

# OPTIMIZATION OF THE PUBLIC GOVERNANCE SYSTEM IN THE NATIONAL SECURITY OF UKRAINE IN VIEW OF HYBRID THREATS

**Oksana Marukhlenko**

*Borys Grinchenko Kyiv Metropolitan University  
Bulvarno-Kudriavska Str., 18/2, Kyiv, Ukraine*

**Nazariy Sitsinskiy**

*Interregional Academy of Personnel Management  
Frometivska Str., 2, Kyiv 03039, Ukraine*

**Andrii Repchonok**

*Leonid Yuzkov Khmelnytskyi University of Management and Law  
Heroes of Maidan Str., 8, Khmelnytskyi, Ukraine*

**Yana Lutsenko**

*National Academy of Security Service of Ukraine  
Mykhaila Maksymovycha Str., 22, Kyiv, Ukraine*

**Serhii Kuzmenko**

*Donetsk State University of Internal Affairs  
Velyka Perspektivna Str., 1, Kropyvnytskyi, Ukraine*

DOI: 10.13165/VPA-26-25-2-03

**Abstract.** *The article examines the issue of optimizing the public governance system in the national security of Ukraine in view of the growing hybrid threats. The aim of the study was to identify structural imbalances to find the role of public governance as a factor in strengthening national security. The research employed the following methods: an integrative approach that combines elements of content analysis of strategic documents, indicator assessment, data normalization, construction of an Integral Index of National Security, and graphical analysis. The need to transform traditional governance approaches is emphasized, taking into account the multidimensionality of current challenges. The proposed Integral Index of National Security covers key areas: military, political, economic, social, and cyberinformation. The results of the assessment demonstrate an imbalance between priority (military and cyber) and vulnerable*

*(economic and political) components. The need for the implementation of hybridized public administration, integrating public and private resources, is identified, and the importance of proactive threat forecasting is emphasized. Conceptual models of management response to hybrid threats are proposed, which involve the active integration of civil society, digital technologies, and the private sector into security processes.*

**Keywords:** national security, hybrid threats, governance, vulnerability, terrorism, security policy, public administration

**Reikšminiai žodžiai:** nacionalinis saugumas, hibridinės grėsmės, valdymas, pažeidžiamumas, terorizmas, saugumo politika, viešasis administravimas.

## Introduction

The current global security environment is characterized by complexity and dynamism and requires a review of traditional approaches to national security and public governance. Under conditions of an ongoing full-scale hybrid war against Ukraine, optimization of the public governance system in the field of national security holds critical importance, since existing mechanisms often prove inert when facing asymmetric threats. The state response must combine institutional stability, digital security, multilevel coordination, and anti-corruption mechanisms. The traditional vision of security, focused mainly on military defense, has significantly expanded to encompass a multidimensional understanding of approaches that go beyond purely military aspects (Loshytskyi et al. 2023).

The research gap lies in the absence of an integrated conceptual model that enables proactive public governance under conditions where the boundary between peacetime and wartime is blurred. The national security system of Ukraine is viewed as a multidimensional construct that integrates economic resilience, political stability, technological advantage, and legal certainty. The main issue is to optimize the public governance system for effective security management in various areas, including cyberspace, psychological impact, and socio-political dimensions (Viter and Rudenko 2025).

The aim of the research is to study the directions of optimization of public governance in the sphere of national security of Ukraine in the conditions of hybrid threats, with emphasis on the formation of paradigms for ensuring the national interests of the state. Based on the above, the study formulates the following research objectives:

- Identify imbalances in the implementation of public governance in the field of security
- Determine the integrated level of national security on the basis of available indicators
- Develop conceptual approaches to an optimal governance model for responding to hybrid threats

National security in the study is considered an object of public policy, which implies an

analysis of the policy-making cycle, from threat identification to the selection of regulatory instruments. The relevance of the methodology is driven by the need to transition toward evidence-based public policy, where managerial decisions are grounded in quantitative measurement of the system resilience index.

## Literature Review

Security no longer refers only to territorial defense but is understood as the capacity of society for rapid recovery. The traditional paradigm of public administration, grounded in rigid hierarchy and *realpolitik*, now conflicts with the modern paradigm of network security, which emphasizes decentralization and the involvement of non-state actors. This study relies on the paradigm of hybridized governance, which combines strategic state leadership with the flexibility of civil society.

