Journal of Theoretical and Applied Information Technology
15st September 2026. Vol.104. No.17

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

FORMATION OF AN INTEGRATED SYSTEM OF PUBLIC ADMINISTRATION IN THE FIELD OF NATIONAL SECURITY IN THE CONTEXT OF HYBRID AND INFORMATION THREATS

VOLODYMYR KYRYLENKO[1], LIUDMYLA LITVIN[2], IVAN TKACHENKO[3], SERHII HODLEVSKYI[4], KYRYLO TKACHENKO[5]

[1] Doctor of Military Science, Professor, Professor of the Department, Yevhen Bereznyak Military Academy, Kyiv, Ukraine

[2] PhD in Law, Associate Professor, Khmelnytskyi, Ukraine

[3] Head of the Military Education Department, Central Directorate of Military Education and Science of the General Staff of the Armed Forces of Ukraine, Kyiv, Ukraine

[4] Candidate of Military Sciences, Head of the Operational Art Department, Advanced Military Studies Institute, National Academy of the National Guard of Ukraine, Kharkiv, Ukraine

[5] Doctor of Philosophy, Deputy Head of the Department of Military Communications and Informatization, National Academy of the National Guard of Ukraine, Kharkiv, Ukraine

E-mail: [1]tvkurus1@ukr.net

ABSTRACT

The formation of an integrated digital public administration system in the field of national security in the context of hybrid and information threats is critically important for ensuring the stability of the state. The problem lies in the insufficient empirical validity of the combination of institutional indicators of governance quality (WGI) with an assessment of the implementation of information and computer technologies (GCI) for countries in a state of active hybrid war. The purpose of the study is to assess the institutional and technological potential of Ukraine to confront modern security challenges based on a comparative analysis with the countries of the European Union and the Baltics, as well as to determine the role of information and computer technologies in the development of an integrated security management model. The methodology is based on WGI and GCI data, using author's indices (INSGI, EUCI, CCI) to assess convergence. The results revealed a persistent institutional gap, but a significant strengthening of the digital component: GCI increased from 65.9 to 83.9 points, the level of cyber convergence reached 89%. A multi-level digital architecture of an integrated public administration system is proposed. The contribution of the study is the development and testing of a comprehensive INSGI index, the application of gap and convergence indices to quantify Ukraine's progress, and the justification of the strategic role of ICT in enhancing institutional capacity. The practical impact of the work is to create a basis for the implementation of digital solutions that allow accelerating convergence to European governance standards and increasing resilience to hybrid threats.

Keywords: *Information Technology, Computer Technologies, Digital Transformation, Public Administration, National Security*

1. INTRODUCTION

The formation of an integrated system of public administration in the field of national security in the context of hybrid and information threats is one of the most pressing challenges of modern statehood. In a world where traditional military conflicts are increasingly complemented by complex instruments of influence – from disinformation and cyberattacks to economic pressure and the

instrumentalization of social divisions – the resilience of state institutions is becoming a decisive factor in the survival and development of democratic societies. This problem is especially acute for countries bordering aggressors or in the zone of geopolitical confrontation, among which Ukraine occupies a special place due to the experience of full-scale war and long-term hybrid aggression.

Despite a significant amount of research on hybrid threats, integrated approaches (whole-of-government, whole-of-society), and critical infrastructure resilience, there is a lack of comprehensive empirical work that combines traditional governance quality indicators (WGI) with an assessment of the implementation and effectiveness of information and computer technologies (GCI) in the context of countries in a state of active hybrid warfare. This is especially true for Ukraine, which has been the object of systemic hybrid aggression since 2014, and full-scale war since 2022. Existing research mostly either focuses on institutional reforms without taking into account the technological dimension, or considers digitalization without linking it to indicators of governance effectiveness. This creates a need for research that would fill this gap by analyzing the dynamics of Ukraine's institutional capacity compared to the EU and Baltic countries, taking into account the role of digital technologies as a strategic factor in increasing resilience.

In accordance with the stated problem, the study aims to find answers to the following questions:

1. What are the main institutional gaps in Ukraine's national security management compared to the EU and the Baltics, and how are they changing over time (2010–2024)?

2. What are the dynamics of Ukraine's cyber resilience and its convergence to the European level in the face of hybrid aggression?

3. How can information and computer technologies help overcome the identified institutional gaps and increase the state's overall ability to resist hybrid threats?

Despite a significant amount of research on hybrid threats, whole-of-government and whole-of-society approaches, as well as the resilience of critical infrastructure, there is a lack of comprehensive empirical work that would combine traditional indicators of public administration quality (Worldwide Governance Indicators) with an assessment of the implementation and effectiveness of information and computer technologies (Global Cybersecurity Index) in the context of countries in a state of active hybrid war. The proposed study attempts to partially fill this gap by analyzing the dynamics of Ukraine's institutional capacity in comparison with the countries of the European Union and the Baltic States – recognized models of effective counteraction to hybrid threats through a combination of institutional reforms and advanced digital technologies.

The novelty of the study lies in the development and testing of the Integrated Index of Public Administration Capacity in the Field of National Security, as well as in the application of gap and convergence indices to assess Ukraine's progress towards European governance standards, taking into account the role of information and computer technologies in the face of extreme security challenges. This approach allows not only to state the existing gaps, but also to identify the areas of greatest adaptability and potential for accelerating institutional transformations.

The article is aimed at a comprehensive assessment of the state and prospects for the formation of an integrated public administration system in Ukraine in the context of hybrid and information threats based on empirical data and comparative analysis.

The scientific novelty of the study lies in:

1) the development and testing of the Integrated National Security Governance Capacity Index (INSGI), which combines four key WGI indicators;

2) the application of gap and convergence indices (EUCI, CCI) to quantify Ukraine's progress towards European standards, taking into account the role of ICT;

3) the substantiation of a multi-level digital architecture of an integrated public governance system based on interagency interaction platforms, artificial intelligence for threat prediction, and mechanisms for public engagement.

Unlike previous works that considered institutional and technological aspects separately, this article for the first time offers a comprehensive empirical assessment of their interaction in the context of a prolonged hybrid war, which allows not only to state existing gaps, but also to identify directions for overcoming them using modern information and computer solutions.

2. LITERATURE REVIEW

The formation of an integrated system of public administration in the field of national security in the context of hybrid and information threats is one of the central challenges of modern statehood, especially for countries bordering aggressors or in

the zone of geopolitical confrontation. Hybrid threats that combine military, economic, informational, cybernetic, and social tools aimed at undermining institutional resilience, social cohesion, and the state's capacity for effective governance [1, 2].

2.1 Conceptualization of hybrid threats and their impact on public administration

Hybrid warfare is defined as the coordinated application of conventional and non-conventional means to achieve political goals without declaring war, with an emphasis on blurring the lines between war and peace [3, 4]. Such threats exploit public administration vulnerabilities, including poor policy effectiveness, corruption, weak rule of law, and limited interagency coordination [5]. Studies show that hybrid actors, primarily the Russian Federation, actively use disinformation, cyberattacks, and migration instrumentalization to destabilize democratic institutions [6, 7].

In the context of public administration, hybrid threats require a shift from a fragmented to an integrated approach that combines whole-of-government and whole-of-society strategies. The OECD [8] in the Public Governance Review of Ukraine emphasizes the resilience of Ukrainian public administration during full-scale aggression, but points to the need to strengthen coordination and anti-corruption mechanisms. Similarly, studies of the Baltic states demonstrate successful examples of integrating national security into the public governance system through the creation of coordination centers and the development of societal resilience [9, 10].

2.2 The role of institutional capacity and governance indicators

The quality of public administration is a key factor in resilience to hybrid threats. The World Bank's Worldwide Governance Indicators (further – WGI), including Government Effectiveness, Rule of Law, Control of Corruption, and Political Stability, are widely used to assess institutional readiness [11]. Low scores on these indicators create vulnerabilities that are exploited by external actors [12].

The research highlights the need for integrated governance models that combine traditional public administration tools with digital resilience. Jungwirth et al. [13] in the JRC report analyze how systemic resilience depends on cross-sectoral coordination in the face of hybrid attacks on critical infrastructure.

