an economic issue but one that affects the whole society, necessitating a more complex strategy and regulation. The EU has taken steps to mitigate the cyber risks associated with hybrid warfare, enhancing network and cognitive security. However, offensive cyber operations could increasingly lead to open armed conflict. During existing conflicts, some cyber operations may undermine public confidence and further escalate the situation. The EU and its Member States must pay closer attention to escalation dynamics in their legislation and practices. It is crucial to scrutinize cyber policies, set specific targets and deadlines, and regularly update them. This will require stakeholders to find the appropriate regulatory levels and align national regulations, practices, and standards.

Keywords: hybrid warfare, cognitive warfare, cybersecurity, European Union, NATO, resilience.

Introduction

Russia's armed attack on Ukraine in February 2022 shaped the European Union's conception of security. In many ways, it can be seen as the culmination of a long-standing conflict that preceded it. The hybrid conflict, which persisted for almost a decade before the large-scale war, also influenced and actively shaped the EU's

security concept.[1] The evolving attitudes and regulations towards cybersecurity have been an intrinsic part of this transformation. The high degree of digitalization in Member States and their societies has made them extremely vulnerable in cyberspace.

It is important to emphasize that, in the context of this study, cybersecurity is a category that encompasses two broad areas: network security and cognitive security. Network security refers to the protection of data in electronic information systems and the systems that manage it,[2] including software, hardware, and human actors. Cognitive security means resilience against cognitive hacking. Cognitive hacking tools include fake news, deepfakes, and disinformation, among others, which are cyberattacks that exploit psychological vulnerabilities to ultimately compromise logical and critical thinking and lead to dissonance.[3] Attacks may be motivated by nation-state geopolitical aspirations, ideological and extremist views, or even economic motives. The Russian hybrid action related to the "yellow vests" protests in France is a typical example. Avaaz examined the top 100 most viewed fake news stories on Facebook from November 2018 to March 2019 related to the protest. These stories covered political anti-establishment (28 %), police brutality (27 %), unrealistic and fabricated support for the movement (19 %), state censorship (14 %), uncontrolled immigration, racism and xenophobia (10 %) and some uncategorized issues (2 %).[4] Russia actively participated in spreading fake news, publishing these stories in German, Spanish, Dutch, Polish, Swedish, and Italian. Astonishingly, the 100 fake stories examined were shared by more than four million people and viewed by over 105 million. The central body of the disinformation campaign, RT France, generated more than 30 million hits during this period.[5] This data alone demonstrates the effectiveness of such a hybrid disinformation campaign. Adding the speed at which

---

1 James K. Wither, "Hybrid Warfare Revisited: A Battle of 'Buzzwords'," *Connections: The Quarterly Journal* 22, no. 1 (2023): 7-27, https://doi.org/10.11610/Connections.22.1.02.

2 Muha Lajos and Krasznay Csaba, *Az elektronikus információs rendszerek biztonságának menedzselése [Managing the Security of Electronic Information Systems]* (Budapest: Nemzeti Közszolgálati Egyetem, 2019), 11, https://tudasportal.uninke.hu/xmlui/handle/20.500.12944/12932. – in Hungarian

3 Kevin Matthe Caramancion, Li Yueqi, Elisabeth Dubois, and Ellie Seoe Jung, "The Missing Case of Disinformation from the Cybersecurity Risk Continuum: A Comparative Assessment of Disinformation with Other Cyber Threats," *Data* 7, no. 4 (2022): 49, https://doi.org/10.3390/data7040049.

4 "Yellow Vests Flooded by Fake News: Over 100M Views of Disinformation on Facebook," *Avaaz Report*, March 15, 2019, accessed October 12, 2023, 5-6, www.politico.eu/wp-content/uploads/2019/03/AVAAZ_YellowVests_100miofake.pdf.pdf.pdf.

5 Jarmo Makela, "Countering Disinformation: News Media and Legal Resilience," Hybrid CoE Paper 1, Workshop organized by the Hybrid CoE and the Media Pool, part of the Finnish Emergency Supply Organization, April 24-25, 2019 (Helsinki, Finland: The European Centre of Excellence for Countering Hybrid Threats, November 2019), 10-13, https://www.hybridcoe.fi/wp-content/uploads/2020/07/News-Media-and-Legal-Resilience_2019_HCPaper-ISSN.pdf.

each piece of content spreads makes the scale of the problem even more apparent. For example, one fake post depicted civilians with bleeding heads, claiming they were victims of police brutality. Published on November 20, 2018, this post was quickly shared by 136,000 people and viewed by more than 3.5 million people. It was later revealed that the pictures were taken in various countries at different times, and the compilation aimed to depict police brutality, radicalize the protesters and stir solidarity among societies in France and other states.[6] Cognitive security has, therefore, become an intrinsic part of cybersecurity, significantly due to Russian hybrid activities and the rise of social media. The primary difference between network security and cognitive security lies in their targets: while classical cyberattacks focus on IT systems, cognitive attacks aim at sub-complexes of the social totality. These two areas are not always sharply separated. They often complement each other to enhance overall effectiveness.

