УДК 355.02:351.86(477)"2000/2022"
DOI: https://doi.org/10.17721/3041-1912.2025/4-1/10

Yurii PUNDA, DSc (Military), Prof.
ORCID ID: 0000-0002-1431-2318
e-mail: yurii.punda@knu.ua
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

LESSONS IDENTIFIED FROM SECURITY GOVERNANCE: THE CASE OF UKRAINE 2000–2022

Background. ***This article examines the evolution of security governance in Ukraine between 2000 and 2022 as a critical determinant of national resilience amid escalating hybrid and armed aggression. The study addresses some systemic gaps between desired and practical governance performance, emphasising the role of strategic foresight, institutional integrity, and civil-military balance in shaping preparedness for large-scale crises.***

Methods. ***The research applies a multi-layered analytical framework combining NATO's DOTMLPFI (Doctrine, Organisation, Training, Material, Leadership, Personnel, Facilities, Interoperability) capability model, strategic foresight methodologies, and causal analysis techniques, including the "5 Whys" approach. The methodological design integrates qualitative content analysis of policy documents, comparative institutional performance assessment, and a system approach to identify structural deficiencies and possible adaptive mechanisms within Ukraine's security and defence sector.***

Results. ***The findings reveal that governance deficits during 2014–2022 were primarily rooted in the absence of institutionalised strategic forecasting, the politicisation of defence planning, and fragmented capability development. However, Ukraine demonstrated outstanding resilience, with societal cohesion, decentralised governance, and rapid technological adaptation compensating for institutional weaknesses. Key governance lessons include the necessity of depoliticising long-term capability development, institutionalising strategic foresight, ensuring transparency and accountability mechanisms, and strengthening strategic communications to align public consensus with threat perception.***

Conclusions. ***The Ukrainian case highlights that effective security governance aligns resources, institutions, and societal resilience in a volatile, uncertain, complex, and ambiguous (VUCA) environment. The findings contribute to the broader discourse on resilience of democracies by demonstrating that the quality of governance is a crucial variable in preparedness, response and recovery after a crisis. These findings have practical implications for reforming security governance models in democracies facing hybrid threats, highlighting the need for adaptive, proactive, and value-driven institutional ecosystems.***

Keywords. ***Lessons learned in security governance; security strategic planning; security capabilities development, resilience of democracies, DOTMLPFI.***

Background

The Russian invasion of Ukraine, launched in 2014 and intensified in 2022, catalysed a radical reassessment of security management paradigms not only for Ukraine but also for democratic societies around the world. The case of Ukraine – a country with a post-Soviet institutional legacy, fragile democratic consolidation, and influenced by military and hybrid aggression – offers a unique empirical prism for examining the prerequisites and shortcomings of national resilience and security governance in the 21st century. This article examines how the structural and procedural characteristics of Ukrainian governance in the security and defense sector shaped its preparedness and response to systemic threats between 2000 and 2022.

Modern security management requires more than simply building military capabilities – it depends on institutional integrity, public trust, strategic foresight, and a real commitment to democratic values. In this context, the trajectory of Ukraine's security system from an under-resourced, politically fragmented security and defense structure to a force capable of confronting a more resourceful aggressor gives an opportunity to extract both cautionary and instructive lessons. Of particular importance for the analysis are examples of institutional weaknesses identified in the early stages of Russian aggression, such as the opaque selection of security and defense leadership, inconsistent planning cycles, reactive rather than proactive threat assessment, and the sources of Ukraine's resilience during a full-scale Russian invasion, which most analysts found unexpected.

The purpose of the article is to systematically analyze the evolution of security governance in Ukraine during the period 2000–2022 in order to identify key structural weaknesses and adaptive mechanisms that influenced national resilience, and to formulate conceptual and practical lessons for improving governance in the security and defense sector. The study specifically seeks to assess the roles of strategic foresight, institutional integrity, and civil-military relations in shaping the effectiveness of state responses to hybrid and large-scale military threats, as well as to develop evidence-based recommendations applicable to Ukraine and other democratic states operating in a VUCA security environment.

The article's central hypothesis is that quality governance in the security and defense sector is one of the fundamental elements of national resilience. In the absence of one of these elements, vulnerability increases; in states where both elements are strong, there are better opportunities to withstand complex, long-lasting existential crises.

The article offers practical lessons (application directions) that other countries can apply, taking into account their own contexts.

Sourses. The study is particularly relevant for its analysis of Ukraine's experience confronting Russia in a hybrid threat environment, where conventional warfare is complemented by cyber operations, disinformation campaigns, and economic and political subversion. Governance failures before 2014 convincingly illustrate "resilience gaps" – vulnerabilities that arise when state institutions are not ready for coordinated multi-domain aggression (Center for Strategic and International Studies, 2025; Beliakova, & Detzner, 2023). Conversely, the post-2014 period was marked by new approaches to security governance adaptation, driven by both international support and domestic reforms (CSIS, 2025). It is noteworthy that Ukraine has begun to integrate scenario planning, strengthen civil-military cooperation, and institutionalise the system of strategic communications, whose activities are primarily aimed at strengthening the democratic legitimacy

ISSN 3041-1912 (Print), ISSN 3041-1920 (Online)

© Punda Yurii, 2025

Вісник Центру політичних досліджень Київського національного університету імені Тараса Шевченка

of the country's leadership and national unity (Helmus, & Holynska, 2024). By analyzing the achievements and failures in security governance over a specified period, this article aims to highlight in some way the possible consequences of the implementation of similar threats for other democracies.