2.3 Cybernetic and informational dimensions of threats

Information and cyber operations are at the heart of modern hybrid strategies. The Global Cybersecurity Index (further – GCI) demonstrates a correlation between the level of cyber readiness and the overall resilience of the state [14]. Ukraine has shown a significant improvement in the Global Cybersecurity Index despite the war, illustrating the adaptability of public administration [15].

The literature focuses on the key role of strategic communications and media literacy in countering disinformation as an integral part of hybrid threats [1, 16]. In the Baltic States, a whole-of-society approach involving civil society, the private sector, academic institutions, and the media in countering disinformation and strengthening societal resilience has become a recognized model for the European Union as a whole [2, 17, 18].

2.4 Integrated models and experience of EU countries

The European Union is actively developing a comprehensive framework for countering hybrid threats, in particular through the Strategic Compass [19], the Critical Object Resilience Directive (CER Directive) and other instruments that focus on increasing the resilience of critical entities and strengthening coordinated governance at the EU level [2, 19, 20]. Research highlights the importance of convergence of candidate countries such as Ukraine to European standards of public governance and security management as a necessary prerequisite for effective integration and strengthening resilience to external threats [8, 21, 22].

In this context, the experience of the Baltic States is a particularly valuable benchmark, as they have successfully integrated national security, societal resilience and whole-of-society approaches into the public administration system and have become a model for other EU states [9, 23].

2.5 Gaps in the literature and directions for further research

The existing literature describes well the nature of hybrid threats and individual elements of resilience, but there is a lack of empirical studies of integrated indices of public administration in the context of national security for countries in a state of prolonged hybrid war. The combination of traditional indicators of governance quality (WGI) with the assessment of the implementation and effectiveness of information and computer technologies (GCI) in models of interagency coordination remains especially insufficiently

studied, data-driven governance and societal resilience [24, 25]. Comprehensive models that integrate WGI/GCI with indicators of digital transformation of public administration, such as the use of AI threat monitoring systems, interagency interaction platforms, and whole-of-society citizen engagement tools, need to be developed.

Recent publications in 2025 significantly complement the understanding of the relationship between institutional capacity and digital resilience in the face of hybrid threats. In particular, the updated OECD report "Public Governance Review of Ukraine" emphasizes the need to implement adaptive coordination mechanisms, and new research by the International Telecommunication Union emphasizes the growing role of national cybersecurity systems as an integral part of overall risk management. In addition, the work of European think tanks indicates that EU candidate countries should accelerate the digital transformation of the security sector to achieve NIS2 and EU Cyber Resilience standards. These sources confirm the relevance of our approach, which integrates WGI and GCI into a single analytical framework, and allow us to compare Ukraine's dynamics with the latest European trends.

Thus, the literature review confirms the relevance of the formation of an integrated public administration system as a key element of national resilience. The experience of the EU, the Baltic States and the empirical data of WGI/GCI create a solid basis for further analysis of the Ukrainian case with an emphasis on the role of modern information and computer technologies in strengthening institutional capacity and accelerating convergence to European standards.

Summarizing the literature review, the following unresolved issues can be identified:

1) the lack of quantitative models that would simultaneously assess institutional capacity (WGI) and the level of implementation of information and computer technologies (GCI) in countries with active hybrid warfare;

2) the lack of development of integral indices that allow tracking convergence to European security management standards;

3) the lack of empirically based recommendations for a digital architecture that would combine interagency coordination, AI-based analytics, and public engagement.

Filling these gaps is the scientific and practical value of our study, which offers a new integrated approach to assessing and shaping the system of public management of national security.

3. MATERIALS AND METHODS

The empirical basis of the study is the data of two authoritative international sources: the Worldwide Governance Indicators (WGI) of the World Bank and the Global Cybersecurity Index (GCI) of the International Telecommunication Union. These databases were chosen because of their high-quality methodology, broad international recognition, and immediate relevance to assessing the institutional capacity of a state in the face of hybrid and information threats.

Worldwide Governance Indicators [15] contain aggregate indicators of the quality of public administration in the form of percentile ranks (scale 0-100), formed on the basis of surveys of experts, enterprises and the population. Four key indicators were selected for the analysis: Government Effectiveness, Political Stability and Absence of Violence/Terrorism, Rule of Law and Control of Corruption. The study period covers 2010–2024 with a special focus on 2014–2024. The comparison was made with the average values for the European Union (EU-27) and the Baltic States (Estonia, Latvia, Lithuania), which are considered as relevant benchmarks due to common historical experience and successful counteraction to hybrid threats.

Based on the selected WGI indicators, a composite indicator (Integrated National Security Governance Index, INSGI) was formed. Additionally, the gap indicators (GAP) between Ukraine, the EU and the Baltic States, as well as the EU Convergence Index (EUCI) according to the benchmark normalization method were calculated.

To assess cyber resilience, data from the Global Cybersecurity Index [14] for 2020 and 2024 were used. Based on them, the cybersecurity gap and the Cyber Convergence Index (CCI) were calculated.

This methodological approach provides a comprehensive quantitative assessment of institutional capacity, combining traditional governance indicators with an assessment of the level of implementation and effectiveness of information and computer technologies. The use of international standardized data in combination with author's composite indices makes it possible to make an objective comparison, identify the dynamics of changes over time, and substantiate recommendations for priority digital technologies to strengthen the resilience of public administration in the face of long-term hybrid threats.

4. RESULTS

4.1 Empirical Analysis of the Institutional Capacity of Public Administration in the Field of National Security

The empirical basis of the study is the Worldwide Governance Indicators (WGI) data developed by the World Bank [15]. This authoritative tool assesses the quality of public administration based on aggregated data in countries around the world, including surveys of experts, businesses and the population. Four key indicators were selected for the analysis, which are most relevant to the topic of the study:

– Government Effectiveness (GE) – the quality of formulation and implementation of state policy, the competence of the state apparatus;

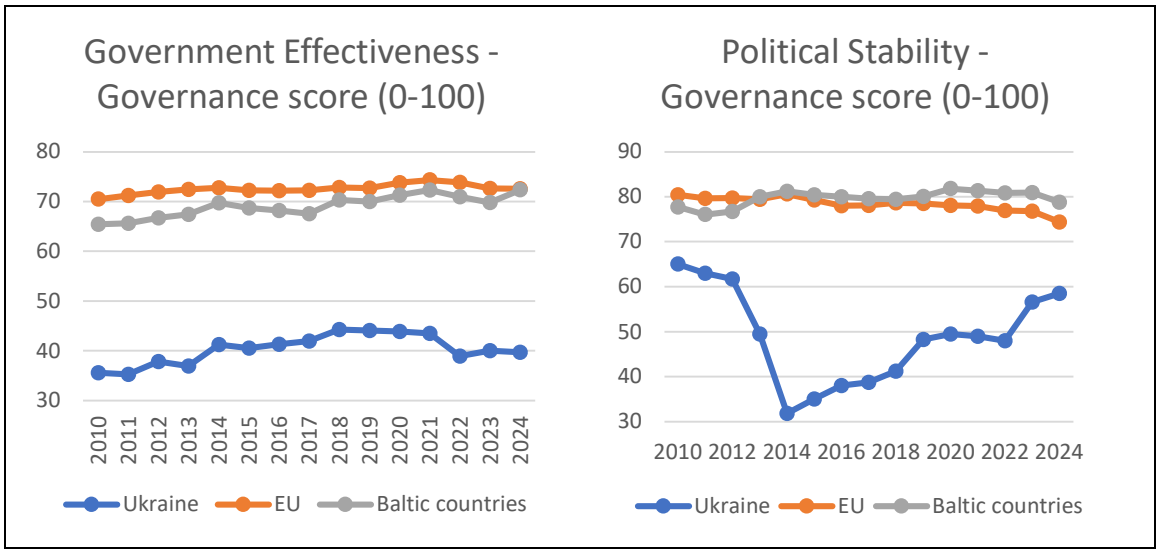
– Political Stability and Absence of Violence/Terrorism (PV) – perception of the likelihood of political destabilization and violence, including hybrid threats;

– Rule of Law (RL) – the level of the rule of law, trust in the legal system and its effectiveness;

– Control of Corruption (CC) – perception of the level of corruption in the public sector.

The choice of these indicators is due to their direct relevance to the formation of an integrated public administration system in the context of hybrid and information threats. They make it possible to assess the institutional capacity of the State to coordinate the efforts of the different authorities, ensure stability and counteract internal vulnerabilities exploited by external actors.