Hybridity's cyberspace-connected toolbox has made it possible to attack not only the (social) networks of the states involved in the hybrid conflict but also those of geopolitical adversaries. In the case of these hybrid threats, the likelihood of open military confrontation is relatively low. Instead, using hybrid assets intends to assert the interests at stake in the geopolitical contest and weaken opposing interest groups.[7] The Russian state employs a very advanced hybrid warfare. According to Makhmut Gareev, Russia aims to achieve political objectives through information warfare without resorting to military force. This creates so-called controlled chaos in the targeted state. Gerasimov added that the ultimate goal is to destroy the self-organizing capacity of the attacked state.[8]

As a result, although EU Member States were not directly involved in the Russian-Ukrainian hybrid conflict and war, their networks have been under attack, necessitating serious steps to enhance their cybersecurity. In this paper, I will examine the measures the EU has been compelled to take in the field of cybersecurity (network and cognitive security) due to the events between Russia and Ukraine. The study focuses on two periods: the decade before the outbreak of the large-scale Russian aggression, characterized primarily by hybrid conflict, and the period immediately before and during the war.

EU Responses to the Challenges of the Hybrid Conflict Period

In the early 2010s, the European Union recognized the necessity of intervention in the field of cybersecurity. The problem is inherently cross-border and affects the entire community. Without cooperative, supportive, guiding, coordinating,

---

6 Avaaz Report "Yellow Vests Flooded by Fake News," 21-22.

7 Ádám Farkas, *A védelem és biztonság-szavatolás szabályozásának alapkérdései Magyarországon* (Budapest: Magyar Katonai Jogi és Hadijogi Társaság, 2022), 35.

8 Katri Pynnöniemi, "The Concept of Hybrid War in Russia: A National Security Threat and Means of Strategic Coercion," *Hybrid CoE Strategic Analysis* 27, Hybrid CoE, May 18, 2021, 4-5, https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-27-the-concept-of-hybrid-war-in-russia-a-national-security-threat-and-means-of-strategic-coercion/.

and facilitating joint action, member states cannot effectively address the long-term cybersecurity problems and challenges.[9]

The Commission and the High Representative for Foreign Affairs and Security Policy jointly developed the EU's cybersecurity strategy. The strategy presents an almost utopian vision of cyberspace,[10] reminiscent of the early 2000s during the emergence of Web 2.0. In this vision, cyberspace promotes political and social integration, breaks down barriers between countries, communities, and citizens,[11] and is a place where freedom and fundamental rights are upheld. One of the key elements of the EU's international cyber policy is to ensure that cyberspace remains a place of freedom and fundamental rights.[12] The strategy has established that cyberspace can only fulfill its mission if the EU's traditional norms are fully respected.[13] It also outlined five strategic priorities to implement these principles:

1. achieving resilience against cyber-attacks
2. drastically reducing cybercrime
3. developing cyber defense policy and capabilities for the Common Security and Defence Policy (CSDP) [14]
4. Developing cybersecurity industrial and technological resources
5. Establishing a coherent international policy for the European Union in cyberspace and promoting the Union's core values.[15]

The cybersecurity strategy broadly outlines the motives for cyberattacks, including criminal acts (by individuals or groups), terrorism, politically motivated attacks, and state-sponsored cyberattacks. The European Union has developed

---

9 Helena Carrapico and Andre Barrinha, "European Union Cyber Security as an Emerging Research and Policy Field," *European Politics and Society* 19, no. 3 (2018): 299-303, https://doi.org/10.1080/23745118.2018.1430712.

10 Gergely Gosztonyi, "Aspects of the History of Internet Regulation from Web 1.0 to Web 2.0," *Journal on European History of Law* 13, no. 1 (2022): 168-173.

11 Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace" (Brussels: European Commission, February 7, 2013), Join(2013) 1 final, 2, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013JC0001.

12 "Cybersecurity Strategy of the European Union" (2013), 17.

13 "Cybersecurity Strategy of the European Union" (2013), 4.