Nilsson et al. (2025) and Khidasheli (2024) agree that the main threat of hybrid attacks is their ambiguity and ability to operate below the threshold of traditional military responses. At the same time, other features have been emphasized. Nilsson et al. (2025) provide more detail on the range of sectors in which they manifest themselves, while Khidasheli (2024) emphasizes the difficulties of detection and counteraction. The issue of EU security policy formation arises, especially in the context of the fight against terrorism and for Eastern European countries. Kryshchanovych et al. (2022) consider security mainly through the prism of European integration processes and the challenges of terrorism, while Bondarenko et al. (2022) focus on the internal structural shortcomings of the national security system of Ukraine.

Goncharuk et al. (2023) and Schmitt and Koutroumpis (2025) agree on the importance of digital resilience and the role of technology but differ on the proposed tools. Goncharuk et al. (2023) analyze public governance reform in general, while Schmitt and Koutroumpis (2025) focus specifically on artificial intelligence (AI) as a tool to counter cyberthreats. The novelty of this study, compared with existing research, lies in the development of an original Integral Index of Ukraine's National Security (IIUNS). Unlike general governance indices, the index focuses on the points of interaction between public administration mechanisms and security indicators under conditions of martial law.

## Method

### Research design

The research procedure consisted of the following stages:

- 1) Determining the level of progress in optimizing public governance in the national security based on the adoption of the National Security Strategy of Ukraine (President of

Ukraine 2020) for 2021–2024 and indicators reflecting the results of the strategy's implementation (Democracy Index, World Governance Indicators, Cybersecurity Index, Corruption Index, Rule of Law Index, Terrorism Index)

2) Analyzing the dynamics of public governance indicators for 2019–2023 (World Bank 2023)

3) Calculating the Integral Index of National Security of Ukraine based on the author's methodology

## Methods

Different time horizons are deliberately applied across analytical stages. A comparison between 2021 and 2024 enables assessment of the impact of the National Security Strategy of Ukraine before and during the active phase of the war, while data for 2019–2023 support analysis of long-term trends in state regulation. The IIUNS calculation relies on data available at the beginning of 2024, reflecting the current condition of the system. It is important to note that under wartime conditions, data collection is constrained; the use of indicators from international institutions constitutes a necessary measure to ensure the objectivity and validity of the results.

In order to determine the results of the implementation of the National Security Strategy of Ukraine, the indicator monitoring method was applied. The method of a graphical comparison was used to clarify the dynamics of the implementation of public governance functions in terms of the efficiency of state authorities and the capacity of regulatory activities for 2019–2023 (with the latest data available). The level of national security of Ukraine was determined by using the author's method of the IIUNS.

## Sample

Five key areas (military, political, economic, social, and cyberinformation) were used to select the components of the IIUNS, with each area characterized by two specific indicators. Each reflects critical dimensions of the functioning of the national security space in accordance with the provisions of the National Security Doctrine of Ukraine (Verkhovna Rada of Ukraine 2018; President of Ukraine 2020) and the approaches of NATO (NATO 2022). The corresponding indicators are distributed as follows:

- Military sphere: Defense spending (% of GDP) (SIPRI 2025), GFP Index (Global Firepower 2026)

- Political sphere: Stability Index (WGI) (World Bank 2023), Democracy Index (EIU) (Economist Intelligence Unit 2024)

- Economic sphere: GDP per capita (World Bank 2024), inflation rate (International Monetary Fund 2026)

- Social sphere: Human Development Index (United Nations Development Programme 2025), unemployment rate (World Bank 2021)

- Cyberinformation sphere: Cybersecurity Index (International Telecommunication Union 2025), e-government survey (United Nations 2024)

The capabilities of Microsoft Excel and gretl were used as tools.

The IIUNS was calculated by using the formula:

$$IIUNS = \sum (w_i \times S_i),$$

$$\text{where } S_i = (I_{i1} + I_{i2})/2,$$

where  $S_i$ —security sub-indices (military, political, etc.);  $w_i$ —sphere weight (determined by the entropy method to objectify the impact of indicators on data variance);  $I_{i1}$  and  $I_{i2}$ —indicators' Min–Max values. Reverse normalization was applied for indicators with negative interpretation (unemployment, GFP rating).

The use of a linear additive model combined with the entropy method for determining weighting coefficients  $w_i$  makes the contribution of each domain objective. Weights follow data dispersion. Higher variability leads to higher weight. Such a rule reduces the risk of subjective neutralization of critical problems within a specific domain. Min–Max normalization aligns heterogeneous measurement units to a common scale from 0 to 1.

