https://doi.org/10.31861/mediaforum.2026.18.98-119
УДК: 342.81
© *Ivan Osadtsa*[1]

POLITICAL PARTICIPATION AND SECURITY RISKS OF INTERNET VOTING IN UKRAINE UNDER MARTIAL LAW

The article examines internet voting as a potential mechanism for ensuring political participation in Ukraine under martial law. The full-scale war has significantly complicated access to traditional electoral procedures for military personnel, internally displaced persons, citizens abroad, and residents of affected territories, thereby making the search for alternative instruments to preserve the inclusiveness of the electoral process particularly relevant. It is argued that internet voting is capable of reducing spatial and organizational barriers to participation; however, at the same time, it generates serious security risks. The main threats include the cyber vulnerability of infrastructure, external interference, problems of remote voter identification, risks of violating the secrecy of the vote, and undermining the legitimacy of results. The article demonstrates that, in wartime, trust in digital elections is determined not only by the technological reliability of the system, but also by the institutional resilience of the state and the level of public trust. It is concluded that the possible introduction of internet voting in Ukraine requires a phased approach, proper regulatory framework, a high level of cybersecurity, and preliminary testing.

Keywords: *political participation, internet voting, electronic democracy, electoral process, martial law, cybersecurity, legitimacy, trust, Ukraine.*

Політична участь і безпекові ризики інтернет-голосування в Україні в умовах воєнного стану

У статті досліджено інтернет-голосування як потенційний механізм забезпечення політичної участі в Україні в умовах воєнного стану. Повномасштабна війна істотно ускладнила доступ до традиційних виборчих процедур для військовослужбовців, внутрішньо переміщених осіб, громадян за кордоном та мешканців постраждалих територій, що актуалізує пошук альтернативних інструментів

[1] Candidate of Political Sciences, Associate Professor at the Department of International Relations and Social Communications, Yuriy Fedkovych Chernivtsi National University, Ukraine, E-mail: i.osadtsa@chnu.edu.ua; https://orcid.org/0000-0001-5593-5944.

збереження інклюзивності виборчого процесу. Обґрунтовано, що інтернет-голосування здатне зменшувати просторові та організаційні бар'єри участі, однак водночас породжує серйозні безпекові ризики. До основних загроз віднесено кібервразливість інфраструктури, зовнішнє втручання, проблеми дистанційної ідентифікації виборців, ризики порушення таємниці голосування і підриву легітимності результатів. Показано, що в умовах війни довіра до цифрових виборів визначається не лише технологічною надійністю системи, а й інституційною стійкістю держави та рівнем суспільної довіри. Зроблено висновок, що можливе впровадження інтернет-голосування в Україні потребує поетапності, належного нормативного врегулювання, високого рівня кіберзахисту та попереднього тестування.

Ключові слова: *політична участь, інтернет-голосування, електронна демократія, виборчий процес, воєнний стан, кібербезпека, легітимність, довіра, Україна.*

Introduction. Relevance of the study. The issue of internet voting occupies an important place in contemporary studies of the transformation of democracy, since the digitalization of state institutions changes the nature of interaction between the citizen and the political system. In contemporary scholarly discussions, attention is increasingly shifting from basic electronic services and petitions to a reconsideration of the very procedure of expressing political will. In this context, internet voting emerges as one of the most controversial and, at the same time, symbolic forms of electronic democracy, directly related to the fundamental basis of the democratic order – elections.

The relevance of this topic for Ukraine is particularly intensified under martial law, which has radically changed the social, territorial, and security conditions for the exercise of political rights. The mass displacement of millions of citizens, the destruction of infrastructure, the temporary occupation of territories, and the difficulty of involving military personnel in traditional voting procedures transform the issue of ensuring political participation from a technical task into a problem of the democratic resilience of the state. Under such conditions, internet voting is considered a potential mechanism for reducing the distance between the citizen and the electoral procedure, as it may ensure participation in voting regardless of the voter's physical location.

Although in the international literature internet voting is often interpreted as an instrument for expanding the accessibility of elections and as a response to the crisis of traditional participation (Abdala 2024; Germann 2021; Goodman 2020; International IDEA 2025), its possible introduction in Ukraine touches upon a set of fundamental issues, including the secrecy of the vote, reliable voter verification, personal data protection, resilience to external interference, and public trust in the results. In wartime, these challenges are further aggravated by the experience of constant cyberattacks and the threat of hybrid interference by the aggressor state. This raises the question of whether the democratic logic of citizen inclusion can be combined with strict requirements for the security and legitimacy of the electoral process.

Finally, the Ukrainian case is also important for comparative political science. Unlike most discussions on the modernization of elections in peacetime or under pandemic conditions, this case concerns the functioning of democratic procedures in the environment of a full-scale war. Studying this experience makes it possible to understand more deeply the limits of applicability of digital electoral technologies and to determine the extent to which the expansion of political participation can coexist with the priority of security. This makes the topic relevant both from the practical perspective of ensuring electoral rights and from the theoretical perspective of conceptualizing digital democracy in crisis conditions.

Problem statement. The main scholarly problem lies in the fact that, under martial law in Ukraine, there is an objective need to search for new ways of ensuring political participation; however, digital instruments designed to expand access to elections simultaneously generate increased security threats. As a result, a fundamental contradiction emerges between the democratic logic of inclusion and the logic of security and protection of the integrity of the electoral process.

