CZU: 351.86:004.056.5:659.3/.4(478:479.24) https://doi.org/10.59295/pas2025v2.04

INTERFERENCES BETWEEN CYBERSECURITY AND DISINFORMATION: PERSPECTIVES ON VULNERABILITIES IN THE REPUBLIC OF MOLDOVA AND AZERBAIJAN

Diana HIRBU[6]

Rasul BAKHSHALIYEV[7]

Abstract. ***The article examines the relationship between cybersecurity and disinformation within the Republic of Moldova and Azerbaijan, focusing on the ways digital attacks and the manipulation of information work in concert within a hybrid framework of threats to national stability. This paper demonstrates that the vulnerabilities faced by the two countries are based on the consolidation of state institutions, external geopolitical pressures, media polarization, and low digital literacy.***

In each scenario, cyberattacks are either preceded or combined with disinformation campaigns intended to erode public trust and the legitimacy of state institutions. They call for an integrated strategic approach grounded in interinstitutional cooperation, the implementation of international standards, digital education, and international partnerships with the European Union and NATO. The core conclusion is that digital and societal security are interdependent, and that sustainable cyber resilience can only be gained by integrating the technical, educational, and institutional dimensions of modern defense.

Keywords: *cybersecurity, disinformation, Republic of Moldova, Azerbaijan, hybrid threats, national stability, digital attacks, information manipulation, vulnerabilities.*[8]

Theoretical and Conceptual Landmarks of Cybersecurity and Disinformation

Globalization, digitalization, and the interconnection of technological systems at the international level have generated not only economic benefits but also new forms of security vulnerabilities. In this context, states and international organizations have been compelled to redefine traditional security paradigms to include the cyber dimension as well (Nye, 2017: 45).

Cybersecurity is a complex, multidimensional, and continuously evolving concept. It integrates technical, legal, political, social, and cultural aspects. From this perspective, a theoretical and conceptual approach is indispensable for understanding the mechanisms that govern the security of cyberspace and for developing effective public policies (Bendiek, Porter 2013: 12). It is a collection of policies, technical mechanisms, and legal arrangements designed at a theoretical level to safeguard information systems and the

[6] PhD., associate professor, Moldova State University, Republic of Moldova, Faculty of International Relations, political and Administrative Sciences

[7] PhD student, Moldova State University, Republic of Moldova

[8] The present article was developed within the institutional project "The Contribution of the EU and Romania to Civil Security in the Republic of Moldova: Policies, Strategic Partnerships, and the Consolidation of European Identity", implemented in accordance with code 25.80013.0807.46ROMD

data that is processed in the digital environment. However, recent studies indicate that cybersecurity also emerges as a social process which needs to be combined with security culture and digital education in a fundamental sense (Rotaru, Țăranu 2020: 34). The word "cybersecurity" started appearing in the 1990s, with the globalization of computer networks, but the meaning of cybersecurity has evolved from mere protection of data and IT systems. The cybersecurity process is a way of dealing with the risks that exist in the digital world by striking a balance between freedom, control, and protection (Dunn, Cavelty 2008: 4).

Cybersecurity is increasingly becoming a cross-cutting issue in public governance—affecting defense, digital economy, education, and data protection. It is the policy of translating conceptual frameworks into operational mechanisms and is now perceived even more as a part of nation building — an issue of national power. States are establishing national cybersecurity strategies and institutions or digital resilience agencies. Conflicts in cyberspace — which are frequently anonymous — have become tools of geopolitical influence (Rid, 2020: 55).

In the Republic of Moldova, the National Cybersecurity Strategy promotes institutional capacity strengthening, the enhancement of public–private cooperation, development of digital competencies, and security of critical infrastructures (Bulearca, 2020: 57). The earliest academic works referencing cybersecurity appeared after 2014, when cyberattacks on public institutions and discussions around European integration were intensifying. According to the expert V. Balan cybersecurity constitutes an integral part of national security, safeguarding critical infrastructures, information flows and personal data (Balan, 2018: 52).

For scientists from Azerbaijan, cybersecurity involves both strategic and societal aspects, in the specific area of protection of informational sovereignty, critical infrastructures and the online environment from hybrid threats (Hasanov, 2021: 72). Here, the focus is on developing a conceptual model which achieves a balance between innovation, freedom and digital security.

