

# Cyber governance, disinformation and digital trust: lessons from the 2022 Ukraine case study

Agnieszka ROGOZIŃSKA,  
War Studies University, Warsaw, Poland  
a.rogozinska@akademia.mil.pl

## Abstract

The rapid digital transformation of contemporary societies has significantly increased dependence on digital infrastructures while simultaneously exposing governments, institutions and citizens to cyber threats, disinformation and declining digital trust. The objective of this study is to examine how cyber governance mechanisms contribute to institutional resilience and the preservation of digital trust during geopolitical crises, using the 2022 Ukraine case as an illustrative example. The paper builds upon existing research concerning cybersecurity, cyber resilience, information disorder and digital governance, while extending recent discussions published in *Smart Cities and Regional Development Journal* on digital governance, resilient public administration and information security. A qualitative case study methodology was adopted, based on the analysis of publicly available governmental reports, cybersecurity assessments, policy documents and academic literature. The collected materials were examined using qualitative thematic analysis and triangulation of secondary sources in order to identify governance mechanisms influencing institutional resilience and information integrity. The findings indicate that resilience in digitally dependent societies cannot be explained solely through technological capabilities. Effective cyber resilience requires adaptive governance structures, cross-sectoral coordination, transparent strategic communication and trust-preserving institutional practices. The analysis further demonstrates that cyber incidents and disinformation campaigns reinforce one another, creating multidimensional governance challenges that may significantly undermine institutional legitimacy and public confidence when responses are fragmented or inconsistent. Conversely, coordinated governance frameworks substantially strengthen institutional resilience and improve the ability to maintain digital trust during crises. The study has practical implications for policymakers, public institutions and organizations responsible for cybersecurity, crisis management and digital governance by highlighting the importance of integrating cybersecurity policies with strategic communication and resilience planning. The main contribution of the paper lies in proposing a unified analytical perspective that combines cyber governance, disinformation and digital trust within a single governance framework, thereby extending current research on resilient digital ecosystems under conditions of geopolitical instability.

**Keywords:** institutional resilience, strategic communication, information integrity, crisis governance, cyber-enabled hybrid threats

## 1. Introduction

The accelerating digitalization of contemporary societies has fundamentally transformed governance, communication systems and institutional functioning. While digital technologies have enhanced efficiency, accessibility and connectivity, they have simultaneously increased exposure to cyber threats, information manipulation and systemic vulnerabilities. As a result, cybersecurity is increasingly understood not only as a technical issue but also as a governance challenge closely associated with institutional trust, societal resilience and crisis preparedness. [5], [6]

The events surrounding Ukraine in 2022 provide a significant case illustrating how cyber governance and information integrity interact during periods of geopolitical instability. The conflict demonstrated that cyber operations are no longer limited to technological disruption but function alongside disinformation campaigns aimed at shaping public

narratives, influencing perceptions and undermining institutional legitimacy. [7], [8] Cyber governance has emerged as an essential component of resilience in digitally dependent societies. [5], [12]

Although existing research extensively discusses cybersecurity and information warfare, less attention has been devoted to the interrelationship between cyber governance, disinformation and digital trust within crisis environments. [5], [7] Recent studies published in *Smart Cities and Regional Development Journal* have also emphasized the growing importance of digital governance, institutional resilience, smart public administration and cybersecurity within the context of digitally transformed societies [17], [18], [19]. This study seeks to address this gap by examining how governance mechanisms influence resilience against information manipulation and support trust preservation in digital ecosystems. [7], [13] The novelty of this study lies in integrating cyber governance, disinformation and digital trust within a unified analytical framework applied to the Ukraine 2022 case. [1], [3], [14], [16]

The study also contributes to ongoing discussions on smart governance and resilient digital ecosystems by linking cyber governance with institutional trust and crisis management. This paper investigates the interrelationship between cyber governance, disinformation and digital trust through the lens of the 2022 Ukraine case study. The study seeks to answer the following research question: How do cyber governance mechanisms support resilience against disinformation and contribute to the preservation of digital trust during geopolitical crises?

This study adopts a qualitative case study methodology to examine the relationship between cyber governance, disinformation and digital trust during the events in Ukraine in 2022. Ukraine was selected as a critical case due to the convergence of cyberattacks, disinformation campaigns and geopolitical instability occurring simultaneously within a highly digitized environment. The qualitative approach enables an in-depth exploration of governance mechanisms, institutional responses and trust-related dynamics that cannot be adequately captured through quantitative indicators alone. The analysis relies on triangulation of secondary sources, including governmental reports, cybersecurity assessments, academic literature and policy documents, thereby strengthening analytical reliability and reducing interpretative bias.

