

THE REPUBLIC OF MOLDOVA AND UKRAINE: INSTITUTIONAL POLICIES, RESPONSE CAPACITIES AND THE EVOLUTION OF INFORMATION RESILIENCE IN THE REGIONAL CONTEXT

Victoria BEVZIUC*

Abstract: *The article highlights the similarities and differences between the Republic of Moldova's national policies regarding information resilience and the Ukrainian institutional regulations and capacities to face modern security challenges. It examines the evolution of strategic communication, cybersecurity, counter-disinformation mechanisms, and interinstitutional coordination in both countries within the context of the evolving regional security environment. The analysis focuses on the legal and institutional frameworks developed to enhance societal resilience against information manipulation, foreign influence, and hybrid threats. While Ukraine has significantly strengthened its information resilience capacities through wartime reforms and close cooperation with international partners, the Republic of Moldova is still consolidating its institutional architecture and legislative framework. The paper identifies common strategic objectives, including the protection of democratic processes, critical infrastructure, and public trust, while emphasizing differences in implementation, institutional maturity, and operational experience. The comparative approach provides insights into best practices and policy gaps, highlighting the importance of adaptive governance, regional cooperation, and alignment with European standards. The findings contribute to the broader discussion on strengthening information resilience in Eastern Europe and offer recommendations for improving national preparedness against emerging hybrid threats.*

Keywords: *cyber security, national policies, disinformation, hybrid threats.*

INTRODUCTION

Russia's full-scale invasion of Ukraine on 24 February 2022 fundamentally transformed not only the security environment of Eastern Europe but also the nature of modern warfare. Military operations have been accompanied by extensive information campaigns combining cyberattacks, psychological operations, social media manipulation, propaganda, artificial intelligence-generated content, and coordinated disinformation. Information warfare has become an operational domain equal to land, sea, air, and cyberspace.

The Republic of Moldova is one of the states that has suffered the most under the impact of modern security challenges, such as cyberattacks and the conflict in Ukraine. Due to its geographical location close to the war zone, limited economic and energy resources, as well as its position between East and West, the Republic of Moldova has become highly exposed to regional instability. Both security threats have caused significant consequences, including inflation, energy insecurity, refugee influxes and

* PhD, associate professor, Moldova State University, Faculty of International Relations, Political and Administrative Studies, <https://orcid.org/0000-0001-9189-641X>, e-mail: victoriabevziuc@yahoo.ro.

political tensions, while also threatening the good functioning of institutions and digital infrastructure. As a result, the Republic of Moldova's role in addressing these security challenges consists of reinforcing its national security policies and strategies, improving institutional resilience and, without a doubt, consolidating cooperation with international organisations.

The management of the information space in the Republic of Moldova represents an essential component of national security, given the vulnerabilities associated with disinformation, media polarization, and external information interference. In recent years, the Republic of Moldova authorities have developed a series of policies and institutional mechanisms aimed at monitoring, regulating, and countering information threats.

Ukraine represents one of the most relevant examples in Eastern Europe in the field of information security due to its extensive experience with external disinformation campaigns, particularly in the context of its conflict with the Russian Federation. Ukrainian institutional policies focus on protecting the information space, strengthening societal resilience, and coordinating responses to information threats. The Ukrainian government quickly recognized that military resistance alone would be insufficient without protecting the national information environment. Consequently, Ukraine adopted numerous legislative amendments, strengthened existing institutions, and created new mechanisms designed to detect, monitor, and neutralize hostile information operations.

METHODOLOGY

This study employs a comparative qualitative research design based on the analysis of national strategic documents, legislation, institutional frameworks, and policy reports concerning information resilience in the Republic of Moldova and Ukraine. The research applies comparative policy analysis to identify similarities and differences in governance structures, legal provisions, strategic priorities, and institutional capacities for countering hybrid threats, disinformation, and information warfare. Data are collected through document analysis of official governmental publications, national security strategies, cybersecurity policies, and relevant reports issued by international organizations. The findings are interpreted using a comparative analytical framework that assesses the level of institutional development, policy coherence, and alignment with European and Euro-Atlantic resilience standards.

THEORETICAL AND CONCEPTUAL FRAMEWORK. LITERATURE REVIEW

The study of security challenges in international relations has undergone a notable evolution starting with the second part of the 20th century, being influenced by the transformations of the international system. Literature initially developed around the concerns of maintaining the international order, the prevention of armed conflicts and managing rivalries between states, and later included new dimensions generated by globalisation, technical progress and the emergence of non-traditional threats.

One of the central concepts analysed in the historiography of international relations is security. The first relevant works appeared in the context of the Cold War, when security was examined almost exclusively in terms of military confrontation. Authors such as A. Wolfers, helped shape early debates, emphasising the ambiguous and multidimensional character of security according to the perceptions of state actors (Wolfers, 1952: 483-492). Later, B. Buzan played a crucial role in expanding the research

sphere, analysing security not only at the military level, but also political, economic, societal and environmental, which opened new research directions in the domain (Buzan, 1983: 75-83).

The concept of information resilience has attracted increasing scholarly attention in the context of hybrid warfare, strategic competition, and digital transformation. Researchers have emphasized that information resilience extends beyond cybersecurity, encompassing the ability of institutions and societies to anticipate, withstand, respond to, and recover from information-related threats, including disinformation, propaganda, and foreign information manipulation. This multidimensional perspective has become particularly relevant for states exposed to persistent hybrid threats.

Among the leading scholars in this field, P. W. Singer and Emerson T. Brooking argue that contemporary conflicts are increasingly fought within the information domain, where digital platforms have become strategic battlefields shaping public opinion and political decision-making. Their work highlights the role of social media, artificial intelligence, and networked communication in amplifying information operations and influencing democratic processes (Singer & Brooking, 2018).

Theoretical approaches to resilience have been significantly influenced by David J. Snowden and Brian Walker, who conceptualize resilience as the adaptive capacity of complex systems to absorb shocks while maintaining essential functions. Applied to the information environment, resilience involves institutional adaptability, effective governance, strategic communication, media literacy, and public trust (Snowden & Boone, 2007; Walker et al., 2004).

The phenomenon of disinformation has been extensively examined by Claire Wardle and Hossein Derakhshan, who distinguish between misinformation, disinformation, and malinformation. Their conceptual framework has become a cornerstone for understanding different forms of information disorder and for developing policies aimed at countering information manipulation while safeguarding freedom of expression (Wardle & Derakhshan, 2017).

The European perspective on information resilience has been shaped by studies conducted by the European Union Agency for Cybersecurity (ENISA), the European External Action Service (EEAS), and the NATO Strategic Communications Centre of Excellence (NATO StratCom COE). These institutions emphasize that societal resilience depends on coordinated governance, cybersecurity, critical infrastructure protection, strategic communication, and cooperation between public authorities, the private sector, civil society, and international partners (ENISA, 2023; European External Action Service, 2022; NATO Strategic Communications Centre of Excellence, 2023).

In the context of Eastern Europe, scholars have increasingly focused on the experiences of Ukraine and the Republic of Moldova as frontline states confronting hybrid threats. Comparative studies underline that Ukraine has developed extensive institutional capacities following the full-scale Russian invasion, while the Republic of Moldova continues to strengthen its legal and institutional framework through reforms aligned with European Union standards. These studies demonstrate that information resilience is not solely a technological issue but also a matter of democratic governance, institutional credibility, and societal cohesion (European Commission, 2023; European Union Institute for Security Studies, 2023; United Nations Development Programme, 2023).