The analysis was carried out at the level of Ukraine, the average value for the European Union (EU-27) and the average value for the Baltic countries (Estonia, Latvia, Lithuania). Such a comparative approach is justified by the fact that the Baltic countries face similar hybrid and information threats, have common historical experience and at the same time have achieved a high level of integration into European and transatlantic security structures. Comparison with the EU average makes it possible to compare Ukrainian indicators with the pan-European standard. The analysis period covers 2010–2024. with a special focus on 2014-2024. The results are visualized in Figure 1.



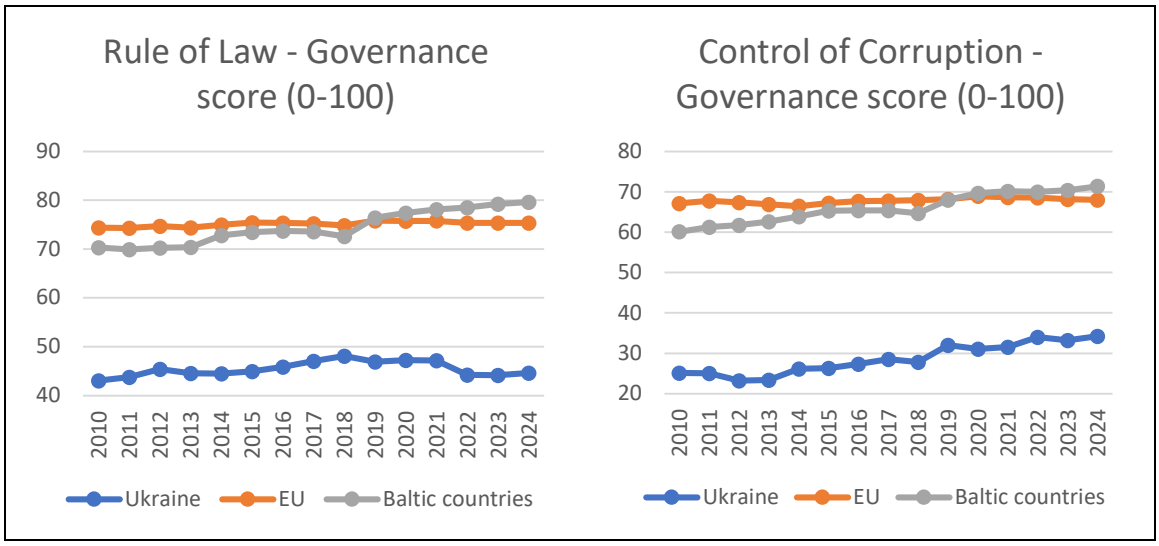


Figure 1: Dynamics of Worldwide Governance Indicators for Ukraine, the Baltic States (average) and the EU (average), 2010–2024
Source: Built by the authors based on [15]

The analysis shows that Ukraine is steadily lagging behind both comparative groups in all the indicators under study. The most significant gaps in 2024 were recorded in the Government Effectiveness and Control of Corruption indicators, where the difference between Ukraine and the EU average was 32.8 and 33.7 points, respectively. The lag in the Rule of Law indicator (30.8 points) also remains significant. At the same time, the smallest gap is observed in the Political Stability and Absence of Violence/Terrorism indicator (15.9 points), which is associated with the mobilization of state institutions and society in the context of a full-scale war.

The dynamics of indicators shows that after 2014 Ukraine demonstrated a gradual improvement in the areas of Government Effectiveness, Rule of Law and Control of Corruption, although these positive trends did not allow to reach the level of the Baltic States and the average European values. Especially indicative is the growth of the Control of Corruption indicator from 25.2 points in 2014 to 34.2 points in 2024, which reflects the results of anti-corruption reforms and institutional transformations. At the same time, the Political Stability indicator suffered a sharp decline in 2014-2015. as a result of Russian aggression, but later demonstrated recovery dynamics and reached 58.5 points in 2024.

The comparison with the Baltic countries is especially indicative, as they have similar historical experience in countering external influence and hybrid threats. The average values of indicators in the Baltic region in 2024 were in the range of 71-80 points, which is almost twice as high as Ukrainian indicators in certain areas. This confirms the importance of further strengthening the institutional capacity of the state, the development of interagency coordination and the introduction of integrated mechanisms of public administration in the field of national security.

For a more comprehensive assessment of the prerequisites for the formation of an integrated system of public administration in the field of national security in the context of hybrid and information threats, it is advisable to move from the analysis of individual indicators to a generalized indicator that reflects the aggregate capacity of state institutions to ensure coordination, resilience and effective response to security challenges. For this purpose, the study forms the Integrated National Security Governance Index (INSGI).

In order to assess the consistency of the selected governance indicators and substantiate the possibility of their aggregation into an integrated index, a correlation analysis was carried out using the Pearson coefficient.

The results indicate the presence of strong statistically significant positive relationships between the key indicators of the Worldwide Governance Indicators for the CoE countries and Ukraine in 2024. In particular, the Government Effectiveness indicator has a very high level of correlation with Rule of Law ($r = 0.968$; $p < 0.01$) and Control of Corruption ($r = 0.946$; $p < 0.01$), while there is also a close relationship between Rule of Law and Control of Corruption ($r = 0.957$; $p < 0.01$). This indicates that these indicators reflect a

single latent dimension of institutional quality and capacity of public administration, which creates methodological grounds for their integration into the Generalized Indicator (INSGI).

The index was calculated on the basis of four Worldwide Governance Indicators, which directly characterize the institutional components of security governance:

$$INSGI = \frac{GE + PV + RL + CC}{4},$$

where: – Government Effectiveness; – Political Stability and Absence of Violence/Terrorism; – Rule of Law; – Control of Corruption.$GEPVRLCC$

To form an integral indicator, the method of linear aggregation with equal weights (equal weighting) was used, which is one of the most common approaches to the construction of composite indices. According to the recommendations of the OECD and the Joint Research Centre of the European Commission, the use of the same weights is appropriate in cases where all components of the index are measured in a single scale and there are no sufficient theoretical or empirical grounds for giving individual indicators greater significance [26]. Similarly, Greco et al. [27] note that under conditions of equivalence of components, the integral indicator can be defined as the non-weighted arithmetic average of indicators. Since all selected Worldwide Governance Indicators are presented in a single percentile scale (0-100) and reflect interrelated aspects of the institutional capacity of the state in the field of national security, each of them was given equal weight.

Thus, the proposed index integrates the key characteristics of public administration that determine the country's ability to ensure national security in the face of modern hybrid and information threats.

To determine the scale of Ukraine's institutional lagging behind European benchmarks, two gap indicators were additionally calculated:

$$GAP_{EU-UA} = INSGI_{EU} - INSGI_{UA};$$
$$GAP_{BALT-UA} = INSGI_{BALT} - INSGI_{UA},$$

where GAP_{EU-} characterizes the distance between Ukraine and the middle level of the European Union countries, and $GAP_{BALT-UA}$ between Ukraine and the Baltic countries, which are considered as an example of successful formation of sustainable models of public administration in the face of external security challenges.

The results of the calculations are visualized in Figure 2.