The theoretical and conceptual basis of cybersecurity in Azerbaijan shows an integrative direction, that integrates technological, legal and societal dimensions in order to a national digital governance model. The research in the Azerbaijani perspective contributes to the development of a new knowledge on the development of Eurasia's information security model with its focus on strategic autonomy, international cooperation and resilience. In the academia of Azerbaijan and the Republic of Moldova, cybersecurity is not only a system of technical measures but a series of interactions between the state, the private sector, society, in which resilience becomes a major indicator of stability.

As of now, cybersecurity and disinformation are at an intersection: disinformation can be supported up to the extent of cyberattacks (e.g. unauthorized access to data, leaks, digital manipulation of information, or defamation), for example, while cybersecurity must cope not just with data thefts, but also information compromise, destabilization of communication infrastructures, and shaping public opinion. Accordingly, cyber vulnerabilities can become targets for disinformation campaigns, while disinformation is able to increase cyber risks by weakening the public or institutional responses (Sánchez González et al., 2025).

According to Moldavian associate professor, Laura Tugarev, disinformation serves as a manipulative form of communication designed to distort reality and shape public perception using a variety of strategies. This view is intended to underscore both its intentional nature and strategic nature, linking "fake news" to a general media manipulation paradigm by weaving the term "fake news" into a much broader media manipulations context.

Moldavian expert Lilia Zaharia considers that disinformation is what she referred to as deliberate production and dissemination of false or misleading content that affects people socially and politically (Zaharia, 2023). She emphasizes society's role in disinformation, connecting the role to media literacy and citizens' susceptibility to crises.

In public policy studies in the Republic of Moldova, disinformation is considered as a type of hybrid threat and categorized according to the risk for the safety of society as a whole (Rusu, 2022). This focuses on the state's capacity to construct institutional responses and counteraction campaigns through strategic communication.

In Azerbaijan, disinformation is seen as being mostly framed in terms of national security and information conflicts. Analyses of the phenomenon by the Topchubashov Center define the phenomenon as a strategic instrument used by state and non-state actors to undermine social cohesion and manipulate international perceptions (Mammadov, 2023). The Center's work highlights the role of disinformation in discrediting politically active women and framing public discourse through appeals to emotion and cultural stereotypes in a report devoted to gendered disinformation (Mammadov, 2024).

Disinformation is perceived as a ubiquitous entity in the sphere of security, frequently incorporated into a continuum of hybrid warfare (Aliyev, 2022), the AIR Center (Center of Analysis of International Relations) further highlights. The analyses conducted by the institute discuss the persistence of disinformation campaigns directed against Azerbaijan, especially in relation to the Karabakh conflict, while focusing on the need for building institutional resilience and addressing cooperation with international parties to respond to the campaigns.

An examination of the scientific and analytical literature of the Republic of Moldova and Azerbaijan reports that the concept of disinformation moved from a media to a strategic and security perspective. Both schools in the country emphasize the deliberateness and coordinated nature of the phenomenon. Also, the concentration on media education in the Republic of Moldova, and the attention paid to information security in institutions in Azerbaijan are indicative of the cultural and institutional context in which these have been raised.

Disinformation is thought of as a weapon for influence and for disruption, and tackling it demands a holistic strategy that engages with technological analysis, media literacy and coherent public policies. Cyberattacks and disinformation overlap, providing a fragile environment under which digital and social security are deeply interconnected, for which an integrated strategic response based on international cooperation and the reinforcement of internal resilience is necessary. The interdependence can be attributed to the fact that cyberspace is no longer merely a technological realm but a social, political and economic ecosystem in which information became widespread and perception was weaponized (CyberPeace Institute, 2023).

Cyberattacks are not simply intended to compromise critical infrastructures or steal data, but are increasingly integrated with informational operations intended to sway public opinion, generate confusion, and undermine trust in democratic institutions (WEF, 2025). This process, commonly referred to as the "hybridization of threats," mixes technical measures (for example DDoS attacks or server compromises) with psychological ones (the dissemination of false narratives on social media) (UN, 2021).

In such a world, securing cybersecurity is inseparable from defending social cohesion. Digital vulnerability creates societal vulnerability: absence of access to legitimate information sources, algorithmic manipulation of website contents, and the exploitation of collective fear become powerful tools of internal destabilization (EU DisinfoLab, 2024).

