DOI: 10.52363/passa-2025.1-13
UDC: 351.746:004.056

Kurilo A., *PhD in Public Administration, senior researcher, National University of Civil Defence of Ukraine, Cherkasy*
ORCID: 0000-0002-5139-0278

ADVANCING OF SOCIO-POLITICAL MECHANISMS FOR MANAGING STATE INFORMATION SECURITY

The article explores the contemporary challenges facing public administration in the domain of information security under the conditions of martial law in Ukraine. The author conducts an analysis of the socio-political mechanisms essential for building an effective system to safeguard the national information space amid hybrid warfare and external aggression by the Russian Federation. Key issues identified include the lack of effective coordination among public authorities, deficiencies in the regulatory and legal framework, and the generally low level of media literacy among the population. In response to these challenges, the author proposes a comprehensive set of measures aimed at enhancing public administration. These include fostering interagency cooperation, reinforcing societal resilience to disinformation, and reforming state information policy to meet the exigencies of wartime conditions.

Keywords: *information security, public administration, martial law, disinformation, information policy, hybrid warfare, state security.*

Formulation of the problem. Amid the full-scale armed aggression of the Russian Federation against Ukraine, the task of ensuring information security has emerged as a critical component of national security. Public administration in this field is confronted with multifaceted threats—ranging from cyberattacks and propaganda to information terrorism directed at eroding public trust in state institutions and destabilizing the societal fabric. This problem is further exacerbated by fragmented governance mechanisms, the absence of a coherent legislative strategy, and the urgent need to adapt to the evolving nature of hybrid aggression.

Analysis of recent research and publications. This study draws on the contributions of both Ukrainian and international scholars (such as O. Senchenko, V. Tertichko, S. Lutsenko, V. Golobutsky, Pocheptsov, O. Danilyan, V. Stepanov, O. Valevsky, B. Kormych, Yu. Dreval, among others), who have explored the challenges of information security in the context of wartime threats. Their research highlights the significance of state policy in combating disinformation campaigns, the role of strategic communications, and the necessity of enhancing digital resilience. Nonetheless, many of these studies fall short in proposing concrete mechanisms for adapting public administration to the realities of hybrid warfare and often lack a holistic perspective on the interaction between political institutions, civil society, and the information landscape.

Problem Statement.The aim of the study is to identify priority areas for improving the socio-political mechanisms of public governance in the field of national information security under martial law conditions. To achieve this goal, the current legal and regulatory framework of Ukraine was analyzed, key problems in the functioning of the public administration system in the information sphere were identified, and practical proposals were developed to enhance interaction mechanisms between state authorities, civil society, and the media.

The resolution of the outlined tasks was carried out using an interdisciplinary approach, which included systems analysis, risk assessment, and the study of real-life cases of countering information threats. The study proposes a set of measures to update the public governance model of information security, including: the establishment of a national information coordination center for interagency cooperation; strengthening the capacity of local self-government bodies to respond to informational challenges; implementation of nationwide media literacy programs for the population; and ensuring robust cybersecurity for the country's critical information infrastructure.

Presenting main material. In the contemporary era marked by the rapid advancement of digital technologies and the global expansion of the information space, the issue of information security has acquired critical importance. Information now serves not only as a resource but also as a strategic instrument capable of fostering societal development or, conversely, destabilizing political systems. This issue has become particularly acute following the imposition of martial law in Ukraine, prompted by the armed aggression of the Russian Federation. In the informational domain, the conflict has taken the form of an intense hybrid

warfare campaign, characterized by disinformation operations, psychological pressure, and cyberattacks targeting critical infrastructure.

As information technologies permeate all facets of life—from government institutions to private communications—ensuring a robust level of information security has become a fundamental condition for safeguarding national sovereignty, institutional stability, and public order. This is especially vital in the context of hybrid warfare, where manipulation of public perception, dissemination of fake news, and deliberate distortion of facts are deployed as tools to shape political outcomes, influence public opinion, and undermine societal resilience [1].

According to Ukraine's Information Security Strategy, the key priorities in this domain include protecting the vital interests of the state and its citizens from the spread of false information, preserving the integrity of information systems, preventing the misuse of digital technologies, and safeguarding public consciousness from manipulation. The relevance of these objectives has significantly increased under the conditions of Russian aggression, where the state must simultaneously confront both conventional military threats and a sophisticated information war [2].