The interpretation of the result is possible according to the corresponding scale of the IIUNS value: from 0.8 to 1.0—high level of national security; from 0.6 to 0.79—acceptable level, requires improvement; from 0.4 to 0.59—increased risk, turbulence zone; from 0 to 0.39—critical threat to national security. Threshold values rely on widely accepted development index assessment approaches, including the UNDP Human Development Index. This approach enables comparison of the obtained results with those of other countries under conflict conditions.

## Results

Monitoring the indicators of implementation of the National Security Strategy of Ukraine (Table 1) is treated as an instrument for assessing public policy effectiveness. The results indicate that the most substantial progress occurred in policy priority areas, particularly cybersecurity and digital transformation, where the Cybersecurity Index increased from 65.93 to 83.93. At the same time, a decline in the Democracy Index from 5.57 to 4.9 serves as a direct indicator of the temporary restriction of selected political instruments in order to secure national defense.

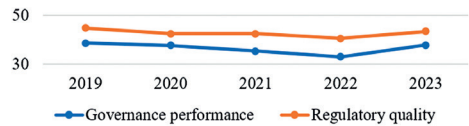
**Table 1.** Key directions for the implementation of the National Security Strategy of Ukraine and the dynamics of its changes

| Action (Strategy Section)                                 | Description                                                                                     | Index                                         |        |
|-----------------------------------------------------------|-------------------------------------------------------------------------------------------------|-----------------------------------------------|--------|
|                                                           |                                                                                                 | 2021                                          | 2024   |
| Strengthening democratic civilian oversight (IV, 63)      | Ensuring the legality of the actions of security agencies through democratic control mechanisms | Democracy Index                               |        |
|                                                           |                                                                                                 | 5.57                                          | 4.9    |
| Improving governance and accountability (IV, 63)          | Increasing the efficiency and transparency of the work of government agencies                   | Worldwide Governance Indicators               |        |
|                                                           |                                                                                                 | 35.24                                         | 37.74  |
|                                                           |                                                                                                 | Regulatory Quality                            |        |
|                                                           |                                                                                                 | 42.38                                         | 43.40  |
| Strengthening the national cybersecurity system (III, 52) | Modern capabilities of cybersecurity and cyber defense entities                                 | Cybersecurity Index                           |        |
|                                                           |                                                                                                 | 65.93                                         | 83.93  |
| Eliminating anti-corruption (III, 53)                     | Increasing transparency and accountability of state bodies to reduce corruption                 | Corruption Index                              |        |
|                                                           |                                                                                                 | 32                                            | 35     |
| Advocating justice reform (III, 53)                       | Improving access to justice and fair justice                                                    | World Justice Project (WJP) Rule of Law Index |        |
|                                                           |                                                                                                 | 0.51                                          | 0.49   |
| Implementing digital transformation (III, 51)             | Introducing IT technologies to simplify access to public services and improve their quality     | eGovernance Index                             |        |
|                                                           |                                                                                                 | 0.8029                                        | 0.8841 |
| Countering challenges for law enforcement (III, 45)       | Countering separatism, terrorism, and extremism                                                 | Terrorism Index                               |        |
|                                                           |                                                                                                 | 2.304                                         | 1.686  |

Source: Created by the authors based on World Bank (2023), Economist Intelligence Unit (2024), International Telecommunication Union (2025), Transparency International (2024), World Justice Project (2024), United Nations (2024), Institute for Economics & Peace (2024), President of Ukraine (2020).

A moderate improvement in the fight against corruption indicates increased transparency in public administration. A deterioration in the Rule of Law Index indicates a slowdown in reform processes in the justice sector. The decreased Terrorism Index indicates a strengthening of internal security and counterterrorism. Overall, current trends indicate an asymmetric development of national security sectors.

We track the dynamics of the implementation of public governance functions in terms of the efficiency of state authorities and the capacity of regulatory activities for 2019–2023 (Figure 1).



**Figure 1.** Dynamics of public governance indicators (World Bank 2023)  
Source: Developed by the authors

An analysis of the dynamics of public governance indicators for 2019–2023 (Figure 1) demonstrates the stability of “Regulatory Quality” relative to “Government Effectiveness.” This pattern indicates that Ukraine’s security-related legal and regulatory framework proved more resilient to systemic shocks than the operational mechanisms of the executive branch.

In accordance with the specified research methodology, the data of the IIUNS components are shown below (Table 2). To ensure transparency of the IIUNS calculations, raw statistical data were processed using Min–Max normalization, which reduced them to a unified scale of [0;1]. The use of the entropy method to determine weighting coefficients eliminated the subjectivity inherent in expert surveys. The calculations showed that the military and cyberinformation ( $w = 0.25$ ) sectors exert the greatest influence on data dispersion and, accordingly, on the overall level of security.