At the beginning of the full-scale Russian invasion, Ukraine's resilience was largely based on society's readiness to confront the enemy, when citizens actively self-organized and took the initiative, complementing the government's efforts. This included massive volunteer efforts to support the armed forces and provide humanitarian aid. The member of the Ukrainian parliament, Iryna Nykorak, emphasised that resilience was based on the "initiative of people" – thousands of Ukrainians who queued up at recruitment centres or supported the army as volunteers and socially responsible businesses (CSIS, 2025).

But even before the full-scale aggression, since 2014, the Ukrainian government, security and defense forces, and civil society have tried to take various measures to counter a more powerful enemy and avoid a very likely economic or civilian collapse in the event of a real war.

For example, even before the 2022 full-scale invasion, Ukraine invested in building institutions for strategic communications and countering disinformation. This included civil society organisations such as StopFake and Detector Media, founded or reoriented in 2013–2014 to expose Russian narratives. In 2021, the Government of Ukraine established the Centre for Strategic Communications and Information Security and the Centre for Countering Disinformation to coordinate with civil society and combat disinformation. The Armed Forces of Ukraine formed the Department of Strategic Communications in 2020 and have been conducting training in information operations with Western partners since 2014. Media literacy programs such as Learn to Discern, launched in 2015, have reached millions of Ukrainians, significantly increasing their resilience to disinformation. Close cooperation between state institutions and civil society organizations has proven to be invaluable in achieving unity of efforts in the information field. Civil society was seen as the "biggest partner" in the joint response. Such cooperation was also implemented in military procurement and recruitment at the unit level, where crowdfunding and support for public organizations filled gaps in state resources (Helmus, & Holynska, 2024.).

Ukraine has developed a legal framework to protect critical infrastructure. The Law of Ukraine "On Critical Infrastructure", which came into act in 2021 (On Critical Infrastruc-ture…, 2021), defined the legal and organizational framework for the creation and operation of the national critical infrastructure protection system, which are fully consistent with European Union standards. (Aebi, Haur, & Kamberaj, 2024).

The corporatisation of state-owned enterprises of the military-industrial complex was carried out, which, according to the authors, was intended to reduce corruption risks and increase transparency in defense supplies (Beliakova, & Detzner, 2023). In July 2023, Ukroboronprom was transformed into a joint-stock company as part of broader reforms to improve transparency and compliance with international standards (Joint-stock company "Ukrainian Defense Industry (JSC Ukrainian Defense Industry, 2023).

Ukraine's resilience has been built through efforts to develop communications between security and defence sector components and society, including local communities, volunteer networks, businesses and civil society organisations. An important factor was the development of local self-government – the decentralization reform after 2014. After the invasion, this allowed territorial communities to respond effectively to the challenges of war, in particular through autonomy in resource management and interaction with local non-governmental organizations (Swedish Civil Contingen-cies Agency, 2023).

Pre-war efforts to synchronize Ukraine's energy system with the European Network of Transmission System Operators for Electricity allowed for emergency synchronization in March 2022, ensuring the power system's resilience during the invasion. At the same time, Ukraine was not fully prepared for such large-scale attacks on its energy system and lost significant generation capacity (Rimutis, 2024).

The organisational structure of Ukrainian Rail Road, with six independent regions, an excess of qualified personnel (engineers, technical specialists), and its own repair facilities, allowed the company to quickly adapt, carry out repair work, and function smoothly as a "lifeline" for the country. The company also used the old but reliable Soviet-era communications system "Selector" for communication between units. (Aebi, Haur, & Kamberaj, 2024).

The rapid implementation of commercial solutions such as Starlink, combined with old but reliable communication systems and significant volunteer efforts, ensured uninterrupted communication despite the attacks. Mobile operators have introduced free domestic roaming and reduced the cost of services, and the government has created a business-friendly environment (Aebi, Haur, & Kamberaj, 2024).

Overall, the reviewed literature demonstrates that, despite substantial efforts to reform and adapt the security governance system, Ukraine entered the full-scale phase of the war with a combination of partial preparedness and systemic vulnerabilities. This contradiction between demonstrated resilience and insufficient institutional readiness remains a central unresolved problem in academic discourse and constitutes a key analytical gap for further research.

Methods

This study uses a multi-level methodological framework to systematically identify structural weaknesses and adaptive mechanisms in Ukraine's security management between 2000 and 2022. The research architecture integrates complementary qualitative and analytical methods, each applied at specific stages of the study to ensure methodological coherence and analytical depth.

At the problem formulation and theoretical justification stage, a systems approach was applied to conceptualise security management as an integrated architecture linking institutions, capabilities, and societal resilience. This approach structured the research problem within the broader framework of national resilience and the VUCA environment, ensuring coherence between the research hypothesis and the analytical design.

At the empirical data collection and primary analysis stage, a qualitative content analysis of strategic, policy, and analytical documents was conducted. This method was used to identify patterns of governance behaviour, institutional responses, and reform trajectories, as well as to identify discrepancies between policy declarations and actual implementation results.

In the analytical phase of the institutional effectiveness assessment, a comparative analysis was conducted to examine differences in governance models between 2014 and 2022. This method enabled the identification of dynamic

Вісник Київського національного університету імені Тараса Шевченка. Воєнні науки. Для службового користування

changes in institutional capacity, civil-military interaction, and strategic planning approaches.

To assess the structure and completeness of security capabilities and link the quality of governance to operational readiness, the study uses the NATO DOTMLPFI framework.

The causal diagnosis phase used the "5 Whys" method to trace governance failures to their root causes. This method allowed for the decomposition of complex systemic problems into underlying structural and procedural factors, thereby supporting the formulation of evidence-based lessons learned.

