

05

STRATEGIC PLANNING:

A TRANSDISCIPLINARY ANALYSIS OF UKRAINE'S EXPERIENCE FOR STATES WITH HIGH SECURITY RISKS

**PLANIFICACIÓN ESTRATÉGICA: UN ANÁLISIS TRANSDISCIPLINARIO DE LA EXPERIENCIA DE UCRANIA
PARA ESTADOS CON ALTOS RIESGOS DE SEGURIDAD**

Tetiana Bielska¹

E-mail: tetiana.bielska@kname.edu.ua

ORCID: <https://orcid.org/0000-0002-2792-4700>

Vasyl Shkoliarenko²

E-mail: vasyl1970@yahoo.com

ORCID: <https://orcid.org/0000-0001-8274-2232>

¹ O. M. Beketov National University of Urban Economy in Kharkiv. Kharkiv, Ukraine.

² Military Academy named after Yevhenii Berezniak. Kyiv, Ukraine.

Suggested citation (APA, 7th edition)

Bielska, T., & Shkoliarenko, V. (2026). Strategic planning: A transdisciplinary analysis of Ukraine's experience for states with high security risks. *Revista Transdisciplinaria de Estudios Sociales y Tecnológicos*, 6(3), 52-67.

Submission: 06/26/2026

Acceptance: 08/07/2026

Publication: 09/01/2026



ABSTRACT

The transformation of the international security environment has highlighted the need to reconsider traditional approaches to strategic planning. The purpose of this study is to conduct a transdisciplinary analysis of Ukraine's experience in strategic planning during full-scale war and to identify conceptual approaches, institutional mechanisms, and practical lessons that can be adapted by states facing high levels of contemporary security risks. In this research, strategic planning represents the process of strategy development as a course of action that orchestrates strategic ends, ways, and means in order to accomplish higher national political objectives. For Ukraine, the latter were consolidated exclusively into the preservation of Ukrainian national statehood and the creation of conditions for enduring and just peace. The research employs a qualitative methodology based on comparative analysis, systems analysis, institutional analysis, and synthesis of contemporary academic literature on defence planning, capability development, multidomain operations, and strategic resource management. The findings demonstrate that effective strategic planning should be understood as an adaptive governance system integrating strategic security environment analysis, capability-based and risk-oriented planning, multidomain operations, strategic resource governance, whole-of-government and whole-of-society coordination, and international interoperability. Based on these findings, the study proposes the Transdisciplinary Strategic Planning Framework for High-Risk States, which integrates six mutually reinforcing dimensions into a unified analytical model. The study argues that Ukraine's wartime experience should be regarded not only as a national case of defence adaptation but also as a valuable source of transferable strategic principles for countries confronting military, hybrid, cyber, and transnational security threats.

Keywords:

Strategic planning, security and defence, multidomain operations, capability-based planning, risk management, resilience, security governance.

RESUMEN

La transformación del entorno de seguridad internacional ha puesto de relieve la necesidad de reconsiderar los enfoques tradicionales de la planificación estratégica. El objetivo de este estudio es realizar un análisis transdisciplinario de la experiencia de Ucrania en planificación estratégica durante una guerra a gran escala e identificar enfoques conceptuales, mecanismos institucionales y lecciones prácticas que puedan ser adaptadas por los Estados que enfrentan altos niveles de riesgos de seguridad contemporáneos. En esta investigación, la planificación estratégica representa el proceso de desarrollo de la estrategia como un curso de acción que coordina fines, métodos y medios estratégicos para lograr objetivos políticos nacionales superiores. Para Ucrania, estos últimos se consolidaron exclusivamente en la preservación de la identidad nacional ucraniana y la creación de condiciones para una paz duradera y justa. La investigación emplea una metodología cualitativa basada en el análisis comparativo, el análisis de sistemas, el análisis institucional y la síntesis de la literatura académica contemporánea sobre planificación de la defensa, desarrollo de capacidades, operaciones multidominio y gestión de recursos estratégicos. Los hallazgos demuestran que la planificación estratégica eficaz debe entenderse como un sistema de gobernanza adaptativo que integra el análisis del entorno de seguridad estratégica, la planificación basada en capacidades y orientada al riesgo, las operaciones multidominio, la gobernanza de los recursos estratégicos, la coordinación de todo el gobierno y de toda la sociedad, y la interoperabilidad internacional. A partir de estos hallazgos, el estudio propone el Marco de Planificación Estratégica Transdisciplinaria para Estados de Alto Riesgo, que integra seis dimensiones que se refuerzan mutuamente en un modelo analítico unificado. El estudio sostiene que la experiencia de Ucrania durante la guerra debe considerarse no solo como un caso nacional de adaptación de la defensa, sino también como una valiosa fuente de principios estratégicos transferibles para países que enfrentan amenazas militares, híbridas, cibernéticas y de seguridad transnacional.