A comprehensive approach to information security encompasses three interdependent dimensions:

State information security — the protection of governmental information systems, prevention of data breaches, mitigation of cyber threats, and defense of critical infrastructure, which has become a primary target of hostile cyberattacks.

Public information security — countering disinformation and psychological operations designed to erode public morale and discredit state institutions.

Personal information security — ensuring the protection of personal data, promoting digital literacy, and fostering a culture of responsible and informed use of information resources.

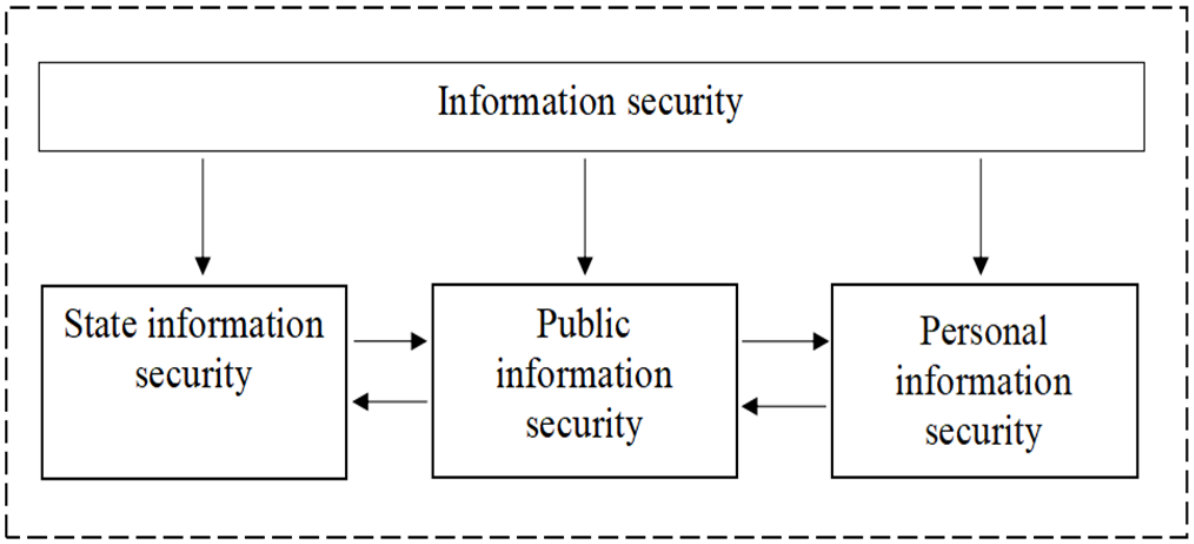

Fig. 1. Systemic expression of information security

Source: author's development

The socio-political mechanism of public administration in the field of information security under martial law must be grounded in the principles of democracy, legality, transparency, and adaptability to emerging threats. Its key components include:

- the development of a robust regulatory and legal framework for cybersecurity;
- effective coordination among public authorities, civil society, and the private sector;
- international cooperation in combating cyber threats;
- strengthening countermeasures against enemy propaganda;
-the establishment of a strategic communications system and the promotion of media literacy.

In the current context of Russia's full-scale war against Ukraine, information security has evolved from being a component of state policy to a critical element of national survival. Particularly dangerous are hostile information operations that aim to incite panic, erode public morale, discredit the Armed Forces of Ukraine, and undermine national identity.

Consequently, enhancing the socio-political mechanism for managing information security requires a comprehensive and systemic approach. This entails improvements in legal regulation, the integration of advanced technologies, and the promotion of public awareness and education. Only through a synergistic interaction between the state, society, and each individual citizen can an effective system for countering information threats be established—threats which, under wartime conditions, pose dangers comparable to conventional military

aggression.

Modern digital communication technologies play an essential role in this struggle, serving as tools for rapid information dissemination, public mobilisation, and the consolidation of national identity. Thus, it is crucial to analyse how the digital environment transforms the interaction between the state and citizens, especially during wartime.