In parallel, the interpretation phase used a strategic foresight methodology to assess the role of proactive management, scenario planning, and risk modeling in shaping national resilience. This method helped assess how the absence or presence of forward-looking mechanisms influenced preparedness and response outcomes.

Finally, the synthesis phase used an inductive-deductive approach to summarize the findings and formulate conceptual lessons. Induction was used to derive patterns from empirical observations of Ukraine's governance experience, while deduction ensured their coherence with existing theoretical frameworks of security and resilience governance.

The integration of these methods provides a comprehensive analytical toolkit that allows not only to diagnose governance shortcomings, but also to generate transferable lessons for democratic states operating in conditions of hybrid threats and strategic uncertainty.

Results

Perhaps careful preparation would have stabilised the front line before the Russians occupied more than 20% of Ukraine's territory, including the strategically important coast of the Sea of Azov. According to the author, *the main reason for the inadequate preparation for Russia's confrontation was the poor quality of governance in the security and defense sector and the failure of the strategic forecasting system as its defining element.*

Let's look at some considerations.

National resilience today is mostly understood as the ability of a state to *anticipate, neutralise and recover from* a wide range of crises of a national scale of any nature, not only in the military sphere, but also in other areas – cyber, informational, socio-economic and environmental, etc., and various combinations thereof. In this context, governance in the Security and Defence Sector plays a fundamental role in building and maintaining national resilience.

Indeed, effective security governance encompasses three interrelated functions: *managing crisis preparedness, managing crisis response, and managing post-crisis recovery* at the highest level with a focus on security capabilities.

These functions can be implemented by:

- early development of security capabilities based on strategic foresight;
- coordinated deployment of security capabilities during a crisis;
- restoration of security capabilities, taking into account the lessons learned and with adequate feedback mechanisms with direct executors.

At the same time, strategic resilience requires more than just material readiness; it requires security governance structures that are proactive, transparent, accountable, value-based and lead the Security and Defence Sector. That is why it is advisable to consider governance in the security and defence sector through the prism of DOTMLPFI, since governance, in this case, acts precisely as leadership or the highest level of management of national security and defence capabilities. And, at the same time, governance in the security and defense sector is not just an administrative function, but also a key element of the architecture of national resilience. Countries that build integrity, foresight, and adaptability into their security management are more likely to survive and evolve in a VUCA environment.

One of the most critical shortcomings identified at the initial stage of Russia's military aggression against Ukraine was the *lack of adequate military capabilities* to deter or repel a full-scale invasion (Carlough, & Harris, 2025). On the other hand, the greatest achievement of countering Russian aggression in the first stages of the full-scale invasion was the resilience of Ukraine, which manifested itself in an exceptional level of mutual trust of political institutions and citizens of Ukraine – readiness citizens of Ukraine self-organized and joined the defense of Ukraine, while state institutions armed them with minimal bureaucratic restrictions (CSIS, 2025). In this case, it can be considered that the *lack of capabilities and poor governance in preparation for the Russian invasion were compensated at the expense of citizens and society.* And it was the readiness of citizens and society to resist that refuted those forecasts that were based on "military arithmetic", that is, a simple comparison of military potentials.

This deficit can be explained by *systemic deficiencies in strategic forecasting and suboptimal resource allocation in the security and defense sector*.

It is well known that effective governance should be based on forecasting the development of the situation and creating a vision (visualisation) of the goal to achieve, to which the state's resources and efforts are directed (Organisation for Economic Co-operation and Development (OECD), 2025; NATO Allied Command Transformation (NATO ACT), 2024). At the same time, Russia's actions on the eve of the invasion were not properly anticipated, leading to a chaotic response in the first days of the invasion.

Indeed, prior to 2014 and even in the period before 2022, Ukrainian security and defense planning did not adequately take into account the scale, nature, and hybrid nature of Russian operations, as evidenced by the early days of the full-scale Russian invasion. This gap reflected not only the lack of an effective institutionalised forecasting scheme and its implementation, but also the political underestimation (on the verge of deliberate distortion) of Russia's long-term revisionist ambitions.

Thus, Ukraine's mistakes illustrate how insufficient scenario modelling and failure to prioritize investments in critical capabilities can have close to catastrophic consequences.

Lessons Identified. For further analysis of the problem of the lack of necessary security and defence capabilities, we will use the "5 whys" approach (Serrat, 2009; Ohno, 1998). Its application allows us to formulate some lessons from the Ukrainian experience of governance in the security and defense sector during the preparation and repulsion of the Russian invasion. Their list is certainly not exhaustive, but, in the author's opinion, it allows us to identify important lessons of security governance and outline possible ways of developing governance in the field of security and defense, the implementation of which will significantly increase national resilience.

Lesson № 1. The formulation of the lessons can begin with the answer to the first "Why" – "Why was the quality of governance poor?". The most obvious answer is perhaps that no one has tested this quality and assessed the availability of capacities due to the lack of verified or established procedures.

Видавництво Національного університету "Київський авіаційний інститут"

Therefore, *lesson № 1* concerns the urgent need to *develop clear procedures and indicators to assess the effectiveness, transparency and accountability* of government actors in this sector.