**Table 2.** The author’s calculation of the IIUNS component values

| Sector            | Indicator                                                                | Normalized | Subindex |
|-------------------|--------------------------------------------------------------------------|------------|----------|
| Military          | Defense spending in GDP (34.48%) (SIPRI 2025)                            | 1          | 0.97615  |
|                   | GFP index (0.369) (Global Firepower 2026)                                | 0.9523     |          |
| Political         | Stability Index (-1.43) (World Bank 2023)                                | 0.2908     | 0.3886   |
|                   | Democracy Index (4.9) (Economist Intelligence Unit 2024)                 | 0.4864     |          |
| Economic          | GDP per capita (5389.5 USD) (World Bank 2024)                            | 0.0204     | 0.0904   |
|                   | Inflation Rate (12.6%) (International Monetary Fund 2026)                | 0.07       |          |
| Social            | HDI (0.779) (UNDP 2025)                                                  | 0.6695     | 0.6934   |
|                   | Unemployment rate (9.8%) (World Bank 2021)                               | 0.7173     |          |
| Cyber-information | Cybersecurity Index (83.93) (International Telecommunication Union 2025) | 0.8357     | 0.86135  |
|                   | E-Government Survey (0.8841) (United Nations 2024)                       | 0.8870     |          |

Source: Developed by the authors

The contribution of each component to the overall model is shown in Table 3. The political sector and the economic component received low values.

**Table 3.** Components of the IIUNS model

| Sector           | Subindex | Sector Weights | Contribution |
|------------------|----------|----------------|--------------|
| Military         | 0.97615  | 0.25           | 0.24         |
| Political        | 0.3886   | 0.2            | 0.08         |
| Economic         | 0.0904   | 0.1            | 0.01         |
| Social           | 0.6934   | 0.2            | 0.14         |
| Cyberinformation | 0.86135  | 0.25           | 0.22         |

Source: Developed by the authors

To test model reliability, a sensitivity analysis was conducted. When weighting coefficients varied within  $\pm 10\%$ , the IIUNS value remained within the range of 0.67–0.71, which confirms the stability of the obtained result (0.69) and its classification within the “acceptable level” zone. Model validation through comparison with real-world events confirmed that a sharp increase in the military sub-index (0.97) correlates with the actual rearmament of the Armed Forces of Ukraine and the transition to NATO standards, as reflected in the Global Firepower ranking.

The lowest values are in the political and economic spheres, which require increased optimization of public governance and economic activity. The model verification showed that the standard deviation for different aggregation methods is  $\sigma = 0.03$ . The identified asymmetry in sectoral development (Table 3) does not represent an accidental governance failure. It reflects a deliberate choice of state policy priorities under conditions of limited resources. The low contribution of the economic sector (0.01) and the political sector (0.08) indicates the vulnerability of civilian institutions, which are sacrificed to maintain a critical level of defense capability. This finding supports our argument for a transition toward a hybridized model in which economic resilience is integrated into defense planning as an equal component.

Based on the results of the study, a comparative analysis with the experience of Israel is conducted. Israel’s military spending in 2024 increased by 65%, reaching approximately 8.8% of GDP (\$46.5 billion), which is comparable to Ukraine’s (\$64.7 billion) (SIPRI 2025). In the cyberinformation sector, Israel updated its National Cybersecurity Strategy, emphasizing a comprehensive approach to strengthening national cyber resilience (INCO 2025), which reflects a similar Ukrainian trend in the growth of the Cybersecurity Index.

Discussion

Optimizing Ukraine’s public governance system in the field of national security in the context of hybrid threats is a multifaceted and key task. The obtained results are confirmed in the studies that emphasize a proactive approach (Ferris et al. 2025), which indicates a fundamental paradigm shift in national security. The specified change consists of a shift

from a reactive model, defined as a response to an act of aggression, to a preventive “state-as-sensor” model capable of identifying hybrid influences at the stage of their emergence. Separate works also coincide with the author’s conclusions that public administration should actively shape the security environment (Viter and Rudenko 2025) and prevent threats before they escalate.

The complexity of hybrid threats makes interoperability and standardization critical for effective optimization of public administration. The ultimate goal is to build a system where information flows freely, actions are precisely coordinated, and vulnerabilities are minimized, thereby enhancing overall national security (Jungwirth et al. 2023), which is consistent with the obtained results.