Information and communication technologies have fundamentally reshaped public discourse, government-society interaction, and civic engagement. Under martial law, introduced in response to Russia's military aggression, the Internet has assumed a heightened role as a platform for influence, mobilisation, and protection of the national information domain.

The Internet offers individuals unique opportunities to articulate their views, exchange ideas, and engage others in discussions on socially important issues. This is especially vital for those with limited access to objective information through traditional regional or national media channels. Social networks, blogs, forums, and other digital platforms have become not only channels for alternative or critical viewpoints but also tools for coordinating collective action.

In wartime, the Internet becomes a space for active information resistance. Citizens, volunteers, journalists, military personnel, and analysts use digital tools to disseminate truthful information, debunk disinformation, maintain societal morale, and strengthen Ukraine's international information support.

Several key aspects illustrate the impact of the Internet on the information environment under martial law:

Accessibility and decentralisation of information.
The Internet ensures access to diverse sources of information—including independent media, citizen journalism, and international platforms—allowing for a more comprehensive and objective understanding of the situation, including developments on the battlefield, humanitarian crises, and violations of human rights.

Influence on public opinion. Social media platforms have become central arenas for the rapid spread of information, analysis of societal sentiments, identification of community needs, and the shaping of public discourse. The dissemination of verified information about the war is essential for maintaining public trust, societal unity, and resilience against information warfare.

Coordination and mobilisation. Digital communications facilitate swift organisation and coordination among civic initiatives, volunteer networks, charities, and even military units. Appeals for aid, logistics coordination, and support for affected populations are efficiently managed online. The Internet serves as a decentralised mobilisation mechanism, reducing dependence on hierarchical structures.

Risks of disinformation and information warfare. Despite its advantages, the Internet is also a conduit for fake news, manipulation, and hostile psychological operations. In this context, promoting information hygiene, critical thinking, and media verification becomes a strategic priority.

Cybersecurity, privacy, and data protection. Under martial law, safeguarding digital infrastructure, securing personal data, and protecting communication channels is of paramount importance. Ensuring the privacy of citizens, particularly those in temporarily occupied territories, remains a critical element of the nation's information security framework.

In the current context, public administration must not only regulate the information environment but also ensure equitable access to reliable information at both national and regional levels. This requires a multidimensional approach, including:

- assessing the availability and accessibility of traditional media (print, television, radio) and digital platforms across different regions of Ukraine;

- evaluating the quality and relevance of information content with consideration for linguistic, generational, professional, and socio-cultural diversity of audiences;

- fostering digital inclusion and promoting media literacy among all segments of the population.

Equally important is the reinforcement of an inclusive and sustained information dialogue between the state and civil society. This dialogue must be open, bilateral, and continuous. It should involve not only state institutions but also representatives from local communities, the private sector, academia, educational institutions, youth organisations, and national minorities.

To institutionalise such dialogue, it is recommended to:

- introduce regular public consultations and thematic forums;

- establish online platforms for citizen feedback and communication;

- implement e-democracy instruments (e.g., electronic petitions, online voting tools);

- provide specialised training for public officials on effective public engagement during periods of crisis.

In conditions of armed conflict, inclusiveness, transparency, and accessibility of communication channels become critical. These factors play a pivotal role in fostering public trust, increasing civic engagement, and ensuring the efficiency of information security governance. Under martial law, the ability of public institutions to maintain a steady flow of reliable information and facilitate responsive communication becomes a key determinant of societal cohesion and resilience.

Strengthening the information dialogue between authorities and citizens represents a fundamental element in building an inclusive, transparent, and effective system of public administration. Such a system must be capable of accommodating diverse societal interests, supporting democratic development, and ensuring national information security. The relevance of this issue is heightened under martial law, as the availability of credible information, responsive communication, and opportunities for public participation have a direct impact on social stability, trust in public institutions, and overall national security.

Political will, administrative competence, and sensitivity to public needs are essential prerequisites for addressing wartime challenges effectively. However, dialogue alone is insufficient. It must be supported by tangible policy measures and visible government action that reflects a genuine commitment to solving urgent social problems. A governance system grounded in transparency and responsiveness will enhance the state's capacity to manage information policy and uphold social cohesion [3].