Historically, exclusive reliance on political loyalties, opacity of appointments, and lack of independent oversight have led to the formation of a closed institutional environment where accountability has been replaced by negative discretion and transparency has been undermined by excessive secrecy. This lack of a feedback loop between governance and its effectiveness led to unreasonable threat assessments, misallocation of limited resources, and, worst of all, underdeveloped crisis response capabilities. Therefore, from a systemic point of view, the effectiveness of governance (strategic management) can be measured through its ability to anticipate new threats, efficiently allocate and manage resources, and generate adequate security and defense capabilities based on the concept of DOTMLPFI. Thus, the quality of governance does not appear as an abstract normative category but should be empirically assessed by the extent to which it ensures the availability of accessible, adequate to the crisis's conditions, and sustainable capabilities to counter the crisis on D-day – the moment of its appearance. It is also obvious that in preparation for the crisis, the quality of governance can be assessed by comparing the available capabilities and those necessary to counteract the forecasted crisis. Here again, high-quality forecasting of the nature of possible crises is important. However, an extremely negative impact on the forecasting system in the security and defense sector is its dependence on political influence, when future challenges are "tailored" to political guidelines. Thus, it would be logical to conclude that the *forecasting system should be as politically independent as possible and be trusted by different strata and political groups of the population*.

Taking into account the level at which strategic forecasting of the nature of possible crises in the field of security and defense should be carried out, the key priority for the development of governance in this area should be the development of *quantitative and qualitative indicators* of the effectiveness of governance, such as, for example, preparedness indices, monitoring and refinement of forecasts of the nature of possible crises, indicators of the allocation of budgets and resources, normalization of planning phases in the field of national security and defense, and the results assessment of each phase, etc. The main idea of this approach is to find the balance between transparency, accountability and information confidentiality norms. The case of Ukraine highlights that excessive secrecy without accountability undermines resilience, and that national resilience can only benefit from institutionalising mechanisms for monitoring, evaluating and continuously improving the integrity and effectiveness of governance in its security and defence architecture.

Lesson № 2. The second "Why?" – "Why was there no system for assessing the quality of governance?" entails the answer "because no one was interested in responsibility for the implementation of long-term programs", which is always combined with an attempt to redistribute limited resources. *Hence lesson 2 – the need to ensure strategic sustainability: institutionalization of long-term, resource-intensive programs for the development of security and defense capabilities.*

An important governance lesson that emerges from Ukraine's experience in resisting Russian aggression is the need to *create a sustainable system for the implementation of long-term, resource-intensive programs for the development of security and defense capabilities*. This lesson is quite complex and difficult and it is advisable to consider it according to the three components of creating such a system.

At the heart of any capacity development is the choice of investment priorities. However, this process is often politicized, lacks transparency, and is prone to informal influence or rent-oriented (even corrupt) behavior. Blurred accountability in public investment management inevitably leads to inefficient spending with little operational return. The Ukrainian case shows that if the *mechanisms for prioritizing investments* are not structured on evidence-based projections and are not monitored, national resilience thresholds will remain critically low, regardless of the amount of spending.

The implementation period of security and defense programs typically spans several election cycles. However, in fragile democracies, or countries with polarized societies, changes in the political landscape after elections tend to lead to the disruption and sometimes even premature termination of security and defense programs. One way out of this situation is to create a depoliticized institutional framework to ensure the sustainability of strategic programs, insulating the development of security and defense capabilities from the negative impact of temporary or changing political will. Ukraine's fragmented, non-systematic efforts to procure and modernize weapon systems (such as multifunctional missile systems), which later proved necessary during the repulsion of the Russian invasion, underscore the *need to embed hard thresholds for the cancellation of programs* in the governance structure in the security and defense sector.

Capability development must go beyond the mere procurement of weapons or equipment. Developing application doctrines, creating infrastructure and organizational structures, and training personnel for the correct using of new systems at the current stage of technology development is quite time-consuming. Due to that governance in the security and defense sector should primarily ensure the synchronization, resource supply and monitoring of *each DOTMLPFI* capability component, and not just the acquisition of its main carrier. After all, failure to take into account one component often leads to insufficient or improper use of assets, including weapons.

Summing up the conclusions on the adequacy of prioritizing strategic investments, the sustainability and heredity of the implementation of programs in electoral cycles and the introduction of an integrated approach to capability development, it can be argued that the accelerated evolution of modern wars requires *adaptability in the logic of management with the simultaneous provision of sustainability of long-term programs realization and resourcing.* In the era of strategic unpredictability and constant external influences, governance in the security and defense sector should further focus on institutionalizing capacity development through adaptive "vision-oriented" planning, ensuring the sustainability of security programs' resourcing, and transparent investment logic.

Lesson № 3. Let's move on to the third "Why?" – "Why was no one interested in responsibility for the implementation of long-term programs of predecessors?". The answer to it may be somewhat unexpected, since it requires a critical look at one of the basic postulates of democratic civilian control. However, the civil-military sphere divides the areas of responsibility into political and military. But if the responsibility is blurred, no one is responsible for the result.

Therefore, lesson 3 can be formulated as *the need to rethink civil-military relations to ensure doctrinal stability in the security and defense sector.*

Вісник Київського національного університету імені Тараса Шевченка
Військово-політичні науки

ISSN 1728-3817

One of the most complex and politically sensitive governance issues in the security and defense sector, which has already quite often come to the attention of analysts, mostly in the form of weak signals but has been very painful for Ukraine, is the excessive dependence of security governance on electoral cycles and political instability. Moreover, in the context of modern hybrid threats, characterized by information warfare, foreign interference in the electoral process and manipulation of public discourse, external actors can significantly influence the election results and indirectly the domestic political agenda. And, as a rule, external influence is aimed precisely at defense and security programs in the entire spectrum of their life cycle – from determining investment priorities to applying their product. The ultimate goal of such influences is to undermine the enemy's defensive capabilities or build up their own.