14 László Knapp, "A terrorizmus elleni küzdelem az Európai Unió jogában: A terrortámadásra adandó válasz a szolidaritási és a kollektív védelmi klauzula tükrében [The Fight against Terrorism in the Law of the European Union: The Response to a Terrorist Attack in the Light of the Solidarity and Collective Defense Clause]," in *A terrorizmus elleni küzdelem aktuális kérdései a XXI. Században [Current issues of the fight against terrorism in the XXI. Century],* ed. Róbert Bartkó (Budapest: Gondolat Kiadó, 2019), 119-136, https://dfk-online.sze.hu/a-terrorizmus-elleni-kuzdelem-aktualis-kerdesei-a-xxi-szazadban. – in Hungarian

15 "Cybersecurity Strategy of the European Union (2013)," 5.

legal norms to deal more robustly and effectively with cybercrime and cyberterrorism. However, regarding cyberspace activities that affect international law—such as cyberattacks and their attribution, cyber sovereignty, armed attacks, and state self-defense—the strategy states that "the Union does not expect the creation of international legal instruments on cyberspace issues." [16] The consequences of this erroneous position became evident by the end of the decade, especially during the Russian-Ukrainian confrontation and the war that broke out in February 2022. The conflict highlighted the need for robust international legal instruments in cyberspace, given the extensive use of hybrid warfare tools. In response, the EU launched its cyber diplomacy toolbox to at least partially remedy this shortcoming.

The 2013 strategy fails to adequately capture the unique characteristics of cyberspace, which differs significantly from the traditional physical space. As a result, it does not provide a clear framework for applying EU core values specifically to cyberspace, nor does it address the distinct attributes of cyberspace that are only perceptible within that realm.[17] Furthermore, due to the cross-border nature of cyberspace and the differing regulatory frameworks among EU Member States, it has been deemed unfeasible for the EU to develop centralized European oversight. Therefore, the responsibility for cybersecurity initiatives remained primarily with individual Member States and the private sector.[18] The European Union's approach has been criticized as counterproductive, particularly because achieving harmonization of regulations has been identified as its primary objective during this period. This objective necessitates either the establishment of a central EU institution with a broader mandate than ENISA,[19] or enhancing ENISA's capabilities to coordinate national authorities' activities and develop and implement a unified protection protocol. The EU's initial position is seen as flawed, but efforts are underway to move beyond it. Factors such as the growing influence of social media platforms, their commercial practices, and their implications for security and society,[20] as well as the proliferation of hybrid

[16] "Cybersecurity Strategy of the European Union (2013)," 18.

[17] Such features include the redefinition of concepts of geometric space, overcoming traditional notions of geographical distance, the delimitation of internal and external cyberspace, and the use of layering theories (which are essential for identifying regulatory objects). Additionally, it involves overriding the linear or hyper-differentiated nature of norms and learning (becoming super-hyper-differentiated), the metamorphosis of social relations (such as increased capacity for syndication and the malleability of social networks), and the relativization of the concept of time. There are also changes in the subject of fundamental rights (e.g., data, assets in games), their characteristics (with social media becoming the most important space for freedom of expression), and their limits (e.g., private curation).

[18] "Cybersecurity Strategy of the European Union (2013)," 19.

[19] European Union Agency for Cybersecurity.

[20] Enikő Kovács-Szépvölgyi, "A digitális gyermekvédelem egyes aspektusai [Some Aspects of Digital Child Protection]," in *Széchenyi István Egyetem Új Nemzeti Kiválóság*

scenarios from Russia and China in recent years, have contributed to this reassessment. Nevertheless, recognizing the importance of securing cyberspace to safeguard traditional spaces represented a significant step forward.

The illegal annexation of Crimea and the Russian support to separatists in Donbas in 2014-15, and their cyberspace consequences, compelled the EU to take action. In 2015, the Council of the European Union issued its *Conclusions on Cyber Diplomacy*, highlighting cybersecurity, human rights, international law, and the rule of law in cyberspace as persistent challenges for the Common Foreign and Security Policy. The Council emphasized that these challenges could only be addressed through a comprehensive, multifaceted, and coherent international cyberspace policy. Meanwhile, it stressed the importance of promoting and protecting a single, open, free, and secure cyberspace that can only be achieved by fully respecting the EU's core values of democracy, human rights, and the rule of law. To this end, the document stated that a coherent and comprehensive EU approach to cyber diplomacy is needed, and it was approved two years later.[21] The goals set, such as preserving fundamental values, respect for freedoms, gender equality, competitiveness, and prosperity, also highlighted significant differences in the understanding of cybersecurity between Western and Eastern states, which were already becoming increasingly evident as geopolitical faultlines.

Following Russia's actions against Ukraine, the European Union also recognized the importance of addressing hybridity, including disinformation. In response, it established the East StratCom Task Force in 2015 to enhance the EU's capacity to anticipate, detect, and respond to disinformation produced by external actors.

The Commission's 2016 communication, including on cyberspace, highlighted that, despite positive developments, the EU remains vulnerable to cybersecurity incidents. It emphasized that cyberspace-based operations, often tools of hybrid attacks, pose significant dangers.[22] These attacks, executed by perpetrators of hybrid threats, "could even lead to the destabilization of countries or political institutions." [23]

Program Tanulmánykötet 2021/2022 [István Széchenyi University New National Excellence Program Study Volume 2021/2022] (Győr: Széchenyi István Egyetem, 2022), 227-236, https://tud.sze.hu/images/%C3%9ANKP/2021-2022/UNKP_2022_0725_Tanulma%CC%81nyko%CC%88tet%20beli%CC%81v.pdf. – in Hungarian

[21] Council of the European Union, "Council Conclusions on Cyber Diplomacy," 6122/15, Brussels, February 11, 2015 (OR. en), https://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf.