Hybrid warfare combines conventional military force with cyber operations, economic coercion, political influence, intelligence activities, and strategic

communication. Russian military doctrine increasingly integrates information operations as a central component of conflict (Galeotti, 2019; RAND Corporation, 2016).

Disinformation differs from misinformation because it involves the intentional dissemination of false or manipulated information designed to influence political behaviour or undermine public trust. During the invasion, Russian information operations pursued several objectives:

- delegitimizing the authorities;
- reducing public morale;
- undermining trust in state institutions and international partners (Wardle & Derakhshan, 2017; Center for Strategic and International Studies [CSIS], 2022).
- discouraging military mobilization;
- undermining international support;
- manipulating foreign public opinion;
- creating confusion through contradictory narratives.

Recent studies identify Ukraine as one of the world's most significant laboratories for counter-disinformation governance under wartime conditions (Marushchak, Petrov, Khoperiya, 2025).

In the view of the American professor M. C. Libicki, cyberattack is defined as “the deliberate disruption or corruption by one state of a system of interest to another state” (Libicki, 2009: 23). This definition suggests that cyberattacks are not accidental events, but rather planned and strategic actions carried out by state actors to undermine the security of another state. Moreover, it highlights that power is increasingly exercised through the manipulation and destabilisation of digital infrastructures.

Cyber conflict is viewed by realism through the lens of power, state security and anarchy, treating cyberattacks as other instruments through which states compete to protect their territory and advance their interests. Realists consider cyberattacks to be potentially cheaper, faster and more effective than defence, leading states to develop their own cyber capabilities to respond to emerging risks. At the same time, it is mentioned that most cyberattacks have tended to produce low-level disruption, espionage or limited damage rather than decisive strategic effects and therefore do not fully correspond to the full war-like escalation realists might expect in traditional warfare (Craig & Valeriano, 2018: 1-5).

In liberal thinking, the international system consists of a variety of powerful actors beyond the state, such as individuals, private companies and activist groups. Liberals argue that governments cannot secure cyberspace alone, because the private sectors own and operate much of the Internet's infrastructure; consequently, states must rely on state-corporate cooperation. In this context, cyberattacks are less likely to occur between liberal democracies, which prefer cooperation and mutual consent to maintain peace. However, when such incidents do occur between allies, liberals may categorise them as cyber espionage rather than acts of war. The promotion of international agreements and institutions, such as the Council of Europe Convention on Cybercrime, is seen as an effective way to manage conflicts and reduce the threat of cyberwar (Isnarti, 2016: 157-158).

Constructivism views cyberwar and cyberspace as social constructs shaped by the interests, identities and perceptions of international actors. Moreover, constructivists analyse how technological innovations have been socially transformed into threats to

national security. In this context, the problem of cyberwar is often rooted in the socially constructed fear of potential attacks instead of the frequency of the attacks themselves. Ultimately, it is noted that cyberwar is driven by (mis)perceptions and establishing shared norms, identity and communication between states, cyberwar would be less likely to happen (Isnarti, 2016: 157-158).

The Moldovan analyst I. Bucătaru characterises cyberattacks as a major threat, particularly organised ones that are capable of causing critical destabilisation to national infrastructure, the economy and national security. The author also emphasises that cyberattacks can be executed with relatively limited resources, may have long-term effects and allow the attacker to remain anonymous (Bucătaru, 2016: 509-510). This perspective reinforces the idea that cyberattacks represent a significant threat to national and international security, functioning as a strategic instrument that is easier to deploy and manage compared to other more dangerous alternatives.

The Romanian researchers A. V. Vevera and A. M. Udrioiu define a cyberattack in their article as “a malicious attempt to cause temporary or permanent damage to the components of an Internet network” (Vevera & Udrioiu, 2018: 8). This definition emphasises the intentional nature of cyberattacks and their potential to damage digital infrastructure. In addition, it also refers to the consequences of attacks, which can be both short-term and long-term, reflecting the multidimensional dynamics of an attack.

DATA RESULTS

The legislative and institutional framework of the Republic of Moldova is complex. The country has legislation regulating electronic communications, mass media, and cybersecurity. The National Regulatory Agency for Electronic Communications and Information Technology (ANRCETI) and the Center for Strategic Communication and Countering Disinformation (CSRM) are the main institutions involved in managing the information space, monitoring public content, and coordinating responses to disinformation campaigns (European Commission, 2024; Government of the Republic of Moldova, 2023).

The Government of the Republic of Moldova has developed strategies and action plans for cybersecurity and the protection of critical information infrastructure. These policies aim both at the technical protection of networks and information systems and at preventing the spread of disinformation through official channels and online environments. The strategies emphasize coordination among ministries, local authorities, the media, and civil society (Government of the Republic of Moldova, 2025; European Union Agency for Cybersecurity [ENISA], 2023; European Commission, 2024).

The Republic of Moldova has begun developing a specific legislative framework for information security and combating disinformation in response to increasing informational vulnerabilities, public polarization, and exposure to external influence campaigns. This legislation aims to protect critical infrastructure, prevent information manipulation, and ensure a secure information environment for citizens (European Commission, 2024; Council of Europe, 2024; Government of the Republic of Moldova, 2023).

To start with, the National Security Strategy of the Republic of Moldova, adopted in 2023, is the most important legal act in the national security and defence policy, which settles the functioning, steps, mechanisms and instruments of governance within the security system. Among the main dangers mentioned in the strategy are cyber threats, mainly originating from state actors targeting national and regional critical infrastructure,

for example private and public institutions, as well as risks associated with the evolution of information and communication technologies. Additionally, there are specified two causes that make the cyber domain vulnerable to attacks in the Republic of Moldova: the outdated IT infrastructure of institutions and the limited level of cybersecurity awareness among public servants and the population. There are established key objectives for sustaining cybersecurity and resilience, including the creation of a new institution competent in the cybersecurity domain, the organisation and participation in cybersecurity and defence exercises, as well as alignment with EU norms related to cyberspace security (Hotărâre nr. HP391 din 15.12.2023). The strategy is seen as the foundational document, reflecting all the vulnerabilities faced by the Republic of Moldova. Its importance lies in the complex description of solutions addressing cybersecurity.

Another important document that reinforces the legal framework of the Republic of Moldova is the National Cybersecurity Programme for 2026-2030. The programme sets objectives and actions regarding the development, consolidation and implementation of measures and priorities concerning cybersecurity. Likewise, the document contributes to the implementation of the 2030 Agenda for Sustainable Development by integrating its objectives into the national framework. The fulfilment of the programme is expected to generate a notable impact on the Republic of Moldova's cybersecurity sector. Among the main benefits are the consolidation of institutional capacity, the expansion of international cooperation, the increasing trust in digital services and the enhancement of societal cyber resilience. Moreover, this document supports the country's EU integration process, protects citizens' interests and sustains economic development in the fields of digitalisation and innovation (Hotărâre din 2025 cu privire la aprobarea Programului național de securitate cibernetică pentru anii 2026-2030). This programme is an important step towards a more secure cyberspace and a better organised national security framework. Moreover, it allows institutions to prevent and respond to cyber threats rapidly.