Another critical dimension involves analysing the typology and content of media from the perspective of fostering national cultural and spiritual development, patriotism, and ethical values. In times of external aggression, the media assume a strategic role in maintaining national morale, disseminating knowledge of history and traditions, and cultivating a collective identity. Therefore, it is important to systematically monitor both the quantitative and qualitative indicators of such information initiatives.

Enhancing information and communication technologies—such as interactive television, digital platforms, and online media—constitutes a vital condition for improving media effectiveness. These tools contribute to the democratisation of the information environment, promote transparency in governance, and increase public participation in political life. This

becomes especially important during wartime, when an informed and united society is crucial for national resilience.

Moreover, computer-based technologies play a significant role in supporting public decision-making. Their use enables the simulation of alternative policy scenarios, facilitates the inclusion of public opinion, and helps mitigate the influence of subjective biases.

E-government platforms, in particular, have become instrumental in enhancing civic engagement under conditions of martial law, where traditional forms of citizen-state interaction may be disrupted. These digital systems offer not only access to public services but also tools for submitting appeals, participating in policy consultations, and monitoring government performance. Successful international examples, such as Sweden's Your Voice and South Korea's e-People platforms, demonstrate the transformative potential of e-governance for ensuring transparency and sustained public feedback.

At the same time, caution must be exercised regarding the risks associated with excessive digitalisation of governance processes. As T. Roszak has warned, information technologies may inadvertently contribute to the centralisation of authority and undermine democratic mechanisms. In wartime, such risks are magnified, as information systems could be misused for increased surveillance or control, thereby threatening individual rights and freedoms.

Thus, it is essential to recognise the dual nature of digital technologies in their impact on the state and society. While they enhance informational sovereignty, improve public engagement, and increase administrative efficiency, they also present significant challenges—such as the proliferation of disinformation, propaganda, and radical content—especially during information warfare. Therefore, a key priority of state information security policy should be the development of robust mechanisms for protecting society from manipulation, while simultaneously advancing the principles of digital democracy. This approach is particularly vital in the current security environment, where information resilience has become a cornerstone of national sovereignty and social solidarity.

Under the conditions of martial law in Ukraine, information threats aimed at destabilizing society through the deliberate dissemination of manipulative, destructive, or falsified content have intensified. These threats seek to undermine the moral and psychological resilience of the population, erode trust in state institutions, and foster societal fragmentation. In the realm of public administration, such dynamics open new avenues for influencing public opinion and

reshaping the political orientations of various social groups—often to the advantage of hostile foreign actors or destabilizing domestic forces.

The rapid proliferation and increasing accessibility of technological advancements significantly shape citizens' worldviews, largely through the pervasive influence of digital reality. Virtual environments are increasingly redefining the landscape of modern politics and governance, displacing or distorting traditional mechanisms of public dialogue.

Information technology in politics and public administration presents both opportunities and challenges. On one hand, it facilitates prompt interaction between citizens and the state, enhances transparency, and broadens public engagement in governance processes. On the other hand, it introduces new forms of inequality, impedes access to objective information, and heightens the risk of abuse and digital surveillance. During wartime, these risks are magnified, as information security becomes inextricably linked to national security.

Against this backdrop, the challenge of maintaining a balance between safeguarding the state in the information space and upholding fundamental rights and freedoms—including the right to privacy—assumes particular importance. The protection of personal data, transparency in processing information about individuals, and the promotion of digital literacy are emerging as essential conditions for ensuring societal resilience in the face of modern cyber threats.

In response to these challenges, it is advisable to establish a specialized Privacy Assessment Unit within an independent Digital Security Centre (DSC). This unit could play a pivotal role in developing standards for personal data protection, ensuring compliance with privacy principles, auditing digital platforms, and advising public authorities on the ethical use of data. Moreover, it would contribute to cultivating a culture of digital security in society—an especially vital task in wartime, when information constitutes a strategic asset.

The functions of the Privacy Assessment Unit within the DSC would be instrumental in building a comprehensive system of information security under martial law. These functions would include enhancing public awareness, safeguarding personal data, and strengthening trust in public digital services—particularly critical amid heightened threats from external aggressors.