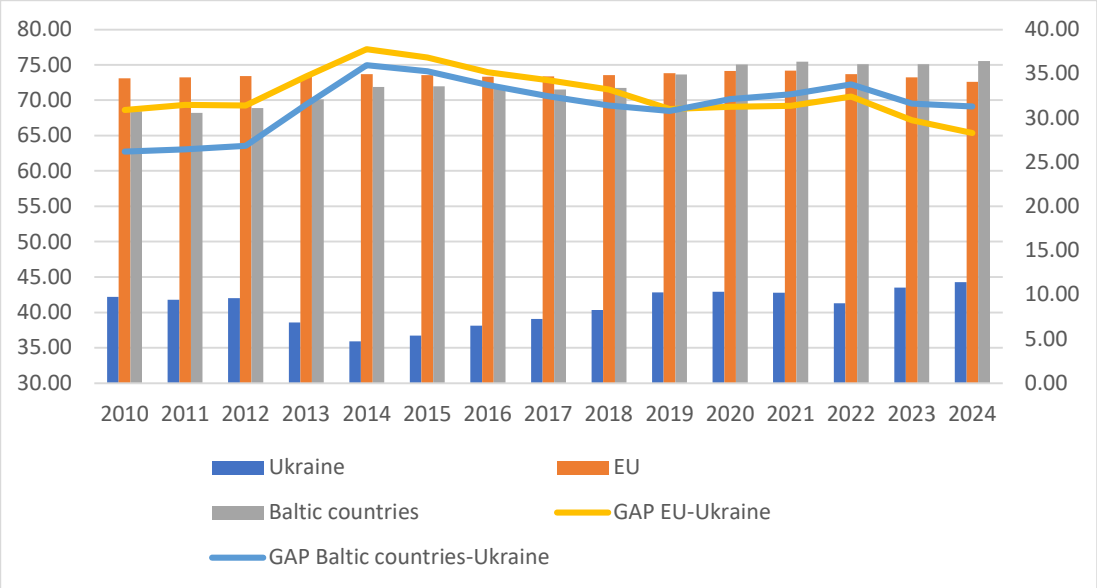


Figure 2: Dynamics of the Integrated Index of Public Administration Capacity in the Field of National Security (INSGI) and the gaps between Ukraine, the EU and the Baltic States in 2010–2024
Source: Built by the authors based on [15]

The analysis of the results presented in Figure 2 shows that there is a significant and long-lasting institutional gap between Ukraine and the European Union countries, as well as between Ukraine and the Baltic States. In 2010, the value of the integral index for Ukraine was 42.20 points,

while the EU average reached 73.10 points, and the Baltic States – 68.40 points. Accordingly, the gap between Ukraine and the EU was 30.90 points, and between Ukraine and the Baltic countries – 26.20 points.

The greatest deterioration of the situation was observed in 2014 after the start of Russian aggression against Ukraine. The INSGI value decreased to 35.93 points, which was the lowest in the entire study period. At the same time, the gap with the European Union increased to 37.76 points, and with the Baltic countries to 35.95 points. This indicates a significant weakening of the institutional stability of the state as a result of the security crisis and large-scale challenges to the public administration system.

Since 2016, there has been a gradual recovery of the integral indicator. In 2024, the INSGI value reached 44.26 points, which is the highest result for the entire period of the study. Despite the full-scale invasion of the Russian Federation in 2022, Ukrainian institutions retained their ability to function and adapt, which was reflected in the positive dynamics of the integral index.

Of particular importance is the reduction of the gap between Ukraine and the European Union. If in 2014 the gap was 37.76 points, then in 2024 it decreased to 28.31 points. A similar trend is observed for the Baltic countries: the corresponding gap decreased from 35.95 to 31.28 points. Although the scale of the lag remains significant, the revealed dynamics indicate a gradual strengthening of the institutional foundations of the public administration system and its adaptation to the conditions of prolonged external pressure.

At the same time, the comparison with the Baltic States is especially important in the context of the study, as they have experience in countering hybrid threats, have successfully integrated into European and transatlantic security structures, and have formed effective mechanisms of interagency coordination. In 2024, the average INSGI value in the Baltic States was 75.53 points, which was almost 1.7 times higher than the Ukrainian indicator.

Thus, the results of the analysis of the integral index confirm that the formation of an effective system of public administration in the field of national security remains one of the key areas of strengthening Ukraine's resilience to hybrid and information threats [28]. At the same time, the gradual reduction of gaps with the EU and the Baltic States indicates the presence of positive institutional changes and creates the basis for the further development of an integrated model of security governance.

To assess the degree of Ukraine's approximation to the average level of the European Union countries for individual components of the public administration system in the field of national security, the EU Convergence Index (EUCI) was calculated. The methodological basis of the calculation is the benchmark normalization approach, which is widely used in studies of convergence and integration readiness of candidate countries for EU membership. The essence of the approach is to determine the relative level of achievement by national indicators of reference values taken as a basis for comparison. A similar approach is used in studies of Ukraine's integration readiness into the European Union, where national indicators are evaluated relative to the corresponding European average values [29].

The calculation was carried out according to the formula:

$$EUCI_i = \frac{X_{UA,i}}{X_{EU,i}} \times 100\%,$$

where: $EUCI_i$ – convergence index to the EU by the corresponding indicator; $X_{UA,i}$ – the value of the indicator in Ukraine; $X_{EU,i}$ – the average value of the indicator in the countries of the European Union.

The value of the index at the level of 100 % indicates that the average European level has been fully reached for the corresponding indicator. Values below 100% characterize the degree of lagging behind the European benchmark, while approaching the indicator to 100% reflects the process of institutional convergence and increasing compliance with EU standards. The use of this approach provides an opportunity to directly compare the level of Ukraine's approximation to European benchmarks for different components of the public administration system, regardless of their absolute values.

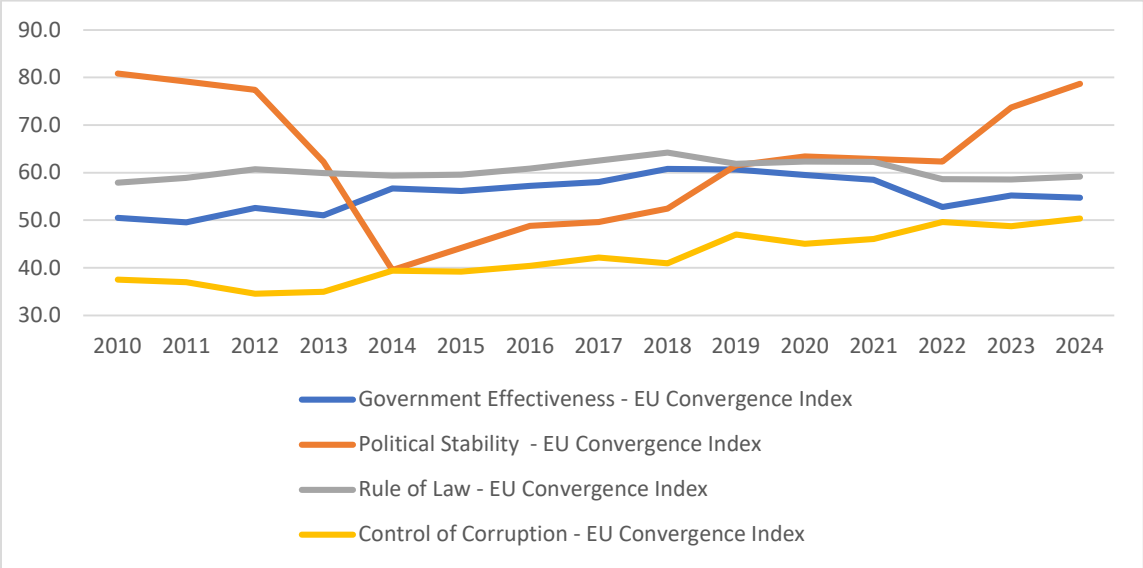


Figure 3: Dynamics of Ukraine's Convergence Index to the EU Average Level by Components of the Public Administration System in the Field of National Security in 2010–2024, %
Source: calculated by authors based on [15]

The results of the calculations show (Figure 3) that the process of Ukraine's approximation to European standards is uneven in different components of the public administration system. The highest level of convergence during most of the study period was observed in the Political Stability and Absence of Violence/Terrorism indicator. Despite the sharp drop of the index after the beginning of Russian aggression in 2014 to 39.5%, its gradual recovery was observed in the future. In 2024, the figure reached 78.7%, which is the best result among all the components studied. Such dynamics may indicate an increase in the adaptability of Ukrainian institutions and society to conditions of prolonged external pressure, as well as an increase in the ability of the state to ensure political stability even in the face of a full-scale war.

The Government Effectiveness indicator shows more moderate progress. The convergence rate has increased from 50.5% in 2010 to 54.7% in 2024. Despite some positive changes, this means that the efficiency of the functioning of the state apparatus and policy implementation mechanisms is still only slightly more than half of the average European level. In the context of hybrid threats, it is this component that determines the ability of the state to coordinate the activities of numerous actors in the security and defense sector.

A similar situation is observed in the Rule of Law indicator, where the level of convergence during the study period fluctuated between 58–64 %. In 2024, its value was 59.1%, which indicates some progress in strengthening legal institutions, but at the same time indicates the preservation of significant potential for further improvement of legal mechanisms for ensuring security and countering destructive influences.