Last but not least, the integration of cybersecurity within the Digital Transformation Strategy of the Republic of Moldova 2023-2030 is essential for creating a secure and adaptable digital environment. Through the involvement of the government, the private sector and civil society, the strategy aims to create cybersecurity as a shared responsibility. The strategy stresses key priorities, including the establishment of a national cybersecurity authority, professional training for public officials and constant reporting of incidents by critical services experts. Furthermore, the document proposes the operationalisation of the Cybersecurity Coordination Council in order to safeguard critical infrastructure and improve state information systems (Republica Moldova: Strategia de transformare digitală 2023-2030. Ministerul Dezvoltării Economice și Digitalizării, 2023: 33-35). The interconnection between cybersecurity and digitalisation is closely linked in terms of ensuring the safe and efficient development of digital systems. This relation is essential to preserve in order to protect critical infrastructure and maintain trust in digital services.

The adoption of these three strategic documents demonstrates the Republic of Moldova's commitment to reinforcing its cybersecurity structure and tackling emerging cyberattacks. In the context of the EU integration process and rapid digitalisation, the development of coherent mechanisms and strategies is crucial for ensuring national resilience and security. Moreover, these strategies demonstrate that cooperation between public authorities, private companies and international partners can facilitate their

implementation and the achievement of key goals. Together, these strategies contribute to the development of the states' main priorities, improve institutional capacities and support the protection of critical infrastructure.

A significant step in addressing this issue was the adoption of the Law regarding cybersecurity in 2023, alongside the support of the EU. The law provides principal notions related to the subject, the principles of ensuring cybersecurity, the national coordination of institutions, as well as the financing process (Lege nr. 48 din 16-03-2023 privind securitatea cibernetică). The law is extremely important because it transposes the European standards aimed at strengthening the resilience of critical infrastructure. The adoption of this law represents a crucial development in the national security framework, particularly in addressing cyber threats. At the national level, the creation of a more coordinated and preventive approach to cybersecurity helps to enhance stability and resilience. Moreover, the law contributes to the alignment of the Republic of Moldova's legislation with EU norms and standards, which reveals the constant effort in addressing the problem and cooperating with the EU.

Another important law is the Law on the approval of the Information Security Concept of the Republic of Moldova, adopted in 2017. The law establishes the national framework for ensuring information security as a fundamental part of national security. It highlights the main risks, objectives, principles and directions for protecting the informational space of the country. With a strong focus on cyber threats, the law sets the clear basis in the field of information security and institutions (Lege nr. 299 din 21-12-2017). In the context of increasing hybrid threats and regional instability, the law suggests the Republic of Moldova's early recognition of information security as a deliberate priority. Moreover, it shows the continuous effort and modernisation in order to implement the main mechanisms.

An important component of the Republic of Moldova's institutional framework is the Government Decision regarding the establishment, organisation and functioning of the Cybersecurity Agency. The decision underlines the mission, the domain of activity, functions, attributions and rights of the agency. At the same time, it establishes the organisation and structure that ensure the proper functioning of the agency and the implementation of state policies in the cybersecurity domain (Hotărâre nr. 1028 din 21-12-2023). The decision is essential because it provides a clear institutional mechanism for the prevention and response to cyber incidents. It also contributes to the consolidation of state capacities in protecting the state, as well as enhancing international cooperation and aligning the Republic of Moldova's cybersecurity governance with European standards.

Another important institutional element of the Republic of Moldova's cybersecurity structure is the Government Decision regarding the establishment, organisation and functioning of the Coordinating Council in the field of cybersecurity, adopted in the context of the Law on Cybersecurity. The institution represents a key mechanism responsible for the strategic and operational coordination of national cybersecurity policies. The council defines its mission, attributions, organisation and functional composition. The institution should coordinate the implementation of national strategies, harmonise policies and improve cooperation in tackling cyber risks (Hotărâre nr. 333 din 08-05-2024). The establishment of this council is highly significant because it reflects the growing complexity of cybersecurity challenges, which require more specialists and coordinated institutional action. Moreover, it improves the state's ability to face cyber incidents in an efficient and strategic manner. At the same time, its

composition demonstrates a broader approach, involving not only security institutions but also ministries such as energy, finance and health.

In terms of cybersecurity, the Republic of Moldova has progressively developed a comprehensive legal and institutional framework. Through several laws and strategies, the country has established a structured system to prevent, detect and respond to cyber threats. These instruments have aligned the Republic of Moldova with European standards and values, strengthening its own resilience. Even though the Republic of Moldova's cybersecurity development is seen as an ongoing process, it requires constant effort, improvement, investment and strong collaboration. All these practices position the Republic of Moldova as an important actor in managing modern security challenges.

Previously analysed in the context of cybersecurity, the National Security Strategy of the Republic of Moldova further provides security measures in relation to the ongoing border conflict. Among regional and global security threats, the war in Ukraine is the key factor that destabilises the national security of the Republic of Moldova. In the field of military security and national defence, the strategy outlines the insufficient dotation of the armed forces and the reduced public support for the defence of the country. In order to make a more resilient contribution, the country must adopt an integrative and anticipative approach. These two approaches help combine the information with its analysis and to predict possible scenarios in the case of war. Moreover, it is crucial to develop the defence potential of the country by modernising the equipment and technologies used by the armed forces (Hotărâre nr. HP391 din 15.12.2023). The National Security Strategy is a key document in ensuring stability, as the Russian aggression in Ukraine has intensified pressure across the region. By implementing its main objectives in the field of security and national defence, the strategy intends to strengthen the state's determination against external threats. Through the modernisation of the defence sector, the institutional capability to respond to challenges will become more coordinated and efficient.

The National Defence Strategy of the Republic of Moldova for 2024-2034 represents another essential policy instrument aimed at guaranteeing peace, stability and the protection of constitutional democracy. The strategy outlines the potential risks in the national defence domain, as well as the main objectives of defence policy and the necessary steps and resources for their implementation. At the same time, the strategy emphasises the strategic cooperation with the UN, NATO and the EU, as well as the clear need to upgrade the national army (Hotărâre nr. 319 din 26-12-2024). In the context of the Russian invasion against Ukraine, this strategy serves as a critical shift from an underfunded military posture towards a modernised model of national resistance. The war led to the strengthening of military capacities, closer alignment with European security standards and the consolidation of main priorities in facing emerging security threats, such as the conflict in Ukraine.

In a similar context, the Military Strategy of the Republic of Moldova for 2025-2035 was adopted to define the long-term development of national defence and to align the armed forces with the changing security environment. Some of the key priorities of the strategy are the modernisation of military capabilities, strengthening operational preparation and of course, maintaining positive partnerships with international organisations. At the same time, the Military Strategy emphasises the participation in international operations and gradual integration into European security frameworks, as seen in previous strategies (Hotărâre din 2025 cu privire la aprobarea Strategiei militare a Republicii Moldova pentru anii 2025-2035). The conflict in Ukraine has accelerated

the urgency of modernising defence structures and adopting a more comprehensive approach to national security. In this sense, the strategy is a necessary adaptation to face emerging threats, alongside a prepared and professional army.