The research is based on secondary data analysis, including publicly available governmental reports, cybersecurity assessments, academic publications, policy documents and verified incident reports concerning cyber activities associated with the Ukraine crisis. Particular attention was devoted to materials published by international organizations, cybersecurity institutions and policy-oriented entities addressing hybrid threats, cyber resilience and digital trust. The collected materials were examined through qualitative thematic analysis to identify recurring governance patterns, institutional responses, and trust-related vulnerabilities. The study focuses on three principal analytical dimensions:

- cyber governance frameworks and institutional coordination;
- disinformation and digital manipulation;
- preservation of digital trust under crisis conditions.

The selection of these dimensions was motivated by their interconnected role in shaping societal and institutional resilience within digital environments. Cyber governance frameworks influence decision-making capabilities and crisis response effectiveness, while disinformation campaigns directly affect information integrity and trust formation. Simultaneously, digital trust determines the extent to which individuals and organizations rely on institutions, communication systems and digital infrastructures during periods of uncertainty. [16]

A case study method was chosen because it enables an in-depth examination of a contemporary and dynamic environment where cyber incidents and information operations interact simultaneously [10]. The Ukraine context represents an appropriate case due to the visibility of cyber-enabled disruptions and the global significance of digital information warfare during the conflict period. The events of 2022 provide a unique opportunity to observe how cyber governance structures function under pressure and how digital trust may be strengthened or weakened through institutional actions and communication practices. [1], [3]

The research process involved comparative examination of publicly documented cyber incidents, disinformation narratives, institutional responses and policy measures introduced during the examined period. Reports from cybersecurity agencies, international institutions and academic sources were compared to identify similarities, contradictions and dominant explanatory patterns. Such triangulation of secondary sources increases analytical reliability and reduces the risk of relying on isolated interpretations. [18], [19]

Although the study relies on publicly available information, limitations exist due to restricted access to classified intelligence, operational cybersecurity data and continuously evolving geopolitical developments. The dynamic nature of cyber threats also limits the possibility of producing fully exhaustive conclusions, as digital incidents and information campaigns frequently change over time. Nevertheless, the selected sources provide sufficient evidence to identify broader trends and implications relevant to governance and resilience studies. [28], [47]

Furthermore, it should be emphasized that the objective of this research is not to establish technical attribution of cyber incidents but rather to examine broader governance implications associated with cybersecurity, information integrity and trust preservation. Consequently, the study contributes to the growing body of interdisciplinary research linking cyber governance with societal resilience and digital trust in crisis environments.

Another limitation concerns the exclusive reliance on secondary data. Future studies may incorporate interviews with policymakers, cybersecurity practitioners and institutional decision-makers to strengthen empirical validation.

The paper is structured as follows. Section 2 presents the theoretical foundations of cyber governance and digital trust. Section 3 discusses the methodology applied in the study. Section 4 analyzes the Ukraine case study, focusing on cyber incidents and information manipulation. Section 5 discusses the broader implications of the findings, while the final section summarizes conclusions and recommendations for future governance strategies.

## **2. Cyber Governance and Digital Trust**

### ***2.1. The Concept of Cyber Governance***

Cyber governance refers to the institutional, legal and operational arrangements established to manage cyber risks, responsibilities and digital infrastructures [5]. Unlike traditional cybersecurity approaches focused primarily on technical protection, cyber governance emphasizes strategic coordination, institutional preparedness and resilience-building across multiple stakeholders. [28], [47]

Modern cyber governance frameworks involve governments, international organizations, private sector actors and civil society. Their role is not only to respond to cyberattacks but also to establish preventive measures, communication strategies and trust-building mechanisms capable of minimizing systemic vulnerabilities [6]. This multidimensional perspective recognizes that cyber threats affect not only technological systems but also economic stability, public confidence, institutional legitimacy and democratic processes. [16], [22]

The growing dependence of governments, organizations and societies on interconnected digital infrastructures has transformed cyber governance into a strategic necessity rather than an optional institutional function. As digital systems increasingly support administration, communication and economic activity, institutions are expected to ensure continuity, security and operational adaptability in response to evolving cyber risks. [16], [22]

During periods of geopolitical instability, cyber incidents frequently extend beyond technical disruption and may affect institutional legitimacy, economic continuity and public confidence. The Ukraine case underscores the need for adaptive governance frameworks capable of maintaining secure communication channels, responding to cyber risks and countering disinformation simultaneously. [1], [3]

Furthermore, contemporary cyber governance increasingly requires international cooperation and cross-sectoral collaboration. Since cyber threats often transcend national boundaries, effective governance frameworks depend on information sharing, coordinated cybersecurity strategies and harmonized legal mechanisms among state and non-state actors. Organizations such as NATO, the European Union Agency for Cybersecurity (ENISA) have emphasized the importance of collective resilience and coordinated policy responses to cyber threats [2], [14].

