CZU: 342.841:004.056.5:351.86 https://doi.org/10.59295/pas2025v2.02

ELECTORAL SECURITY IN THE DIGITAL ERA

Marcel BENCHECI[2]

Vitalii PIRGARI[3]

Abstract. ***The article examines the impact of modern technologies on electoral processes and the importance of securing information communication in the context of contemporary cyber and informational threats. Through an interdisciplinary analysis, the study highlights the opportunities offered by digitalization – including electronic voting, block chain, and artificial intelligence – alongside the major vulnerabilities generated by cyberattacks, disinformation campaigns, and unauthorized access to data. The paper integrates relevant international examples and proposes a set of strategic measures to strengthen electoral security, including resilient cyber infrastructure, digital literacy for citizens, and international cooperation.***

Keywords: *electoral processes, disinformation campaigns, cyber threats, cyberattacks, cyber resilience, electoral security* [4].

The electoral process is the building block of any democracy, and the legitimacy of state institutions depends on citizens' faith in the fairness and transparency of elections. In this time of digitalization, when information technologies saturate every aspect of social life — including electoral systems — the security of informational communication has become not only a technical requirement but also a strategic issue of national security. Risks to election outcomes and political stability/social cohesion of the state are also generated due to the vulnerabilities of digital systems and the exposure of the information space to manipulation and disinformation campaigns (Howard, Ganesh, and Liotsiou, 2018).

The rapid digitalization of electoral systems has yielded clear advantages—administrative efficiencies, easier access to voters and heightened transparency of operations—but has come with greater exposure to cyber and informational risks (Bada and Nurse, 2019). The key point of the current article is to strike the right balance between technological evolution and the safeguard of informational communications in an effort to achieve the integrity of the electoral process and institutional resilience.

For one thing, modern technologies — electronic voting, digital voter registries, block chain, artificial intelligence — offer efficiency, transparency, and increased access to citizens. On the other hand, they offer an array of potential threats: cyberattacks on critical infrastructure, private information exposure, opaque micro-targeting of voters, and algorithmic manipulation over social networks (Shao et al., 2018). Furthermore,

[2] Doctor of Political Science, Senior Researcher, Institute of Legal, Political and Sociological Research, State University of Moldova, Republic of Moldova

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

[4] The article was developed within the framework of the research project *"The National Security of the Republic of Moldova in the Context of Accession to the European Union: Legal, Political, and Sociological Approaches"*, sub-program code 010501.

hostile state and non-state actors increasingly use hybrid threats — integrating technical strikes and informational campaigns — to change electoral results and delegitimize democratic institutions (Bradshaw and Howard 2019). An aspect of this issue matters because the electoral process is of two dimensions to its own right, being an internal democratic exercise and a component of national critical infrastructure with external and geopolitical implications.

Recent experiences in the Euro-Atlantic region show that outside interference in elections—like the U.S. elections in 2016, Brexit in 2016, and the EU elections in 2019—doesn't just aim to sway voter choices; it also seeks to erode trust in our democratic processes as a whole (Tucker et al., 2018). Once that trust is broken, it's incredibly difficult to rebuild, even when elections are conducted fairly on the surface.

Modern Technologies in Electoral Processes

The deep transformations associated with digitalization have altered not only how people exercise their right to vote but the very architecture of security for democracies as well. Up to now, elections were almost completely dependent on conventional devices — paper ballots, manual registers, and simple logistical procedures — while we are now experiencing a deepening interdependence between the mechanics of elections and IT systems.

Specialized literature underlines that, even though such innovations increase efficiency and accessibility, at the same time they create a variety of vulnerabilities that bring elections to a true target for cyber and informational attacks (Springall et al., 2014; Garnett, 2020). A good example is the electronic voter registries as a mandatory innovation to simplify the electoral system and lower "multiple voting" fraud. In reality, those systems have been extraordinarily effective instruments, and potentially vulnerable targets. The illicit access attempts to electoral databases in US electoral databases reported during 2016 showed that the security of an election didn't necessarily come from direct manipulation of votes, but from having the public perceive the integrity of the voter lists compromised (Mueller, 2019).