Palabras clave:

Planificación estratégica, seguridad y defensa, operaciones multidominio, planificación basada en capacidades, gestión de riesgos, resiliencia, gobernanza de la seguridad.

INTRODUCTION

The transformation of the international security environment following the Russian Federation's full-scale invasion of Ukraine in 2022 has profoundly redefined the traditional paradigms of strategic planning in the security and defence sectors. Contemporary conflicts are no longer confined exclusively to the military domain but increasingly encompass closely interconnected dimensions such as cyber operations, critical infrastructure protection, economic resilience, information warfare, hybrid threats, energy security, civil protection, and cooperation between public and private institutions. Consequently, strategic planning has evolved into a complex and multidimensional process that requires the integration of military, political, economic, technological, legal, and institutional capabilities, together with permanent coordination mechanisms involving the State, the private sector, and civil society. Under these conditions, transdisciplinary approaches have gained increasing relevance by enabling the design of adaptive planning systems capable of responding to environments characterized by high levels of uncertainty, rapid change, and multiple simultaneous threats of diverse nature.

The growing complexity of the international strategic environment has exposed the limitations of traditional planning models, which have been primarily centered on military preparedness and conventional responses to interstate conflicts. Today, national security depends on the continuous interaction between military capabilities, institutional resilience, technological innovation, risk management, public governance, and international cooperation. Consequently, strategic planning can no longer be understood solely as a process of defining military objectives but rather as an integrated governance system that articulates public policies, operational capabilities, strategic resources, and decision-making processes aimed at ensuring state stability in the face of complex and multidomain threats. This conceptual transformation has fostered the development of new analytical approaches designed to integrate dimensions that have traditionally been examined independently, thereby promoting more flexible, coordinated, and sustainable responses to prolonged crisis scenarios.

Within this context, Ukraine represents one of the most significant contemporary examples of the comprehensive transformation of national security governance under conditions of high-intensity interstate warfare. Since the onset of the full-scale invasion, the country has simultaneously modernized its operational planning processes, defence capability development, interagency coordination, civil-military cooperation, strategic communications, cyber defence, military logistics, and international security partnerships while sustaining continuous military operations across multiple fronts. This experience extends far beyond its national context and constitutes an important reference

for other states facing elevated security risks, including those confronted with hybrid threats, terrorism, transnational organized crime, border conflicts, military aggression, or increasing geopolitical competition. Consequently, the Ukrainian case offers an exceptional opportunity to examine how strategic planning systems can adapt when uncertainty, the pace of change, and the convergence of multiple threats replace traditional security paradigms.

Scientific interest in understanding the transformations resulting from the Russia-Ukraine war has increased considerably in recent years. Nevertheless, the available academic literature continues to exhibit a high degree of disciplinary specialization. Most existing studies analyses separately issues related to the international security architecture, strategic culture, military planning, technological innovation, risk management, or institutional cooperation, without integrating these components into a comprehensive analytical framework capable of explaining strategic planning as a transdisciplinary system. This fragmentation limits the development of conceptual models applicable to contemporary security environments, where the interaction among military, political, economic, social, and technological factors largely determine the effectiveness of national security policies.