Taken together, these three strategies play a crucial role for the Republic of Moldova's resilience and preparedness towards the war in Ukraine. By addressing different dimensions of national security, such as institutional enforcement, military readiness and long-term defence planning, the strategies pursue an interconnected goal of preserving stability within the country. One document establishes the overall direction for managing security threats, while another focuses on translating priorities into concrete defence objectives and continuous cooperation. A third provides an overview for transforming the armed forces into a more modern and adaptable structure.

An important legal framework addressing this issue is represented by the Law on the Security and Intelligence Service of the Republic of Moldova. The law was adopted for the reorganisation and modernisation of the activity of the SIS. It establishes the attributions, organisation and the responsibilities in preventing threats towards the state's security, external influence and destabilisation actions. Moreover, it highlights the consolidation of the national army capacities and the protection of strategic infrastructure in emergency situations (Lege nr. 136 din 08-06-2023). In a tense regional context, the law reshapes the new goal of the institution in managing interferences caused by the war in Ukraine. The modifications introduced by the law reinforce the Republic of Moldova's position in tackling security risks and acting more efficiently against attempts to undermine national stability. By adopting this law, the institutional coordination becomes more coherent and strengthens the capacity of state authorities to prevent destabilisation actions.

In a similar context, the Law on Counterintelligence Activity and Foreign Intelligence Activity establishes the concrete actions in conducting security operations. The law provides the legal framework for the activities carried out by the intelligence services and manages the threats coming from foreign states or organisations. The adoption of the law reflects the growing need to protect national security after the Russian aggression against Ukraine intensified espionage, disinformation campaigns and attempts to destabilise institutions (Lege nr. 179 din 07-07-2023). The law is especially important because the Republic of Moldova became more exposed to regional threats, particularly due to the conflict. By improving the intelligence coordination, the security operations will be more efficient and better adapted to risks. The Republic of Moldova's attempt to face geopolitical realities is reflected in strengthening the process of the security operations, which are essential for protecting sovereignty and internal order.

The last important law examined in this analysis is the Law on the Centre for Strategic Communication and Countering Disinformation and on the Amendment of Certain Normative Acts. In the context of numerous cases of propaganda, disinformation and external interference, mostly generated by the conflict in Ukraine, the establishment of such a centre is crucial for preventing these situations. The law sets out the institution's mission, organisational structure and financing process. The main goal of the centre is to consolidate and improve efforts to combat disinformation, manipulation and external influence. All these factors affect the realisation of national interests and the objectives of national security (Lege nr. 242 din 31-07-2023). The relevance of establishing this centre lies in the highly exposed regional information space to propaganda and hybrid influence campaigns. This institution helps manage and respond more effectively to cases that can destabilise public opinion and weaken trust in institutions. Moreover, it

contributes to reducing the impact of external narratives linked to the conflict, especially those generated through Russian channels. By supporting informed decision-making within society, people are able to critically assess the geopolitical situation near the country.

In the context of the war in Ukraine, the analysed laws demonstrate the Republic of Moldova's initiative to address the security risks generated by the conflict in the neighbouring country. It is essential to reinforce the legal framework in order to maintain stability and ensure the protection of citizens. At the same time, external influence is increasing and the need for competent authorities is vital for maintaining national order. The level of security in a state corresponds to the institutional capacity to anticipate, manage and respond rapidly to emerging threats. In this sense, the adopted legal measures aim to strengthen resilience and ensure the stability of the country.

In conclusion, all the strategies and laws adopted by the Republic of Moldova reflect a coordinated response to both cyberattacks and the conflict in Ukraine. The constant effort made for strengthening institutional resilience, enhancing the capacity to prevent cyber threats and improving cooperation, have accelerated the Republic of Moldova's European path. Moreover, by modernising the legal framework, the country seeks to reduce vulnerabilities linked to external interference and regional stability. Overall, these measures and their impact demonstrate a comprehensive approach to national security, intended to ensure long-term stability and determination in an evolving geopolitical environment.

The Center for Strategic Communication and Countering Disinformation seeks to develop institutional capacities and educate citizens in order to increase information resilience. In this regard, emphasis is placed on strengthening interinstitutional cooperation and partnerships with civil society and academia to effectively identify and counter manipulative narratives.

Furthermore, the strategy promotes institutional transparency and access to verified information, contributing to increased public trust and the development of critical thinking among citizens. It also provides for the development of media and digital literacy skills, enabling citizens to identify and critically evaluate sources of information in the context of a complex information environment.

The Republic of Moldova's legislation regarding information security and the fight against disinformation continues to evolve, reflecting the need to adapt to emerging information threats. Strengthening institutions, increasing technical capacities, and implementing effective monitoring and response mechanisms are essential for protecting the information space and enhancing society's resilience against information manipulation. Together with other public institutions and international partners, the Center for Strategic Communication and Countering Disinformation (CSRM) continuously monitors information flows, identifying fake news and manipulative materials that could affect public opinion or national security. At the same time, the authorities organize public information and media literacy campaigns to increase citizens' ability to recognize disinformation.

The Republic of Moldova cooperates with the European Union, NATO, and regional organizations through the exchange of best practices, training programs, and technical support in the field of information security. This cooperation enables the implementation of international standards and the development of national capacities to prevent cross-border information threats.

The institutional policies of the Republic of Moldova for managing the information space are still undergoing consolidation. Recent experiences demonstrate that success depends on effective institutional coordination, the active involvement of civil society, and international partnerships. Rapid adaptation to new forms of disinformation and the implementation of proactive mechanisms for education and monitoring are essential for protecting national information security.

Ukraine has developed a comprehensive legislative framework regarding information security and the protection of the information environment, including specific legislation aimed at combating disinformation and external information interference.

Since 2014, and particularly following the full-scale Russian invasion in February 2022, Ukraine has significantly transformed its legal framework governing information security, media regulation, and the protection of the national information space. These legislative developments reflect the recognition that the information environment has become a critical domain of modern warfare, where disinformation, psychological operations, and cyber-enabled influence campaigns are employed alongside conventional military operations. Consequently, Ukraine has adopted a comprehensive set of legal measures designed to strengthen national resilience while aligning its legislation with European democratic standards (Giles, 2016; Paul & Matthews, 2016). The introduction of martial law under Presidential Decree No. 64/2022 marked a fundamental turning point in the regulation of information activities. The declaration of martial law created the legal basis for the implementation of temporary restrictions aimed at safeguarding national security and ensuring coordinated public communication during an armed conflict (President of Ukraine, 2022a). Shortly thereafter, Presidential Decree No. 152/2022 enacted the decision of the National Security and Defense Council concerning a unified information policy under martial law. This measure established a coordinated communication mechanism among the country's principal television broadcasters through the "United News" national telethon. Although the initiative generated debate regarding media pluralism, Ukrainian authorities argued that the centralization of official communication was necessary to prevent the dissemination of contradictory information, reduce public panic, and limit opportunities for hostile information manipulation during wartime (President of Ukraine, 2022b; Council of Europe, 2023).