An important component of cyber governance is also the concept of digital trust, which refers to confidence in digital institutions, information systems and communication environments. Trust plays a fundamental role in ensuring effective governance because institutional legitimacy depends on transparency, accountability and the reliability of digital infrastructures. [16], [25]

Consequently, cyber governance should be understood not merely as a technical management process but as a multidimensional framework integrating cybersecurity, institutional coordination, strategic communication and trust preservation. Such an approach becomes particularly relevant in crisis situations characterized by uncertainty, information disruption and hybrid threats. [22], [44]

## ***2.2. Disinformation and Information Warfare***

Disinformation refers to intentionally misleading or false information disseminated to manipulate perceptions, influence political attitudes, or destabilize institutional trust [7]. Unlike misinformation, which may result from unintentional inaccuracies, disinformation is deliberate and strategically designed to influence audiences and shape public narratives. The emergence of hybrid conflicts has intensified the role of information warfare, where cyber tools and media narratives operate simultaneously to achieve strategic objectives. Unlike traditional propaganda, contemporary digital disinformation campaigns are decentralized, fast-moving and highly adaptive. [8] They frequently exploit social media platforms, digital news ecosystems, online forums and automated communication mechanisms to maximize reach and influence. [27], [44]

The effectiveness of disinformation is often linked to the speed at which emotionally persuasive content circulates within digital ecosystems. Information characterized by emotional intensity, controversy, or political polarization tends to receive higher levels of engagement, increasing the probability of rapid dissemination. Digital platforms may unintentionally facilitate the spread of misleading narratives through recommendation algorithms designed to prioritize user interaction rather than factual accuracy. [18], [19] Furthermore, digital literacy and the competencies of public actors represent important factors influencing the ability of institutions and societies to respond effectively to information manipulation and fake news in digitally mediated environments. [20]

Disinformation campaigns commonly employ several manipulative techniques, including selective framing, fabricated narratives, misleading contextualization, emotional persuasion and repetitive exposure. Such strategies are intended not only to distort factual understanding but also to create uncertainty and confusion among audiences. In many cases, the objective is not necessarily to convince individuals of a particular narrative but rather to weaken confidence in all available information sources.

In the context of geopolitical crises, information warfare functions as a strategic instrument capable of influencing public opinion, institutional legitimacy and international relations. The events surrounding Ukraine in 2022 demonstrated how digital information environments can become contested domains where competing actors seek to influence

both domestic and international audiences. Narratives disseminated through online environments attempted to shape perceptions of legitimacy, responsibility and geopolitical positioning, illustrating the strategic significance of information control. [1], [3], [14]

Furthermore, disinformation may contribute to the erosion of digital trust, particularly when institutions struggle to provide timely, transparent and reliable communication. The weakening of trust in governments, media organizations and public institutions may substantially reduce societal resilience. In such circumstances, individuals may become more susceptible to conspiracy theories, misinformation and politically motivated narratives. [25]

Countering disinformation therefore requires an integrated governance approach combining cybersecurity measures, institutional transparency, strategic communication and media literacy. As hybrid threats continue to evolve, strengthening resistance to information manipulation becomes essential for maintaining institutional legitimacy and public confidence in digital environments.

### **3. Cyber Governance and Disinformation in the 2022 Ukraine Context**

#### ***3.1. Cyber Threats and Digital Infrastructure Vulnerabilities***

The events in Ukraine in 2022 illustrated the strategic dependence of contemporary societies on digital infrastructures during periods of geopolitical instability. Cyber-related incidents targeting communication systems, governmental institutions and critical digital services revealed how vulnerabilities in digital environments may directly affect institutional continuity and public confidence. [1], [3]

Cyber disruptions included attempts to compromise governmental websites, digital services and communication systems. Such incidents demonstrated the vulnerability of digital ecosystems during periods of conflict and reinforced the need for robust cyber governance mechanisms capable of ensuring operational continuity. Digital infrastructure supporting governmental administration, public communication, financial transactions and emergency coordination became particularly important in maintaining societal stability under crisis conditions. [1], [3]

The disruption of digital services has consequences extending beyond immediate technical failures. Interruptions in communication systems, public administration platforms and digital information channels may significantly affect public confidence and organizational stability. Cyber resilience depends on governance structures that combine technological preparedness with institutional coordination. [12] The reliability of digital services directly influences public trust in institutions, especially when access to verified information becomes crucial for crisis response and collective decision-making. [28], [47]

The Ukraine case illustrated that technological defense alone is insufficient. Effective resilience requires preparedness strategies, stakeholder cooperation and adaptive governance mechanisms capable of responding to evolving cyber risks. Cyber resilience

therefore depends not only on technical capabilities such as network security, encryption systems, or incident detection mechanisms but also on institutional preparedness and coordinated response frameworks. [14], [28]

An important characteristic of cyber threats during geopolitical instability is their adaptive and dynamic nature. Threat actors frequently modify attack strategies, exploit emerging vulnerabilities and target communication channels capable of influencing institutional functionality and societal behavior. As a result, cybersecurity strategies must continuously evolve to address changing risks, technological dependencies and emerging forms of digital disruption.