A first stream of research examines the transformation of the international security architecture, European defence policies, and collective security mechanisms that have emerged following the conflict. These studies demonstrate that the war has accelerated European defence integration, strengthened the European Union's strategic autonomy, and redefined various instruments of international security cooperation. They also analyses Ukraine's growing role as a key element in maintaining the geopolitical stability of the European continent and explore possible configurations of the post-war European security system. However, although these studies provide valuable insights into the geopolitical transformations generated by the conflict (Cardwell & Moret, 2023; Evangelista, 2024; Fiott, 2023), they devote comparatively limited attention to strategic planning methodologies that can be adopted by national security and defence institutions (Genini, 2025; Helwig, 2023; Kotlyar & Lyman, 2025).

A second stream of research focuses on strategic culture, institutional resilience, and the adaptation of national defence systems to the evolving characteristics of contemporary warfare. From this perspective, several scholars argue that a state's ability to confront complex threats depends not only on its military resources but also on the strength of its institutions, organisational learning, continuous innovation, and the capacity to transform decision-making structures as strategic environments evolve. These studies have significantly expanded the theoretical understanding of resilience and institutional adaptation (Fedorchak, 2024; Götz & Staun, 2022). Nevertheless, they

continue to examine these processes from relatively independent perspectives without fully integrating them into comprehensive strategic planning models (Reznikova, 2022; Reznikova et al., 2024).

A third line of research has focused on capability-based planning, multidomain operations, and the transformation of military structures. These studies demonstrate that technological evolution and the convergence of the land, air, maritime, space, cyber, and information domains have substantially reshaped operational planning processes, requiring coordination mechanisms that are considerably more flexible and integrated than those employed in conventional warfare. At the same time, military capability management has increasingly incorporated approaches based on interoperability standards (Horbatiuk et al., 2025; Kurashkevych & Tushko, 2025), technological development, and adaptive planning, all of which have become fundamental components of the modernization of Ukraine's armed forces (Lutsyk et al., 2023; Semenenko et al., 2024).

Another important research stream has examined risk management, crisis response, and the strategic management of resources within the security and defence sector. These studies argue that contemporary military operations depend increasingly less on isolated military superiority and increasingly more on institutional capacity to identify risks, anticipate future scenarios, manage critical resources, and ensure operational continuity throughout prolonged conflicts. Consequently, strategic planning now incorporates continuous processes of threat assessment, vulnerability analysis, organizational resilience enhancement, and the optimization of financial, logistical, and technological resources (Ignatiev et al., 2025; Ketners, 2025; Pashchenko & Ivashchenko, 2023). From this perspective, national security is understood as an integrated system in which the efficient management of strategic resources is as essential as the development of military capabilities (Petrukha et al., 2025; Rohulia et al., 2025).

In parallel, a growing body of research has incorporated institutional cooperation and the so-called *whole-of-society approach*, recognizing that effective responses to complex threats require the coordinated participation of military organizations, government agencies, private enterprises, academic institutions, and civil society organizations. This perspective moves beyond the traditional paradigm of state defence by considering national resilience as dependent upon the integration of human, technological, economic, and institutional resources within a governance architecture capable of responding coherently to crisis situations. Within this framework, public-private partnerships, interinstitutional cooperation (Dragan et al., 2025; Masitoh et al., 2025), and multilevel coordination have become strategic components for strengthening

states' capacity to respond to persistent and multidimensional threats (Roelsgaard Obling et al., 2026).

Collectively, these studies have substantially advanced scholarly understanding of the transformation of contemporary security and defence systems. Nevertheless, a comparative review of the literature reveals several important research gaps. First, fragmented disciplinary approaches continue to dominate the field, treating military planning, public administration, cybersecurity, institutional resilience, and international cooperation as largely independent areas of inquiry, thereby limiting a comprehensive understanding of their interrelationships. Second, Ukraine's wartime experience continues to be presented primarily through sector-specific analyses and case studies, restricting the identification of institutional principles that could be transferred to other states facing comparable security challenges. Finally, there remains a lack of an integrated conceptual framework capable of linking the strategic, operational, institutional, and governance dimensions of strategic planning into a unified model suitable for prolonged multidomain conflicts characterized by persistent uncertainty.