Control of Corruption remains the most problematic area. Although the convergence rate has increased from 37.5% in 2010 to 50.4% in 2024, it continues to be the lowest among all the indicators studied. This indicates that corruption risks continue to constitute one of the key internal vulnerabilities of the national security system. In the context of hybrid threats, such vulnerabilities can be exploited by external actors to weaken state institutions, undermine public trust, and reduce the effectiveness of managerial decisions [30].

In general, the results of the Convergence Index analysis confirm that over the past decade Ukraine has made significant progress in approaching European standards of public administration. At the same time, none of the studied indicators as of 2024 exceeded the level of 80% of the EU average, which indicates that the institutional transformation is incomplete. The greatest results have been achieved in the field of ensuring political stability, while improving the efficiency of public administration, strengthening the rule of law and further reducing corruption risks remain key tasks in the formation of an integrated system of public administration in the field of national security.

At the same time, modern hybrid threats are complex in nature and are not limited to institutional or managerial challenges. One of the key areas of

their implementation is the information and cyber space, in which states face cyberattacks on critical infrastructure, disinformation operations, interference with digital control systems, and other forms of destructive influence. In this regard, the assessment of the capacity of the public administration system in the field of national security needs to be supplemented with indicators that characterize the level of cyber resilience of the state.

To solve this subtask, the study used the Global Cybersecurity Index (GCI), developed by the International Telecommunication Union. This international index assesses the level of readiness of states to counter cyber threats based on five main components: Legal Measures, Organizational Measures, Technical Measures, Capacity Development, and International Cooperation [14].

The use of GCI in this study is due to the fact that information and cyber attacks are one of the central tools of modern hybrid conflicts. Unlike traditional indicators of governance quality, which characterize the general state of state institutions, GCI allows you to assess the specialized capacity of the state to ensure digital security, protection of the information space and the resilience of critical management systems.

For the comparative assessment, the GCI values for Ukraine, the European Union Member States and the EU average in 2020 and 2024 were used (Figure 4).

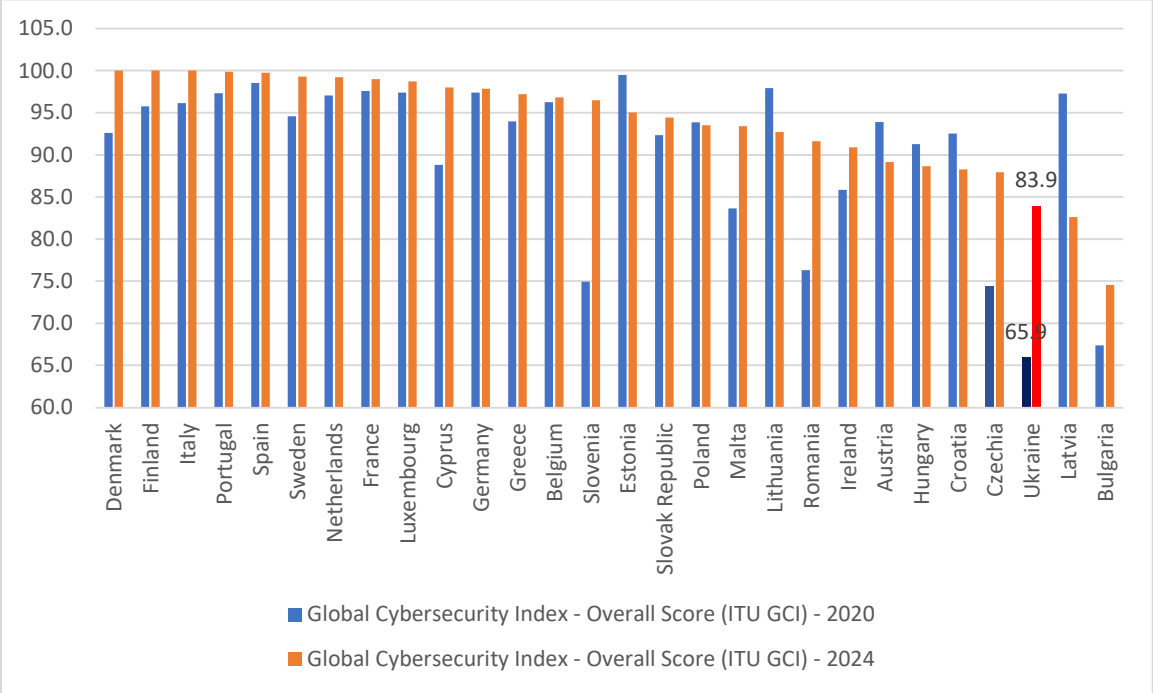


Figure 4: Dynamics of the Global Cybersecurity Index of Ukraine and the European Union in 2020–2024
Source: compiled by authors based on the World Bank [31]

Additionally, the cybersecurity gap between Ukraine and the European Union is calculated:

$$CyberSecurityGAP_{EU-UA} = GCI_{EU} - GCI_{UA},$$

where $CyberSecurityGAP_{EU-UA}$ characterizes Ukraine's lagging behind the average level of cybersecurity of the EU countries.

To determine the degree of Ukraine's approximation to the European level of cyber resilience, the Cyber Convergence Index was used:

$$CCI = \frac{GCI_{UA}}{GCI_{EU}} \times 100\%$$

where CCI (Cyber Convergence Index) reflects the level of Ukraine's achievement of the average level of cybersecurity of the European Union.

The results of the analysis indicate a significant improvement in Ukraine's position in the field of cybersecurity during the study period. In 2020, Ukraine's Global Cybersecurity Index was 65.9 points, which was significantly lower than the European Union average of 91.3 points. Accordingly, the cybersecurity gap between Ukraine and the EU was 25.4 points, and the level of

cyberconvergence of Ukraine to the European standard was 72.2%.

In 2024, there is a significant increase in Ukraine's cyber resilience: the GCI value has increased to 83.9 points. At the same time, the average of the European Union was 94.3 points. As a result, the gap was more than halved – from 25.4 to 10.3 points, and the cyberconvergence index increased to 89.0%. This dynamic is especially indicative given that in 2022 Ukraine was under the influence of large-scale cyberattacks aimed at government agencies, energy infrastructure and information systems.

Comparison with the Baltic States demonstrates a more complex dynamics of cyber capability development. Ukraine in 2020–2024 demonstrated the most significant improvement among the countries studied: the value of the Global Cybersecurity Index increased from 65.9 to 83.9 points, i.e. by 18.0 points. At the same time, some Baltic countries, which are traditionally considered as examples of the formation of sustainable models for countering hybrid threats, recorded a decrease in indicators in 2024 compared to 2020. In particular, the index of Estonia decreased from 99.5 to 95.0 points, Lithuania – from 97.9 to 92.7 points, and Latvia – from 97.3 to 82.6 points. At the same time, these changes do not indicate a loss of their cyber capabilities, as the Baltic States continue to remain among the states with a high level of digital readiness due to developed institutional mechanisms, integration into European and transatlantic security structures, and many years of experience in countering cyber threats. On the other hand, the rapid growth of Ukraine's indicator indicates an accelerated institutional and organizational strengthening of cybersecurity in the context of large-scale hybrid aggression.

The results obtained complement the conclusions of the INSGI and EUCI analysis. If the institutional indicators of the WGI reflect the overall capacity of public administration, then the GCI demonstrates a specific dimension of the state's readiness to counter information and cyber threats. The cumulative analysis of these indicators confirms that the formation of an integrated system of public administration in the field of national security requires the simultaneous development of management institutions, legal mechanisms and digital resilience of the state.

Summarizing the results of the empirical analysis, it can be stated that the institutional development of Ukraine in the field of public management of national security is characterized by a combination of structural lagging behind the average European level and the Baltic States with a noticeable positive dynamics of convergence. The most significant gaps remain in Government Effectiveness, Rule of Law and Control of Corruption, while the greatest progress has been made in Political Stability and Cyber Resilience (GCI).

Empirical analysis has shown that overcoming these gaps requires not only traditional institutional reforms, but also the active implementation of modern information and computer technologies that can significantly increase the coordination, transparency and digital resilience of the state in the face of hybrid threats.