This problem has manifested itself quite acutely in Ukraine. After all, Russian hybrid intervention has directly affected all aspects of security and defense policy. Each election-related change of leadership in Ukraine has led to radical changes in the foreign policy vector, the associated priorities of defense planning, and all other aspects of the development of security and defense capabilities. At the same time, external interference in the formation of security and defense policy is not only a problem for Ukraine. It is also typical for members of military-political alliances, especially if the alliances include countries with different military and political weight; and for countries polarized by national, religious or other characteristics.

This vulnerability requires a *rethinking of civil-military relations structure*, in particular finding a balance between democratic control and strategic sustainability. Changes in foreign and defense policy after elections carry the above-described risks of changing the fundamentals of foreign and security policy, and, as a result, disrupting capability development programs due to changing doctrinal frameworks. This is how a conflict arises between temporary political priorities and long-term national security and defense needs. Therefore, the lesson is clear: *to ensure national resilience, there must be institutional safeguards that protect security and defense doctrines and programs from excessive politicization*. An effective civil-military balance requires clear legal mandates (descriptions of authority, responsibility and accountability) for political and security and defense institutions, independent advisory bodies and mechanisms that support the strategic sustainability of elected institutions. Without such buffers, there are high levels of risks of undermining national resilience through internal conflicts and failures in security and defense governance.

Lesson № 4. Therefore, lesson No. 4, which concerns civil-military relations, can be formulated as the necessity to single out the selection and development of strategic leaders in a separate direction of ensuring national security.

The Ukrainian experience has revealed a critical vulnerability in the process of selecting and developing strategic leaders in the security and defense sector. The politicization of appointment processes and the lack of institutional safeguards contributed to the penetration of foreign influence into the leading echelons of national security and defense. This became especially evident in the early stages of Russian aggression in 2014, when a significant number of high-ranking officials were put on the wanted list or prosecuted for treason – a phenomenon that signaled the hurt of the national security and defense system up to the strategic level (Punda 2025, pp. 285–296).

Indeed, modern conflicts are not limited to kinetic operations – rather, influencing strategic leadership has become a real battleground of cognitive warfare. Disinformation campaigns and malicious destruction of the reputation of nationally oriented leaders, artificial promotion of biased or in one way or another affiliated with the enemy to leadership positions are increasingly used to delegitimize authorities, undermine national unity and create conditions for managerial paralysis. Such actions create a toxic environment in which strategic leadership loses legitimacy in the eyes of society, and political decisions lose the necessary support. Taking into account the above-mentioned considerations regarding the need to modernize civil-military relations, it can be concluded that there is a need to introduce parallel lines of selection and development of strategic leaders – one political (ensuring legitimacy and civilian control) and one professio-nal (ensuring competence and coherence with policy). Institutional mechanisms such as strategic leadership review boards, integrity-based promotion systems, and digital monitoring of reputation manipulation should be integrated into human capital management strategies.

Failure to ensure the integrity of leadership jeopardizes doctrinal sustainability, undermines the morale of the population, and damages the credibility of institutions. The Ukrainian case illustrates that the *selection of strategic leaders should be reconsidered not only as a function of personnel management but also as a principle of national security and resilience*.

Lesson № 5. The fourth "Why?" – "Why was no one interested in responsibility for the implementation of long-term programs?" may have the answer "Because no one understood what needed to be achieved". Such an answer leads us to the next lesson No. 5 – *the need for a clear formulation of a strategic vision and the formation of a public consensus on the perception of threats.*

A critical weakness in the governance of Ukraine's Security and Defense Sector prior to the Russian invasion was the lack of a clear, coherent, and socially acceptable vision of threats. Of course, it was quite clearly described in the top-level security and defense planning documents. However, declaring such a list in regulatory documents is not effective without continuous communication with citizens and the demonstration of concrete steps for its implementation, not only at the national level of governance but also at the regional and sectoral management levels.

"Threat visualization" is of particular importance for the formation of transparent mechanisms for the distribution of national resources. After all, the rule "what is financed is doing" is absolutely clear in modern democratic societies. Therefore, periodic threats declarations for which no resources are allocated, or the allocation of resources to measures unrelated to real threats, can only undermine trust in the government and have an extremely negative impact on the quality of governance and national resilience.

Lesson 5 emphasizes the need to formulate a publicly endorsed strategic vision that should, at a minimum, determine the nature and sources of anticipated threats, as well as justify allocating resources to prepare for possible crises. That is, in democratic societies, the vision of security and the legitimacy of security and defense spending should be based on *effective strategic communications and broad public understanding.*

The Ukrainian experience demonstrates how the ambiguity in threat perceptions, exacerbated by the doctrine of "multi-vector foreign policy", contributed to strategic paralysis. Changes in political orientations after election

Видавничий Дім «Гельветика»
Київський університет імені Бориса Грінченка

cycles led to radical changes in security and defense priorities, redistribution of budgets, and, finally, gaps in capability. This institutional vulnerability was further exploited and developed by Russian hybrid strategies, including disinformation and manipulation of perceptions elites and the public.

Thus, the lesson involves the institutionalization of a *stable narrative of national security and defense,* resistant to electoral and political divergences. It is advisable to develop and implement a model of a "scenario communication strategy" that integrates public consultations and expert consensus. In any case, it is important that changes in external or defense priorities are accompanied by public justification and discussion, thus ensuring co-responsibility citizens for national resilience, security and defense. Conversely, the failure to ensure public consensus on threat perceptions undermines the legitimacy of governance in the security and defense sector and creates fertile soil for foreign influence and internal fragmentation.