Key functions may include:

Conducting trainings and seminars: In the context of armed conflict and hybrid threats, disseminating knowledge about personal data protection and digital security is crucial.

Organizing educational initiatives for students, civil servants, critical infrastructure personnel, and the general public will foster a culture of safe digital practices during crises.

Monitoring technological and research trends: Ongoing analysis of emerging digital technologies—especially those actively deployed during the war (e.g., cyber defence, telemedicine, e-governance)—will help assess their implications for privacy and mitigate risks of misuse.

Developing standards and guidelines: Given the exceptional legal regime, there is a pressing need for clear regulations and practical guidelines governing personal data processing in situations such as mobilization, evacuation, social assistance, and the registration of displaced persons.

Conducting vulnerability assessments: Regular audits of data processing systems used in wartime contexts (e.g., military administrations, humanitarian centres) will help identify security gaps and minimize risks of unauthorized access.

Ensuring legal compliance: In light of temporary restrictions on certain rights, it is essential to provide expert guidance on adherence to national and international data protection legislation, particularly in decisions made under martial law.

Research and evaluation of data practices: Analyzing how data is collected and used—by both governmental and non-governmental actors, including international organizations—will help evaluate whether such practices comply with ethical and legal standards during wartime.

Certification and auditing services: Independent certification of personal data processing systems within public and private institutions will bolster confidence in their security amidst increased digital workloads and cyberattacks.

Developing privacy policy recommendations: Tailored privacy policies for sectors critical to wartime functioning—such as education, healthcare, logistics, and defence—will contribute to the stability and resilience of governance systems.

Engaging with the public and media: Transparent, proactive communication regarding personal data risks, protection mechanisms, and timely responses to inquiries from journalists, volunteers, and human rights defenders are vital components of public trust.

In addition to these functional responsibilities, the independence of the Digital Security Centre must be ensured for its effective operation. Its organizational structure should incorporate mechanisms of autonomous oversight, free from political or administrative

interference. One such mechanism could be the establishment of a supervisory board composed of representatives from academic institutions, civil society organizations, human rights entities, and journalistic associations. In a time of martial law, such public involvement is not only a safeguard against authoritarian tendencies but also a key factor in maintaining confidence in the state as a guarantor of digital rights.

The legal status, authority, and procedures for forming the governing bodies of the DSC should be clearly articulated in dedicated legislation—or even constitutionally enshrined—to prevent politicization or undue influence from any branch of government. This approach would facilitate the creation of a truly independent institution, capable of operating effectively under emergency conditions.

Conclusions. Achieving effective public administration in the realm of information security under martial law necessitates a comprehensive modernisation of the existing socio-political mechanisms. It is imperative to develop a coherent and forward-looking state policy that not only addresses current information threats but also anticipates future challenges in a proactive and strategic manner. Central to this effort is the establishment of resilient and coordinated interaction among government institutions, civil society, and the media sector.

The approaches outlined in this article are intended to support the enhancement of national information security and to foster greater societal resilience in the face of hybrid threats. By integrating legal, technological, and communicative strategies, Ukraine can strengthen its capacity to protect the national information space and ensure long-term stability in the context of ongoing external aggression.

References:

1. Horbulin, V. P., Dodonov, O. H., & Lande, D. V. Information operations and societal security: Threats, counteraction, modeling (Monograph). Kyiv: Intertekhnolohiia, 2009. 164 p.
2. On the Information Security Strategy. Decree of the President of Ukraine dated 25.02.2017 No. 447/2021 URL: https://zakon.rada.gov.ua/go/447/2021 (accessed: 03.05.2024)
3. Averyanova N.M. Hybrid war: Russian-Ukrainian confrontation. Young Scientist, 2017. No. 3 (43). P. 30-34

4. Marits, D. O. (2018). The right to anonymity as an inalienable human right. Entrepreneurship, Economy and Law, 2, 160–164. Retrieved March 23, 2024, from http://www.pgp-journal.kiev.ua/archive/2018/2/30.pdf
5. Razmietaeva, Y. S. (2016). Privacy in the information society: Issues of legal understanding and regulation. Scientific Bulletin of Uzhhorod National University. Series: Law, 37(1), 43–46.