4.2 The role of information and computer technologies in enhancing institutional capacity and convergence to EU standards

Modern information and computer technologies (ICT) are a strategic tool for the formation of an integrated system of public administration in the field of national security in the context of hybrid and information threats. They provide a data-driven approach to coordination, rapid threat detection, and increased process transparency.

Based on the results of empirical analysis, a matrix of ICT compliance with key components of institutional capacity has been developed.

Table 2: Information and Computer Technologies for Strengthening the Components of the Integrated System of Public Management of National Security

Capacity component (WGI / GCI)	Recommended ICTs	Main functions	Examples of implementation (Baltics/EU/Ukraine)	Sources
Government Effectiveness	Unified digital platforms for interagency coordination (API Gateway, low-code platforms); artificial intelligence systems for predictive analytics and situation centers; digital twins (Digital Twins); Real-time digital dashboards	Real-time government data integration; interdepartmental exchange; risk forecasting; decision support; Simulation of response scenarios	Estonia: X-Road; EU: Destination Earth (Digital Twin), European Digital Strategy; Ukraine: Diia, interdepartmental digital dashboards	OECD [8]; X-Road Global [32]; European Commission [33]; Ministry of Digital Transformation of Ukraine [34]
Political Stability and Absence of Violence/ Terrorism	Hybrid Threat Intelligence platforms; AI information space monitoring systems (NLP/ML); early detection of disinformation; automated fact-checking and social media analysis platforms	Detection of disinformation campaigns and information operations in real time; monitoring the risks of political destabilization; analysis of narratives and networks of influence; supporting strategic communications and crisis response	Lithuania: systems of strategic communications and monitoring of information threats; Latvia: National Security and Strategic Communication Framework; Ukraine: Center for Countering Disinformation, Center for Strategic Communications and Information Security; EU: EU Hybrid Toolbox, EUvsDisinfo, Rapid Alert System	Giannopoulos et al. [1]; Jungwirth et al. [13]; Danchenkova [16]; Council of the European Union [19]; European External Action Service [35]
Rule of Law	e-Justice Systems; electronic document management with a qualified electronic signature (QES); digital state registers; blockchain solutions to ensure the integrity of records; AI systems to support legal analysis and judicial administration	Increasing transparency and accountability of court procedures; ensuring the immutability and traceability of data; reduction of the terms of consideration of cases; automated audit of legal processes; reducing opportunities for manipulation and interference in document flow	Estonia: e-Justice and State Digital Infrastructure X-Road; EU: eIDAS 2.0, European Digital Identity Framework, digital interaction of judicial systems; Ukraine: Unified Judicial Information and Telecommunication System, "Electronic Court", Digital State Registers	Kalniete and Pildegovičs [10]; OECD [8]; European Commission [36]
Control of Corruption	AI systems for monitoring public procurement and electronic declarations; Big Data analytics to identify anomalies and conflicts of interest; automated risk-scoring models; continuous audit and anti-corruption analytics systems; Open digital registers and transparency platforms	Detection of corruption risks and suspicious transactions in real time; automated audit of public procurement and financial transactions; analysis of connections between subjects and potential conflicts of interest; prioritization of inspections based on risk assessment; Increasing transparency and accountability of the public sector	Ukraine: ProZorro, DOZORRO risk indicator system, Unified State Register of Declarations; Estonia: e-Governance Academy digital solutions for transparent governance and e-public services; EU: ARACHNE (Analytical System for Risk Assessment for the Use of EU Funds), European Public Prosecutor's Office (EPPO) digital analytics tools	OECD [8]; ProZorro [37]; European Commission [36]; e-Governance Academy [38]
Global Cybersecurity Index	SIEM systems with AI-driven SOAR (Security Orchestration, Automation and Response); Cyber Threat Intelligence (CTI) platforms; Extended Detection and Response (XDR) systems;	Detection, analysis and neutralization of cyber threats in real time; automated incident response; cyber intelligence sharing; predicting and preventing attacks; ensuring the	Estonia: NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), Cyber Range Estonia, National Cyber Security System; EU: EU Cybersecurity Reserve, Cyber Europe Exercises, Joint Cyber Unit, NIS2	International Telecommunication Union [14]; ENISA [39]; European Commission [40]; NATO CCDCOE [41]

	automated incident response mechanisms; Integrated Cyber-Physical Security Systems to Protect Critical Infrastructure	resilience of critical infrastructure and continuity of public services	Implementation Framework; Ukraine: National Coordination Center for Cybersecurity (NCCC), State Special Communications Service, integration of state information systems with SIEM/SOC solutions, protection of the digital ecosystem "Diia"	
Whole-of-society / Cross-sectoral coordination	Mobile e-participation platforms; digital platforms for interaction between the state, citizens and business; federated data lakes with AI agents to analyze public signals; crowdsourced threat monitoring systems; open data and digital consulting platforms	Ensuring constant interaction between government agencies, civil society, business and academia; involving citizens in policy-making; collective identification of social, informational and security risks; support for collaborative data-driven decision-making; increasing trust in state institutions	Estonia: Rahvaalgatus.ee (Citizens' Initiative Portal) is a digital platform for civic initiatives and citizen participation in policymaking; Lithuania: E. pilietis / e-participation and digital citizen consultation platforms; EU: European Citizens' Initiative and Digital Decade framework as mechanisms for digital participation and multilateral governance; Ukraine: Diia as a platform for digital interaction between the state and citizens, including wartime services, electronic petitions and integration of civil services	Aoki and Tay [42]; European Commission [43]; OECD [44, 45]; Ministry of Digital Transformation of Ukraine [34]

Source: compiled by the authors on the basis of Worldwide Governance Indicators, Global Cybersecurity Index and analysis of international experience

The presented technologies allow you to move from traditional to integrated digital control. In particular, the further development of the Ukrainian Diia (diia.gov.ua) platform through integration with AI threat monitoring modules, blockchain registers, and SIEM systems can become the basis of a national "digital shield". Estonia's experience with the X-Road architecture (x-road.global) and e-Governance Academy demonstrates that the systematic implementation of such solutions significantly increases resilience to hybrid threats even in countries with limited resources.

Thus, information and computer technologies not only complement traditional institutional mechanisms, but also become their digital basis, ensuring the efficiency, transparency and adaptability of the public administration system in the context of a prolonged hybrid war.

5. DISCUSSION

The results of the empirical analysis confirm the central thesis of the study: the formation of an integrated system of public administration in the field of national security in the context of hybrid and information threats is not only an institutional, but also a technological task. Ukraine's persistent lagging behind in Government Effectiveness, Rule of Law, and Control of Corruption indicators is combined with a noticeable positive trend in convergence in Political Stability and Cyber Resilience (GCI increased to 89.0% of the EU level in 2024). This indicates the high adaptability of Ukrainian institutions, but emphasizes the need for active use of information and computer technologies to overcome the bottlenecks of the governance system.

The choice of the Worldwide Governance Indicators as a basic tool for assessing institutional capacity is justified by their high validity, reliability and widespread use in international comparative studies [11, 12]. At the same time, the Global Cybersecurity Index, developed by the ITU, is a standardized tool that allows you to assess the state's readiness to counter cyber threats that are at the core of modern hybrid operations [14]. In previous works, these two sets of indicators have been analyzed mainly in isolation. For example, the OECD study [8] focuses on governance aspects, while the ENISA reports [39] focus exclusively on cybersecurity. Our study is the first to integrate these dimensions into a single analytical framework that allows you to quantitatively assess the contribution of digital technologies to overcoming institutional gaps. This approach is especially significant for countries that are in a state of active hybrid warfare, since it is the combination of managerial efficiency and cyber

resilience that determines the state's ability to adapt and maintain functionality under complex pressure.

Digital technologies act as a catalyst for institutional transformation. They make it possible to compensate for the limited efficiency of the state apparatus through the automation of interagency coordination, increase the rule of law through transparent electronic document management and blockchain registers, as well as reduce corruption risks through Big Data analytics and AI risk-scoring models. The experience of the Baltic States, in particular the Estonian X-Road architecture and cyber hubs, confirms that the systematic implementation of such solutions ensures a high level of resilience even in the face of constant hybrid threats [8-10].