These research gaps are particularly significant in an international environment marked by intensifying geopolitical tensions, the expansion of hybrid threats, the increasing sophistication of cyberattacks, the vulnerability of critical infrastructure, and the emergence of new forms of strategic competition among states. Under such conditions, many countries face challenges that exceed the capacities of their traditional security and defence institutions, requiring planning systems that are more flexible, integrated, and anticipatory. Ukraine's experience demonstrates that effective strategic planning depends upon the simultaneous coordination of military capabilities, institutional capacity, technological innovation, international cooperation, societal resilience, and continuous strategic learning. More than a purely military case, Ukraine represents a comprehensive example of the transformation of national security governance under conditions of persistent uncertainty and continuous adaptation.

From a transdisciplinary perspective, strategic planning should be understood as a dynamic process that integrates public policymaking, risk management, resource administration, capability development, interagency coordination, and international cooperation within a unified governance system. Such an approach overcomes the limitations of traditional planning models by combining knowledge derived from military science, public administration, international relations, economics, engineering, cybersecurity, and organizational management. Simultaneously, it facilitates the development of adaptive planning models capable of responding to rapidly changing environments in which institutional learning and strategic flexibility become decisive factors for ensuring national security.

Furthermore, the study of Ukraine's experience possesses practical significance extending well beyond the European context. The lessons derived from its institutional transformation may contribute to strengthening national security systems in states confronted with regional conflicts, hybrid threats, terrorism, organized violence, border disputes, or increasing political and strategic instability. Systematizing these experiences makes it possible to identify institutional principles and governance mechanisms that can be adapted to different national contexts, thereby supporting the design of more resilient, coordinated, and sustainable strategic planning models capable of addressing contemporary security challenges.

Within this context, the present study seeks to contribute to the strategic planning literature by adopting an integrated perspective that conceptualizes security and defence as a complex system in which military capabilities continuously interact with institutional, technological, economic, and social factors. This approach aims to overcome the limitations of prevailing sectoral perspectives while providing an analytical framework capable of facilitating the adaptation of lessons derived from Ukraine's experience to other states exposed to high levels of risk and uncertainty.

The objective of this article is to conduct a transdisciplinary analysis of Ukraine's experience in the strategic planning of security and defence operations during full-scale war in order to identify the conceptual approaches, institutional mechanisms, and practical lessons that may be adapted to the design of strategic planning systems for states facing high levels of contemporary security risk.

MATERIALS AND METHODS

This study employed a qualitative research design grounded in a transdisciplinary approach to examine the transformation of strategic planning within the security and defence sector under conditions of full-scale warfare. The methodological framework integrated comparative analysis, systems analysis, institutional analysis, and qualitative synthesis to examine the interrelationships among strategic planning, capability-based defence planning, multidomain operations, strategic resource management, institutional resilience, and international security governance. The analysis was based on peer-reviewed publications indexed in major international scientific databases, complemented by official strategic documents, governmental reports, and analytical publications related to Ukraine's security and defence reforms.

The analytical process comprised four sequential stages. First, the relevant scientific literature was systematically reviewed to identify the principal theoretical approaches and emerging research trends in contemporary strategic planning. Second, a comparative analysis was conducted

to examine the evolution of strategic planning models and institutional practices developed in response to high-intensity armed conflict. Third, evidence derived from Ukraine's wartime experience was analyzed through a systems perspective to identify the interactions among military capabilities, institutional governance, technological innovation, resource management, resilience, and international cooperation. Finally, the findings were synthesized into an integrated conceptual model, resulting in the development of the *Transdisciplinary Strategic Planning Framework for High-Risk States*, which provides a comprehensive analytical framework for understanding strategic planning in complex and multidomain security environments.

Artificial intelligence (ChatGPT, OpenAI) was employed exclusively as a supporting research tool for language editing, improvement of academic writing, text organization, and the generation of preliminary visual concepts. All research design, conceptual development, literature analysis, interpretation of findings, source verification, and final conclusions were independently conducted and validated by the authors, who assume full responsibility for the scientific content, accuracy, and integrity of this article.