The study of Aristovnik et al. (2022) confirms our conclusion about the coexistence of different management models within the framework of one public administration system, demonstrating that elements of different models complement, rather than replace, each other. This correlates with our results on the asymmetric development of national security sectors and the need for hybridized public administration. Similarly, the study on the digital transformation of public administration in the face of constant threats emphasizes that digital transformation has become a necessity for the state in response to crises, which is consistent with our conclusions about the dominance of the cyberinformation component in the IIUNS (Eom and Lee 2022).

At the same time, existing studies emphasize the primacy of economic security as the basis of national security, which differs from our results. The emphasis is on the integration of economic security and national security, demonstrating an integrated approach to economic and national security, which contrasts with our model, where the economic component is given low priority (Vakkuri et al. 2025).

The dynamics of democratic indicators require separate attention. The decline in the Rule of Law Index from 0.51 to 0.49 and in the Democracy Index from 5.57 to 4.9 is statistically significant and reflects objective restrictions on rights and freedoms associated with martial law. In our view, a direct correlation exists. Stronger security control aimed at reducing the “terrorism index” inevitably leads to a temporary narrowing of democratic space.

For comparative validation of our model, Israel was selected as a country with a similar profile of security threats. A comparison of military expenditures, 8.8% of GDP in Israel versus over 30% in Ukraine, and updated cybersecurity strategies (INCO 2025) shows that successful optimization of governance under conditions of war requires the creation of a “security ecosystem” in which the private sector becomes the driver of the economy.

Based on the obtained results, several approaches can be proposed for the formation of optimal public governance systems in the field of national security (Table 4).

**Table 4.** Comparative analysis of models for resilience to hybrid threats

| Model name                              | Main focus                                                                                                      | Contribution to the optimization of public governance                                                                                                                                                   | Relevance for Ukraine                                                                                       |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| Integrated resilience system            | Systemic resilience of society as a whole to hybrid threats; strategic decision-making support for policymakers | Provides a holistic understanding of societal vulnerabilities, guides systemic resilience building, allows for impact monitoring, and serves as a strategic framework for comprehensive countermeasures | Provides a basis for a holistic approach to Ukraine’s national security in the context of hybrid aggression |
| Tactical action model                   | Emphasis on short-term responses versus long-term resilience building                                           | Emphasizes the need for dynamic adaptation, continuous vulnerability identification, and understanding the interplay between immediate responses and long-term resilience                               | Helps to plan both immediate and strategic measures                                                         |
| Concept of hybridized public governance | Understanding and managing hybridity in the context of public governance                                        | A foundation for the development of effective organizational structures and governance mechanisms to support stakeholder cooperation, goal alignment management, and accountability                     | Provides tools for integrating civil society and the private sector into the security system                |

Source: Developed by the authors

The models proposed by the authors (Table 4) shift the paradigm of public administration in Ukraine toward a hybridized governance framework. The most significant obstacle to implementation lies in the need for deep reform of the law enforcement and judicial systems, since, in the absence of institutional trust, the involvement of civil society in security processes remains fragmented.

The limitations of this study include the following:

- The use of a linear aggregation formula tends to smooth extreme failures in individual subsectors, which necessitates a future transition to nonlinear multiplicative models.
- Time lags in reports produced by international organizations do not fully capture operational changes in governance systems.
- The high intensity and volatility of military operations render any predictive models short-term in nature.

Despite these limitations, the proposed methodology and models are transferable and adaptable to other countries experiencing sustained pressure from hybrid threats and requiring rapid transformation of the public sector. In contrast to traditional approaches, our model proposes a concept of hybridized public governance and specific public policy instruments for integrating civil society into security decision-making processes. The outcome is a predictive model for responding to asymmetric influences.

## Conclusions

1. The study confirmed that traditional hierarchical structures under conditions of full-scale aggression need to be replaced with proactive and networked management mechanisms. The main result of the work was the creation of the Integral Index of National Security of Ukraine, which covers five key areas (military, political, economic, social, and cyberinformation) and allows for a quantitative assessment of the level of state security. The calculated index (IIUNS = 0.69) indicates a very acceptable level of security in wartime.
2. The assessment results revealed a profound asymmetry: high levels of military and cybersecurity coexist with critical vulnerabilities in the economic and political sectors. This imbalance is a consequence of the total concentration of resources on defense needs, which is justified in the short term. The interdependence between security measures and the state of democracy was confirmed. A decline in democracy and rule-of-law indices alongside improvements in counterterrorism performance indicates a complex “security trade-off” that Ukraine is experiencing.
3. Complementary models of public governance are proposed: a comprehensive resilience system, a tactical response model, and a concept of hybridized public administration, which together form a multi-level response to hybrid challenges. The models have high potential for generalization and can be used by other countries (in particular, the Baltic and Eastern European states) facing hybrid threats, serving as a roadmap for strengthening national resilience.
4. For further optimization of the public governance system in the field of Ukraine’s national security, with due regard to hybrid threats, it is proposed to develop legislative instruments to formalize the participation of the private sector and civil society in security processes based on cofinancing and joint governance mechanisms. Additionally, it is advisable to implement common standards for operational coordination and information sharing among all actors within the security sector. Further research should focus on developing dynamic monitoring tools that account for the nonlinear nature of hybrid influences and allow for real-time adjustment of state policy.