For the practical implementation of the proposed approach, the authors have developed **a multi-level architecture of digital resilience of the integrated system of public administration in the field of national security**. The proposed architecture is based on the principles of integrated data management, intelligent analysis of information, automated response to threats and involvement of society in the processes of ensuring national resilience.

The first, **the infrastructure level**, forms the technological basis of the system and provides for the creation of a single digital environment for the exchange of information between government agencies, security sector entities and other participants in the management system. It is based on the state data fabric, built on the principles of compatibility of information systems and federated data organization (federated data lakes). This approach ensures secure interdepartmental exchange of information, eliminates fragmentation state data and creates conditions for the formation of a single information space for managerial decision-making.

The second, **analytical layer**, ensures the transformation of large amounts of data into analytical knowledge necessary to predict and prevent security risks. This layer uses artificial intelligence technologies, predictive analytics, Hybrid Threat Intelligence platforms, as well as machine learning and natural language processing (NLP/ML) systems to detect information operations, disinformation campaigns, and potential scenarios for the development of hybrid threats.

The third, **operational level**, is focused on ensuring rapid response and incident management. It includes the integration of SIEM/SOAR solutions, cyber intelligence systems, automated mechanisms for detecting and neutralizing cyber threats, as well as digital situation centers using real-time analytical panels. public services.

The fourth, **societal level**, implements the whole-of-society principle through the formation of digital mechanisms for interaction between the state, citizens, business and civil society. It provides for the development of e-participation platforms, crowdsourced monitoring systems, as well as the use of AI agents to analyze public signals and support joint decision-making. Expanding the functionality of national digital platforms, in particular the Diia ecosystem, can become an important element in the formation of a sustainable digital environment for interaction between the state and society.

Thus, the proposed architecture allows vertical integration between the strategic, managerial and operational levels of public administration, as well as horizontal interaction between different institutions, sectors of the economy and social groups. Its implementation will help reduce institutional gaps, increase the efficiency of coordination and form an adaptive system for responding to hybrid and information threats.

The results are consistent with the OECD [8] conclusions on the need to strengthen the capacity of Ukrainian public administration and complement them with a technological dimension, demonstrating that information and computer technologies can act as a key mechanism for accelerating Ukraine's institutional convergence to European governance standards. Further research should be aimed at empirically verifying the effectiveness of the proposed architecture, assessing the impact of digital solutions on the level of state resilience, and developing dynamic models for predicting hybrid threats using artificial intelligence technologies.

Thus, the integrated system of public administration, formed on the basis of modern information and computer technologies, is not only a tool for the digital transformation of public administration, but also a strategic element of ensuring national security and strengthening Ukraine's role in the formation of the European architecture of resilience in the face of long-term hybrid threats.

Comparing the results with previously known facts indicates a qualitative leap in understanding the role of ICT. While previous studies [1, 2] described hybrid threats mainly in conceptual terms, our study provides quantitative estimates that demonstrate an unprecedented growth in Ukraine’s GCI (by 18 points in 4 years) – this is the highest rate among all the countries compared, including the Baltics. At the same time, the decline

in GCI indicators in Estonia, Latvia and Lithuania in 2024 does not indicate a loss of their capabilities, but rather reflects increased requirements and a revision of the methodology, which emphasizes the need for continuous improvement. Thus, our findings not only confirm the OECD's [8] conclusions on the need to strengthen governance capacity, but also add a technological dimension to them, demonstrating that the systematic implementation of digital platforms, AI analytics and automated response systems is a key catalyst for accelerating institutional convergence towards European standards. This creates new knowledge that is different from incremental developments and offers practical tools for other states facing similar threats.

6. CONCLUSIONS

Based on the empirical analysis and answers to the research questions, the following conclusions can be drawn.

The institutional gap between Ukraine and the EU and the Baltics remains significant, especially in the indicators of government effectiveness (difference of 32.8 points), rule of law (30.8) and control of corruption (33.7). At the same time, the positive dynamics of INSGI (growth from 35.93 in 2014 to 44.26 in 2024) indicates the adaptability of Ukrainian institutions even in conditions of full-scale war. The greatest approximation to the European level is observed in the indicator of political stability (EUCI = 78.7%), which is explained by the mobilization of society and state structures.

Ukraine's cyber resilience demonstrates impressive progress: GCI increased from 65.9 (2020) to 83.9 (2024), and the cyber convergence index reached 89% of the EU average. This is an unprecedented growth rate, which exceeds the indicators of the Baltic countries for the same period, which indicates the high ability of the state to digitally transform the security sector even in extreme conditions.

The proposed multi-level digital architecture (infrastructure, analytical, operational and public levels) based on interagency interaction platforms, AI forecasting, SIEM/SOAR solutions and e-participation tools can become an effective mechanism for overcoming the identified institutional gaps. Its implementation will allow to increase the coordination, transparency and adaptability of the public management system of national security.

Thus, the study confirms that an integrated public management system, formed on the basis of modern information and computer technologies, is not only a tool for digital transformation, but also a strategic factor in ensuring the stability of the state in the face of long-term hybrid threats.

Despite the results obtained, there are still aspects that require further study:

1) empirical verification of the proposed digital architecture in pilot projects at the level of individual ministries or regions;

2) development of dynamic models for predicting hybrid threats using artificial intelligence and machine learning technologies based on real data;

3) assessment of the long-term effectiveness of whole-of-society engagement practices in the digital environment, in particular the impact of e-petitions and crowdsourcing systems on the quality of management decisions;

4) adaptation of the developed INSGI and CCI indices for other countries facing hybrid threats, in order to create an international basis for comparative analysis of the sustainability of public administration.

Author Contributions:

Conceptualization – V. Kyrylenko; Methodology – V. Kyrylenko, L. Litvin; Data curation – L. Litvin, I. Tkachenko; Formal analysis – I. Tkachenko, S. Hodlevskyi; Visualization – S. Hodlevskyi; Writing – original draft – V. Kyrylenko, L. Litvin; Writing – review & editing – K. Tkachenko, S. Hodlevskyi; Supervision – K. Tkachenko; Project administration – V. Kyrylenko; Resources – I. Tkachenko, K. Tkachenko. All authors have read and agreed to the published version of the manuscript.

REFERENCES:

[1] G. Giannopoulos, H. Smith, and M. Theocharidou, *The Landscape of Hybrid Threats: A Conceptual Model*. Luxembourg: European Commission, 2020. [Online]. Available: https://euhybnet.eu/wp-content/uploads/2021/01/Conceptual-Framework-Hybrid-Threats-HCoE-JRC.pdf

[2] M. Wigell, H. Mikkola, and T. Juntunen, *Best Practices in the Whole-of-Society Approach in Countering Hybrid Threats*. Brussels, Belgium: European Parliament, 2021, doi: 10.2861/379.

[3] A. Bratko, D. Zaharchuk, and V. Zolka, "Hybrid warfare – a threat to the national security of the state," *Revista de Estudios en Seguridad*

Internacional, vol. 7, no. 1, 2021, doi: 10.18847/1.13.10.

[4] M. Galeotti, "Hybrid, ambiguous, and non-linear? How new is Russia's 'new way of war'?" *Small Wars & Insurgencies*, vol. 27, no. 2, pp. 282–301, 2016, doi: 10.1080/09592318.2015.1129170.

[5] M. Masyk, Z. Buryk, O. Radchenko, V. Saienko, and Y. Dziurakh, "Criteria for governance institutional effectiveness and quality in the context of sustainable development tasks," *International Journal for Quality Research*, vol. 17, no. 2, pp. 501–514, 2023, doi: 10.24874/IJQR17.02-14.

[6] V. Ratsiborynska, "EU-NATO and the Eastern Partnership countries against hybrid threats: From the EU Global Strategy till the war in Ukraine," *Horizon Insights*, vol. 4, no. 4, pp. 20–31, 2021, doi: 10.31175/hi.2021.04.03.

[7] L. Lonardo, *Addressing Hybrid Threats: European Law and Policies*. Cheltenham, U.K.: Edward Elgar Publishing, 2024.

[8] OECD, *Public Governance Review of Ukraine*, OECD Public Governance Reviews. Paris, France: OECD Publishing, 2026, doi: 10.1787/7810f059-en.