On the one hand, internet voting may be considered a mechanism for adapting the electoral procedure to emergency conditions. It is capable of becoming an instrument for involving those categories of citizens who, due to war, forced displacement, military service, or residence abroad, have limited access to traditional voting procedures. On the other hand, it is precisely under martial law that the vulnerability of any digital system to cyberattacks, external interference, and information operations aimed at undermining trust in and the legitimacy of election results increases significantly.

Of course, the scholarly problem is not limited to the question of the technical feasibility of implementing internet voting. It consists in determining whether this instrument, in the current realities of Ukraine, can simultaneously ensure broader political participation without undermining the security, procedural, and legitimizing foundations of the electoral process. It is this dilemma that determines the logic of the subsequent analysis.

In this context, the article aims to analyze internet voting as a potential instrument for ensuring political participation in Ukraine under martial law and to identify the key security risks of its possible implementation. To this end, attention is focused on four interrelated aspects: the inclusive potential of internet voting, the specific features of exercising electoral rights in wartime, the system of security threats accompanying the digitalization of the electoral process, and the prospects for applying such a mechanism in Ukraine, taking into account international experience and the national context.

Analysis of recent studies and publications. The scholarly discourse on internet voting is characterized by a variety of approaches that can be structured into several main areas. The first cluster includes works devoted to the impact of internet voting on the dynamics of electoral participation. In these studies, this mechanism is interpreted as a means of reducing the transaction costs of participation, eliminating spatial barriers, and increasing the convenience of the procedure, particularly for voters abroad or in remote regions (Germann 2021; Goodman 2020). At the same time, studies show that the positive effect on turnout is not automatic and depends largely on the political context and the design of the electoral system (Abdala 2024; Stockemer, Wigginton 2024, 621–623).

The second area focuses on the issues of public trust and legitimacy. Within this approach, it is shown that citizens' willingness to recognize the results of digital voting is formed at the intersection of trust in state institutions and trust in technological solutions (Abdala et al. 2025, 783–796; Decman, Kozel 2023, 1–23; Sindermann et al. 2023). In this context, the technical perfection of the system alone does not guarantee its public acceptance; thus, trust acts not as a secondary consequence, but as a basic condition for the viability of remote voting.

The third body of literature is devoted to issues of cybersecurity and infrastructure protection. Internet voting is analyzed here as a complex sociotechnical system whose vulnerability extends to authentication

channels, user devices, administration procedures, and audit mechanisms (Cybersecurity … 2020; Heinl et al. 2022; IFES 2022; National Institute … 2024). Even the Estonian case, which is most often considered the main example of functioning internet voting, has been criticized by cybersecurity experts, which highlights the need for independent testing, secure management of cryptographic keys, and institutional readiness to respond to incidents (Ehin et al. 2022; Springall et al. 2014).

A separate regulatory and standard-setting area is represented by documents of key international institutions – the Council of Europe, the Venice Commission, the OSCE/ODIHR, and International IDEA (Council of Europe 2017; International IDEA 2025; International IDEA 2023; National Institute … 2024; OSCE Office 2013; OSCE Office 2024; Venice Commission 2020). This framework establishes the priority of ensuring that digital innovations comply with basic democratic principles – secrecy, equality, verifiability, and freedom of expression of the will.

The fifth group consists of studies on the organization of the electoral process in crisis conditions – during pandemics, armed conflicts, or mass population displacement (International IDEA, Elections… 2023; International IDEA 2025; International IDEA 2022; International IDEA, European Parliament 2023). These works shift the analysis from the plane of technological optimism to the plane of crisis management of democracy, equality of access, and institutional resilience. In the same context, the Ukrainian academic discourse is developing, focusing on the legal preconditions for post-war elections and the transformation of political participation under the conditions of the Russian invasion (Didenko 2023, 55–56; Monastyrskyi 2025, 308–309; Symysenko 2025; Chaika 2024, 140–147; Sikora 2024, 64–70). Ukrainian scholars emphasize the dual nature of electronic democracy: on the one hand, it is capable of supporting citizens' engagement under conditions of migration (Didenko 2023, 57–58; Monastyrskyi 2025, 309); on the other hand, it functions in an environment of increased security threats (Symysenko 2025; Chaika 2024, 146–147; Sikora 2024).

Despite the existence of a substantial body of research, a research gap remains. International studies predominantly analyze digital elections in stable democracies, while Ukrainian studies often focus on the general legal aspects of post-war recovery. This creates the need for a comprehensive understanding of internet voting in Ukraine specifically through the prism

of martial law, as an instrument that requires simultaneous consideration of its inclusive potential and increased security risks.

The scientific novelty of the article lies in the fact that internet voting in the Ukrainian context is considered not merely as a technological instrument for modernizing the electoral process, but as a political and institutional mechanism assessed through the relationship between inclusive potential and security risks under martial law. The study also clarifies the limits of applicability of international experience with internet voting for Ukraine, taking into account the specific nature of the full-scale war, the increased cyber threat, and the transformation of the conditions for exercising electoral rights.

Methodological basis of the study. The methodological basis of the article consists of a combination of several mutually complementary approaches that make it possible to consider internet voting not only as a technological innovation, but also as a political and institutional phenomenon closely linked to the issues of security, trust, and legitimacy of the electoral process. This approach is determined by the specific nature of the research subject, since under martial law the assessment of digital electoral mechanisms cannot be limited to questions of technical efficiency or procedural convenience.