[22] European Commission, High Representative of the Union for Foreign Affairs and Security Policy, "Joint Communication to the European Parliament and the Council – Joint Framework on Countering Hybrid Threats; a European Union Response," JOIN/2016/018 final/3, point 4.4 Cybersecurity, Brussels, April 6, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018.

[23] "Opinion of the European Economic and Social Committee on the 'Communication to the European Parliament, the Council, the European Economic and Social Committee

It is no coincidence that the EU felt the need to adapt and update the 2013 strategy, leading to its finalization in 2017. The introduction to the strategy states that threats have grown exponentially over the years, and cybersecurity is fundamental for keeping our everyday lives safe. Cyberattacks can be attributed to state and non-state actors, blurring the line between traditional and cyberspace security actors. The strategy stresses that some states are imposing their geopolitical interests through cyberspace operations and warns that unless the EU can significantly improve its cybersecurity, the risk will increase with the expansion of digitalization. The strategy asserts that EU resilience to cyberattacks is a realistic goal if a number of objectives are achieved: strengthening ENISA; full implementation of the NIS Directive;[24] rapid emergency response as a key to resilience; enhancing research and development; building a cyber skills base, i.e., by strengthening education; and promoting cyber hygiene and awareness.[25]

In 2017, two years after the declaration of a single EU Cyber Diplomacy, the Council of the European Union launched the Cyber Diplomacy Toolbox, the EU's instrument for a common response to malicious cyber activities. This toolbox is designed to prevent conflict, mitigate cybersecurity threats, and stabilize international relations. The EU diplomatic response aims to be proportionate to the scope, scale, duration, intensity, complexity, sophistication, and impact of any cyber activity. The toolbox was further detailed in 2019 through a Council Regulation and Decision. These rules apply in the event of a cyberattack with significant external impact or an attempted cyberattack against the EU or one of its Member States. Unlawful activities that access, interfere with, or monitor an information system are considered attacks. Attacks on critical infrastructure, systems providing essential social and economic activities, systems providing critical government functions, and governmental response teams, among others, are considered malicious. To determine significant impact, factors such as the scope and scale of disruption, the number of natural or legal persons, entities, and Member States attacked, the economic loss caused, and the amount and scale of data assets affected are examined. This allows the Union to prevent perpetrators of such attacks from entering or transiting the territory of the Union, as well

and the Committee of the Regions: Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry' (COM(2016) 410 final)," Document 52016AE4559, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016AE4559.

[24] "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union," https://eur-lex.europa.eu/eli/dir/2016/1148/oj.

[25] European Commission, "Joint Communication to the European Parliament and the Council – Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU (JOIN/2017/0450 final)," Document 52017JC0450, Brussels, September 13, 2017, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2017:0450:FIN.

as freezing funds and economic resources in their possession.[26] These provisions strongly express the Union's intention to sanction external attackers in response to the proliferation of attacks in the second half of the 2010s. The EU acted decisively by creating a legal regime that uses a cyber diplomacy toolbox and sanctions through the Common Foreign and Security Policy. In July 2020, the Council of the European Union imposed sanctions on Russian, Chinese, and North Korean hackers involved in cyberattacks such as the "Wannacry" and "NotPetya" attacks. Additionally, in October 2020, sanctions were imposed on Russian hackers involved in the cyberattacks on the German Parliament in 2015, with eight individuals and four organizations sanctioned.[27]

In 2018, the EU adopted an action plan against misinformation, allocating shared competences between national and EU institutions. The coordinated response is based on four pillars:

(1) Improving the capacity of EU institutions;

(2) Coordinated response to misinformation;

(3) Mobilizing the private sector;

(4) Improving societal resilience.

The plan called for bolstering EU bodies that could contribute to these efforts, establishing an alert system capable of real-time reporting of disinformation activities, and designating contact points within member states. By mobilizing the private sector, the document emphasized the role and responsibility of platforms, highlighting their previous inadequacies in addressing the problem effectively.[28]

In line with the Action Plan, a Rapid Alert System was established in 2019 to facilitate the exchange of information and coordinate the actions of national and EU institutions against disinformation. This system involves a network of 27 national contact points designed to coordinate efforts and share best practices. However, sharing competences among different entities can complicate prob-

[26] "Council Regulation (EU) 2019/796 of 17 May 2019 Concerning Restrictive Measures against Cyber-Attacks Threatening the Union or Its Member States," https://eur-lex.europa.eu/eli/reg/2019/796/oj; "Council Decision (CFSP) 2019/797 of 17 May 2019 Concerning Restrictive Measures against Cyber-Attacks Threatening the Union or Its Member States," https://eur-lex.europa.eu/eli/dec/2019/797/oj.