## Data Availability Statement

The data used to support the findings of this research are available from the corresponding authors upon request.

## References

1. Aristovnik, A., E. Murko, and D. Ravšelj. From neo-weberian to hybrid governance models in public administration: Differences between state and local self-government. *Administrative Sciences*, 2022, Vol. 12, No. 1, p. 26. <https://doi.org/10.3390/admsci12010026>.
2. Atlantic Council. Advancing freedom, defeating authoritarianism: A democracy agenda for 2025-2029. 2024. <https://www.atlanticcouncil.org/in-depth-research-reports/report/advancing-freedom-defeating-authoritarianism-a-democracy-agenda-for-2025-2029/>.
3. Bondarenko, S. et al. Improving the state system of strategic planning of national security in the context of informatization of society. *Journal of Information Technology Management*, 2022, Vol. 14, p. 1–24. [https://dspace.nadpsu.edu.ua/bitstream/123456789/4515/1/JITM\\_Volume%2014\\_Issue%20Special%20Issue\\_%20Digitalization%20of%20Socio-Economic%20Processes\\_Pages%201-24.pdf](https://dspace.nadpsu.edu.ua/bitstream/123456789/4515/1/JITM_Volume%2014_Issue%20Special%20Issue_%20Digitalization%20of%20Socio-Economic%20Processes_Pages%201-24.pdf)
4. Economist Intelligence Unit. The democracy index. 2024. <https://www.eiu.com/n/global-themes/democracy-index/>.
5. Eom, S. J., and J. Lee. Digital government transformation in turbulent times: Responses, challenges, and future direction. *Government Information Quarterly*, 2022, Vol. 39, No. 2, 101690. <https://doi.org/10.1016/j.giq.2022.101690>.
6. Ferris, S. P., and R. M. Ferris. The market knows best: Using data from prediction markets to assess national security threats. *Military Intelligence Professional Bulletin*, 2025. <https://mipb.ikn.army.mil/issues/jul-dec-2025/the-market-knows-best/>.
7. Global Firepower. 2026 military strength ranking. 2026. <https://www.globalfirepower.com/countries-listing.php>.
8. Goncharuk, N. et al. Reformation public governance in Ukraine in the context of European integration: Current state, problems and priorities. *Economic Affairs*, 2023, Vol. 68, No. 3, p. 1613–27. <http://dx.doi.org/10.46852/0424-2513.3.2023.27>.
9. INCO. Israel national cyber security strategy 2025. 2025. [https://www.gov.il/BlobFolder/news/cyber\\_strategy\\_2025/he/israel\\_national\\_cybersecurity\\_strategy\\_feb2025.pdf](https://www.gov.il/BlobFolder/news/cyber_strategy_2025/he/israel_national_cybersecurity_strategy_feb2025.pdf).
10. Institute for Economics & Peace. Global peace index 2024. 2024. <https://www.economicsandpeace.org/wp-content/uploads/2024/06/GPI-2024-web.pdf>.
11. International Monetary Fund. Inflation rate, average consumer prices. 2026. [https://www.imf.org/external/datamapper/PCPIPCH@WEO/OEMDC/ADVEC/WEO\\_WORLD](https://www.imf.org/external/datamapper/PCPIPCH@WEO/OEMDC/ADVEC/WEO_WORLD).
12. International Telecommunication Union. Global cybersecurity index 2024. 2025. <https://www.itu.int/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx>.
13. Jungwirth, R. et al. Hybrid threats: A comprehensive resilience ecosystem. Publications Office of the European Union, 2023. <https://doi.org/10.2760/37899>.
14. Khidasheli, T. Hybrid threats and resilience. Friedrich Naumann Foundation, 2024. <https://www.freiheit.org/sites/default/files/2024-12/hybrid-threats-and-resilience-final.pdf>.
15. Kryshchanovych, M. et al. Problems of European integration in the construction of EU security policy in the context of counter-terrorism. *International Journal of Safety and Security Engineering*, 2022, Vol. 12, No. 4, p. 501–6. <https://doi.org/10.18280/ijss.120411>.
16. Loshytskiy, M. et al. Modern realities of ensuring the national security of Ukraine in conditions of armed aggression. *Research Revolution*, 2023, Vol. 8, No. 1, p. 157–82. <https://remittancesreview.com/menu-script/index.php/remittances/article/view/306/175>.