Lesson № 6. Another option for answering the fourth "Why?" could be "Because there are no institutions in the state that are responsible for visualizing the strategic vision and strategic forecasting in the field of security in general".

Hence lesson No. 6 – *the need to institutionalize strategic forecasting and scenario planning in the security and defense sector*

Russia's full-scale invasion in 2022 clearly revealed the limitations of the decision-making approach, which relies solely on real-time situational threat assessments and response, without taking into account long-term strategic planning and systems analysis. Instead, strategic resilience depends on the ability to anticipate, model, and prepare for complex, multidimensional crisis trajectories.

Strategic foresight should go beyond intelligence analysis and include scenario planning, risk modeling, and the identification of critical uncertainties. This process increases national preparedness, ensuring time gain, resource optimization, and organizational coherence between government and security structures.

Moreover, this *predictive capacity must be institutionally independent*, protected from short-term political pressures, and embedded in national security standard operating procedures (SOP). As the case of Ukraine has shown, scenarios that were once considered implausible should be included in preparedness planning processes.

Thus, Lesson 6 emphasizes that modern governance in the security and defense sector should consider strategic forecasting not as an additional elective-like burden but as one of the fundamental principles. *Strategic forecasting creates a forward-looking management logic, which is crucial for national resilience in an unstable geopolitical environment*.

Lesson № 7. And finally, the fifth why? "Why a strategic vision and public consensus were not formulated" entails a very complex answer – the weakness of civilian oversight of the Security and Defense Sector, the incomplete transformation from a post-Soviet institution, the lack of real partnerships with identical institutions of democratic countries, the inertia of thinking, etc. Accordingly, there are several identified lessons as a response to this question.

The confrontation between Ukraine and Russia is not just a regional geopolitical crisis, but also the front line of the global struggle between democratic and autocratic political systems. At the heart of this systemic conflict is a fundamentally different attitude to human rights: in democracies, human rights are not only moral imperatives, but also basic principles of governance; in autocracies, they are nothing more than slogans, which are used at the necessary moment for political control and the preservation of the regime.

The development of governance in the security and defense sector should be based on human rights and freedoms, ensuring the coexistence of operational efficiency with the ethical foundations of democracy. The experience of Ukraine confirms that *the alignment of governance with human rights is not only a normative position, but also a security imperative*, since this has become the basis for uniting the citizens of Ukraine in crisis conditions. The basis of such unity should primarily be the trust of citizens in the country's institutions and strategic leaders, who are able to inspire the achievement of a clearly formulated vision.

Lesson 7 emphasizes that protecting citizens' rights and dignity is not an auxiliary function but a central axis of national resilience and governance in the security and defense sector. In democratic systems, the protection of civil liberties, minority rights, and institutional checks and balances underpins public trust and fosters cohesion in crisis situations. Instead, autocracies instrumentalize legal systems and suppress dissent, making themselves inherently fragile under pressure.

Ukraine's fight illustrates how the protection of liberal democratic values, in particular human rights, has become both a target and an instrument of hybrid warfare. Russian narratives have deliberately discredited human rights discourses as "Western instruments of destabilization" while using identity politics and cultural imagery as weapons to undermine democratic consensus.

Lesson № 8. The experience of Ukraine confirms the fact that *democratic values – freedom, dignity, the rule of law – do not provide security by themselves*. Although these principles constitute the normative basis of the Western political order, passive presence in such an environment does not offer protection from external manipulation, coercion, subversion or war. Therefore, values need not only to be declared, they need to be actively defended, promoted and communicated with society, and, if necessary, protected by force.

The open ideological opposition of the Russian federation to liberal-democratic values underscores the reality that the global security landscape is as much a battle of narratives as it is a battle of armies. Ukraine's struggle has exposed the vulnerability of a society that treats the protection of values as a secondary task. Information warfare, legal manipulation and cultural revisionism have become tools by which authoritarian states undermine democratic integrity from inside.

Thus, modern security governance should include a clear architecture for protecting (and promoting) universal human values, which provides for effective strategic communications, legal resilience, civic education, etc.

For Ukraine and young democracies, the introduction of value resilience into national planning is an objective requirement of our time. The lesson is clear: *those who do not prepare to defend their own values become vulnerable to the infiltration of authoritarian ideologies and the "corrosion" of national resilience*. Security governance in the 21st century should consider the protection of values as a strategic goal, not declarations of intent.

Lesson № 9. Another policy lesson emerging from Ukraine's experience in security governance concerns the limitations of collective defense mechanisms and external security guarantees. Despite the fact that Ukraine received formal security guarantees, in particular under the 1994 Budapest Memorandum, in 2014 it was left alone in the face of russian aggression. This revealed a critical flaw in the international security architecture: the gap between declarative solidarity and effective defense.

Вісник Київського національного університету імені Тараса Шевченка

ISSN 1728-3817

Lesson 9 highlights that *alliances that are not based on shared readiness, values, and training are structurally fragile*. Institutional inertia, lack of interoperable mechanisms, and divergent perceptions of threats among allies can paralyze decision-making in moments of crisis. As the case of Ukraine shows, even democracies may be hesitant to act decisively to defend proclaimed values if systems of coordination, threat perception, and strategic decision-making are inert and unbalanced.

Ukraine's lesson for the international community is clear, but at the same time constructive: alliances must be implemented, not just voiced. Formal treaties must be accompanied by exercises, training, doctrinal convergence and strong political will. In addition, *alliances must create platforms for strategic communication,* to reaffirm shared values at risk and prevent fragmentation under pressure and, as a result, to make quick and effective collective decisions in crisis conditions.