Furthermore, cyber incidents targeting critical infrastructure may generate indirect consequences extending far beyond the digital domain. Failures affecting energy systems, financial services, transportation networks, or public communication mechanisms may disrupt everyday societal functioning and contribute to increased uncertainty among citizens. In such circumstances, cyber governance frameworks become essential instruments supporting continuity of operations and crisis resilience. [28], [47]

The Ukraine case also revealed the importance of cooperation among governmental institutions, private technology providers, cybersecurity organizations and international partners. Public-private partnerships proved particularly relevant in responding to digital threats, enabling more effective incident management, rapid information exchange and enhanced cybersecurity preparedness. Such collaborative governance models represent an essential component of resilience strategies within digitally dependent societies. [14], [28]

In addition, digital infrastructure vulnerabilities demonstrated the necessity of integrating cybersecurity planning into broader national security and crisis management strategies. Institutions responsible for governance are expected to anticipate cyber risks, establish continuity mechanisms and ensure effective communication systems capable of maintaining trust during periods of uncertainty. Cybersecurity should no longer be viewed solely as a technical issue but rather as a strategic governance challenge closely connected with institutional resilience and societal stability. [28], [47]

The Ukraine case in 2022 provides several concrete examples illustrating the relationship between cyber threats and national digital resilience. One of the most notable incidents occurred in February 2022, when the satellite communication network operated by Viasat experienced a large-scale cyberattack affecting communication systems in Ukraine and several European countries. [14], [28]

The incident highlighted the strategic importance of digital communication infrastructure in modern geopolitical conflicts and demonstrated how cyber-enabled disruptions may extend beyond national borders, affecting both governmental and civilian systems. [3], [12] The Viasat incident indicates how cyber-enabled disruptions increasingly affect both civilian and governmental infrastructures simultaneously. This blurring of boundaries between military and civilian targets reflects the hybrid character of contemporary cyber

conflicts and reinforces the need for governance mechanisms capable of coordinating responses across institutional sectors. [44]

In addition to satellite communication disruptions, Ukrainian governmental institutions experienced repeated cyber-related incidents targeting public administration systems, governmental websites and communication channels. Such disruptions aimed not only to interfere with institutional functioning but also to weaken confidence in governmental stability and crisis response mechanisms. The visibility of these incidents reinforced concerns regarding the vulnerability of public digital infrastructure during periods of intensified geopolitical tension. [13], [14]

Another important aspect of the Ukraine case involved the use of destructive malware targeting governmental and institutional systems. The coordinated nature of such attacks suggests that cyber operations function not only as instruments of disruption but also as mechanisms intended to generate uncertainty and institutional pressure. Cybersecurity preparedness should be integrated with governance planning and crisis communication strategies. At the same time, technological resilience mechanisms contributed to maintaining communication continuity. The deployment of alternative communication technologies, including satellite-supported digital infrastructure, played a significant role in supporting operational functionality and reducing the impact of disruptions. Such developments demonstrate that cyber resilience depends on adaptive governance structures capable of rapidly integrating technological, organizational and institutional responses to emerging threats. [12], [14]

The Ukraine case therefore highlights that digital resilience should not be interpreted solely through technological capabilities. Instead, resilience emerges through the interaction of governance frameworks, preparedness strategies, infrastructure adaptability and trust-building mechanisms capable of maintaining institutional continuity during crisis situations.

### ***3.2. Disinformation Campaigns and Narrative Manipulation***

Alongside cyber-related disruptions, disinformation became one of the most influential dimensions of the Ukraine crisis, shaping perceptions, influencing public discourse and challenging institutional credibility. [13] Disinformation campaigns commonly relied on selective framing, emotionally persuasive messaging, fabricated information and repeated exposure to misleading narratives. Social media platforms played an important role in amplifying information flows, often accelerating the spread of unverified content. The speed and accessibility of digital communication environments enabled information to circulate almost instantly, reducing the time available for verification and increasing susceptibility to manipulation. [1], [3]

The objectives of such campaigns extended beyond simple misinformation. In many instances, information manipulation aimed to undermine trust in public institutions, create confusion and uncertainty, influence international public opinion and weaken social

cohesion and resilience. Rather than exclusively persuading audiences to accept a particular narrative, many campaigns sought to generate informational ambiguity, making it increasingly difficult for individuals to distinguish between factual reporting and manipulative content. [28], [47]

The Ukraine case demonstrated how digital environments may become contested spaces where information itself functions as a strategic resource. Governance responses require not only cybersecurity measures but also communication strategies designed to support information integrity and public confidence. Institutional communication became essential in maintaining stability, as delayed or inconsistent responses frequently increased opportunities for misinformation to proliferate. [3], [14]

A key feature of digital disinformation campaigns is their adaptability. Information actors often modify narratives according to political developments, emotional responses and audience engagement patterns. This dynamic character makes disinformation particularly difficult to counter, as manipulative narratives evolve rapidly and exploit existing social divisions, political polarization and emotional vulnerability. Digital platforms characterized by algorithmic personalization may unintentionally reinforce exposure to selective information environments, contributing to the formation of fragmented information ecosystems.