Strengthening internal resilience, therefore, calls for investing in technology – firewalls, encryption, or instituting incident response centers – as well as education and culture – including digital literacy, critical thinking, and trust in independent media. At the international level, cooperation is laid out as a basic pillar. As cyberattacks and disinformation campaigns go beyond borders, states should cooperate through information sharing, regional incident response centers, and legislative harmonization of the protection of critical infrastructures (ENISA, 2024).

The European Union advocates for this comprehensive perspective under its European Cybersecurity Strategy, integrating both technology and society to form a new kind of "collective cyber resilience" (European Commission, 2023). Therefore, we should acknowledge the complex reality in the intersection of cyberattacks and disinformation: state defense in the 21st century is no longer confined to computer networks but extends to a defense of information and psychological health of its people. A good strategy demands that a balance be struck between digital and societal safety, around international cooperation and on enhancing internal trust, all of which will keep any democratic system from being vulnerable to hybrid aggressions.

The geostrategic context of the Republic of Moldova and Azerbaijan in the field of information security

The Republic of Moldova lies in the "near neighborhood" of the Russian Federation and experiences hybrid forms of pressure – disinformation, cyberattacks and electoral interference among them (OSCE, 2025). Meanwhile, cooperation with the European Union comprises the reinforcement of digital resilience and the fight against disinformation (European Commission 2025).

Azerbaijan is also situated in a strategically important area (the South Caucasus) and is placed at increased cyber and informational risks. The national cyber incident response agency (AZ-CERT) together with the local structures is intensifying their actions in the field of digital security (Bakunetwork, 2025). Disinformation, both internally and externally, is now identified as a key concern in information security (Trend.az, 2025).

Both countries demonstrate vulnerabilities as a result of their fragile geostrategic location, the development of digital infrastructures, informational polarization, and external influence (EAP-CSF, 2025). Nevertheless, the Republic of Moldova enjoys European assistance for the consolidation of democracy, whereas Azerbaijan has a more centralized security posture

Cyber Trends and Vulnerabilities in the Republic of Moldova and Azerbaijan

In the Republic of Moldova, enhancing the institutional and regulatory structure of cybersecurity is a necessary condition for safeguarding informational sovereignty and democratic stability (Balan, 2021: 88). This goal is also consistent with the increasing overlap between disinformation and cybersecurity, showing a set of linked weaknesses that threaten the stability of institutions and the trust of the public.

The electoral infrastructure is, above all, a regular casualty of cyberattacks. Government websites and digital systems relevant to the electoral process have been clogged with mass unauthorized login attempts and Distributed Denial of Service (DDoS) attacks, which aim to block access to government records and show confusion at crucial points in the electoral scenario. For example, media channels on TV and radio received more than 36 million fake requests in mere minutes (Moldova1, 2025). Meanwhile, OSCE reports attest to the presence of planned cyberattacks in the context of the 2025 parliamentary elections which have targeted government infrastructure and messaging infrastructure of electoral authorities (OSCE, 2025). Independent journalism of the press has also shown that these attacks were part of a general campaign to destabilize a society by hacker groups with external support (The Record, 2025). Such incidents not only interfere with the operations of the institutions but also erode citizens' views on security and transparency in electoral processes, based on findings by cybersecurity scholars (DFRLab, 2025). And, via automation of fake networks and creation of video content for the distribution by algorithms, similarly organized disinformation campaigns have been escalated. These tools are used to magnify anti-European themes and fragment society, contributing to an unstable informational environment (OSCE, 2025). Despite the ever-increasing assistance from the European Union, the resilience of the Republic of Moldova against these threats is still relatively weak. The most frequent causes are the media polarization, poor digital literacy and insufficiently implemented institutional resources to deal with the multifaceted phenomena (European Commission, 2025).

These actions are having specific consequences in cybersecurity. Disinformation, on the other hand, erodes public trust in state institutions and diverts resources that are meant to be dedicated to shielding vital infrastructures, forcing authorities to answer informational crises rather than strengthen technological protection (EAP-CSF, 2025).