Lesson № 10. The evolution of warfare in the 21st century demonstrates that superiority in combat increasingly depends not on numerical superiority but on the *speed of technological adaptation and the dissemination of best practices*. Ukraine's experience in repelling Russia's large-scale invasion has revealed a critical characteristic: the strategic advantage has the side that adapts faster rather than simply possessing more armaments.

Management systems in the security and defense sector must institutionalize mechanisms for rapid technological adaptation and accelerated learning. This includes streamlining procurement cycles, integrating frontline feedback into defense industry capability development and personnel training, and removing bureaucratic hurdles that hinder the deployment of new tools, tactics, and systems. The example of Ukraine's successful use of commercial drone technologies and decentralized command-and-control networks illustrates this flexibility.

Moreover, the proliferation of innovations on the battlefield – ensuring the rapid transfer of local effective practices (e.g., in electronic warfare, anti-drone tactics, or logistical improvisation) between units and commands – requires special processes for rapid doctrine updates, simulation training, and inter-species coordination. Without such mechanisms, battlefield superiority remains localized and unstable.

Thus, the war in Ukraine has shown that governance in the security and defense sector must consider technological adaptability, updating doctrines and training as decisive factors for resilience and victory. In this sense, flexibility rises from the level of competitive advantage, to the level of existential demand.

Discussion and conclusions

The results of this study support the central hypothesis that the quality of governance in the security and defense sector is a crucial variable in shaping national resilience in the face of hybrid and large-scale military threats. The Ukrainian case demonstrates that governance must synchronize strategic foresight, institutional integrity, capability development, and societal mobilization into a holistic security architecture.

From a theoretical perspective, the study findings contribute to the discourse on Democracy Resilience by highlighting a critical asymmetry: while democratic systems have inherent advantages in adaptability and social cohesion, they remain vulnerable to governance fragmentation, politicization, and insufficient institutionalization of long-term strategic planning. This can create a situation in which resilience emerges despite governance shortcomings, but such resilience is neither sustainable nor scalable without systemic reforms.

The discussion of the empirical results shows that Ukraine's resilience during a full-scale invasion was largely compensatory. Social cohesion, decentralized governance, and technological adaptability acted as force multipliers that compensated for pre-existing institutional weaknesses. However, this model of "compensatory resilience" should be interpreted as a high-risk configuration, as it relies on extraordinary mobilization rather than on stable institutional capacity. The study therefore highlights the need to move from reactive resilience to proactive, foresight-oriented governance systems.

A key finding of the study is the strategic role of institutionalized forecasting and scenario planning. By 2022, the inefficiency of these mechanisms significantly limited preparedness and contributed to suboptimal resource allocation. On the contrary, the integration of forecasting tools, such as scenario modeling, risk assessment, and early warning systems, is becoming a critical factor in facilitating proactive governance. In this respect, the findings are consistent with contemporary NATO and OECD approaches that emphasize a shift from linear planning to adaptive, scenario-based decision-making models.

In terms of practical implications, the study suggests a set of governance-oriented lessons that can be applied to defense planning and governance systems. These include:

- depoliticizing and institutionalizing long-term capability development programs;
- establishing measurable performance and accountability indicators for governance;
- developing two-way systems for strategic leadership selection (political legitimacy and professional competence);
- institutionalizing strategic communications to ensure public consensus on threat perceptions;
- integrating technological adaptation mechanisms into governance processes.
- Together, these actions form a governance transformation agenda that can improve preparedness, response, and recovery capabilities in democracies facing hybrid threats.

Further research could focus on analyzing the increasing complexity, rapid technological change, and the blurring of boundaries between the military and non-military domains of the future security environment. There is a need to develop quantitative indicators to assess the quality of governance within the DOTMLPFI framework, enabling comparative analysis across countries. Future research should explore integrating artificial intelligence and big data analytics into strategic foresight processes, especially in the context of hybrid threats. Additionally, the relationship between societal resilience and institutional capacity warrants further study, particularly to identify optimal governance configurations that balance state power and citizen participation.

Finally, the broader strategic impact of this research lies in its potential to shape paradigm shifts in security governance in democratic systems. By demonstrating that resilience is not an emergent property but a function of purpo-seful governance design, the research provides a conceptual framework for rethinking national security strategies. In this sense, Ukraine's experience serves not only as an example, but also as a promising model that highlights both the risks of governance failure and the opportunities for building adaptive, resilient, and value-based security systems in the 21st century.

Військовий університет імені Івана Черняховського
Копія. Не для продажу

ISSN 3041-1912 (Print), ISSN 3041-1920 (Online)

Sources of funding. This study did not receive any grant from a funding institution in the public, commercial, or non-commercial sectors.