The institutional approach makes it possible to analyze internet voting as an element of the electoral institution, rather than as an isolated digital solution. Within this approach, attention is focused on norms, procedures, control mechanisms, forms of legitimation, and the interaction of internet voting with other components of the electoral process. This makes it possible to assess the extent to which digital mechanisms can be integrated into the architecture of democratic elections without undermining its basic principles.

The systems approach is used to examine internet voting as a complex node of interaction between digital infrastructure, public administration, legal regulation, cybersecurity, and public trust. Its application makes it possible to avoid technological reductionism, that is, reducing the problem exclusively to the technical parameters of the platform. In this context, the viability of internet voting is determined not only by software or authentication channels, but by the functioning of the entire system – from the institutional capacity of the state to society's readiness to recognize the results of a digital procedure as legitimate.

The risk-oriented approach is of key importance for this study. It makes it possible to shift the focus from the potential advantages of internet voting to the analysis of its vulnerabilities, threats, and possible consequences of failure. For a country at war, this approach is particularly justified, since any change in the electoral procedure must be assessed not only by the criterion of expanding access to participation, but also by the relationship between democratic gain and security risk. This allows internet voting to be considered not through the logic of technological optimism, but through the logic of a cautious assessment of its political and institutional acceptability.

The method of analyzing scholarly sources, international standards, and normative documents also plays an important role in the study. It is used to systematize the main theoretical approaches to internet voting, summarize international requirements for digital electoral procedures, and outline the Ukrainian normative and political context. This forms a conceptual framework within which internet voting can be assessed not only as a technology, but also as an object of political, legal, and security analysis.

The comparative method is applied to compare the Ukrainian situation with international practice, primarily with the experience of Estonia as the most relevant example of the nationwide implementation of internet voting (Vassil et al. 2016, 457; Turnbull-Dugarte, Devine 2023). This comparison is used not for the mechanical transfer of foreign models into Ukrainian conditions, but to identify the institutional preconditions under which digital electoral technologies can function relatively successfully, as well as to determine the factors that limit their application in a crisis environment.

In addition, the study uses elements of a case study, which makes it possible to specify theoretical provisions through the analysis of a particular international case. This is important in order to avoid an overly abstract consideration of internet voting and to correlate general analytical conclusions with the actual practice of the functioning of such systems.

Results of the study. Political participation in a democratic system is not limited to the formal existence of the right to vote, but presupposes a real opportunity to exercise this right without excessive barriers, discrimination, or disproportionate risks. That is why electoral participation is increasingly considered not only as a legal category, but also as a function of institutional accessibility. In this sense, internet voting

is an important object of analysis, since it directly affects the accessibility of the electoral procedure.

In its most general form, internet voting is a form of remote electronic expression of political will in which a voter casts a vote via the Internet using a specialized digital system. Its key difference from other forms of electronic voting lies in its remote nature and the absence of the need for physical presence at a polling station. It is this feature that determines its inclusive potential.

Internet voting reduces the importance of geographical distance, which is especially important for citizens who are outside the country or far from a polling station. The time, financial, and physical effort required to travel to the place of voting often turns a formally guaranteed right into an opportunity that is difficult to realize in practice. Works devoted to the participation of citizens abroad emphasize that remote formats can significantly expand the participation of this category of voters (Monastyrskyi 2025, 310; Germann 2021; International IDEA, European Parliament 2023). For Ukraine, this is of particular importance, since a significant part of its citizens are outside the state, and their political integration into the national electoral process constitutes a separate problem.

At the same time, internet voting reduces the time and administrative costs of participation. A voter does not have to adjust to the working hours of a polling station, spend time travelling, waiting in queues, or searching for the required address. In the literature, this is described as a reduction in the "cost of voting", that is, the resources necessary to exercise the right to vote (Abdala 2024; Goodman 2020, 1160–1162). Although this effect does not always lead to a noticeable increase in overall turnout, it may be significant for groups for whom barriers to participation are systemic.

Internet voting may also play a separate role as a symbolic mechanism of inclusion. For a citizen who has been forcibly displaced, is staying in another region, or is abroad, the opportunity to vote without a complicated procedure of returning to the place of registration means not only functional convenience, but also the preservation of a connection with the political community. In contemporary societies, where an increasing share of citizens' interaction with the state takes place through digital services, internet voting is also perceived as a continuation of the broader digital transformation of public administration (Chaika 2024, 147; International IDEA 2025).

At the same time, the inclusive potential of internet voting should not be overestimated. The reduction of some barriers may be accompanied by the strengthening of others – digital inequality, lack of skills, absence of a secure device, or unstable access to the Internet. Moreover, the democratic value of elections is determined not only by the number of those who voted, but also by whether the procedure preserves freedom, secrecy, equality, and trust. That is why the effectiveness of internet voting should be assessed not only through the parameter of convenience, but through the relationship between accessibility, security, and public trust (Abdala et al. 2025, 790; Agbesi et al. 2024; International IDEA 2025).

For Ukraine, the problem of participation is particularly sensitive. Martial law changes the basic conditions of access to voting, and therefore any instrument capable of supporting or expanding participation naturally attracts attention. However, the Ukrainian context also shows that inclusion cannot be achieved at the cost of neglecting security. Internet voting makes sense as a mechanism of political participation only when it does not undermine the foundations of the electoral process itself.