RESULTS AND DISCUSSION

The conducted transdisciplinary analysis demonstrates that Russia's full-scale invasion of Ukraine has fundamentally transformed both the content and the logic of strategic planning in the security and defence sector. Prior to 2022, strategic planning in Ukraine, similarly to many countries operating in relatively stable security environments, was largely based on medium- and long-term forecasting, predefined planning cycles, and institutional procedures that assumed a comparatively predictable security environment. However, the realities of prolonged high-intensity warfare, characterised by multidomain operations, rapidly changing threats, technological innovation, and continuous uncertainty, required the transition from static planning models toward adaptive strategic governance capable of responding to dynamically evolving operational conditions.

The Ukrainian experience indicates that strategic planning should no longer be perceived as a linear sequence of planning activities but rather as a continuous adaptive decision-making process that integrates strategic analysis, operational management, institutional learning, and rapid policy adjustment. In this regard, strategic planning increasingly performs not only a coordinating function but also becomes an instrument for ensuring national resilience under conditions of permanent security instability.

The analysis identified three interrelated groups of strategic challenges that have significantly influenced the

transformation of Ukraine's planning system. The first group concerns institutional weaknesses inherited from the pre-war security architecture. Although Ukraine initiated comprehensive security and defence reforms after 2014, the full-scale invasion exposed persistent structural limitations affecting strategic decision-making. These include fragmented governance structures, insufficient coordination among security institutions, overlapping responsibilities between civilian and military authorities, and decision-making procedures that proved insufficiently flexible under rapidly changing operational conditions. Such institutional constraints complicated the timely adaptation of strategic plans during the initial stages of the invasion and demonstrated the necessity of strengthening integrated governance mechanisms.

These findings are consistent with the conclusions of Reznikova (2022), who argues that strategic analysis of the security environment should constitute a permanent element of national security governance rather than an episodic analytical exercise conducted exclusively during formal planning cycles. According to this approach, the strategic environment requires continuous monitoring of military, political, economic, technological, informational, and social factors affecting national security, thereby enabling timely adaptation of strategic priorities. Moreover, Reznikova et al. (2024) demonstrate that the Russian aggression has fundamentally transformed Ukraine's strategic culture, leading to the emergence of more adaptive decision-making mechanisms, greater institutional flexibility, and stronger integration between defence planning and broader public governance.

The second group of challenges relates to the multidomain character of contemporary warfare. Unlike conventional military conflicts, Russia's aggression simultaneously combines kinetic military operations with cyberattacks, information warfare, attacks against critical infrastructure, energy coercion, diplomatic pressure, economic disruption, and psychological operations. Consequently, operational planning can no longer be confined to purely military activities but requires simultaneous coordination of military, cyber, information, diplomatic, economic, technological, and societal instruments.

This multidimensional transformation corresponds to the concept of multidomain operations proposed by Semenenko et al. (2024), who argue that modern military operations should integrate all operational domains within a unified planning framework capable of synchronising land, air, maritime, cyber, space, and information activities. Similar conclusions are presented by Fedorchak (2024), who demonstrates that resilient fighting power increasingly depends on the adaptability of military organisations, continuous institutional learning, technological innovation, and the ability to rapidly integrate operational experience into strategic decision-making processes.

Collectively, these studies indicate that successful strategic planning is becoming progressively more dependent on multidimensional coordination rather than on superiority within any single operational domain.

The third group of challenges concerns the growing importance of societal resilience as a strategic planning variable. The Ukrainian experience clearly demonstrates that national resilience during prolonged armed conflict depends not only on military capabilities but also on the effectiveness of public administration, institutional adaptability, cooperation with local governments, engagement of civil society, participation of the private sector, protection of critical infrastructure, and sustained international support. Strategic planning therefore extends beyond the traditional responsibilities of defence institutions and increasingly incorporates the principles of comprehensive security governance.