Furthermore, disinformation campaigns rely on technological capabilities such as automated accounts, manipulated visual materials, artificial amplification mechanisms and coordinated online behavior. Such practices may create an illusion of widespread public consensus or artificially intensify political narratives. In crisis situations, manipulated information may significantly influence public reactions, emergency responses and trust in institutional decision-making. [18], [19], [27]

The erosion of digital trust represents one of the most serious consequences of information manipulation. Public trust in governmental institutions, media organizations and digital communication channels may weaken rapidly when misinformation becomes widespread. Reduced trust can limit institutional effectiveness, complicate crisis response efforts and increase public uncertainty. Maintaining digital trust has become an essential objective of cyber governance strategies. [22], [25]

Addressing disinformation therefore requires a multidimensional response involving governments, international organizations, technology companies, researchers and civil society actors. Effective countermeasures include strategic communication, media literacy programs, fact-checking mechanisms, transparent governance and enhanced cooperation among stakeholders. The Ukraine case highlights the importance of institutional preparedness and coordinated communication strategies in mitigating the destabilizing consequences of information warfare and strengthening societal resilience against digital manipulation. From a governance perspective, the effectiveness of institutional communication became increasingly dependent on credibility, transparency and the speed of response to emerging narratives. [1], [18]

### **3.3. Institutional Responses and Governance Mechanisms**

Institutional coordination played a fundamental role in maintaining digital continuity during the Ukraine crisis. Public institutions, international organizations, private technology companies and cybersecurity actors cooperated to strengthen digital resilience and minimize disruption [14]. The events of 2022 demonstrated that effective crisis response depends on coordinated governance structures capable of integrating cybersecurity, communication strategies and institutional preparedness. [14], [28]

Cyber governance frameworks contributed to crisis response through several interconnected mechanisms. First, strategic communication became essential in ensuring reliable and timely dissemination of information to reduce uncertainty and misinformation. During periods of instability, access to verified and transparent communication channels significantly influenced public trust and institutional credibility. Institutions capable of delivering consistent messaging were more successful in countering disinformation narratives and maintaining confidence among citizens and stakeholders. [19], [22]

Second, cross-sector collaboration emerged as an important governance dimension. Cooperation among governmental agencies, cybersecurity organizations, digital platform providers and international institutions enabled more efficient incident detection, information sharing and coordinated response mechanisms. Since cyber threats transcend organizational and geographical boundaries, isolated responses often prove insufficient. The Ukraine case illustrated that resilience depends on collective efforts involving both public and private actors capable of responding to rapidly changing digital risks. [1], [3], [14]

Third, preparedness and resilience planning became critical components of governance effectiveness. Institutional mechanisms designed to ensure operational continuity reduced the likelihood of severe disruption despite cyber-related incidents. Crisis management procedures, cybersecurity protocols and continuity strategies enabled organizations to sustain essential services even under conditions of uncertainty. This finding emphasizes that resilience is not solely reactive but also strongly dependent on pre-established governance capabilities and institutional readiness. [28], [47]

Fourth, public awareness initiatives contributed to strengthening resilience against information manipulation. Governments and public institutions increasingly recognized the importance of supporting digital literacy and encouraging critical evaluation of information sources. In digital environments characterized by rapid information dissemination, citizens capable of identifying misleading narratives become less vulnerable to manipulation. Educational strategies and awareness programs represent important preventive mechanisms within broader cyber governance systems. [16], [22]

The findings indicate that successful crisis management depends on governance systems capable of integrating cybersecurity, communication and trust-building practices.

Technological protection alone does not guarantee resilience if institutions fail to maintain transparency, coordinate effectively, or preserve public confidence during periods of uncertainty. [28], [47]

The Ukraine case further demonstrated that governance effectiveness relies on institutional adaptability. Because cyber threats and disinformation campaigns evolve dynamically, governance mechanisms must remain flexible and responsive to emerging risks. Static or fragmented institutional approaches may reduce response effectiveness and increase vulnerabilities in digital ecosystems. [1], [3]

The relationship between governance, resilience and trust is summarized in Table 1, which presents the principal dimensions observed during the Ukraine 2022 case study. [14], [28]

Table 1. Analytical Dimensions of Cyber Governance and Digital Trust in the Ukraine 2022 Context

| Dimension                 | Key observations in the Ukraine 2022 case                                                              | Implications for resilience                                 |
|---------------------------|--------------------------------------------------------------------------------------------------------|-------------------------------------------------------------|
| Cyber governance          | Increased coordination among governmental institutions, international organizations and private actors | Strengthened operational continuity and crisis response     |
| Digital infrastructure    | Repeated cyber-related incidents targeting public systems and communication channels                   | Need for adaptive cybersecurity frameworks and preparedness |
| Disinformation campaigns  | Dissemination of manipulated narratives through digital platforms                                      | Reduced public confidence and increased uncertainty         |
| Institutional trust       | Pressure on public trust caused by misinformation and digital instability                              | Importance of transparent communication strategies          |
| Public awareness          | Growing need for digital literacy and information verification                                         | Increased societal resistance to manipulation               |
| International cooperation | Support from international cybersecurity actors and organizations                                      | Improved resilience against hybrid threats                  |

*Source: Author’s elaboration based on [1], [3], [14], [28], [47].*

#### 4. Findings and Discussion

The findings indicate that resilience in digitally dependent environments cannot be explained solely through technological capabilities. Although cybersecurity tools remain essential, the Ukraine case illustrates that institutional coordination, governance effectiveness and public trust constitute equally important determinants of crisis resilience.