Martial law radically transforms the conditions under which democratic institutions function. The mass internal displacement of the population, evacuation from dangerous regions, and the prolonged stay of a significant number of citizens abroad complicate the usual model of linking the voter to a specific place of voting. Formally, the right to vote is preserved; however, its practical realization increasingly depends on the state's ability to adapt participation mechanisms to the mobility and dispersion of the population (Didenko 2023, 58; Monastyrskyi 2025, 310; International IDEA 2022; International IDEA, European Parliament 2023).

The issue of participation by military personnel is especially complex. The conditions of service, presence in combat zones, limited mobility, and the priority of security tasks make traditional voting organizationally almost inaccessible for many of them. At the same time, ensuring their right to vote must not create additional security risks or undermine the reliability of the electoral process.

The war affects not only the movement of people, but also the material conditions for holding elections, namely the condition of premises, transport, communications, power supply, the safety of movement, and the work of administrative bodies. Where infrastructure has been destroyed or remains under threat, the conduct of ordinary electoral procedures becomes excessively risky or technically complicated. In addition, the

psychological and social preconditions for participation also change: war affects the level of public anxiety, trust in institutions, information practices, and the perception of procedures. Under such conditions, even a technically sound solution may be politically unacceptable if it appears opaque or too risky (Central Election … 2025).

An important dimension is also the international one. A significant share of Ukrainian citizens are abroad, and therefore the issue of their participation goes beyond the purely internal organization of elections and requires coordination with foreign jurisdictions, appropriate infrastructure, and proper legal regulation (Monastyrskyi 2025, 311–312; International IDEA, European Parliament 2023). As a result, political participation in Ukraine under wartime conditions acquires a new quality: it can no longer be ensured by simply reproducing peacetime procedures and requires adaptive mechanisms that simultaneously take into account accessibility, security, and legitimacy. That is why internet voting enters the field of discussion as one of the possible instruments of crisis democratic adaptation, although it must be assessed much more rigorously than under stable conditions.

The security dimension of internet voting is central to any serious analysis of this technology, and under martial law it becomes decisive. Elections as an institution must not only take place, but also be recognized as fair, free, and credible. That is why trust in the procedure becomes no less important than the result itself. By expanding access to participation, internet voting simultaneously creates new opportunities for technical, organizational, and informational threats (Erben, Kobakhidze 2023).

The most obvious risk is cyberattacks on electoral infrastructure. Unlike paper voting, where large-scale interference requires influence over a large number of physical objects, a digital system concentrates critical functions in electronic infrastructure, which potentially becomes a target for external influence. Attacks may be directed at servers, communication channels, authentication systems, databases, administrative components, or user interfaces. Even if they do not lead to an actual change in the results, the very fact of their occurrence may cause a crisis of trust (Cybersecurity … 2020; IFES 2022; National Institute … 2024). For Ukraine, this risk is particularly high given the constant cyber threat from the aggressor state. In such an environment, the purpose of an attack may be not only falsification, but also destabilization of the process, disruption of voting, or the creation of grounds for non-recognition of the results.

No less important is the problem of voter identification and verification. If traditional voting relies on physical presence, an identity document, and control by the election commission, internet voting requires digital substitutes for these mechanisms. However, even strong electronic authentication does not guarantee that the vote is cast by that specific voter and under conditions of free expression of will. The risks of coercion, the use of another person's device, phishing, compromise of credentials, or malicious software remain (Heinl et al. 2022; International IDEA 2025; OSCE Office 2024).

A separate group of threats concerns the secrecy of the vote. Remote voting takes place in an uncontrolled environment, which does not provide the level of procedural control that exists at a polling station. Voting from home, the workplace, or another private space creates opportunities for family, domestic, administrative, or other forms of pressure, as well as for control over how exactly a person voted. The literature emphasizes that voting in an uncontrolled environment is always associated with particular risks of "coercion and vote buying," and no technical solution is capable of fully eliminating this problem (Heinl et al. 2022; International IDEA 2025; Venice Commission 2020).

The voter's end device also remains a fundamental vulnerability. Even if the central system is well protected, citizens' personal computers or smartphones may become the weak link. An infected or compromised device calls into question both the correctness of vote casting and the secrecy of the vote. This is one of the basic problems of internet voting: the state cannot fully control the environment from which voting is carried out and, therefore, cannot fully guarantee the security of the procedure at the user level.

Another significant risk is related to opacity and limited verifiability for the ordinary citizen. Paper elections, despite their shortcomings, have the advantage of intuitive comprehensibility: the voter sees the ballot paper, the ballot box, the counting process, and the protocols. Internet voting transfers key operations into a technically complex sphere, where trust increasingly depends on experts, system administrators, and audit procedures. The more expert-mediated the procedure becomes, the greater its dependence on institutional trust (Abdala et al. 2025, 791–792; Agbesi et al. 2024, 17–18; Ehin et al. 2022).

In the Ukrainian context, this is compounded by the danger of information and psychological operations aimed at delegitimizing

elections. The adversary does not necessarily need to actually change the voting results in order to achieve a political effect; it is sufficient to create a convincing narrative about interference, data leakage, a technical failure, or the opacity of the system. If the level of public trust is insufficient and the procedure is difficult to understand, such a campaign may be extremely effective. Therefore, internet voting in Ukraine should be considered not only as a cybernetic object, but also as a communicative and legitimizing one.