As can be seen through the process of the strengthening of information security and the resilient response to hybrid attacks in Azerbaijan, a significant transformation has taken place. Yet, vulnerabilities remain, and new domains of synergies are both hindrances and opportunities to new technology. Here the process of digitalization has been associated with a gradual increase in information security risks with respect to the safeguarding of information infrastructures and sensitive data (Aliyev, 2020: 14).

The Azerbaijani government has made great strides in constructing institutional frameworks for digital protection and swift response to cyber incidents. Following the Decree No. 1315 of 17 April 2021, a joint commission was established between the State Security Service of Azerbaijan (SSS) and the Special Communication and Information Security State Service (SSSCIS) to inspect, investigate and enforce security protocols for critical infrastructure (BakuNetwork, 2025). Meanwhile, the Information and Cybersecurity Strategy of the Republic of Azerbaijan 2023–2027 includes the safeguarding of

critical infrastructures, reduction in dependence on foreign technology, development of digital literacy and the support of international cooperation (DigWatch, 2023).

These efforts reflect Azerbaijan's hopes of turning cybersecurity into an essential component of national security. Alternatively, Azerbaijan engages in disinformation campaigns within the framework of its information security strategy. Strategic disinformation—a hybrid tool comprising cyberwarfare, distortion of media and diplomatic leverage—is employed to sow discord within the region and to sully the state's international image (Trend.az, 2025). It is specifically stated in the national strategy that 'improving the security of the information space' and mitigating foreign propaganda are key goals (DigWatch, 2023). Consequently, Azerbaijan has to oversee not only its technology infrastructure but also its information infrastructure, which is saturated with social media campaigns and foreign influence.

The research indicates that Azerbaijan is a regional model among people when it comes to the relationship between the cyberattack and disinformation: during the Nagorno-Karabakh conflict, state information infrastructures were attacked by cyber-infiltration activities in concert with the circulation of disinformation in the region aimed at compromising Azerbaijan's authorities image (BakuNetwork, 2025). Part of the problem is not simply the infrastructure itself but the digital space — the media and national security are interdependent in a vicious cycle that amplifies the consequences of hybrid aggressions. Azerbaijan has increased cooperation with international organizations, primarily NATO, in the field of cyber defense. Recent discussions on creating cooperation in cybersecurity and exchange of expertise attest to Baku's openness to multilateral partnerships (Caliber.Az, 2024; NATO, 2025).

Meanwhile, Azerbaijan's public diplomacy also extends to training sessions and consultancy, held with NATO's Partnership for Peace (PfP) structures in support of combating disinformation and building a culture of digital safety (NATO-PfP, 2025). Azerbaijan is now in the process of maturing out its weak digital regime and has succeeded in becoming a more mature and integrated regime at the same time. Institutional capabilities are growing, the information strategy is becoming clearer and external cooperation is taking on more of a strategic aspect. But there are still weaknesses—not least where hybrid attacks can not only leverage technological vulnerabilities, but also informational and social gap vulnerabilities. The intersecting nature of these dimensions highlights the urgent requirement of a comprehensive strategy: not merely digital infrastructure but information education, digital literacy, and regional cooperation as defense strategies.

Common Elements of Interference: The Republic of Moldova and Azerbaijan

The Republic of Moldova and Azerbaijan share in a number of interrelated vulnerabilities and typical characteristics and profiles of hybrid interference: disinformation campaigns, cyber-invasive attacks, as well as spreading disinformation and other forms of disinformation, that in its interweaving undermine institutional and national coherence.

Disinformation Campaigns Preceding Cyberattacks. Both government offices and other media houses have been on the receiving end of a wave of cyber-attacks, ahead of the parliamentary elections in 2025, with massive disinformation campaigns. A similar

situation occurred in Azerbaijan, with media organizations being targeted in February 2025, together with information-sharing and misleading media narratives. Baku government blamed these efforts on externally backed hackers with the purpose of inciting internal disarray and undermining public institutions (The Record, 2025).

Vulnerabilities in institutions and legislation. Structural weaknesses limit the ability of the Azerbaijani and Moldovan governments to counter these attacks. They are more difficult or even impossible to do without. In the Republic of Moldova, for example, the Foreign Policy Research Institute makes clear that internal weaknesses—including a weak legislative response to disinformation and poor inter-institutional coordination—are entry points used by external actors (FPRI, 2024). In Azerbaijan (EUvsDisinfo, 2021) a lack of any real media regulation mechanisms creates an informational ecosystem ripe for manipulation and propaganda.