First, cyber governance mechanisms proved essential in ensuring continuity of operations during periods of instability. Institutional preparedness, coordination among stakeholders and adaptive responses contributed considerably to reducing vulnerabilities and maintaining operational functionality. [12], [15] The analysis indicates that organizations possessing clearly defined governance frameworks and crisis management procedures were better prepared to maintain essential services and minimize disruption. This finding supports the argument that cybersecurity effectiveness depends on governance maturity rather than exclusively on technological sophistication. [16], [22]

Second, the spread of disinformation demonstrated the fragility of digital trust. Trust in institutions, information sources and digital communication channels can be undermined rapidly when false narratives circulate extensively. Therefore, digital resilience requires communication transparency and information verification mechanisms. In the Ukraine case, the speed at which manipulated information spread highlighted the importance of reliable institutional communication capable of counterbalancing uncertainty and misinformation. Institutions unable to respond effectively to manipulated narratives risked weakening public confidence and increasing informational instability. [14]

Third, the case highlighted the hybrid nature of contemporary threats. [8], [14] Cyber incidents and disinformation frequently function together, reinforcing one another and creating multidimensional challenges for governments and organizations. This interdependence necessitates integrated governance approaches rather than isolated cybersecurity measures. The findings suggest that digital threats should not be viewed solely through technical or informational perspectives but rather through a broader governance framework integrating cybersecurity, communication strategies and resilience planning. [19]

Furthermore, the study highlights that digital trust plays a central role in determining institutional effectiveness during crises. Trust influences how citizens interpret information, comply with institutional guidance and evaluate the credibility of digital communication channels. A reduction in trust may significantly weaken crisis response effectiveness and increase susceptibility to manipulation. Preserving digital trust should be regarded as a strategic priority within cyber governance systems. [22], [25]

Another important finding concerns the role of institutional adaptability. Since cyber threats evolve rapidly and disinformation narratives frequently change according to political and social developments, governance mechanisms must remain flexible and capable of responding to emerging risks. Static institutional structures may become ineffective in highly dynamic digital environments characterized by rapidly shifting technological and informational challenges. [19]

Finally, public awareness emerged as an important protective factor. Individuals capable of critically evaluating digital content are less susceptible to manipulative narratives, suggesting that digital literacy constitutes an essential component of long-term resilience strategies. Educational initiatives supporting media literacy, information verification practices and responsible digital behavior may significantly contribute to strengthening societal resilience against hybrid threats. [28], [44]

Overall, the findings suggest that resilience in the digital age increasingly depends on the successful integration of governance, communication, technological preparedness and trust-building mechanisms. The Ukraine case therefore offers valuable lessons for policymakers, researchers and organizations seeking to improve preparedness against cyber-enabled disruptions and information manipulation. [14], [28]

From a theoretical perspective, the study contributes to existing research by demonstrating the interdependence between cyber governance, disinformation resilience and trust preservation within crisis environments. Rather than treating these dimensions separately, the findings suggest that they function as mutually reinforcing components of institutional resilience. [19], [22]

## **5. Implications for Organizations and Society**

The findings suggest that institutions adopting resilience-oriented governance approaches demonstrate greater adaptive capacity during digitally mediated crises. Cybersecurity policies must extend beyond technical defense and include communication planning, stakeholder engagement and trust management. [28], [47]

Organizations operating in digital environments should also strengthen incident response frameworks and ensure transparency during crises. Maintaining public trust requires consistent communication and effective management of uncertainty.

At the societal level, increased investment in media literacy and digital awareness programs may reduce susceptibility to misinformation and strengthen public resilience against manipulation. [28], [47] This perspective corresponds with SCRD research highlighting that digital transformation requires not only technological development but also institutional capabilities, digital competencies and responsible governance approaches. [20] Furthermore, international cooperation remains critical. Cyber threats and disinformation campaigns often transcend national borders, making collaborative governance frameworks essential for effective response. [19], [27] Public institutions should integrate cybersecurity policies with strategic communication, media literacy programmes and trust-building mechanisms. Such an integrated governance approach may substantially improve preparedness for future hybrid crises.