Significant risks are also associated with the protection of personal data and sensitive electoral information, the continuity of the system's functioning, and the administrative complexity of its maintenance. Internet voting inevitably operates with large volumes of personal data, authentication tools, event logs, and technical information; therefore, any infrastructure vulnerabilities or procedural shortcomings may generate risks of leakage, re-identification, or even suspicion of such a possibility. In wartime, it is especially important to take into account the likelihood of power outages, communication disruptions, or damage to digital infrastructure, which makes issues of redundancy, duplication of channels, and emergency scenarios a fundamental condition for the viability of the system. In addition, internet voting does not simplify, but often complicates administrative procedures: it requires specialized teams of developers, auditors, security administrators, independent observers, certification, testing, incident response, and constant communication with citizens. The experience of Estonia shows that this is not a "digital add-on" to elections, but a complex institutional structure that requires continuous improvement and work with trust (Ehin et al. 2022; Springall et al. 2014, 710–711).

Ultimately, the deepest risk is the risk of undermining the legitimacy of the electoral process. Elections are legitimate when their result is recognized by society as the outcome of a fair and understandable procedure. If a significant share of citizens, political forces, or international partners doubt the reliability of the digital system, even formally correct voting may fail to perform its political function. That is why the security risks of internet voting under martial law are multi-level in nature and include technological, organizational, legal, psychological, communicative, and geopolitical components. The question of its possible introduction in Ukraine cannot be resolved solely on the basis of technical feasibility or user convenience; it requires a much broader assessment of whether an

instrument intended to expand participation may become a new source of vulnerability for democracy.

The consideration of internet voting in Ukraine under martial law inevitably leads to a central dilemma, which may be formulated as follows: "How can the expansion of political participation be combined with the requirements of security, trust, and legitimacy of the electoral process?" This dilemma is not technical, but political in nature, since it concerns the balance between two basic values of democracy (Erben, Kobakhidze 2023).

A democratic order is impossible without inclusiveness. The greater the number of citizens who can actually exercise their right to vote, the more fully elections reflect the political will of society. In wartime, the exclusion of large groups of the population – military personnel, internally displaced persons, and citizens abroad – may not only reduce the level of participation, but also call into question the representativeness of elections as a whole. That is why the argument in favor of internet voting as an instrument of inclusion cannot be considered secondary.

At the same time, elections cannot be legitimate merely because they have included more people. If the procedure is vulnerable to manipulation, opaque, or insufficiently protected, the expansion of participation is achieved at the cost of reduced trust and, consequently, weakened legitimacy. The dilemma does not consist in choosing between "participation" and "security" as absolutely incompatible goals, but in the fact that each side of this formula has limits that cannot be crossed. Excessive dominance of the logic of participation leads to an underestimation of risks and the creation of a convenient but insufficiently reliable procedure. Conversely, excessive dominance of the security logic narrows the democratic meaning of elections if a significant share of citizens is effectively excluded from participation.

In the Ukrainian context, this contradiction is particularly acute, since the high need for adaptive mechanisms of participation is combined with an extremely high level of security threat. Therefore, it is not enough simply to state that internet voting is "convenient" or, conversely, "dangerous." A differentiated assessment is needed, one that takes into account for whom, under what conditions, on what scale, and at what stage such an instrument may be acceptable. Determining the threshold of acceptable risk becomes key. In a democratic electoral process, zero risk does not exist for either paper-based or digital procedures; however, risks must remain such that

they do not call into question the basic principles of elections and can be minimized (Central Election … 2025).

It is also important that participation and security are not external to each other. The security of the electoral process is itself a condition of political participation, since citizens will participate only in elections that they consider genuine, protected, and meaningful. At the same time, participation is a condition of legitimate security: excessive security regulation that effectively narrows the circle of those who can vote undermines the democratic basis of elections. That is why discussions about internet voting in Ukraine should be built around a model of cautious compatibility, rather than radical technological optimism. This means searching for formats in which the expansion of participation will not outpace the institutional and security capacity of the state. In this sense, phased implementation, pilot formats, independent audit, public communication, and careful regulatory consolidation of procedures acquire particular importance.

Assessing the prospects of internet voting in Ukraine requires rejecting both unconditional enthusiasm and absolute denial. Contemporary conditions do indeed create demand for new forms of ensuring political participation; however, martial law makes any radical electoral innovation politically and security-wise extremely sensitive. Therefore, the prospects of internet voting can be considered only as conditional and dependent on a number of basic prerequisites (Central Election … 2025).

First of all, this concerns resilient digital infrastructure. For internet voting, the general digitalization of public services or broad access to the Internet is not sufficient; what is needed is the capacity of critical infrastructure to operate stably under conditions of attacks, disruptions, high load, and emergencies. Protected data centers, backup communication channels, uninterrupted power supply, data backup systems, and clear incident recovery protocols are necessary. A high level of cybersecurity is no less fundamental: a multi-layered security architecture, regular penetration testing, independent audit, continuous network monitoring, and a clear system for verifying results. The experience of Estonia demonstrates that internet voting requires not a one-time launch, but continuous support and improvement (Ehin et al. 2022; Springall et al. 2014, 712).

The next condition is a reliable and socially acceptable system of voter identification. For elections, the criteria here are much higher than for ordinary administrative services: it is necessary to guarantee not only

identity confirmation, but also the uniqueness of the vote, the secrecy of the expression of will, protection against coercion, and resilience to compromise. Proper regulatory framework is no less important. Internet voting cannot be introduced as a purely technical project without a deep legal foundation that clearly defines the procedure for access to the system, audit procedures, appeal mechanisms, data storage rules, the status of digital traces, and algorithms for responding to failures.