[27] Miftahul Khausar and Abdul Rivai Ras, "Establishment of the Cyber Diplomacy Toolbox (CDT) as a Joint Diplomatic Response to the European Union against the Threat of Cyber Attack Activity," *Politicon – Jurnal Ilmu Politik* 5, no. 1 (2023): 29-58, https://journal.uinsgd.ac.id/index.php/politicon/article/view/14833.

[28] European Commission, "Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions – Action Plan against Disinformation," JOIN(2018) 36 final, Brussels, December 5, 2018, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52018JC0036.

lem-solving, and the national toolbox remains the primary resource for addressing these issues.[29] The COVID-19 pandemic brought the issue of disinformation, generating a so-called infodemic, to the forefront. This situation highlighted the need for the EU to distinguish between different forms of false or misleading content, such as illegal and harmful but not illegal content. Disinformation, in the case of the latter, refers to false or misleading information published with the intent to deceive, harm the public interest, or cause economic damage. The previous Action Plan, the Code of Practice, and the practices of the Rapid Reaction Team form the foundation for addressing disinformation activities.[30] However, platform providers responsible for implementing measures to combat disinformation on their platforms remain the primary actors.

In December 2020, the European Commission presented an Action Plan for Democracy in Europe, with its fourth point focusing on the fight against disinformation. This part of the plan emphasizes the need for closer cooperation with the private sector, civil society, academia, and the EU's international partners to understand better and counter hybrid threats. The document criticizes platforms for the opacity of their algorithms and their news practices – issues identified during the evaluation of the Code of Practice. The Commission believes that a stronger and clearer commitment from platform providers and an approach based on an appropriate oversight mechanism are essential to effective action against disinformation.[31] In line with the Action Plan, in 2020, the Commission proposed the Digital Services Act (DSA), which was adopted in Fall 2022. The DSA aims to create a safe, predictable, and trustworthy online environment that respects the rights enshrined in the Charter of Fundamental Rights.

EU Cybersecurity Actions in the Shadow of the Russia-Ukraine War

By the end of 2020, the European Union has displayed a clear intention to strengthen integration in the field of cybersecurity. The new strategy is a very strong and open statement that the European Union as a whole recognizes the problems of cyberspace. According to the strategy, "cybersecurity is an integral part of the security of Europeans... Transport, energy, health, telecommunica-

[29] Makela, "Countering Disinformation: News Media and Legal Resilience," 15.

[30] European Commission, "Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Tackling COVID-19 disinformation – Getting the Facts Right," JOIN(2020) 8 final, Brussels, June 10, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020JC0008.

[31] European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – On the European Democracy Action Plan," COM(2020) 790 final, Brussels, December 3, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A790%3AFIN.

tions, finance, security, space, defense and democratic processes are highly dependent on increasingly interconnected network and information systems." [32] The COVID-19 pandemic has reinforced these trends, accelerating the digitalization of work.[33] Supply chain failures in back-end technology pose a significant problem and have led to geopolitical tensions. The growing number of malicious attacks on critical infrastructures in recent years is also of concern. They obstruct the use of online services and ultimately cause economic damage. There is significant latency in addressing these issues, and the percentage of successful crime detection remains low. The Strategy further states that cybercrime is growing while cyber readiness and cyber awareness among businesses and individuals are low. Additionally, there is a significant lack of cybersecurity skills in the workforce. This deficiency is not only the responsibility of the Member States but also of the EU. Few programs help individuals to catch up. However, most existing initiatives take a holistic approach, which may not effectively address the need to improve cybersecurity skills.[34]

The EU has come a long way in the last decade. Initially, the focus was primarily on the economic impact of cyber threats. There is now a clear recognition that cybersecurity is a societal problem that demands comprehensive attention. What remains less visible is the understanding that cybersecurity is not solely a technological issue; it requires a multidisciplinary approach combining education, research, and normative regulation.

Building on the achievements of previous strategies, the EU sees the use of three main instruments—regulatory, investment, and policy—as essential for action in three areas:

1. resilience, technological sovereignty, and leadership;
2. operational capacity building for prevention, deterrence, and response;
3. promoting a global and open cyberspace.[35]

Implementation will be linked to major digital investments over the next seven years, integrating a range of incentives, obligations, and benchmarks, with a focus on artificial intelligence, encryption, and quantum computing. The European Defence Fund (EDF) will be among the main vehicles in this process. The

[32] European Commission, "Joint Communication to the European Parliament and the Council – The EU's Cybersecurity Strategy for the Digital Decade," JOIN/2020/18 final, Brussels, December 16, 2020, 1, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52020JC0018.