[9] E. Bajarūnas, "Understanding the resilience to hybrid threats in the Baltics," in *Democratic Resilience in the Baltics*, vol. 1, D. Schultz, R. Smaliukienė, and V. Giedraitytė, Eds. Cham, Switzerland: Springer, 2026, pp. 23–39, doi: 10.1007/978-3-031-99286-5_3.

[10] S. Kalniete and T. Pildegovičs, "Strengthening the EU's resilience to hybrid threats," *European View*, vol. 20, no. 1, pp. 23–30, 2021, doi: 10.1177/17816858211004648.

[11] D. Kaufmann and A. C. Kraay, *The Worldwide Governance Indicators: Methodology and 2024 Update*, Policy Research Working Paper. Washington, DC, USA: World Bank Group, 2024. [Online]. Available: http://documents.worldbank.org/curated/en/099005210162424110

[12] S. Handoyo, "Worldwide governance indicators: Cross country data set 2012–2022," *Data in Brief*, vol. 51, Art. no. 109814, 2023, doi: 10.1016/j.dib.2023.109814.

[13] R. Jungwirth *et al.*, *Hybrid Threats: A Comprehensive Resilience Ecosystem (JRC129019)*. Luxembourg: Publications Office of the European Union, 2023, doi: 10.2760/37899.

[14] International Telecommunication Union, *Global Cybersecurity Index 2024*. Geneva, Switzerland: ITU, 2024. [Online]. Available: https://www.itu.int/pub/D-HDB-GCI.01-2024

[15] World Bank, *Worldwide Governance Indicators*, 2025. [Online]. Available: https://databank.worldbank.org/source/worldwide-governance-indicators

[16] O. Danchenkova, "Ukraine's hard-won approach to strategic communications and counter-disinformation: Lessons for Europe and beyond," Tech Policy Press, Mar. 12, 2025. [Online]. Available: https://www.techpolicy.press/ukraines-hardwon-approach-to-strategic-communications-and-counterdisinformation-lessons-for-europe-and-beyond/

[17] V. Víchová, N. Nemečkayová, and J. Syrovátka, *Resilient Europe: Best Practices from Across the Continent in Building Resilient Societies*. Prague, Czech Republic: Center for an Informed Society; Association for International Affairs; EUROPEUM Institute for European Policy, 2024. [Online]. Available: https://www.europeum.org/wp-content/uploads/Vichova-Nemeckayova-Syrovatka-Resilient-Europe.pdf

[18] A. Šimelytė, "Social resilience in the Baltic states and crisis management: Lessons learned and future prospects," in *Democratic Resilience in the Baltics*, vol. 1, D. Schultz, R. Smaliukienė, and V. Giedraitytė, Eds. Cham, Switzerland: Springer, 2026, pp. 125–144, doi: 10.1007/978-3-031-99286-5_8.

[19] Council of the European Union, *A Strategic Compass for Security and Defence*. Brussels, Belgium, 2022. [Online]. Available: https://www.consilium.europa.eu/en/policies/strategic-compass/

[20] European Commission, *Proposal for a Directive of the European Parliament and of the Council on the Resilience of Critical Entities (COM/2020/829 Final)*. Luxembourg: Publications Office of the European Union, 2020. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0829

[21] R. Grieveson *et al.*, *Outlier or Not? The Ukrainian Economy's Preparedness for EU Accession*. Gütersloh, Germany: Bertelsmann Stiftung, 2023, doi: 10.11586/2023087.

[22] O. Shebanina *et al*., "Strategic factors quality of public administration in regional development: The experience of EU countries," *International Journal for Quality Research*, vol. 15, no. 4, pp. 1181–1196, 2021, doi: 10.24874/IJQR15.04-19.

[23] A. Astukevičs and E. Vrobļevska, "The evolution of Latvia's defense and security policy in resilience building," Atlantic Council, Jan. 2, 2026. [Online]. Available: https://www.atlanticcouncil.org/in-depth-research-reports/reports/the-evolution-of-latvias-defense-and-security-policy-in-resilience-building/

[24] L. Maschmeyer, *Assessing Hybrid War: Separating Fact from Fiction*, CSS Analyses in Security Policy, no. 332. Zürich, Switzerland: Center for Security Studies, ETH Zürich, Nov. 2023. [Online]. Available: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-security-studies/pdfs/CSSAnalyse332-EN.pdf

[25] I. Lopatchenko, "Public governance of national security: Detection and neutralization of collaboration activities in a hybrid war," *State Formation*, no. 1(37), 2025, doi: 10.26565/1992-2337-2025-1-18.

[26] M. Nardo, M. Saisana, A. Saltelli, S. Tarantola, A. Hoffmann, and E. Giovannini, *Handbook on Constructing Composite Indicators: Methodology and User Guide*. Paris, France: OECD Publishing, 2008, doi: 10.1787/9789264043466-en.

[27] S. Greco, A. Ishizaka, M. Tasiou, and G. Torrisi, "On the methodological framework of composite indices: A review of the issues of weighting, aggregation, and robustness," *Social Indicators Research*, vol. 141, no. 1, pp. 61–94, 2019, doi: 10.1007/s11205-017-1832-9.

[28] D. Zayats, N. Serohina, O. Bashtannyk, L. Akimova, O. Akimov, and A. Mazalov, "Economic aspects of public administration and local government in the context of ensuring national security," *Economic Affairs*, vol. 69, no. 2, pp. 979–988, 2024, doi: 10.46852/0424-2513.3.2024.23.

[29] O. Semenov, "Financial convergence as an indicator of Ukraine's integration readiness for the European Union," *Economy and Society*, no. 80, 2025, doi: 10.32782/2524-0072/2025-80-49.

[30] V. Nekhai *et al*., "Economic consequences of geopolitical conflicts for the development of territorial communities in the context of economic and national security of Ukraine," *Economic Affairs*, vol. 69, no. 1, pp. 551–563, 2024, doi: 10.46852/0424-2513.2.2024.17.

[31] World Bank, *International Telecommunication Union (ITU) – Global Cybersecurity Index (GCI) Dataset*, World Bank Data360, 2025. [Online]. Available: https://data360.worldbank.org/en/dataset/ITU_GCI

[32] X-Road Global, *X-Road Ecosystem*, 2025. [Online]. Available: https://x-road.global

[33] European Commission, *Destination Earth (DestinE): Digital Model of the Earth*, 2024. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/destination-earth

[34] Ministry of Digital Transformation of Ukraine, *Diia — State Services Online*, 2025. [Online]. Available: https://thedigital.gov.ua/projects/technologies/diia-derzhavni-poslugi-onlajn

[35] European External Action Service, *EUvsDisinfo*, 2025. [Online]. Available: https://euvsdisinfo.eu

[36] European Commission, *Report from the Commission on ARACHNE – Implementation for CAP Expenditure*, 2025. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025DC0058

[37] ProZorro, *The Public Procurement Reform in Ukraine*, 2025. [Online]. Available: https://prozorro.gov.ua

[38] e-Governance Academy, *Digital Governance Solutions and Anti-Corruption Initiatives*, 2025. [Online]. Available: https://ega.ee

[39] European Union Agency for Cybersecurity (ENISA), *ENISA Threat Landscape 2025*, 2025. [Online]. Available: https://www.enisa.europa.eu

[40] European Commission, *Cybersecurity Package: Strengthening the EU's Cyber Resilience*, 2025. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity

[41] NATO Cooperative Cyber Defence Centre of Excellence, *CCDCOE Annual Report 2025*, 2025. [Online]. Available: https://ccdcoe.org

[42] N. Aoki, M. Tay, and S. Rawat, "Whole-of-government and joined-up government: A systematic literature review," *Public Administration*, vol. 102, no. 2, pp. 733–752, 2024, doi: 10.1111/padm.12949.

[43] European Commission, *Digital Decade 2025: eGovernment and Digital Public Services*. Luxembourg: Publications Office of the

European Union, 2025. [Online]. Available: https://digital-strategy.ec.europa.eu/

[44] OECD, *Global Trends in Government Innovation 2024: Fostering Human-Centred Public Services*. Paris, France: OECD Publishing, 2024, doi: 10.1787/c1bc19c3-en.

[45] OECD, *The OECD Reinforcing Democracy Initiative: Digital Technologies and Citizen Participation*. Paris, France: OECD Publishing, 2024. [Online]. Available: https://www.oecd.org/governance/reinforcing-democracy/