In parallel with these institutional measures, the Ukrainian Parliament introduced substantial amendments to criminal legislation addressing collaboration, espionage, and information activities that could facilitate Russian military operations. One of the most significant legislative developments was Law No. 2178-IX, which strengthened Article 114-2 of the Criminal Code by establishing criminal liability for the unauthorized dissemination of information concerning the movement, deployment, or location of Ukrainian armed forces during martial law. The amendments also expanded criminal responsibility for collaboration with occupying authorities and participation in activities supporting the aggressor state's information operations (Verkhovna Rada of Ukraine, 2022a). From a legal perspective, these provisions illustrate Ukraine's transition from a peacetime regulatory model toward a wartime legal regime in which information itself is recognized as a strategic national security asset rather than solely an object of freedom of expression.

A cornerstone of Ukraine's contemporary media reform is the adoption of the Law of Ukraine "On Media" (Law No. 2849-IX), which entered into force in March

2023. The legislation represents one of the most comprehensive reforms of the Ukrainian media sector since independence and constitutes an important element of the country's European integration process. The new law harmonizes national legislation with the European Union's Audiovisual Media Services Directive by extending regulatory oversight to online media platforms, improving transparency requirements regarding media ownership, strengthening the authority of the National Council on Television and Radio Broadcasting, and establishing procedures for restricting media outlets that cooperate with the aggressor state or systematically disseminate disinformation (Verkhovna Rada of Ukraine, 2022b; Council of Europe, 2023). According to the Council of Europe (2023), although certain wartime provisions require careful implementation to preserve media freedom, the overall reform substantially aligns Ukrainian media legislation with European standards.

Another important legislative direction concerns the prohibition of information products that promote or justify Russian aggression. Following the beginning of the full-scale invasion, Ukraine expanded restrictions on the production, importation, distribution, and public dissemination of materials supporting the aggression against Ukraine or legitimizing the occupation of Ukrainian territories. These legal measures prohibit the dissemination of propaganda materials, symbols associated with the aggressor state, and publications that deny or justify Russian military actions. Similar restrictions were introduced regarding audiovisual content, publishing activities, and cultural products originating from the Russian Federation when they contribute to hostile information influence (Verkhovna Rada of Ukraine, 2022a). While such measures represent significant limitations on certain forms of expression, Ukrainian authorities justify them as exceptional responses to the unprecedented scale of information warfare accompanying military aggression.

The evolution of Ukraine's legislative framework demonstrates an increasing convergence between information security and national security policy. Rather than regulating media exclusively through the traditional perspective of freedom of expression, Ukrainian legislation increasingly conceptualizes the information domain as a component of comprehensive national defence. This approach corresponds to broader international debates concerning cognitive warfare, hybrid threats, and strategic communication, which emphasize that hostile actors increasingly seek to influence democratic societies through coordinated information manipulation rather than conventional military force alone (Bjola & Papadakis, 2020; Helmus et al., 2018; Pomerantsev, 2019).

Nevertheless, the Ukrainian model also illustrates the complex legal and normative dilemmas that emerge during prolonged armed conflict. The expansion of governmental authority over media regulation, restrictions on information dissemination, and enhanced supervisory powers of regulatory institutions inevitably raise questions regarding proportionality, judicial oversight, and the preservation of democratic freedoms. International organizations, including the Council of Europe and the Organization for Security and Co-operation in Europe, have therefore emphasized that emergency restrictions adopted under martial law should remain temporary, transparent, and subject to effective legal review in order to maintain compliance with European human rights standards (Council of Europe, 2023; OSCE, 2023). Consequently, Ukraine's legislative experience demonstrates the continuing challenge of balancing national security imperatives with the protection of democratic values in an environment characterized by persistent hybrid threats.

Ukraine's institutional framework for protecting the information environment has evolved considerably since 2014 and has undergone substantial consolidation following the full-scale Russian invasion in 2022. Unlike traditional approaches that assign responsibility for information security to a single governmental authority, Ukraine has developed a multi-institutional governance model integrating national security agencies, media regulators, cybersecurity institutions, strategic communication bodies, and civil society organizations. This comprehensive approach reflects the understanding that contemporary information threats are multidimensional, combining disinformation, cyberattacks, psychological operations, and foreign influence campaigns that require coordinated responses across multiple sectors (Bjola & Papadakis, 2020; NATO StratCom COE, 2023).

At the centre of Ukraine's security architecture is the National Security and Defense Council (NSDC), which coordinates state policy in the fields of national security, cybersecurity, and strategic communications. Since the beginning of the full-scale invasion, the NSDC has assumed an increasingly prominent role in coordinating institutional responses to information threats by facilitating interagency cooperation and adopting strategic decisions concerning the protection of the national information space. The Council also oversees the implementation of national security policies and coordinates activities among ministries, intelligence services, and specialized governmental agencies responsible for countering hybrid threats (National Security and Defense Council of Ukraine, 2024).

One of the most influential institutions created specifically to combat information manipulation is the Center for Countering Disinformation (CCD), established in 2021 under the authority of the NSDC. Although initially conceived as a strategic analytical body, the Center became one of Ukraine's principal institutions following the Russian invasion in February 2022. Its mandate extends beyond conventional fact-checking activities and includes continuous monitoring of the information environment, identification of hostile narratives, analysis of coordinated influence operations, publication of analytical reports, and dissemination of verified information to both domestic and international audiences (Center for Countering Disinformation, 2024). Through systematic monitoring of traditional media, digital platforms, and social networks, the CCD produces daily assessments of disinformation campaigns and provides recommendations to public authorities regarding strategic communication priorities. The institution also maintains close cooperation with European Union institutions, NATO structures, international research organizations, and independent fact-checking networks, contributing to broader efforts aimed at strengthening regional information resilience (OECD, 2023).

The Security Service of Ukraine (SBU) represents another key actor within the national information security system. In addition to its traditional counterintelligence responsibilities, the SBU investigates hostile information operations, identifies individuals collaborating with foreign intelligence services, and counters coordinated influence campaigns designed to undermine state institutions or public confidence. Since 2022, the Service has significantly expanded investigations concerning collaboration with occupying authorities, dissemination of military intelligence benefiting Russian forces, and cyber-enabled influence activities. The SBU also works closely with prosecutors and judicial authorities to enforce criminal legislation concerning collaboration and unlawful dissemination of sensitive military information (Security Service of Ukraine, 2024).

The cyber dimension of information security is primarily coordinated through the National Cybersecurity Coordination Center (NCCC), operating under the NSDC. Recognizing that modern information operations frequently combine disinformation with cyberattacks targeting critical infrastructure, the NCCC coordinates cooperation among governmental institutions responsible for cybersecurity, intelligence, defense, and digital transformation. Its responsibilities include monitoring cyber threats, developing national cybersecurity policies, coordinating responses to cyber incidents affecting public institutions, and strengthening the resilience of critical information infrastructure. The Center also collaborates extensively with the European Union, NATO, and international cybersecurity organizations to exchange threat intelligence and develop common resilience standards (National Security and Defense Council of Ukraine, 2024; NATO, 2024).

An equally important role is played by the Ministry of Culture and Strategic Communications (formerly the Ministry of Culture and Information Policy), which is responsible for developing governmental communication strategies, promoting media literacy, supporting independent journalism, and coordinating public awareness campaigns against disinformation. The Ministry considers information resilience not only a matter of national security but also an essential component of democratic governance and societal cohesion. Consequently, its activities include educational initiatives aimed at improving citizens' ability to identify manipulated content, verify information sources, and recognize foreign propaganda techniques (Ministry of Culture and Strategic Communications of Ukraine, 2024).