Information manipulation through social networks. The diffusion of disinformation in both countries relies heavily on social networks. At last, over 100 inauthentic TikTok accounts appeared in a pro-Kremlin campaign in the Republic of Moldova, where AP News revealed in a few weeks more than 13.9 million views (AP News, 2025). In Azerbaijan, both domestic and foreign groups use social networks to disseminate strategic news and shape perceptions about fighting in the Nagorno-Karabakh region. This includes the information war that unfolded in SA, as newly researched reports indicate that a "weaponization of social media"—that is, purposeful use of social media as tools of regional conflict destabilization—exists (Avetisyan, 2024).

Influence on national cohesion and the State legitimacy. In either case, informational interference affects direct effects on coherence of the internal community. In the Republic of Moldova, attacks on cyberbases and disinformation have disrupted public confidence in electoral institutions and aggravated social polarization and distrust in the process of elections as well as increased social division (OSCE, 2025). Media manipulation with regard to the Nagorno-Karabakh conflict has been employed in Azerbaijan to undermine state legitimacy and exploit ethnic and political frictions (Atlantic Council, 2024). Such phenomena generate a shared regional vulnerability through which digital and social stability are interlinked (FPRI, 2024). The Republic of Moldova and Azerbaijan are vulnerable due to several reasons: Institutions in consolidation. For example, the Republic of Moldova has only recently started developing strong cybersecurity frameworks. In 2023, it introduced the first cybersecurity law, while the private sector continues to experience the problem of in-house IT security employees (StartupMoldova, 2025; CSIS, 2024). This suggests weak institutional capacity which can be exploited by hybrid attacks on the country. In Azerbaijan, although the 2023–2027 Strategy foresees infrastructure development, initiatives still emphasize external dependencies and an inferior level of interinstitutional coordination (DigWatch, 2023).

Geostrategic competition and external pressures. Both are situated in politically sensitive areas, where the external sphere, whether cyber or informational, amplifies internal weaknesses. For instance, in the case of the Republic of Moldova, several reports reflect the worsening of cyberattacks after Russia's invasion of Ukraine, where damage has been done to critical government institutions and there is potentially the loss of the public belief in the state (CSIS 2024). Azerbaijan presents as an example how actors

may make use of local opportunities to use cyber or disinformation in the South Caucasus conflict (BakuNetwork, 2025).

Lack of digital literacy. In an evaluation of digital competence in Azerbaijan, despite a high proportion of Internet users, the digital skills of large population were minimal – only about 7% of respondents reported using digital creation tools or programs for computers (ITU, 2024). It is in the face of this that the population is susceptible to manipulation of knowledge or cyber attacks on human. The Republic of Moldova is in an analogous situation, characterized by extremely quickly digitalized systems and infrastructure, though significant digital education and user skill deficiencies (StartupMoldova, 2025).

Conclusions

The Republic of Moldova and Azerbaijan are both facing similar structural obstacles in addressing cyber and information security. They have also been subjected to mixed attacks of disinformation, information manipulation and acts of digital aggression, demonstrating that their weaknesses are not only due to the absence of sophisticated technical technology but also to poor institutions, media polarization, and the general absence of digital literacy.

Both countries will face significant institutional and cultural obstacles in building digital resilience. Their response to attack depends greatly on not only technology, but also the cooperation among institutions, level of trust in public and the level of education of the population. At the same time, there is a deficiency of legislative structures that conform their institutions with European and international principles and norms and that makes these countries susceptible to outside encroachment and geopolitical competition in the information domain.

On a positive note, progress towards regional unity and international co-operation is evident. Building joint training and cyber incident response programs between the EU and NATO is a major step towards mutual security networking. Creating a "culture of resilience" in terms of transparency, collaboration, and mutual trust. To enhance these relationships, national institutions, the private sector, and civil society need to be strengthened.