Likewise, electronic voting — and, in particular, remote internet voting — is arguably the most controversial innovation. Estonia, a pioneer of i-Voting, has shown that such a system can function on a national scale; however, many independent reports have pointed out its risks. The issue of architectural vulnerabilities, the possibility of malware infection on voters' devices, and interception of data flows are serious threats to the confidentiality and integrity of the vote (Springall et al. 2014). And therein arises one of the major dilemmas of digitalization: increasing accessibility for the diaspora and persons with limited mobility versus the risk that the secrecy of the vote may be compromised.

A further discussed technology is block chain, viewed as an option to guarantee the traceability and immutability of votes. In theory, if the votes are recorded, then there is no possibility to change them, resulting in a lot of security and an aura of transparency. Pilot studies, however, demonstrate that promising as it is, this tech is fraught with scalability and cost problems, while the initial verification step remains vulnerable (Ayed, 2017). On the one hand, the instruments, artificial intelligence (AI) and Big Data deserve legitimate use by institutions to detect anomalous trends, address fraud or optimize logistics.

Conversely, they are used by private, partisan and hostile organizations to micro-target and manipulate electoral preferences, usually in an opaque fashion without democratic oversight. The Brookings Report (2022) points out those abuses of data and algorithms can polarize society, create social polarization and limit opportunities for competitors. Further, the deep fake phenomenon adds another layer of information manipulation — and an even harder one to solve even with experts (Chesney and Citron, 2019).

Even the official mobile applications and web-based platforms on which we depend to facilitate citizens' access to information about polling stations or voting rules aren't without their risks. However, the cloning of such applications is relatively simple and counterfeit versions can be shared rapidly across social networks or obscure websites, which may leave citizens with vulnerabilities to personal data theft (Norris and Grömping, 2019). In settings with uneven levels of digital literacy, like many Eastern European countries, such risks are much greater. Finally, new trends like biometrics for voter authentication, the cloud technology that consolidates results and centralizes all electoral data or the use of IoT in electoral coordination create new points of view – but new sites of attack as well.

The reliance on private international suppliers creates questions of digital sovereignty, turning electoral security into a geopolitical concern (DeNardis, 2020). A careful examination of such developments makes evident that today's tools, rather than being global remedies, are the very instruments of two sides: They aid democracy in improving security with transparency and efficiency, but undercut and expand it through opening up new vectors for attack. Hence, if the integration of these new mechanisms must be accompanied by technical, procedural, and legal safeguards and their assessment cannot be reduced to a cost-benefit analysis, but must be positioned in terms of institutional resilience and national security.

Risks and Threats to Electoral Security

While modern technologies present opportunities for efficiencies and transparency, they also create a range of threats that can be exploited by domestic or foreign actors. The electoral process—known in many states as national critical infrastructure—is now vulnerable to risks that extend beyond traditional fraud and that involve both the cyber and informational domains (Norris and Grömping, 2019). These threats are transnational and render electoral security no longer a purely domestic issue but rather one of global democratic resilience (DeNardis, 2020).

One of the most serious threats comes in the form of cyberattacks on electoral infrastructure. International instances in which servers operating official websites, voter databases, or result transmission systems are targeted include ongoing threats such as denial-of-service attacks, intrusions, or ransomware (Bada and Nurse, 2019). And even where the integrity of the vote is intact, the mere disruption of the functionality of the system is enough to fuel voter mistrust. As in a democratic context, public trust is the cornerstone of legitimacy, such attacks and their psychological effects could be just as destabilizing to societies as a compromise of votes (Mueller, 2019).

Another key area of risk is informational manipulation. In the era of social networks, disinformation campaigns have developed into sophisticated tools for shaping

public attitudes with complex techniques. No longer are they random false news items but carefully constructed narratives; they are the product of algorithms, propagated by algorithms and increasingly crafted with the aid of artificial intelligence (Bradshaw and Howard, 2019).