Complementing these governmental structures is the Centre for Strategic Communication and Information Security (SPRAVDI), established to strengthen public communication and counter hostile narratives in real time. The Centre publishes analytical reports, explains ongoing disinformation campaigns, provides verified information during crises, and supports government institutions in developing coherent strategic messages. Its activities reflect contemporary approaches to strategic communication, emphasizing proactive engagement with the public rather than merely responding to false information after it has already spread. By combining rapid communication with evidence-based analysis, the Centre seeks to reduce the effectiveness of foreign information influence while strengthening public trust in official institutions (Centre for Strategic Communication and Information Security, 2024).

The Ukrainian response to disinformation is also characterized by strong cooperation between governmental institutions and civil society organizations. Independent fact-checking initiatives, including StopFake, VoxCheck, and the Institute of Mass Information (IMI), play an important role in identifying manipulated narratives, verifying public information, and monitoring violations of media standards. Their analytical reports frequently complement governmental assessments and contribute to broader public awareness regarding information manipulation. This cooperation demonstrates that information resilience increasingly depends on partnerships between state institutions, academia, media organizations, and independent civil society actors rather than exclusively on governmental regulation (Pomerantsev, 2019; Helmus et al., 2018).

Operationally, Ukraine has adopted a comprehensive response mechanism based on three complementary pillars: prevention, continuous monitoring, and rapid response. Preventive measures include media literacy programs, strategic public communication, legal regulation, and international cooperation. Continuous monitoring is conducted

through real-time analysis of traditional media, online platforms, social networks, and cyber threats using artificial intelligence, big data analytics, and open-source intelligence (OSINT) methodologies. Finally, rapid response mechanisms involve the prompt publication of verified information, coordinated governmental communication, exposure of hostile narratives, cooperation with digital platforms to limit the spread of harmful content, and judicial action against individuals participating in illegal information activities (OECD, 2023).

Ukraine's institutional experience illustrates that the effectiveness of counter-disinformation policies depends less on the powers of individual institutions than on the quality of coordination among them. The integration of intelligence services, cybersecurity agencies, media regulators, strategic communication centers, and civil society organizations has enabled Ukraine to develop a relatively resilient information governance model despite operating under conditions of large-scale military conflict. At the same time, scholars emphasize that maintaining democratic accountability, institutional transparency, and judicial oversight remains essential to ensure that emergency powers introduced during wartime do not become permanent features of the information governance system (Council of Europe, 2023; Bjola & Papadakis, 2020).

International cooperation has become one of the defining elements of Ukraine's strategy for protecting its information environment and strengthening national resilience against hybrid threats. Since 2014, and particularly after the launch of Russia's full-scale invasion in 2022, cooperation with the European Union (EU) and the North Atlantic Treaty Organization (NATO) has expanded significantly, reflecting the understanding that disinformation campaigns and cyber-enabled influence operations transcend national borders and therefore require coordinated international responses. Beyond military and financial assistance, both organizations have supported Ukraine in developing institutional capacities, harmonizing legislation, improving cybersecurity, and strengthening strategic communication mechanisms (NATO, 2024; European Commission, 2024).

The European Union has played a central role in supporting Ukraine's reforms in the fields of media governance, information security, and democratic resilience. As part of the country's broader European integration process, Ukraine has progressively aligned its legislation with the EU *acquis*, particularly in the audiovisual and digital media sectors. The adoption of the Law on Media (Law No. 2849-IX) illustrates this process by harmonizing national legislation with the Audiovisual Media Services Directive (AVMSD), introducing greater transparency in media ownership, extending regulatory oversight to online media services, and reinforcing safeguards against foreign information interference (Council of Europe, 2023). These reforms have been supported through technical assistance provided by the European Commission and the Council of Europe, which have offered legal expertise, institutional assessments, and recommendations aimed at ensuring that wartime measures remain compatible with European standards concerning freedom of expression and media pluralism (European Commission, 2024).

In addition to legislative support, the EU has invested considerably in strengthening Ukraine's institutional capacity to counter disinformation. Cooperation with the European External Action Service (EEAS), particularly through the EUvsDisinfo initiative, has enabled Ukrainian institutions to exchange information regarding emerging disinformation narratives, identify coordinated foreign influence campaigns, and improve analytical methodologies for monitoring information threats.

This collaboration facilitates the sharing of best practices on strategic communication, fact-checking, digital investigations, and public awareness campaigns while promoting a common understanding of Russian information warfare among European partners (EEAS, 2024). The European Union has also financed numerous projects designed to improve media literacy, support independent journalism, strengthen civil society organizations, and enhance digital resilience across Ukrainian society (European Commission, 2024).

Cybersecurity has become another major area of cooperation between Ukraine and the European Union. Following repeated cyberattacks targeting Ukrainian governmental institutions, energy infrastructure, financial systems, and communication networks, the EU expanded technical assistance aimed at improving cyber resilience through specialized training programs, capacity-building initiatives, and information-sharing mechanisms. Cooperation with the European Union Agency for Cybersecurity (ENISA) and participation in European cybersecurity exercises have contributed to strengthening Ukraine's ability to prevent, detect, and respond to cyber incidents that frequently accompany coordinated disinformation campaigns (ENISA, 2023). This integrated approach reflects the growing recognition that cyber operations and information manipulation constitute complementary components of contemporary hybrid warfare.

Cooperation with NATO has developed along similar lines but places greater emphasis on resilience against hybrid threats, strategic communications, and defense-related information security. Since Ukraine was granted Enhanced Opportunities Partner status in 2020, collaboration has intensified through practical programs focusing on cyber defense, crisis communication, intelligence sharing, and institutional resilience. NATO recognizes information manipulation as an integral element of hybrid warfare and has therefore supported Ukraine in developing capabilities that combine military preparedness with civilian resilience against cognitive and psychological influence operations (NATO, 2024).

One of NATO's principal contributions has been provided through the NATO Strategic Communications Centre of Excellence (StratCom COE) in Riga. Although Ukraine is not a member of the Centre, Ukrainian experts and institutions participate regularly in its training programs, analytical projects, and professional exchanges. These activities include research on Russian information warfare, strategic communication planning, social media manipulation, cognitive warfare, and public diplomacy. The Centre's analytical publications have significantly influenced the development of Ukrainian strategic communication policies by promoting evidence-based approaches to identifying hostile narratives and strengthening institutional coordination (NATO StratCom COE, 2023).

Cooperation also extends to the field of cybersecurity through the NATO Comprehensive Assistance Package (CAP) for Ukraine, which has financed projects aimed at modernizing cyber defense capabilities, protecting critical infrastructure, improving incident response mechanisms, and enhancing interoperability between Ukrainian institutions and NATO structures. Training programs supported by NATO have contributed to developing professional expertise within Ukrainian cybersecurity institutions while facilitating the exchange of intelligence concerning cyber threats originating from state-sponsored actors (NATO, 2024). These initiatives complement broader efforts to integrate cyber resilience into Ukraine's national security architecture

and reflect NATO's increasing emphasis on resilience as a fundamental component of collective security.