This finding is supported by research on public-private partnerships in national security, which demonstrates that cooperation between governmental institutions, business organisations, and civil society has become a critical component of Ukraine's wartime resilience (Dragan et al., 2025). Furthermore, studies on European security transformation emphasise that contemporary security governance requires broader institutional cooperation extending beyond conventional military structures (Fiott, 2023; Helwig, 2023). The concept of **total defence**, developed by Roelsgaard et al. (2026), further reinforces this perspective by highlighting those effective responses to contemporary security threats depend upon coordinated interaction among military organisations, civilian authorities, private actors, and society as a whole.

The conducted analysis suggests that previous studies have generally examined institutional reform, defence planning, multidomain operations, societal resilience, and international cooperation as relatively independent research domains. However, the Ukrainian experience demonstrates that these dimensions have become inseparable components of a unified strategic planning system. Under conditions of prolonged multidomain conflict, strategic planning should therefore be conceptualised not merely as a military planning instrument but as a transdisciplinary governance process integrating strategic analysis, operational management, capability development, resource governance, civil resilience, technological adaptation, and international cooperation into a single adaptive decision-making framework.

This conclusion significantly expands existing theoretical approaches to strategic planning by shifting the analytical focus from military planning alone toward integrated strategic governance. Such an approach appears particularly relevant for states exposed to persistent military, hybrid, terrorist, transnational, or geopolitical security risks, where

planning systems must continuously adapt to rapidly evolving threats while maintaining institutional resilience and societal stability.

The findings demonstrate that strategic planning in security and defence should be conceptualised as a continuously adaptive transdisciplinary governance system integrating strategic security analysis, multidomain operational planning, institutional coordination, resource management, technological innovation, and societal resilience. The Ukrainian experience provides a transferable analytical model that may assist other high-risk states in strengthening their strategic planning systems under conditions of prolonged uncertainty and complex security challenges.

- **Capability-Based and Risk-Oriented Planning as the Foundation of Modern Defence Management**

The second result of the study concerns the transformation of defence planning from traditional force-based planning toward capability-based and risk-oriented planning. The experience of Ukraine demonstrates that contemporary security challenges cannot be addressed solely through increasing the quantity of military assets or expanding force structures. Instead, strategic planning increasingly focuses on the development of institutional capabilities that enable security and defence institutions to respond effectively to rapidly evolving and multidimensional threats. This transformation reflects a broader shift from assessing “what forces are available” to determining “what capabilities are required” to accomplish strategic objectives under conditions of uncertainty.

The transdisciplinary analysis indicates that capability-based planning represents a qualitative change in defence management philosophy. Unlike conventional planning approaches centred on military units, weapons systems, or personnel numbers, capability-based planning evaluates the ability of the entire security ecosystem to generate the desired operational effects. Consequently, planning extends beyond military organisations and encompasses governance mechanisms, institutional coordination, logistics, technological innovation, human capital, cyber resilience, intelligence support, and interoperability with international partners.

Ukraine's ongoing defence reforms increasingly reflect the principles of NATO capability-based planning. As noted by Lutsyk et al. (2023), the adaptation of NATO defence planning methodologies has facilitated the transition from resource-oriented planning toward capability development aligned with strategic objectives and anticipated operational scenarios. Similarly, Kurashkevych & Tushko (2025) demonstrate that the operational planning systems employed by border security units in NATO member and partner states are founded on capability assessment, strategic forecasting, and continuous adaptation

to emerging threats rather than on static force structures. These approaches have become particularly relevant for Ukraine, where operational priorities require constant revision in response to changes on the battlefield and within the broader security environment.

A practical illustration of this transformation is provided by the development of Ukraine's prospective Cyber Forces. Horbatiuk et al. (2025) propose implementing defence planning through the DOTMLPFI capability framework, which integrates eight mutually reinforcing components: Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities, and Interoperability. This framework demonstrates that operational effectiveness depends not only on technological resources but also on coherent doctrinal development, organisational structures, professional education and training, effective leadership, qualified personnel, adequate infrastructure, and compatibility with allied systems. The DOTMLPFI approach therefore exemplifies the transition from planning individual military assets toward managing an integrated capability ecosystem.