[33] Ferencz Jácint, "Blokchain-rendszerű megoldások a munkaviszonyban ["Blockchain-based solutions in the employment relationship]," *Erdélyi Jogélet [Transylvanian Law Society]* 1*,* no. 4 (2020): 21-28, https://doi.org/10.47745/ERJOG.2020.04.02.

[34] European Commission, "Joint Communication to the European Parliament and the Council – The EU's Cybersecurity Strategy for the Digital Decade," 1-4.

[35] European Commission, "Joint Communication to the European Parliament and the Council – The EU's Cybersecurity Strategy for the Digital Decade," 5.

three main areas can be broken down into sub-areas. Resilience, technology sovereignty, and leadership are based on:

a) resilient infrastructure and critical services;
b) the creation of a European cyber shield;
c) an ultra-secure communications infrastructure;
d) securing next-generation mobile broadband networks;
e) a secure post-Internet of Things (IoT) environment;
f) greater global cybersecurity;
g) a more robust presence in the technology supply chain;
h) an EU workforce with cyber skills.[36]

Some of these objectives seem feasible at the EU level, such as transforming the regulatory environment (e.g., the NIS2 [37] Directive and DORA [38] Regulation, the Digital Agenda), enhancing social resilience, and developing individual programs. However, some of the language, such as "ultra-secure system," "European cyber shield," and "increasing the security of the global internet," appears propagandistic and beyond the community's influence and therefore does not seem to be realistic objectives.

Operational capacity building for prevention, deterrence, and response will include:

a) a common cybersecurity unit;
b) addressing cybercrime;
c) active use of the EU cyber diplomacy toolbox;
d) development of cyber defense capabilities.

The creation of a joint cybersecurity unit marks a new departure, as the EU has previously been reluctant to establish such a body. The document emphasizes that this would significantly enhance the European response to cybersecurity crises. A joint cybersecurity unit would serve three main purposes: improving the preparedness of cybersecurity communities, enhancing situational aware-

[36] European Commission, "Joint Communication to the European Parliament and the Council – The EU's Cybersecurity Strategy for the Digital Decade," 6-14.

[37] "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive)," PE/32/2022/REV/2, https://eur-lex.europa.eu/eli/dir/2022/2555/oj.

[38] "Digital Operational Resilience Act (DORA) – Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on Digital Operational Resilience for the Financial Sector and Amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011," https://eur-lex.europa.eu/eli/reg/2022/2554/oj.

ness through better information sharing, and strengthening the coordinated response.[39] In conclusions issued by the Council of the European Union in October 2021, it was confirmed that the Member States agree to set up such an institution, although joining it would be voluntary.

In promoting global and open cyberspace, the EU aims to take the lead in establishing and enhancing standards, regulations, and frameworks for cyberspace. However, this ambition seems utopian given the EU's current geopolitical role, as the US and China have significantly greater resources in this area. Additionally, the EU seeks to move towards creating voluntary, non-binding norms for responsible state behavior under the auspices of the UN. This plan, however, is unlikely to lead to substantial changes, as the absence of real sanctions means that ad hoc power and political interests would likely override the code of conduct. Other points, such as cooperation, strengthening partnerships, and increasing resilience globally, are recurring themes and do not present anything new.[40]

The new cybersecurity strategy represents a major shift towards a more realistic approach, particularly in recognizing the need to create a common entity. However, some goals remain utopian, possibly due to the EU's misjudgment of its geopolitical positioning and global realities. Nevertheless, the new regulation could lead the community toward more effective operational cybersecurity.

The outbreak of the war has led to increased cooperation between NATO and the EU, yielding significant results in cybersecurity, often articulated in military terms. Thus, the central theme of the 2022 NATO summit in Madrid was the Russian-Ukrainian war, support for Ukraine, and finding a solution to the war. The final document emphasized strengthening the strategic partnership while respecting the integrity of both organizations, reinforced by their joint commitment and response to Ukraine. Cyberspace remained a central theme. The summit's communique stated that cyber, space, hybrid, and other asymmetric threats, along with the malicious use of new and disruptive technologies, must be addressed in cooperation.[41] The two organizations are committed to continuing their support for Ukraine against Russia, including the provision of non-lethal defense equipment to enhance Ukraine's cyber defense and resilience.[42] With the Russia-Ukraine war, energy security has become a priority. They aim to accelerate the Alliance's adaptation and increase resilience to cyber and hybrid threats by deploying political and military instruments in an integrated manner.

---

[39] European Commission, "Joint Communication to the European Parliament and the Council – The EU's Cybersecurity Strategy for the Digital Decade," 14-22.

[40] European Commission, "Joint Communication to the European Parliament and the Council – The EU's Cybersecurity Strategy for the Digital Decade," 22-28.