An important feature of Ukraine's international cooperation is the integration of governmental institutions with academic networks, independent research centers, and civil society organizations. Ukrainian experts participate actively in European and transatlantic research projects addressing hybrid threats, digital governance, artificial intelligence, election security, and media resilience. These partnerships facilitate the transfer of knowledge, comparative policy analysis, and the development of innovative tools for detecting coordinated influence campaigns. International cooperation has therefore evolved beyond financial assistance to encompass the creation of transnational epistemic communities capable of producing shared analytical frameworks for understanding contemporary information warfare (Bjola & Papadakis, 2020; Pomerantsev, 2019).

Despite substantial progress, several challenges continue to affect international cooperation in this field. Differences in national legal frameworks, variations in data-sharing procedures, and the rapidly evolving nature of digital platforms complicate coordinated responses to cross-border disinformation campaigns. Furthermore, balancing effective counter-disinformation measures with the protection of fundamental rights remains a common challenge for both Ukraine and its international partners. Consequently, recent European policy documents increasingly emphasize resilience-based approaches that prioritize institutional preparedness, public trust, media literacy, and democratic accountability rather than relying exclusively on restrictive regulatory measures (European Commission, 2024; OECD, 2023).

Overall, Ukraine's cooperation with the European Union and NATO demonstrates that information security has become an integral component of international security governance. The Ukrainian experience confirms that resilience against disinformation depends not only on domestic legislation and institutional capacity but also on sustained international partnerships that facilitate knowledge exchange, technological innovation, strategic communication, and coordinated responses to evolving hybrid threats. As information warfare becomes increasingly transnational, Ukraine's cooperation with European and Euro-Atlantic institutions offers an important model for the development of collective resilience against foreign information interference.

The comparative analysis of the Republic of Moldova and Ukraine demonstrates that both countries have undertaken significant efforts to strengthen the protection of their information environments in response to persistent hybrid threats, particularly those associated with Russian information operations. Although the two states share a similar geopolitical context and face comparable challenges related to disinformation, foreign influence, and cyber-enabled information manipulation, their institutional responses have evolved at different speeds and with varying degrees of complexity.

Ukraine has developed a comprehensive and highly integrated system of information security that combines legislative reforms, specialized institutions, strategic communication capabilities, cybersecurity mechanisms, and international cooperation. The experience gained since 2014, reinforced by the full-scale invasion in 2022, has accelerated the development of an institutional model in which information security is treated as an essential component of national defense. Legislative reforms have expanded the state's capacity to respond to information threats, while institutions such as the National Security and Defense Council, the Center for Countering Disinformation, the

Security Service of Ukraine, and the National Cybersecurity Coordination Center operate within a coordinated governance framework. These institutional arrangements are complemented by advanced monitoring technologies, strategic communication policies, cooperation with civil society, and extensive partnerships with the European Union and NATO (Bjola & Papadakis, 2020; OECD, 2023).

By comparison, the Republic of Moldova has pursued a gradual process of institutional adaptation focused on strengthening democratic resilience while preserving constitutional guarantees concerning freedom of expression. Moldovan authorities have adopted legislative measures addressing disinformation, enhanced the responsibilities of media regulatory bodies, established specialized institutions such as the Centre for Strategic Communication and Countering Disinformation, and expanded cooperation with European partners. Nevertheless, the country's institutional architecture remains in a process of consolidation and faces structural challenges related to limited administrative capacity, resource constraints, political polarization, and the continued influence of external information actors. Consequently, Moldova's approach has generally emphasized preventive measures, media literacy, institutional coordination, and regulatory reforms rather than the exceptional wartime measures observed in Ukraine.

Despite these differences, the comparative analysis identifies several common elements that characterize effective information resilience in both countries. First, information security has increasingly become integrated into broader national security strategies, reflecting the recognition that contemporary conflicts extend beyond conventional military domains into the cognitive and digital spheres. Second, both states acknowledge that effective responses to disinformation require cooperation among governmental institutions, independent media, civil society organizations, academia, and international partners. Third, strategic communication, public trust in state institutions, and media literacy have emerged as fundamental components of long-term societal resilience, complementing legal and technological measures. Finally, cooperation with the European Union, NATO, and other international organizations has significantly contributed to institutional modernization, legislative harmonization, and the development of professional expertise in both countries.

The comparison also illustrates that resilience against information threats cannot be achieved solely through restrictive legislation or technological capabilities. Sustainable resilience depends equally on transparent governance, institutional credibility, democratic accountability, and an informed public capable of critically evaluating information. While Ukraine demonstrates the effectiveness of rapid institutional mobilization under conditions of armed conflict, Moldova provides an example of resilience-building within a democratic framework that prioritizes institutional reform and European integration. Together, these experiences suggest that successful information governance requires a balanced combination of legal regulation, institutional coordination, public communication, international cooperation, and respect for democratic principles.

CONCLUSIONS

The information environment has become a strategic domain of contemporary security, where state and non-state actors increasingly employ disinformation, psychological operations, cyberattacks, and digital influence campaigns to achieve political and military objectives. Consequently, protecting the integrity of the information

space is no longer limited to safeguarding freedom of expression or regulating media activities but has become an essential component of national resilience and comprehensive security policy.

This study demonstrates that both the Republic of Moldova and Ukraine have recognized the strategic importance of information security and have progressively developed institutional and legal mechanisms aimed at countering hybrid threats. Nevertheless, the comparative analysis reveals substantial differences in the scale, pace, and maturity of their responses. Ukraine's prolonged experience with Russian hybrid aggression has accelerated the creation of an integrated system that combines legislative regulation, specialized institutions, strategic communication, cybersecurity, intelligence cooperation, and international partnerships. In contrast, Moldova has focused on strengthening democratic institutions, improving regulatory frameworks, enhancing media literacy, and gradually consolidating institutional capacities while maintaining closer alignment with European standards governing fundamental rights and media pluralism.

The research further indicates that institutional effectiveness depends not only on the existence of specialized authorities but also on the quality of coordination among governmental agencies, independent regulators, civil society organizations, academic institutions, and international partners. Information resilience should therefore be understood as a multidimensional concept encompassing legal preparedness, institutional cooperation, technological capabilities, strategic communication, public trust, and civic education. No single institution can effectively counter contemporary information threats independently; rather, resilience emerges through integrated governance and continuous collaboration across sectors.

Another important finding concerns the growing interdependence between national and international approaches to information security. The experiences of both Ukraine and the Republic of Moldova demonstrate that cooperation with the European Union, NATO, the Council of Europe, and other international organizations has become indispensable for strengthening institutional capacities, harmonizing legislation, improving cybersecurity, and developing common approaches to countering foreign information manipulation. Hybrid threats increasingly transcend national borders, making international cooperation a prerequisite for effective resilience.

At the same time, the study highlights the importance of preserving democratic principles while implementing measures against disinformation. Expanding governmental authority over information flows may enhance national security during periods of crisis; however, such measures should remain proportionate, transparent, legally supervised, and consistent with international human rights standards. Long-term resilience ultimately depends not only on the ability to counter hostile narratives but also on maintaining public confidence in democratic institutions and safeguarding fundamental freedoms.