17. NATO. NATO 2022 strategic concept. 2022. <https://www.nato.int/en/about-us/official-texts-and-resources/strategic-concepts/nato-2022-strategic-concept>.
18. Nilsson, N., M. Weissmann, and B. Palmertz. Hybrid threats and the intelligence community: Priming for a volatile age. *International Journal of Intelligence and Counterintelligence*, 2025, p. 1–23. <https://doi.org/10.1080/08850607.2024.2435265>.
19. President of Ukraine. National security of Ukraine strategy (Decree No. 392/2020). 2020. <https://zakon.rada.gov.ua/laws/show/392/2020#n12>.
20. Schmitt, M., and P. Koutroumpis. Cyber shadows: Neutralizing security threats with AI and targeted policy measures. *IEEE Transactions on Artificial Intelligence*, 2025. <https://doi.org/10.48550/arXiv.2501.09025>.
21. SIPRI. SIPRI military expenditure database. 2025. <https://doi.org/10.55163/CQGC9685>.
22. Transparency International. Corruption perceptions index. 2024. <https://www.transparency.org/en/cpi/2024>.
23. United Nations Development Programme. Human development insights. 2025. <https://hdr.undp.org/data-center/country-insights#/ranks>.
24. United Nations. UN e-government survey 2024. 2024. <https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2024>.
25. Vakkuri, J., J. Johanson, R. Pinheiro, and T. Erkkilä. Public policies for hybrid governance – Introduction. In *Public Policies for Hybrid Governance* (pp. 1–18). Northampton: Edward Elgar Publishing, 2025. <https://doi.org/10.4337/9781035311637.00011>.
26. Verkhovna Rada of Ukraine. On the national security of Ukraine (Law No. 2469-VIII). 2018. <https://zakon.rada.gov.ua/laws/show/2469-19#n355>.
27. Viter, D., and O. Rudenko. National security in the multi-domain environment: Public administration issues. *Public Administration and Law Review*, 2025, Vol. 1, No. 21, p. 40–49. <https://doi.org/10.36690/2674-5216-2025-1-40-49>.
28. World Bank. Unemployment, total (% of total labor force). 2021. <https://data.worldbank.org/indicator/SL.UEM.TOTL.ZS?end=2024&start=1991&view=chart>.
29. World Bank. Interactive data access. n.d. <https://www.worldbank.org/en/publication/worldwide-governance-indicators/interactive-data-access>.
30. World Bank. GDP per capita (current US\$). 2024. <https://data.worldbank.org/indicator/NY.GDP.PCAP.CD?view=chart>.
31. World Justice Project. WJP rule of law index. 2024. <https://worldjusticeproject.org/rule-of-law-index/global/2024/historical>.

O. Marukhlenko, N. Sitsinskiy, A. Repchonok, Y. Lutsenko, S. Kuzmenko

## UKRAINOS NACIONALINIO SAUGUMO VIEŠOJO VALDYMO SISTEMOJE OPTIMIZAVIMAS, ATSIŽVELGIANT Į HIBRIDINES GRĖSMES

**Santrauka.** *Straipsnyje nagrinėjamas viešojo valdymo sistemos optimizavimo Ukrainos nacionalinio saugumo srityje klausimas, atsižvelgiant į augančias hibridines grėsmes. Tyrimo tikslas buvo nustatyti struktūrinius disbalansus, siekiant išsiaiškinti viešojo valdymo, kaip nacionalinio saugumo stiprinimo veiksnio, vaidmenį. Tyrime taikyti šie metodai: integruotas*