## **6. Conclusions**

The 2022 Ukraine case provides important insights into the relationship between cyber governance, disinformation and digital trust during periods of geopolitical instability. The findings suggest that resilience in digital environments depends not only on technological protection but also on governance quality, institutional coordination and trust-preserving communication mechanisms. The findings indicate that cyber resilience requires an integrated approach combining cybersecurity, strategic communication and organizational preparedness. [14], [16]

The analysis revealed that cyber-related disruptions and disinformation campaigns may significantly undermine institutional legitimacy and public confidence. The Ukraine case illustrates that modern threats are hybrid in nature, combining cyberattacks, digital manipulation and narrative influence in ways that affect both institutional functionality and societal stability. Governance systems must evolve to address not only technical vulnerabilities but also informational and organizational challenges. [1], [3]

Cyber governance therefore emerges as a multidimensional framework encompassing preparedness, adaptability, cooperation and trust preservation. Institutions operating in digitally dependent environments should prioritize resilience-oriented strategies capable of maintaining continuity during periods of uncertainty. Effective governance requires collaboration among governmental institutions, private organizations, cybersecurity actors and international partners. [16], [22]

An important finding concerns the role of digital trust in crisis response. Public trust in institutions and communication channels significantly influences the effectiveness of governance mechanisms. When trust is weakened by misinformation or inconsistent communication, societies become more vulnerable to uncertainty and manipulation. Therefore, transparent communication and reliable information systems should be regarded as essential components of cyber governance. [22], [25]

The study also highlights the growing importance of international cooperation in strengthening resilience against cyber-enabled hybrid threats. Since cyber risks often transcend national borders, coordinated governance frameworks and information-sharing practices are necessary. [44], [47]

Despite certain limitations related to reliance on publicly available data, the study contributes to understanding how cyber governance mechanisms influence resilience in crisis situations. The lessons derived from the Ukraine case may support policymakers, researchers and organizations in developing more adaptive strategies for protecting digital ecosystems, maintaining information integrity and strengthening trust in complex digital environments. The present study complements recent SCRD research concerning digital transformation, smart governance and institutional resilience by extending these discussions toward cyber governance and digital trust during geopolitical crises [17], [18]. Future studies may incorporate expert interviews and primary institutional data to provide deeper insight into cyber governance effectiveness during geopolitical crises. [14], [16] Future research should further investigate comparative cyber governance models across different geopolitical environments and examine how digital trust evolves under prolonged hybrid conflict conditions.

## References

- [1] Microsoft, *Defending Ukraine: Early Lessons from the Cyber War*. Redmond, WA, USA: Microsoft Digital Security Unit, 2022.
- [2] European Union Agency for Cybersecurity (ENISA), *ENISA Threat Landscape 2023*. Brussels, Belgium: ENISA, 2023.
- [3] NATO Cooperative Cyber Defence Centre of Excellence, *Cyber Threats and Hybrid Warfare*. Tallinn, Estonia: NATO CCDCOE, 2023.
- [4] World Economic Forum, *Global Cybersecurity Outlook 2024*. Geneva, Switzerland: World Economic Forum, 2024.
- [5] J. Nye, "Deterrence and Dissuasion in Cyberspace," *International Security*, vol. 41, no. 3, pp. 44–71, 2017.
- [6] E. Kello, *The Virtual Weapon and International Order*. New Haven, CT, USA: Yale University Press, 2017.