We should view the cybersecurity problems of the Republic of Moldova and Azerbaijan, however, not as purely an isolated case, but as part of a larger regional effort to address new types of hybrid conflict that the region needs to have as part of its response. A strong foundation for a robust cyber and information defense infrastructure is built on a combination of integrated policy, digital literacy, international cooperation, and strengthening of domestic institutions that has been developed. The key to tackling the challenges posed by the digital terrain is such integration, where technology matters most. And these must emerge only through integrated efforts where technology is a major factor if these countries would like to adapt.

BIBLIOGRAPHY

Aliyev, Kamran. "Cybersecurity Policy and Digital Sovereignty in Azerbaijan." *Caucasus Strategic Studies Review* 6, nr. 2 (2020): 10–18.

Aliyev, Kamran. "Information Warfare and National Security in Azerbaijan." *AIR Center Analytical Review*, Baku, 2022.

AP News. “Moldova’s Election Faces AI-Driven Disinformation from Russia.” *Associated Press*, 22 septembrie 2025. https://apnews.com/article/moldova-election-europe-disinformation-russia-461e9a1c9558ae140c5b7539a5c89fd4.

Atlantic Council. *Information Warfare in the South Caucasus and Moldova.* Washington, D.C.: Atlantic Council, 2024. https://www.atlanticcouncil.org/wp-content/uploads/2024/10/Information-warfare-in-the-South-Caucasus-and-Moldova.pdf.

Avetisyan, Tigran. “Information Warfare in the South Caucasus and Moldova.” *Journal of International Media and Emerging Law*, vol. 10, no. 2 (2024). https://www.swlaw.edu/sites/default/files/2024-12/Avetisyan%20Article%20-%20JIMEL%2010.2%20-%20%2012.09.pdf.

BakuNetwork. “Azerbaijan’s Digital Fortress: A New Era in Cybersecurity Begins.” *BakuNetwork*, 21 iulie 2025. https://www.bakunetwork.org/en/news/analytics/14194.

BakuNetwork. “Azerbaijan’s Digital Frontline: Anatomy of a Hybrid Cyber …” *BakuNetwork*, 6 septembrie 2025. https://www.bakunetwork.org/en/news/analytics/14413.

Bakunetwork. 2025. “Azerbaijan’s National Cybersecurity Initiatives.” *Baku Network*, 2025.

Balan, Viorel. “Transformări conceptuale în arhitectura securității informaționale naționale.” *Revista Administrarea Publică* 3, nr. 1 (2021): 85–93.

Balan, Viorel. *Securitatea informațională și cibernetică: provocări pentru Republica Moldova.* Chișinău: Tipografia Academiei de Administrare Publică, 2018.

Bendiek, Annegret, și Andreas Porter. *European Cybersecurity Policy: Towards a Secure Digital Environment*. Berlin: Stiftung Wissenschaft und Politik, 2013.

Bulearca, Marius. *Securitatea cibernetică în contextul guvernanței digitale*. București: Editura ASE, 2020.

CSIS (Center for Strategic and International Studies). “Strengthening Moldova’s Cyber Landscape.” 8 octombrie 2024. https://www.csis.org/analysis/strengthening-moldovas-cyber-landscape.

CyberPeace Institute. *The Nexus of Cyberattacks and Disinformation.* Geneva: CyberPeace Institute, 2023.

DFRLab (Digital Forensic Research Lab). *Risk Assessment: Moldova’s Electoral Environment in 2025*. Atlantic Council, 9 septembrie 2025. https://dfrlab.org/2025/09/09/risk-assessment-moldovas-electoral-environment-in-2025.

DigWatch. *The Strategy of the Republic of Azerbaijan on Information Security and Cybersecurity for 2023–2027.* Geneva Internet Platform, 2023. https://dig.watch/resource/the-strategy-of-the-republic-of-azerbaijan-on-information-security-and-cybersecurity-for-2023-2027.

EAP-CSF. 2025. “Hybrid Warfare and De-information: How Moldova Counters Russian Propaganda.” *Eastern Partnership Civil Society Forum*, 2 iulie 2025.

EU DisinfoLab. *Disinformation and Hybrid Threats in Eastern Europe.* Brussels: EU DisinfoLab, 2024.

European Commission. 2025. “EU and Moldova Enhance Digital Cooperation for Better Resilience.” *Press Release*, 14 iulie 2025.

European Commission. *EU Cybersecurity Strategy for the Digital Decade.* Brussels: European Union Publications Office, 2023.