References

Aebi, S., Hauri, A., & Kamberaj, J. (2024). *Critical infrastructure resilience in Ukraine: Energy, transportation, and communication*. ETH Centre for Security Studies. https://tinyurl.com/4yxyttxe

Beliakova, P., & Detzner, S. (2023). *Security sector governance and reform in Ukraine*. University of Edinburgh. https://peacerep.org/wp-content/uploads/2023/11/SSG-Report-v3-FINAL-.pdf

Carlough, M., & Harris, B. (2025). *Comparing the size and capabilities of the Russian and Ukrainian militaries*. Council on Foreign Relations. https://tinyurl.com/y39a96ry

Center for Strategic and International Studies. (2025). *Conflict in focus: Whole of society resilience lessons from the Russia-Ukraine war*. CSIS. https://tinyurl.com/4u5ksuy6

Helmus, T., & Holynska, K. (2024). *Ukrainian resistance to Russian disinformation: Lessons for future conflict*. RAND Corporation. https://www.rand.org/content/dam/rand/pubs/research_reports/RRA2700/RRA2771-1/RAND_RRA2771-1.pdf

JSC Ukrainian Defense Industry. (2023). *Charter of the joint stock company "Ukrainian Defense Industry"*. https://ukroboronprom.com.ua/documents/statut

NATO Allied Command Transformation. (2024). *Strategic foresight analysis 2023*. https://www.act.nato.int/wp-content/uploads/2024/05/SFA2023_rev2.pdf

Ohno, T. (1988). *Toyota production system: Beyond large-scale production*. Productivity Press.

Organisation for Economic Co-operation and Development. (2025). *Strategic foresight toolkit for resilient public policy: A comprehensive foresight methodology to support sustainable and future-ready public policy*. OECD. https://tinyurl.com/44hr5pk6

Punda, Y. (2025). *Strategic leader development and selection: Ukrainian lessons identified from 2014*. In *The Conference on Russia 2025: Strategic pathways to ending the Russo-Ukrainian war*. https://www.rusconf.eu/wp-content/uploads/2025/02/Rusconf_25_veeb.pdf

Rimutis, S. (2024). *Lessons of war: Ukraine's energy infrastructure damage, resilience and future opportunities*. GSSC. https://tinyurl.com/4ctm9pmv

Serrat, O. (2009). *The five whys technique*. Asian Development Bank. https://www.adb.org/sites/default/files/publication/27641/five-whys-technique.pdf

Swedish Civil Contingencies Agency. (2023). *Building resilience for the future – Lessons from Ukraine*. MSB. https://tinyurl.com/5a54v3nd

On critical infrastructure, Law of Ukraine. (2021). Verkhovna Rada of Ukraine [in Ukrainian]. [Про критичну інфраструктуру, Закон України. (2021). Верховна Рада України]. https://zakon.rada.gov.ua/laws/show/1882-20#Text

Отримано редакцією журналу / Received: 11.11.25
Прорецензовано / Revised: 10.12.25
Схвалено до друку / Accepted: 18.12.25

Юрій ПУНДА, д-р військ. наук, проф.
ORCID ID: 0000-0002-1431-2318
e-mail: yurii.punda@knu.ua
Київський національний університет імені Тараса Шевченка, Київ, Україна

УРОКИ БЕЗПЕКОВОГО УРЯДУВАННЯ УКРАЇНИ: 2000–2022

В с т у п. ***Досліджено еволюцію безпекового урядування в Україні між 2000 і 2022 рр. як критичний фактор національної стійкості в умовах ескалації гібридної та збройної агресії. Розглянуто деякі системні розриви між бажаними та практичними показниками урядування, підкреслюючи роль стратегічного передбачення, інституційної цілісності та цивільно-військового балансу у формуванні готовності до масштабних криз.***

М е т о д и. ***У дослідженні застосовано багаторівневу аналітичну структуру, що поєднує модель можливостей НАТО DOTMLPFI (Doctrine, Organisation, Training, Material, Leadership, Personnel, Facilities, Interoperability – доктрина, організація, навчання, матеріали, лідерство, персонал, інфраструктура, взаємосумісність), методології стратегічного передбачення та методи причинно-наслідкового аналізу, серед яких і підхід "5 чому". Методологічний підхід інтегрує контент-аналіз політичних документів, порівняльну оцінку інституційної ефективності та системний підхід для виявлення структурних недоліків і можливих адаптивних механізмів для урядування в секторі безпеки й оборони України.***

Р е з у л ь т а т и. ***Показано, що недоліки безпекового урядування протягом 2014–2022 рр. були переважно пов'язані з відсутністю інституціолізованої стратегічної прогнозувальної діяльності, політизацією оборонного планування та фрагментованим розвитком безпекових спроможностей. Однак Україна продемонструвала виняткову стійкість завдяки суспільній згуртованості, децентралізації та швидкій технологічній адаптації, що компенсували інституційні слабкості. Ключові уроки управління передбачають необхідність деполітизації довгострокового розвитку безпекових спроможностей, інституціоналізації стратегічного прогнозування, забезпечення механізмів прозорості та підзвітності, а також зміцнення стратегічних комунікацій для громадського консенсусу у сприйнятті загроз. У дослідженні також визначено дедалі більшу важливість технологічної гнучкості й інтеграції громадянського суспільства як мультиплікаторів сили в сучасних умовах ведення війни.***

В и с н о в к и. ***Український досвід підкреслює, що ефективне урядування в межах архітектури національної безпеки узгоджує ресурси, інституції та суспільну стійкість у нестабільному, невизначеному, складному та неоднозначному (VUCA) середовищі. Результати дослідження сприяють дискусії щодо стійкості демократій, демонструючи, що якість управління є вирішальною змінною в готовності, реагуванні та відновленні після кризи. Ці висновки мають практичне значення для реформування моделей управління безпекою в демократіях, що стикаються з гібридними загрозами, підкреслюючи необхідність адаптивних, проактивних та ціннісно-орієнтованих інституційних екосистем.***

К л ю ч о в і с л о в а : ***вивчені уроки безпекового урядування, безпекове стратегічне планування, розвиток безпекових спроможностей, стійкість демократій, DOTMLPFI.***

Автор заявляє про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The author declares no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

Вибрані історичні праці "Київський університет" Версія НЕ ДЛЯ ДРУКУ