- [7] C. Wardle and H. Derakhshan, *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*. Strasbourg, France: Council of Europe, 2017.
- [8] T. Rid, *Active Measures: The Secret History of Disinformation and Political Warfare*. New York, NY, USA: Farrar, Straus and Giroux, 2020.
- [9] J. W. Creswell and J. D. Creswell, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, 5th ed. Thousand Oaks, CA, USA: Sage Publications, 2018.
- [10] R. K. Yin, *Case Study Research and Applications: Design and Methods*, 6th ed. Thousand Oaks, CA, USA: Sage Publications, 2018.
- [11] N. Perlroth, *This Is How They Tell Me the World Ends: The Cyberweapons Arms Race*. New York, NY, USA: Bloomsbury, 2021.
- [12] European Commission, *The EU Cybersecurity Strategy for the Digital Decade*. Brussels, Belgium: European Commission, 2020.
- [13] Council of the European Union, *Cybersecurity and Digital Resilience Policy Framework*. Brussels, Belgium: Council of the European Union, 2023.
- [14] NATO, *NATO 2022 Strategic Concept*. Brussels, Belgium: North Atlantic Treaty Organization, 2022.
- [15] World Bank, *Digital Development Overview: Digital Resilience and Governance*. Washington, DC, USA: World Bank, 2024.
- [16] L. Floridi, *The Ethics of Information*. Oxford, UK: Oxford University Press, 2013.
- [17] C. Schachtner, "On the way to resilient information security management: Business Continuity Management (BCM) for public institutions," *Smart Cities and Regional Development Journal*, vol. 9, no. 1, pp. 7–15, 2025.
- [18] C. Schachtner, "Wise Governance – Elements of the digital strategies of municipalities," *Smart Cities and Regional Development Journal*, vol. 6, no. 2, pp. 23–29, 2022.
- [19] S. Bradshaw and P. N. Howard, *The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation*. Oxford, UK: Oxford Internet Institute, 2019.
- [20] R. Müller-Török, A. Prosser, and S. Sroka, "The digital (il)literacy of local and regional politicians and civil servants – An analysis based on recent data from Romania," *Smart Cities and Regional Development Journal*, vol. 8, no. 2, pp. 9–18, 2024.
- [21] R. Broadhurst, P. Grabosky, M. Alazab, and S. Chon, "Organizations and cyber crime: An analysis of the nature of groups engaged in cyber crime," *International Journal of Cyber Criminology*, vol. 8, no. 1, pp. 1–20, 2014.
- [22] A. Klimburg, *The Darkening Web: The War for Cyberspace*. New York, NY, USA: Penguin Press, 2017.
- [23] T. Maurer, *Cyber Mercenaries: The State, Hackers, and Power*. Cambridge, UK: Cambridge University Press, 2018.
- [24] M. Castells, *Networks of Outrage and Hope: Social Movements in the Internet Age*, 2nd ed. Cambridge, UK: Polity Press, 2015.
- [25] S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York, NY, USA: PublicAffairs, 2019.
- [26] S. C. Woolley and P. N. Howard, Eds., *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media*. Oxford, UK: Oxford University Press, 2018.
- [27] UNESCO, *Journalism, Fake News & Disinformation: Handbook for Journalism Education and Training*. Paris, France: UNESCO, 2018.
- [28] OECD, *Building Digital Resilience: A Framework for Digital Security and Trust*. Paris, France: OECD Publishing, 2020.
- [29] European Commission, *Tackling Online Disinformation: A European Approach*. Brussels, Belgium: European Commission, 2018.
- [30] European External Action Service (EEAS), *2nd EEAS Report on Foreign Information Manipulation and Interference Threats: Towards a Framework for Networked Defence*. Brussels, Belgium: EEAS, 2023.
- [31] K. T. Brooking and D. G. Singer, *Countering Russian Social Media Influence*. Santa Monica, CA, USA: RAND Corporation, 2018.
- [32] A. Polyakova and C. Meserole, *Exporting Digital Authoritarianism: The Russian and Chinese Models*. Washington, DC, USA: Brookings Institution, 2019.
- [33] Freedom House, *Freedom on the Net 2023: The Repressive Power of Artificial Intelligence*. Washington, DC, USA: Freedom House, 2023.
- [34] Cybersecurity and Infrastructure Security Agency (CISA), *Shields Up: Guidance for Organizations*. Washington, DC, USA: CISA, 2022.

- [35] Mandiant, *M-Trends 2023: Special Report*. Reston, VA, USA: Mandiant, 2023.
- [36] IBM Security, *X-Force Threat Intelligence Index 2024*. Armonk, NY, USA: IBM Security, 2024.
- [37] CrowdStrike, *Global Threat Report 2024*. Sunnyvale, CA, USA: CrowdStrike, 2024.
- [38] Verizon Business, *2024 Data Breach Investigations Report*. New York, NY, USA: Verizon, 2024.
- [39] Check Point Research, *Cyber Attack Trends Report 2023*. Tel Aviv, Israel: Check Point Software Technologies, 2023.
- [40] R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 3rd ed. Indianapolis, IN, USA: Wiley, 2020.
- [41] B. Schneier, *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World*. New York, NY, USA: W. W. Norton & Company, 2018.
- [42] G. Blank and C. Lutz, "Benefits and harms from Internet use: A differentiated analysis of Great Britain," *New Media & Society*, vol. 20, no. 2, pp. 618–640, 2018.
- [43] World Economic Forum, *The Global Risks Report 2024*, 19th ed. Geneva, Switzerland: World Economic Forum, 2024.
- [44] European Parliamentary Research Service (EPRS), *Understanding Hybrid Threats: A European Response*. Brussels, Belgium: European Parliament, 2021.
- [45] M. N. Schmitt, Ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed. Cambridge, UK: Cambridge University Press, 2017.
- [46] United Nations, *Our Common Agenda: Policy Brief 5 – A Global Digital Compact*. New York, NY, USA: United Nations, 2023.
- [47] International Telecommunication Union (ITU), *Global Cybersecurity Index 2024*. Geneva, Switzerland: ITU, 2024.
- [48] European Union Agency for Cybersecurity (ENISA), *Foresight Cybersecurity Threats for 2030: Update 2023*. Athens, Greece: ENISA, 2023.
- [49] A. Gorwa, R. Binns, and C. Katzenbach, "Algorithmic content moderation: Technical and political challenges in the automation of platform governance," *Big Data & Society*, vol. 7, no. 1, pp. 1–15, 2020.
- [50] D. M. West, *The Future of Work: Robots, AI, and Automation*. Washington, DC, USA: Brookings Institution Press, 2018.
- [51] C. R. Sunstein, *#Republic: Divided Democracy in the Age of Social Media*, 2nd ed. Princeton, NJ, USA: Princeton University Press, 2017.