[41] NATO, "Madrid Summit Declaration," issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Madrid, June 29, 2022, articles 6, 15, https://www.nato.int/cps/en/natohq/official_texts_196951.htm.

[42] "Madrid Summit Declaration," point 8.

NATO is on the way to strengthen significantly its cyber defenses through enhanced civil-military cooperation and expanded partnerships with industry.[43] These issues are partially reflected, for example, in the NIS2 regulation, where a significant part of the infrastructure involved is intended to ensure the cybersecurity of supply chains.

At the Madrid summit, the Alliance announced its new Strategic Concept, which outlines five key goals and principles.

1. NATO is determined to defend the freedom and security of allies against threats from all directions.
2. The Alliance is essential to the region's security, founded on the values of individual freedom, human rights, democracy, and the rule of law. These principles align with the aims and principles of the European Union.
3. NATO is a unique and indispensable platform for coordinating and acting on individual and collective security issues. Its commitment to security, solidarity, and mutual defense is indivisible.
4. The Alliance's deterrence and aeoexяe capabilities are the backbone of this commitment.
5. NATO has three core functions: deterrence and defense, crisis prevention and management, and cooperation for security.

NATO will enhance its individual and collective resilience and increase its technological advantage, crucial to the Alliance's core tasks.[44] All post-2018 documents emphasize the common transatlantic values that form the basis of the alliance and the importance of cooperation with the European Union. These documents analyze the security environment and highlight how hostile authoritarian states exploit the interconnectivity, openness, and high degree of digitalization characteristic of NATO states to engage in malicious activities in cyberspace, including disinformation. Russia, identified as the most significant and immediate threat in the Euro-Atlantic, employs traditional, cyber, and hybrid means against the Alliance. Cyberspace is recognized as an area of particular importance, as malicious actors seek to destroy critical infrastructure, disrupt government services, obtain intelligence, steal intellectual property, and obstruct NATO military activities.[45]

In line with the spirit of the Final Document, the European Union took significant steps to strengthen Ukraine's cybersecurity following the outbreak of the war. From March 2022 till February 2023, the EU allocated nearly € 11 million for that purpose. Its primary aim was to support the cyber and data security needs

[43] "Madrid Summit Declaration," art. 10.

[44] "NATO 2022 Strategic Concept," adopted by Heads of State and Government at the NATO Summit in Madrid, June 29, 2022, 3, https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf.

[45] "NATO 2022 Strategic Concept," 3-4.

of Ukrainian authorities, focusing on replacing destroyed hardware and ensuring the continued operation of public services during the war. The Estonian e-Governance Academy led the project implementation, leveraging its digital governance and cybersecurity expertise to support Ukraine in this critical time.[46]

The EU and Ukraine have maintained a dialogue in the field of cybersecurity since the outbreak of the war, with a focus on strengthening resilience. The European External Action Service estimates that "thanks to close cooperation with the EU and other international partners in the area of cybersecurity and cyber defense, Ukraine has shown formidable capacities for fending off cyberattacks and protecting its critical infrastructure." [47]

The final document of the 2023 NATO Vilnius Summit reiterated that common values of human rights, democracy, and the rule of law bind together the Alliance and its members. It emphasized the need to strengthen this cohesion in the face of war on the continent and enhance NATO's 360-degree security. Strengthening national and collective resilience is an essential part of this strategy, along with the cooperation with the European Union as a unique and indispensable partner of NATO for the prosperity and security of the Euro-Atlantic area. This is also necessary as Russia and China have further escalated their actions, including hybrid and cyber attacks against the Alliance, interference in democratic processes, and other disruptive activities. The Russia-Ukraine war has sharply highlighted the extent to which cyberspace is part of modern armed conflict, with incidents potentially amounting to an armed attack under Article 51 of the UN Charter, thus invoking Article 5 of the Washington Treaty, the *casus foederis*. Therefore, NATO will enhance the contribution of cyber defense to its deterrence capabilities by further developing the three levels of cyber defense—political, military, and technical. This approach will ensure civil-military cooperation in peacetime, crisis, and conflict and include, as appropriate, cooperation with the private sector, thereby improving joint situational awareness. However, to be successful, the active contribution of non-EU NATO members to the efforts of EU member states is essential. Russian aggression has deepened EU-NATO cooperation, with an unwavering commitment to further support Ukraine, e.g., by establishing a joint EU-NATO Coordination Group. Significant progress has been made in areas such as countering disinformation, hybrid and cyber threats, and terrorism, as well as building defense capabilities, defense industry, and research. Yet, cooperation should be further expanded in fields like resilience, crit-

[46] "EU Supports Cybersecurity in Ukraine with over 10 Million Euro," *Delegation of the European Union to Ukraine*, October 20, 2022, https://www.eeas.europa.eu/delegations/ukraine/eu-supports-cybersecurity-ukraine-over-10-million-euro_en.