Public trust remains a critical prerequisite. As studies show, internet voting functions relatively successfully only where citizens trust state institutions, technologies, or a combination of these two factors (Abdala et al. 2025, 793; Decman, Kozel 2023, 22; Sindermann et al. 2023). In Ukraine, trust is an especially sensitive issue, since any electoral innovation may immediately become an object of political suspicion and information attacks. Therefore, the prospects of internet voting depend not only on the availability of a software solution, but also on whether society will be convinced that the system is fair, controllable, and not created for situational political interests.

No less important is the phased nature of possible implementation. Internet voting cannot appear immediately as a full replacement for traditional voting. A more realistic scenario is that of limited pilot projects and simulations, with subsequent expansion only after successful audit, public discussion, and independent assessment. In addition, it is advisable to consider it not as a universal mechanism for all voters, but as an instrument potentially more justified for certain categories whose access to traditional voting is particularly complicated. At the same time, such selectivity requires particular caution in order to avoid "unequal security regimes" for different groups of voters (Krimmer et al. 2021, 25).

It is also important not to consider internet voting in isolation. In the contemporary discussion, the problem should not be reduced to the binary opposition of "either paper voting or internet voting," since there is a broader spectrum of solutions – special polling stations, expanded mechanisms for changing the place of voting, postal voting, special procedures for citizens abroad, mobile voting, and other special forms of voting. In this sense, internet voting should be assessed as part of a broader set of instruments for ensuring participation. A culture of transparency is also of decisive importance: the architecture of the system, the principles of its functioning, verification procedures, and rules for responding to problems must be as open as possible to society and the expert community (Council of Europe

2017; International IDEA 2025; OSCE Office 2024; Venice Commission 2020). Finally, even a technically prepared solution may be inappropriate at a political moment when the level of threat remains too high and society is not ready to perceive a change in the electoral procedure as legitimate.

Thus, internet voting in Ukraine can be considered only as a potential direction for the development of the electoral process in the longer term. It is neither a ready-made nor a universal solution for the conditions of martial law, but it also cannot be definitively rejected as unsuitable under any circumstances. Its practical acceptability will depend on whether the state is able to create such a combination of technological capacity, legal regulation, public trust, and security guarantees under which internet voting becomes not a threat, but a support for democratic participation.

Conclusions. The conducted study gives grounds to assert that internet voting should be considered not merely as a technological innovation, but as a political and institutional mechanism that directly affects the accessibility of participation, the level of trust in elections, and the legitimacy of the political order. Accordingly, its analysis cannot be limited to the technical characteristics of the system, but must encompass legal, security, social, and symbolic dimensions.

Under martial law, internet voting acquires particular relevance as a potential instrument for ensuring political participation. The full-scale war has radically changed the structure of access to elections, namely: the mass displacement of the population, the presence of citizens abroad, the difficulty of participation by military personnel, the destruction of infrastructure, and general security threats call into question the possibility of relying exclusively on traditional forms of voting for all categories of voters. Under such conditions, internet voting naturally emerges as one of the possible ways to preserve the inclusiveness of the electoral process.

At the same time, its inclusive potential is not absolute. Internet voting is capable of reducing spatial, time-related, and organizational barriers to participation; however, it does not eliminate all problems and does not guarantee an automatic improvement in the democratic quality of elections. The reduction of some barriers may be accompanied by the emergence of others – digital inequality, dependence on technical literacy, vulnerability of user devices, or difficulties in ensuring the freedom and secrecy of the expression of will.

In the case of Ukraine, it is precisely the security dimension of internet voting that is decisive. The main risks are associated with cyberattacks

on electoral infrastructure, possible interference by the aggressor state, problems of personal data protection, difficulties of reliable remote voter identification, risks of violating the secrecy of the vote, the opacity of the procedure for the general public, and the possibility of informational delegitimization of the results. The totality of these threats indicates that internet voting in Ukraine cannot be assessed according to the logic of ordinary digital modernization.

The key analytical framework for its assessment is the relationship between political participation and security. Expanding participation without an adequate level of protection may undermine trust in and the legitimacy of elections. Conversely, excessive dominance of the security logic may narrow the democratic character of the electoral process if significant groups of citizens remain effectively excluded. Therefore, the issue of internet voting should be considered as a problem of finding a cautious balance, rather than as a sphere for simple normative solutions.

International experience, primarily the Estonian case, shows that internet voting can function as part of an electoral system, but only under conditions of a high level of digital infrastructure, stable institutional capacity, developed audit procedures, continuous security support, and relatively high public trust. At the same time, even successful cases do not eliminate discussions about vulnerabilities and cannot be mechanically transferred to the Ukrainian context, which has been shaped by the conditions of a full-scale war.

The prospects for using internet voting in Ukraine can be considered only if a number of critically important prerequisites are met: resilient digital infrastructure, a high level of cybersecurity, a reliable voter identification system, proper regulatory framework, public trust, transparent verification procedures, and a phased, pilot-based nature of possible implementation. Without these conditions, internet voting risks becoming not a means of expanding participation, but a source of new vulnerability for the electoral process.

Thus, internet voting may be considered a potential instrument for maintaining political participation in Ukraine under martial law; however, its possible implementation is associated with a complex set of risks that directly affect trust in and the legitimacy of the electoral process. That is why the question of its application should be assessed not only in technological terms, but above all in political, legal, and security dimensions.