Finally, the comparative experiences of the Republic of Moldova and Ukraine demonstrate that information resilience is a dynamic process rather than a fixed institutional achievement. As technologies evolve and information threats become increasingly sophisticated, institutional policies must continuously adapt to emerging challenges while preserving democratic legitimacy. Future developments in artificial intelligence, digital platforms, and transnational information ecosystems will require even closer cooperation between governments, international organizations, researchers, technology companies, and civil society. In this context, the experiences of Moldova and

Ukraine provide valuable lessons for other democratic states seeking to strengthen their resilience against hybrid threats while protecting the openness and pluralism that constitute the foundation of democratic governance.

Furthermore, the response capacities of both Moldova and Ukraine reflect different levels of institutional maturity and practical experience, while sharing a common objective: protecting the information space and strengthening societal resilience. The lessons learned from Ukraine's experience, together with the support of international partners, can significantly accelerate the development of information security capacities in the Republic of Moldova within a regional environment characterized by persistent information threats.

BIBLIOGRAPHY

- Buzan, B. (1983). *People, States and Fear: The National Security Problem in International Relations*. Brighton: Wheatsheaf Books.
- Bjola, C., & Papadakis, K. (2020). *Digital propaganda, counter-disinformation and democracy*. Routledge.
- Bucătaru, I. (2016). Atacurile cibernetice și metodele de contracarare a lor la nivel național. În: *Teoria și practica administrării publice. Materiale ale conferinței științifico-practice cu participare internațională*. Chișinău: AAP, p. 509–510.
- Center for Countering Disinformation. (2024). Official website.
- Centre for Strategic Communication and Information Security. (2024). Official website.
- Council of Europe. (2023). *Opinion on the Law on Media of Ukraine*. Strasbourg: Council of Europe.
- Craig, A., & Valeriano, B. (2018). *Realism and Cyber Conflict: Security in the Digital Age*. E-International Relations, p. 1–5.
- European Commission. (2023). *Republic of Moldova 2023 Report*.
- European Commission. (2024). *Republic of Moldova Report 2024*. Brussels: European Commission.
- European External Action Service. (2024). *EUvsDisinfo: Countering pro-Kremlin disinformation*.
- European Union Agency for Cybersecurity. (2023). *ENISA Threat Landscape 2023*. Luxembourg: Publications Office of the European Union.
- Galeotti, M. (2019). *Russian Political War: Moving Beyond the Hybrid*.
- Giles, K. (2016). *Handbook of Russian information warfare*. NATO Defense College.
- Helmus, T. C., Bodine-Baron, E., Radin, A., Magnuson, M., Mendelsohn, J., Marcellino, W., Bega, A., & Winkelman, Z. (2018). *Russian social media influence: Understanding Russian propaganda in Eastern Europe*. RAND Corporation.
- Hotărâre nr. 1028 din 21-12-2023 cu privire la constituirea, organizarea și funcționarea Agenției pentru Securitate Cibernetică. Monitorul Oficial.
- Hotărâre nr. 319 din 26-12-2024 pentru aprobarea Strategiei naționale de apărare a Republicii Moldova pentru anii 2024–2034. Monitorul Oficial.
- Hotărâre nr. 333 din 08-05-2024 cu privire la instituirea, organizarea și funcționarea Consiliului coordonator în domeniul securității cibernetice. Monitorul Oficial.
- Hotărâre nr. HP391 din 15.12.2023 privind aprobarea Strategiei securității naționale a Republicii Moldova. Monitorul Oficial.

- Hotărâre din 2025 cu privire la aprobarea Programului național de securitate cibernetică pentru anii 2026–2030. Guvernul Republicii Moldova.
- Hotărâre din 2025 cu privire la aprobarea Strategiei militare a Republicii Moldova pentru anii 2025–2035. Guvernul Republicii Moldova.
- Isnarti, R. (2016). A Comparison of Neorealism, Liberalism, and Constructivism in Analysing Cyber War. *Andalas Journal of International Studies*, p. 157–158.
- Lege nr. 48 din 16-03-2023 privind securitatea cibernetică. Monitorul Oficial.
- Lege nr. 136 din 08-06-2023 privind Serviciul de Informații și Securitate al Republicii Moldova. Monitorul Oficial.
- Lege nr. 179 din 07-07-2023 privind activitatea contrainformativă și activitatea informativă externă. Monitorul Oficial.
- Lege nr. 242 din 31-07-2023 privind Centrul pentru Comunicare Strategică și Contracarare a Dezinformării și privind modificarea unor acte normative. Monitorul Oficial.
- Lege nr. 299 din 21-12-2017 privind aprobarea Concepției securității informaționale a Republicii Moldova. Monitorul Oficial.
- Libicki, M. C. (2009). *Cyberdeterrence and cyberwar*. RAND Corporation.
- Marushchak, A., Petrov, S., & Khoperiya, A. (2025). Countering AI-powered disinformation through national regulation: Learning from the case of Ukraine. *Frontiers in Artificial Intelligence*.
- Ministry of Culture and Strategic Communications of Ukraine. (2024). Official website.
- National Security and Defense Council of Ukraine. (2024). Official website.
- NATO. (2024). NATO support for Ukraine in strengthening resilience against hybrid threats.
- NATO. (2024). Relations with Ukraine.
- NATO Strategic Communications Centre of Excellence. (2023). *Countering disinformation: Improving institutional resilience*. Riga.
- OECD. (2023). *Disinformation and Russia's war of aggression against Ukraine*. OECD Publishing.
- OSCE. (2023). *Ukraine's media environment under martial law*. Organization for Security and Co-operation in Europe.
- Paul, C., & Matthews, M. (2016). *The Russian "firehose of falsehood" propaganda model*. RAND Corporation.
- Pomerantsev, P. (2019). *This is not propaganda: Adventures in the war against reality*. PublicAffairs.
- President of Ukraine. (2022a). Decree No. 64/2022 on the introduction of martial law in Ukraine.
- President of Ukraine. (2022b). Decree No. 152/2022 on the implementation of the decision of the National Security and Defense Council concerning the unified information policy under martial law.
- Security Service of Ukraine. (2024). Official website.
- Singer, P. W., & Brooking, E. (2018). [referință în text despre războiul informațional și tehnologiile digitale].
- Tyshchuk, V. (2024). Main Criteria for the Classification of Disinformation and Attempts to Criminalisation of Its Spread in Ukraine. *Bratislava Law Review*, 8(1), 203–224.
- Verkhovna Rada of Ukraine. (2022a). Law No. 2178-IX...
- Verkhovna Rada of Ukraine. (2022b). Law of Ukraine No. 2849-IX On Media.
- Vevera, A. V., & Udroi, A. M. (2018). Analiza costurilor unui atac cibernetic. *Revista Română de Informatică și Automatică*, p. 8.

- Walker, B., Holling, C.S., Carpenter, S.R., et al. (2004). Resilience, Adaptability and Transformability in Social-Ecological Systems. *Ecology and Society*, 9, 5–12.
- Wardle, C., & Derakhshan, H. (2017). Information Disorder: Toward an Interdisciplinary Framework for Research and Policymaking. Council of Europe. <https://rm.coe.int/information-disorder-report-november-2017/1680764666>
- Wolfers, A. (1952). “National security” as an ambiguous symbol. *Political Science Quarterly*, p. 483–492.