The new-age phenomenon of the deep fake is also adding to the likelihood that voters will be exposed to visual or audio material that is indistinguishable from reality, potentially eroding civic discernment. Recent research indicates that such tactics are not effective because they persuade, but because they induce confusion and erode collective trust (Brookings, 2022; Chesney and Citron, 2019). Just as troubling is the issue of unauthorized access to voters' personal data. In many countries, electoral registers contain sensitive information that, once infiltrated, can be used not only for electoral fraud but also to support political micro-targeting campaigns (Garnett, 2020).

Many electoral institutions lack the technical infrastructure or resources required in the modern threat environment for a high-tech standard of security. A breach in this area not only undermines public trust in democratic institutions, but also provides yet another powerful instrument for electoral influence that is hard to rein in.

Nor should internal vulnerabilities be ignored. Insufficient training of electoral staff, human errors, and at times even institutional corruption can turn an isolated cyber threat into a widespread crisis. This is also supported by research that emphasizes that electoral security is inextricably linked to not only technology but also the preparedness and accountability of the people who manage the electoral process (Norris and Grömping, 2019). Without clear protocols and an organizational culture centered on security, even advanced systems can be compromised.

A specific dimension is manifested in hybrid threats. These involve cyberattacks, propaganda, and disinformation operations, turning the electoral process into a complex battlefield in which the distinction between informational and cyber warfare has become increasingly blurred (Rid and Buchanan, 2015). An example of external interference in election processes of states such as the United States (2016) and the European Union (2019) is that the ultimate motive is not to influence the result of the election but to discredit the process as a whole (Mueller, 2019). Under this logic, the mere suspicion of an election being manipulated is enough to cause political and social unrest. An exploration of these dangers makes clear that the issue of electoral security has to be examined alongside national security.

Attacks on the electoral process have a direct impact on political stability, social cohesion, and international credibility of the state (DeNardis, 2020). They reduce the democratic election to a vulnerable node in the state's system, which can also be manipulated by malicious actors for geopolitical gain. In such a view, protecting the sanctity of electoral mechanisms is not only a matter of good governance but equally an important element to defend national defense.

Informational Communication and the Dimension of National Security

While contemporary technological solutions influence the technical infrastructure of elections, information communication serves as the symbolic and cognitive locus in which their outcomes are confirmed or contested. Electoral processes are not only con-

cerned with the mechanics of voting, they are linked with information flows that shape collective perception and thus, democratic legitimacy (Norris and Grömping, 2019). In an age of digital society in which social media platforms have become the main source of news for millions of people, it is crucial to have control and security over informational flows as part of the strategy of every state (Bradshaw and Howard, 2019).

The official communication of electoral organizations must be one of the primary sources of increasing public trust. Transparent, swift, and clear messages are sine qua non prerequisites for the electorate to trust in the fairness and adequate running of the proceedings. Lags in communication of results, incoherence, or no clarity can also provide fertile ground for speculation and conspiracy theories. In such a context, even the most minor incident of a small scale can be amplified and exploited by hostile actors to undermine the credibility of the electoral process (OSCE, 2020).

However, manipulated communication, in the form of disinformation and propaganda campaigns, is a direct threat to national security. While cyberattacks are capable of being neutralized with technical measures, informational manipulation operates subtly, penetrating the cognitive and emotional space of voters. It is a problem so pervasive that misinformation in the media can seriously undermine political integrity of a society and the political process.

False narratives, fabricated news, fake social media accounts, and more recently, deep fake content are all tools that are not designed to persuade but to create uncertainty, confusion and, ultimately, social polarization (Chesney and Citron, 2019). According to research carried out by OSCE and the European Union, this erosion of collective trust also has lasting impacts and is far more difficult to restore than after a one-time cyberattack (European Commission, 2018).