Prospects for further research. The prospects for further scholarly work in this field are quite broad. First of all, an in-depth comparative analysis of international experience with internet voting appears necessary, taking into account not only successful practices, but also the reasons for abandoning such models or limiting their application in different countries. This would make it possible to define more precisely the limits of applicability of internet voting for Ukraine.

Research on public trust in digital forms of voting remains an important direction. Empirical data are especially needed on how different groups of citizens perceive internet voting, which factors shape their readiness or unwillingness to trust such a procedure, and how the war influences these perceptions.

The analysis of participation models for military personnel, internally displaced persons, and citizens abroad requires separate attention. These categories are central to the discussion of electoral inclusiveness in the wartime and post-war periods and therefore require specialized studies that take into account legal, organizational, and security parameters.

Another promising direction is the study of the institutional, legal, and technological prerequisites for the possible pilot introduction of internet voting in Ukraine. This is not about immediate normative approval, but about developing criteria by which the state's readiness for limited test formats could be assessed.

Finally, the relationship between the digitalization of elections and the legitimacy of democracy under wartime conditions requires further conceptual reflection. This topic may become the basis for a broader theoretical analysis of how contemporary democracies adapt their basic political procedures to an environment of prolonged crises and conflicts.

References:

1. Didenko, O. M. 2023. Shchodo pravovoi osnovy dlia provedennia povoiennykh vyboriv v Ukraini [On the Legal Basis for Holding Post-War Elections in Ukraine]. Yurydychnyi naukovyi elektronnyi zhurnal [Legal Scientific Electronic Journal] 12: 55–58 (In Ukrainian). https://doi.org/10.32782/2524-0374/2023-12/9

2. Monastyrskyi, M. V. 2025. Dystantsiine holosuvannia ukrainskykh hromadian za kordonom na pershykh povoiennykh vyborakh i referendumi pro vstup Ukrainy do Yevropeiskoho Soiuzu [Remote Voting of Ukrainian Citizens Abroad in the First Post-War Elections and the Referendum

on Ukraine's Accession to the European Union]. Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia: Pravo [Scientific Bulletin of Uzhhorod National University. Series: Law] 90, no. 1: 308–313 (In Ukrainian). https://doi.org/10.24144/2307-3322.2025.90.1.40

3. Symysenko, I. 2025. Politychna uchast ta elektronna demokratiia: vyklyky v umovakh rosiiskoho vtorhnennia v Ukrainu [Political Participation and Electronic Democracy: Challenges in the Context of the Russian Invasion of Ukraine]. Naukovi pratsi Mizhrehionalnoi Akademii upravlinnia personalom. Politychni nauky ta publichne upravlinnia [Scientific Works of the Interregional Academy of Personnel Management. Political Sciences and Public Administration] 1(77): 169–175 (In Ukrainian). https://doi.org/10.32689/2523-4625-2025-1(77)-24

4. Chaika, I., and Tsokur Ye. 2024. Tsyfrovizatsiia vyboriv v Ukraini i sviti: etychni vymiry fenomenu [Digitalization of Elections in Ukraine and the World: Ethical Dimensions of the Phenomenon]. Humanities Studies 20(97): 140–147 (In Ukrainian). https://doi.org/10.32782/hst-2024-20-97-16

5. Sikora, I. I. 2024. Dovira elektoratu do elektronnykh tekhnolohii u vyborchomu protsesi: svitovyi dosvid [Electorate Trust in Electronic Technologies in the Electoral Process: Global Experience]. Visnyk NTUU "KPI". Politolohiia. Sotsiolohiia. Pravo [Bulletin of NTUU "KPI". Political Science. Sociology. Law] 3(63): 64–70 (In Ukrainian). https://doi.org/10.20535/2308-5053.2024.3(63).313502

6. Abdala, M. B. 2024. "In-Person or Convenience Voting? The Role of the Direct Costs in Explaining Preferences for Voting Modalities." Electoral Studies 91: 102851. https://doi.org/10.1016/j.electstud.2024.102851.

7. Abdala, M., Plescia C., Boyer M., and Brunetti A. 2025. "Trust in Government or in Technology? What Really Drives Internet Voting." Political Research Quarterly 78, no. 2: 783–796. https://doi.org/10.1177/10659129251321424

8. Agbesi, S., Budurushi J., Dalela A., Nissen C., and Kulyk O. 2024. "How to Increase Transparency and Trust in Internet Voting Systems: An Experimental Study." Proceedings of the 13th Nordic Conference on Human-Computer Interaction: 1–18. https://doi.org/10.1145/3679318.3685362

9. Central Election Commission of Ukraine. 2025. Report of the Central Election Commission for 2024. Kyiv. https://www.cvk.gov.ua/wp-content/uploads/2025/04/Zvit-CVK_2024_eng.pdf

10. Council of Europe. 2017. Recommendation CM/Rec(2017)5 of the Committee of Ministers to Member States on Standards for E-Voting. Strasbourg. https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680726f6f

11. Cybersecurity and Infrastructure Security Agency, Election Assistance Commission, Federal Bureau of Investigation, National Association of Secretaries of State. 2020. Risk Management for Electronic Ballot Delivery, Marking, and Return. https://www.cisa.gov/sites/default/files/2024-02/Final_%20Risk_Management_for_Electronic-Ballot_05082020_508c.pdf

12. Decman, M., and Kozel E. 2023. "Examining the Impacts of Technology and Trust on I-Voting Acceptance in the COVID-19 Aftermath." International Journal of Electronic Government Research 19, no. 1: 1–23. https://doi.org/10.4018/IJEGR.327454