*požiūris, apjungiantis strateginių dokumentų turinio analizės elementus, rodiklių vertinimą, duomenų normalizavimą ir integralaus nacionalinio saugumo indekso sudarymą, grafinę analizę. Akcentuojamas poreikis transformuoti tradicinius valdymo metodus, atsižvelgiant į dabartinių iššūkių daugialypiškumą. Siūlomas integralus nacionalinio saugumo indeksas apima pagrindines sritis: karinį, politinį, ekonominį, socialinį ir kibernetinės informacijos. Vertinimo rezultatai rodo disbalansą tarp prioritetinių (karinių ir kibernetinių) ir pažeidžiamų (ekonominių ir politinių) komponentų. Nustatytas hibridizuoto viešojo administravimo, integruojančio viešuosius ir privačius išteklius, įgyvendinimo poreikis ir pabrėžiama proaktyvaus grėsmių prognozavimo svarba. Siūlomi konceptualūs valdymo reagavimo į hibridines grėsmes modeliai, apimantys aktyvų pilietinės visuomenės, skaitmeninių technologijų ir privačiojo sektoriaus integravimą į saugumo procesus.*

---

**Oksana Marukhlenko**

Doctor of Science in Public Administration, Associate Professor, Professor of the Department of Management, Faculty of Economics and Management, Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine. <https://orcid.org/0000-0001-8050-6615>  
Email: oksana.marukhlenko3@yahoo.com

**Nazariy Sitsinskiy**

Doctor of Science in Public Administration, Professor of the Department of Public Management and Administration, Interregional Academy of Personnel Management, Kyiv, Ukraine. <https://orcid.org/0009-0005-3179-6878>  
Email: urijsosnickij32@gmail.com (the author is a correspondent)

**Andrii Repchonok**

Doctor of Philosophy in Law, Associate Professor of the Department of Criminal Law and Procedure, Leonid Yuzkov Khmelnytskyi University of Management and Law, Khmelnytskyi, Ukraine. <https://orcid.org/0009-0007-4122-1124>  
Email: repchonok.andriy12@ukr.net

**Yana Lutsenko**

PhD in Law, Associate Professor of the Educational and Scientific Institute of State Security, National Academy of Security Service of Ukraine, Kyiv, Ukraine.  
<https://orcid.org/0000-0001-9780-4387>  
Email: yana.lutsenkoo1@gmail.com

**Serhii Kuzmenko**

Doctor of Science in Public Administration, PhD in Law, Professor of the Department of Economics and Public Administration, Educational and Scientific Institute of Law and Social Management, Donetsk State University of Internal Affairs, Kropyvnytskyi, Ukraine.

<https://orcid.org/0000-0002-5325-9433>

Email: [serhii.kuzmenkoo12@gmail.com](mailto:serhii.kuzmenkoo12@gmail.com)

---

### **Oksana Maruhlenko**

Viešojo administravimo mokslų daktaras, docentas, Vadybos katedros profesorius, Ekonomikos ir vadybos fakultetas, Boryso Grinčenkos Kijevo metropolijos universitetas, Kijevas, Ukraina. <https://orcid.org/0000-0001-8050-6615>

El. paštas: [oksana.marukhlenko3@yahoo.com](mailto:oksana.marukhlenko3@yahoo.com)

### **Nazariy Sicinskiy**

viešojo administravimo mokslų daktaras, Viešojo valdymo ir administravimo katedros profesorius, Tarpreregioninė personalo valdymo akademija, Kijevas, Ukraina.

<https://orcid.org/0009-0005-3179-6878>

El. paštas: [urijsosnickij32@gmail.com](mailto:urijsosnickij32@gmail.com) (autorius yra korespondentas)

### **Andrii Repchonok**

teisės filosofijos mokslų daktaras, Baudžiamosios teisės ir proceso katedros docentas, Leonido Juzkovo Chmelnyckio vadybos ir teisės universitetas, Chmelnyckis, Ukraina.

<https://orcid.org/0009-0007-4122-1124>

El. paštas: [repchonok.andriy12@ukr.net](mailto:repchonok.andriy12@ukr.net)

### **Jana Lucenko**

teisės mokslų daktarė, Ukrainos nacionalinės saugumo tarnybos akademijos Valstybės saugumo švietimo ir mokslo instituto, Specialiojo skyriaus Nr. 1, docentė, Kijevas, Ukraina.

<https://orcid.org/0000-0001-9780-4387>

El. paštas: [yana.lutsenkoo1@gmail.com](mailto:yana.lutsenkoo1@gmail.com)

### **Serhii Kuzmenko**

viešojo administravimo mokslų daktaras, teisės mokslų daktaras, Ekonomikos ir viešojo administravimo katedros profesorius, Teisės ir socialinio valdymo švietimo ir mokslo institutas, Donecko valstybinis vidaus reikalų universitetas, Kropivnyckis, Ukraina.

<https://orcid.org/0000-0002-5325-9433>

El. paštas: [serhii.kuzmenko12@gmail.com](mailto:serhii.kuzmenko12@gmail.com)