In this environment, independent media and fact-checking institutions are indispensable agents in democratic security. They act as an incisive lens between state institutions and ordinary people, verifying or falsifying information circulating in the public sphere. But to varying extents, the success of such mechanisms is a function of population digital literacy (Guess, Nyhan, and Reifler, 2020). Without careful media education, even very advanced fact-checking systems can fall further into the mainstream of manipulative content. A crucial factor also is institutional coordination. Electoral security cannot be an exclusive concern of electoral commissions — it also needs to involve security services, communication regulatory authorities, and partnerships with global digital platforms. Without cooperation among these entities (effective cooperation can be hard to achieve), the state's response is fragmented and inconsistent. Thus, it is shown in the experience of the European Union that, while the EU has established rapid alert mechanisms and codes of good practice in combatting disinformation, only by creating a coordinated multi actor response can any one incident be prevented from turning into a national crisis (European Commission 2018). Informational attacks are not only about changing the mechanics of the democratic process — they are about undermining institutional legitimacy and fracturing society as such, and are intended to damage institutional legitimacy, as well as break-up social cohesion. A state where citizens are not sufficiently confident that elections are fair is a state of fragility, vulnerable not just to internal turmoil, but also to external pressure. Therefore, in this view, informational

communication is not only an incidental point of electoral security but also a cornerstone of national resilience (DeNardis 2020).

Measures to Strengthen Electoral Security

An investigation of the risks and weaknesses shows that safeguarding the electoral system cannot be achieved through a single means – *technological or written legislation*, but a complex and synergistic strategy that integrates the technical, institutional and societal aspects (Garnett, 2020). When not part of a broader vision, even the most advanced solutions can be fragile and democratic legitimacy can be contested. The technical one is that we also should build a more resilient cyber infrastructure which can help to detect and react to attack attempts in real time. Those having done it before have shown us that infrastructural redundancy, constant scrutiny, and the red teaming exercises are very essential techniques to avoid major instabilities (ENISA, 2020). Moreover, the advanced encryption of data flows and the use of multifactor authentication for access to electoral IT systems should be required not considered as an option, but as a minimum standard (OSCE, 2020).

The institutional aspect is a key determinant, not merely technology. Electoral security necessitates coordination among a mix of institutional organizations in state: electoral commissions, cybersecurity, intelligence and communication agencies. The European Union has found that strong alert systems and best practice sharing among states can indeed contribute to response capabilities (European Commission, 2018). Without such coordination, technical vulnerabilities can be exacerbated by scattered decision-making, transforming a single hack into a widespread political crisis.

The dimension of society is as important as the technological one. In an information environment thick with propaganda and disinformation, the citizen remains the most vulnerable link. Therefore, digital education and media literacy programs become an integral part of national security (Guess, Nyhan, and Reifler, 2020). Strengthening the resilience of society by building awareness about the phenomenon and using open knowledge of factual references and by cooperating the state, media and NGOs is needed to counter the manipulation of opinion (Bradshaw and Howard, 2019). Simultaneously, electoral staff should be trained constantly, as human error or institutional neglect can make even the most secure technological systems susceptible (Norris and Grömping, 2019).

Another key dimension is international cooperation. Cyberattacks and disinformation efforts do not recognize national borders. And thus joining regional and global cooperation networks (ENISA, OSCE, NATO) is not a formal solidarity endeavor but a strategic necessity. The exchange of indicators of compromise, the organization of joint exercises, and alignment with international security standards enhance collective resilience and deter hostile actors (NATO, 2021).

The legal framework should finally reflect the current complexity of electoral processes. The clear regulation of elections as part of critical infrastructure, the definition of institutional responsibilities, as well as the introduction of severe penalties for actors involved in cyberattacks or disinformation campaigns are fundamental keys to democratic security (Bada and Nurse, 2019). An efficient regulatory framework, with strong enforcement, would signal to constituents that the electoral process is protected at the highest level. Combined, these actions show that electoral security cannot merely be viewed as a technological exercise: it emerges as an integrated national strategy in which

state, society and the international community has shared complementary responsibilities (DeNardis, 2020). Only in this way can elections remain what they really are: the true expression of the people's will, the bedrock of political stability and the guarantee of the continuity of the rule of law.