13. Ehin, P., Solvak M., Willemson J., and Vinkel P. 2022. "Internet Voting in Estonia 2005–2019: Evidence from Eleven Elections." Government Information Quarterly 39, no. 2: 101718. https://doi.org/10.1016/j.giq.2022.101718

14. Erben, P., and Kobakhidze G. 2023. "What Would It Take to Hold Elections in Ukraine?" IFES, September 21. https://www.ifes.org/news/what-would-it-take-hold-elections-ukraine

15. Germann, M. 2021. "Internet Voting Increases Expatriate Voter Turnout." Government Information Quarterly 38, no. 2: 101560. https://doi.org/10.1016/j.giq.2020.101560

16. Goodman, N., and Stokes L. 2020. "Reducing the Cost of Voting: An Evaluation of Internet Voting's Effect on Turnout." British Journal of Political Science 50, no. 3: 1155–1167. https://doi.org/10.1017/S0007123417000849

17. Heinl, M., Gölz S., and Bösch C. 2022. "Remote Electronic Voting in Uncontrolled Environments: A Classifying Survey." ACM Computing Surveys 55, no. 8: 167. https://doi.org/10.1145/3551386

18. IFES. 2022. Understanding Cybersecurity Throughout the Electoral Process: A Reference Document. An Overview of Cyber Threats and Vulnerabilities in Elections. https://www.ifes.org/sites/default/files/2022-10/Understanding_Cybersecurity_Throughout_the_Electoral_Process_A_Reference_Document_FINAL.pdf

19. International IDEA. 2023. Elections during Emergencies and Crises: Lessons for Electoral Integrity from the Covid-19 Pandemic. Stockholm: International IDEA. https://doi.org/10.31752/idea.2023.24

20. International IDEA. 2025. Online Voting: Current and Future Practices. Stockholm: International IDEA. https://doi.org/10.31752/idea.2025.69

21. International IDEA. 2023. Special Voting Arrangements: The International IDEA Handbook. Stockholm: International IDEA. https://doi.org/10.31752/idea.2023.84

22. International IDEA. 2022. Supporting Ukraine's Democracy After the War: Key Issues, Comparative Experience and Best Practices. Stockholm: International IDEA. https://doi.org/10.31752/idea.2022.39

23. International IDEA, European Parliament. 2023. Parliamentary Electoral Dialogue: Challenges and Needs for Holding Out-of-Country Voting for Ukraine's Post-War Elections – Key Takeaways. https://www.idea.int/sites/default/files/2023-10/Ukraine%20OCV%20Dialogue%20-%20Key%20Takeaways.pdf

24. Krimmer, R., Duenas-Cid D., and Krivonosova I. 2021. "New Methodology for Calculating Cost-Efficiency of Different Ways of Voting: Is Internet Voting Cheaper?" Public Money & Management 41, no. 1: 17–26. https://doi.org/10.1080/09540962.2020.1732027

25. National Institute of Standards and Technology. 2024. Cybersecurity Framework Election Infrastructure Profile. Gaithersburg, MD: NIST. https://doi.org/10.6028/NIST.VTS.200-1

26. OSCE Office for Democratic Institutions and Human Rights. 2013. Handbook for the Observation of New Voting Technologies. Warsaw: OSCE/ODIHR. https://www.osce.org/sites/default/files/f/documents/0/6/104939.pdf

27. OSCE Office for Democratic Institutions and Human Rights. 2024. Handbook for the Observation of Information and Communication Technologies (ICT) in Elections. Warsaw: OSCE/ODIHR. https://cdn.osce.org/sites/default/files/f/documents/c/9/558318_0.pdf

28. Sindermann, C., Rozgonjuk D., Solvak M., Realo A., and Vassil K.. 2023. "Internet Voting: The Role of Personality Traits and Trust across Three Parliamentary Elections in Estonia." Current Psychology 42: 26555–26569. https://doi.org/10.1007/s12144-022-03644-4

29. Springall, D., Finkenauer T., Durumeric Z., Kitcat J., Hursti H., MacAlpine M., and Halderman J. 2014. "Security Analysis of the

Estonian Internet Voting System." Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security: 703–715. https://doi.org/10.1145/2660267.2660315

30. Stockemer, D., Wigginton M. 2024. "The (Complex) Effect of Internet Voting on Turnout: Theoretical and Methodological Considerations." Policy & Internet 16, no. 3: 607–627. https://doi.org/10.1002/poi3.393

31. Turnbull-Dugarte, S., and Devine D. 2023. "Support for Digitising the Ballot Box: A Systematic Review of I-Voting Pilots and a Conjoint Experiment." Electoral Studies 86: 102679. https://doi.org/10.1016/j.electstud.2023.102679

32. Vassil, K., Solvak M., Vinkel P., Trechsel A., and Alvarez R. 2016. "The Diffusion of Internet Voting. Usage Patterns of Internet Voting in Estonia between 2005 and 2015." Government Information Quarterly 33, no. 3: 453–459. https://doi.org/10.1016/j.giq.2016.06.007

33. Venice Commission. 2020. Principles for a Fundamental Rights-Compliant Use of Digital Technologies in Electoral Processes. Strasbourg. https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD%282020%29037-e

Надійшла до редакції / Received: 24.12.2025 *Схвалено до друку / Accepted: 23.03.2026*

Опубліковано / Published: 29.05.2026