[47] "Ukraine and EU Held the Second Round of the UA-EU Cybersecurity Dialogue," *European External Action Service*, September 29, 2022, https://www.eeas.europa.eu/eeas/ukraine-and-eu-held-second-round-ua-eu-cybersecurity-dialogue_en.

ical infrastructure protection, new and disruptive technologies, space, geostrategic competition, and closer collaboration with industry and academia.[48] In addition to enhancing the capabilities and resilience of NATO, the EU, and individual member states in cyberspace, these goals and tasks also include preparing for major escalation in the international security environment.

Conclusion

Russia's hybrid, and later conventional warfare, incorporating hybrid elements, has prompted the European Union to develop the cybersecurity capabilities of the organization and its Member States and identify social resilience as a priority. Given Russian and Chinese cybercultures, NATO recognized cyberspace as another domain of warfare; hence, the core purpose of the Alliance extends to this domain. NATO is continuously investing in operational capabilities in cyberspace (e.g., the cyber operations doctrine) and societal resilience, articulating multilayered expectations and seeking to raise awareness down to the civilian level.

As a result of these efforts, the European Union's approach to cybersecurity has also undergone a significant, 180-degree turn in recent years. Compared to a decade ago, the security of cyberspace and related systems is now assessed not only as an economic issue but also one that affects the whole of society, significantly impacting the lives and living spaces of the state, the economy, and individuals. Therefore, it requires a much more complex strategy and regulation. The EU has also taken steps to reduce cyber hazards arising from hybridity, including disinformation, which could lead to more effective regulation of social media platforms. However, there is still a long way to go to achieve this.

It should also be pointed out that human society is interconnected in many ways, and the number of cyber threats is extraordinary, requiring an urgent response. Cyberattacks are highly diverse; some threaten territorial integrity, political independence, national security, the Union, or a Member State to such an extent that a *casus foederis* may be invoked. This perspective is supported by Healey and Singh, who reason that given the prevailing trends contributing to the escalation of tensions, future de-escalation actions may no longer effectively defuse tensions. This is especially true if individual states see past incidents as reasons to develop their own capabilities or begin to view cyber operations as provocative. Offensive cyber operations are thus more likely to escalate into an open armed conflict, making even moderate operations significantly more serious.[49] The report, presented by Susan Davis considers operations that undermine public confidence in an existing conflict through cyber means particularly

[48] NATO, "Vilnius Summit Communiqué," issued by NATO Heads of State and Government Participating in the Meeting of the North Atlantic Council in Vilnius, July 11, 2023, points 1, 6, 18, 23, 61, 66, 73, 74, https://www.nato.int/cps/en/natohq/official_texts_217320.htm.

[49] Jason Healey and Virpratap Vikram Singh, "Situational Cyber Stability and the Future of Escalating Cyber Conflict," in *Cyberspace Strategic Outlook 2030: Horizon Scanning and Analysis*, ed. Pirek Pernik (Tallinn, Estonia: NATO CCDCOE Publications, 2022), 19-

problematic. Such operations lead to a higher degree of escalation in a crisis, demonstrating that NATO, the EU, and their member states must pay greater attention to the dynamics of escalation in their legislation and practices, as evidenced by the Russian-Ukrainian war.

Given the urgency, stakeholders need to adapt their cyber policies accordingly, setting more specific targets and deadlines that must be regularly updated.[50] It is important for the relevant actors to find the appropriate regulatory levels and to align national regulations, practices, and standards as far as possible. The EU has made substantial progress with initiatives like NIS2 and DORA. However, the minimum level of adoption advocated by some Member States still results in multi-speed cybersecurity regulation, standards, and practices. But as the adage goes, a system is only as secure as its weakest link.

Disclaimer

The views expressed are solely those of the author and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

Acknowledgment

Connections: The Quarterly Journal, Vol. 22, 2023, is supported by the United States government.

About the Author

Roland Kelemen, PhD, is a lawyer and serves as an adjunct professor at Széchenyi István University Faculty of Law and Political Sciences. He was a Fulbright scholar for 2021-2022, participating in the "Cybersecurity in Universities – Study Visits to the U.S." program.
https://orcid.org/0000-0002-5419-8425
E-mail: Kelemen.roland@ga.sze.hu

31, 29, https://ccdcoe.org/library/publications/cyberspace-strategic-outlook-2030-horizon-scanning-and-analysis/.

[50] Susan Davis, "NATO in the Cyber Age: Strengthening Security and Defence, Stabilising Deterrence," General Report, adopted on October 13, 2019, by the Science and Technology Committee at the 65th Annual Session of the NATO Parliamentary Assembly in London, United Kingdom, 5-11, https://www.nato-pa.int/document/2019-nato-cyber-age-strenghtening-security-and-defence-stabilising-deterrence.