Comparative Study (International Examples)

As an international experience shows, the digitalization of electoral processes does not take the shape of a single model but results from a varied array of solutions influenced by democratic legacy, the level of technological development and public trust in state institutions (Norris and Grömping, 2019). As the first country to have internet voting (i-Voting) nationwide, Estonia has arguably produced the most renowned digital electoral laboratory of all. Even amid numerous criticisms of this model, it's been adapted and polished to an approach based on verifiability, transparency, and trust in a robust digital identity system (Vassil and Solvak, 2016). Meanwhile, the United States is a divided nation due to its federal structure. After the 2016 races, when there were several reports of external interference, U.S. governmental officials formally made the electoral process part of the nation's critical infrastructure (Mueller, 2019). For its part, the European Union has chosen a regulatory and cross-border cooperation paradigm that empowers member states. The EU has developed an ecosystem of regulations to secure both critical infrastructures and the information space through the NIS Directive, the GDPR Regulation, and the Code of Practice on Disinformation (European Commission 2018; ENISA 2020).

The Republic of Moldova is in an early, but important stage of electoral digitalization. For the purposes of centralizing results and validating lists of voters, the Central Electoral Commission (CEC) has introduced the State Automated Information System titled "Elections" (SIASA; CEC 2021). In addition, the "Alegeri.md" platform and the establishment of the Electronic Register of Voters are two significant steps towards greater transparency and public access to information (Promo-LEX 2020). However, independent reports have reported deficiencies in cybersecurity and inadequate technical capacity to address hybrid threats, such as disinformation campaigns during electoral situations (OSCE/ODIHR, 2021). This unique feature is evident in Moldova's high degree of susceptibility to external interference which is proved by several international evaluations of its information space's vulnerability (CoE, 2022).

The comparison of these models provides some important lessons. Estonia demonstrates that full digitalization is possible when a robust digital identity framework exists. The US shows that democratic resilience can be enhanced through audits and minimum security standards. The European Union stresses the need for coordination and for a common regulatory framework. Meanwhile, in the Republic of Moldova, digital electoral infrastructure is still maturing: resource constraints and geopolitical pressures are further factors for the fragility of an already complex transition.

Conclusions

The article confirms that the electoral process in the digital era should not be regarded as a purely administrative issue but a vital aspect of national security infrastructure. Modern technologies, spanning electronic registries to online voting to block chain and artificial intelligence, have great potential to fundamentally change the process of inter-

action between citizens and democratic institutions. But the transition does not come without risks. Digitalization leads to unprecedented levels of exposure to cyberattacks, foreign interference, and disinformation campaigns, with elections being transformed into a realm of strategic confrontation.

The key conclusion is that electoral security is no longer an exclusively technical matter, merely a case of database protection or the security of the IT infrastructure. It should be seen as a dynamic interrelationship between technology, communication, and public trust. The best of technical infrastructure can't stand any chance if voter trust has been eroded by informational manipulation. In the same way, the most transparent institutional communication has no value if technology is compromised and results can be contested.

In this regard, we consider it most important to orient the country's policies toward strengthening democratic resilience. First, it is necessary to treat electoral processes as critical infrastructure in national legislation, to safeguard elections in a way similar to legislation used in other strategic sectors, such as energy or transportation. Second, the technological infrastructure should be protected by ensuring mandatory standards: end-to-end encryption, multifactor authentication, independent external audits, and rapid response protocols in the event of an attack. It is important to build interinstitutional coordination arrangements as a single unit and to facilitate cooperation among electoral authorities, security services, and communications regulatory authorities to enable a unified and coherent response to hybrid threats. Similarly, the role of society must also be involved in the field by carrying out digital education programmes and media literacy initiatives that aim to reduce citizens' susceptibility to disinformation. Thirdly, cooperation among nations is critical. Attacks on democratic processes are transnational and, in this regard, the only practical means to counter them is to enable the ongoing exchange of best practices and integration into regional security networks.

Thus electoral security is not a one-off goal but a constantly evolving process, in which the state is forced to weigh technological innovations against protection mechanisms as well as public trust constantly. It is only through a holistic national strategy supported by international cooperation and societal resilience that the integrity of elections as the real expression of popular will and as a source of stability in a democratic state.