EUvsDisinfo. “Disinformation and Information Manipulation in Azerbaijan.” *EUvsDisinfo*, 17 decembrie 2021. https://euvsdisinfo.eu/disinformation-and-information-manipulation-in-azerbaijan/.

FPRI (Foreign Policy Research Institute). *Russia’s Information War in Moldova.* Philadelphia: FPRI, 3 octombrie 2024. https://www.fpri.org/article/2024/10/russias-information-war-in-moldova/.

Hasanov, Elvin. “Technological Aspects of Cyber Defense in Azerbaijan.” *Journal of Information Security and Innovation* 3, nr. 1 (2021): 70–78.

ITU (International Telecommunication Union). *Azerbaijan Digital Skills Assessment.* 2024. https://www.itu.int/dms_pub/itu-d/opb/phcb/D-PHCB-CAP_BLD.05-2024-PDF-E.pdf.

Mammadov, Aysel. “Gendered Disinformation in Post-Conflict Societies.” *Topchubashov Center Working Papers*, nr. 12 (2024): 14–26.

Mammadov, Aysel. “Strategic Disinformation and Hybrid Influence in the South Caucasus.” *Topchubashov Center Policy Briefs*, Baku, 2023.

Ministerul Economiei al Republicii Moldova. Strategia Națională de Securitate Cibernetică 2023–2027. Chișinău, 2023.

Moldova1. „Atacuri cibernetice masive asupra site-urilor publice în timpul campaniei electorale.” *Moldova1.md*, 28 septembrie 2025. https://moldova1.md/p/58335.

NATO. 2025. “Azerbaijan and NATO Deepen Cooperation in Cyber Defence.” *NATO Newsroom*, 2025.

NATO-PfP Azerbaijan. “Public Diplomacy.” *NATO Partnership for Peace (PfP) Azerbaijan Portal*, accesat 2025. https://nato-pfp.mfa.gov.az/en/category/public-diplomacy.

Nye, Joseph S. Power in the Cyber Age: From Realism to Complex Interdependence. Oxford: Oxford University Press, 2017.

OSCE (Organization for Security and Co-operation in Europe). *Republic of Moldova – Parliamentary Elections, 28 September 2025: Statement of Preliminary Findings and Conclusions.* OSCE/ODIHR and OSCE PA, 30 septembrie 2025. https://www.osce.org/odihr/598219.

OSCE Secretariat. “Experts and policymakers from Moldova and Ukraine strengthen co-operation in cyber/ICT security at OSCE workshop.” 20 octombrie 2025. https://www.osce.org/secretariat/599921.

Rotaru, Ioan; Andrei Țăranu. *Securitatea cibernetică și societatea informațională*. București: Editura Tritonic, 2020.

Rusu, Mariana. “Dezinformarea ca amenințare hibridă la adresa securității societale.” *Revista de Politici Publice și Securitate*, vol. 5, nr. 2 (2022): 45–58.

Sánchez González, F., Pastor-Galindo, J., & Ruipérez-Valiente, J. A. 2025.) “Toward Interoperable Representation and Sharing of Disinformation Incidents in Cyber Threat Intelligence.” *ArXiv preprint*.

StartupMoldova. “Moldova Grows Its Firewalls and Shows that Cybersecurity is Easy.” 2025. https://www.startupmoldova.digital/moldova-grows-its-firewalls-and-shows-that-cybersecurity-is-easy.

The Record. “Azerbaijan Blames Russian State Hackers for Media Cyberattacks.” *The Record by Recorded Future News*, 5 mai 2025. https://therecord.media/azerbaijan-blames-media-cyberattacks-russia-apt29.

Trend.az. 2025. “Azerbaijan Accents Game-Changing Role of De-information Fight.” *Trend.az*, 30 septembrie 2025.

Tugarev, Laura. *Manual de educație media și gândire critică.* Chișinău: Universitatea de Stat din Moldova, 2021.

United Nations. *The Age of Digital Interdependence: Report of the High-Level Panel on Digital Cooperation.* New York: United Nations, 2021.

Zaharia, Lilia. “Dezinformarea în Republica Moldova: provocări și soluții educaționale.” *Pro-Fact Moldova Reports*, Chișinău, 2023.