BIBLIOGRAPHY

Ayed, Ahmed Ben. 2017. "A Conceptual Secure Blockchain-Based Electronic Voting System." *International Journal of Network Security & Its Applications* 9 (3): 1–9.

Bada, A., şi Jason R. C. Nurse. 2019. *The Cyber Security Body of Knowledge*. University of Bristol.

Bradshaw, Samantha, şi Philip N. Howard. 2019. *The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation*. Oxford Internet Institute.

Brookings Institution. 2022. *Artificial Intelligence and Democracy: Risks and Opportunities*. Washington, DC: Brookings.

CEC. 2021. *Raport privind utilizarea Sistemului Informațional Automatizat de Stat „Alegeri"*. Chișinău: Comisia Electorală Centrală a Republicii Moldova.

Chesney, Robert, şi Danielle Citron. 2019. "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security." *California Law Review* 107 (6): 1753–1819.

CoE. 2022. *Assessment of the Information Environment and Hybrid Threats in the Republic of Moldova*. Strasbourg: Council of Europe.
DeNardis, Laura. 2020. *The Internet in Everything: Freedom and Security in a World with No Off Switch*. New Haven: Yale University Press.
ENISA. 2020. *Election Cybersecurity: Challenges and Opportunities*. Athens: European Union Agency for Cybersecurity.
European Commission. 2018. *Action Plan Against Disinformation.* Brussels: European Commission.
Garnett, Holly Ann. 2020. "Evaluating Cybersecurity in Elections: A Critical Review and Research Agenda." *Electoral Studies* 68: 102–187.
Guess, Andrew, Brendan Nyhan, și Jason Reifler. 2020. "Exposure to Untrustworthy Websites in the 2016 U.S. Election." *Nature Human Behaviour* 4 (5): 472–480.
Howard, Philip N., Bharath Ganesh, și Dimitra Liotsiou. 2018. *The IRA, Social Media and Political Polarization in the United States, 2012–2018*. Computational Propaganda Research Project, University of Oxford.
Mueller, Robert S. 2019. *Report on the Investigation into Russian Interference in the 2016 Presidential Election*. Washington, DC: U.S. Department of Justice.
NATO. 2021. *NATO's Approach to Countering Disinformation.* Brussels: North Atlantic Treaty Organization.
Norris, Pippa, și Max Grömping. 2019. *Electoral Integrity Worldwide.* Oxford: Oxford University Press.
OSCE. 2020. *Handbook for the Observation of New Voting Technologies*. Warsaw: OSCE Office for Democratic Institutions and Human Rights.
OSCE/ODIHR. 2021. *Election Observation Mission Final Report: Republic of Moldova Early Parliamentary Elections, 11 July 2021*. Warsaw: OSCE Office for Democratic Institutions and Human Rights.
Promo-LEX. 2020. *Raport de Monitorizare a Alegerilor Prezidențiale 2020 în Republica Moldova*. Chișinău: Promo-LEX.
Rid, Thomas, și Ben Buchanan. 2015. "Attributing Cyber Attacks." *Journal of Strategic Studies* 38 (1–2): 4–37.
Shao, Chengcheng, Giovanni Luca Ciampaglia, Onur Varol, Alessandro Flammini, și Filippo Menczer. 2018. "The Spread of Low-Credibility Content by Social Bots." *Nature Communications* 9: 4787.
Springall, Drew, Travis Finkenauer, Zakir Durumeric, J. Alex Halderman, Nadia Heninger, et al. 2014. "Security Analysis of the Estonian Internet Voting System." In *Proceedings of the 21st ACM Conference on Computer and Communications Security*, 703–20.
Tucker, Joshua A., Andrew Guess, Pablo Barberá, Cristian Vaccari, Alexandra Siegel, Sergey Sanovich, Denis Stukal, și Brendan Nyhan. 2018. "Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature." *Political Polarization* 1–95.
Vassil, Kristjan, și Mihkel Solvak. 2016. *E-Voting in Estonia: Technological Diffusion and Other Developments Over Ten Years (2005–2015)*. Tartu: University of Tartu Press.