From a transdisciplinary perspective, the significance of the DOTMLPFI framework extends beyond military planning. Each component interacts with broader governance processes involving public administration, strategic resource allocation, educational policy, digital transformation, organisational management, and international cooperation. Consequently, capability development should be understood as a multidimensional governance process rather than a purely military activity. This broader interpretation significantly expands the theoretical understanding of strategic planning and reinforces the necessity of integrating defence management with public governance.

Another important finding concerns the growing integration of risk management into strategic planning processes. Traditional planning models generally regarded risks as external factors capable of disrupting predetermined plans. However, Ukraine's wartime experience demonstrates that risks should instead be incorporated directly into planning methodologies and continuously reassessed throughout the implementation of strategic decisions.

The conceptual foundations for this approach are reflected in the work of Pashchenko & Ivashchenko (2023), who argue that risk management within the Ministry of Defence and the Armed Forces of Ukraine should become an integral element of strategic governance rather than an auxiliary administrative procedure. Their research highlights the importance of identifying, evaluating, monitoring, and mitigating strategic risks throughout the planning cycle to improve institutional responsiveness and decision-making quality.

The necessity of integrating dynamic risk assessment into defence planning is further confirmed by Ignatiev et al.

(2025), who demonstrate that full-scale military operations generate highly interconnected military, political, economic, cyber, informational, and humanitarian threats that continuously evolve during armed conflict. Under such conditions, planning systems based on static assumptions rapidly become obsolete. Instead, strategic planning requires continuous reassessment of the security environment, enabling decision-makers to revise operational priorities in accordance with emerging risks and changing strategic conditions.

Similarly, Rohulia et al. (2025) emphasise that effective crisis management increasingly depends on proactive risk mitigation strategies rather than reactive emergency responses. Their findings suggest that resilience can be significantly strengthened when strategic planning incorporates systematic risk identification, scenario development, institutional preparedness, and coordinated response mechanisms before crises escalate. These conclusions reinforce the understanding that uncertainty should not be treated as an exception to planning but rather as one of its permanent operating conditions.

The Ukrainian experience therefore demonstrates a fundamental conceptual shift: risks are no longer perceived merely as external constraints that interfere with planning processes but become planning variables that actively shape strategic priorities, capability development, institutional adaptation, and resource allocation. This transformation significantly enhances organisational flexibility, enabling security institutions to revise operational objectives and planning assumptions as the strategic environment evolves.

The conducted analysis also reveals that capability-based planning and risk-oriented governance are mutually reinforcing rather than independent management approaches. Capability development requires continuous assessment of evolving risks to determine future operational requirements, while effective risk management depends upon the availability of appropriate institutional capabilities capable of responding to identified threats. The interaction between these two planning dimensions creates an adaptive decision-making system capable of functioning under prolonged multidomain conflict and persistent uncertainty.

This integrated perspective addresses an important gap identified in the existing literature. Previous studies have primarily examined capability-based planning (Kurashkevych & Tushko, 2025; Lutsyk et al., 2023), cyber capability development (Horbatiuk et al., 2025), and risk management (Ignatiev et al., 2025; Pashchenko & Ivashchenko, 2023; Rohulia et al., 2025) as separate research areas. However, the Ukrainian experience demonstrates that these dimensions constitute interconnected elements of a single adaptive strategic planning

architecture. Their integration provides a more comprehensive framework for defence management that is particularly relevant for states facing complex military, hybrid, cyber, terrorist, or transnational security threats.

The findings demonstrate that capability-based planning and risk-oriented governance should function as mutually reinforcing components of an adaptive strategic planning system. Ukraine's experience confirms that the development of defence capabilities should integrate institutional reform, human capital, technological innovation, interoperability, and continuous risk assessment into a unified governance framework. Such an approach enhances strategic adaptability and provides a transferable model for strengthening defence management systems in states confronted with high levels of contemporary security risks.

• **Multi-Domain Operations, Cyber Defence and Border Security: From Sectoral Planning to Integrated Security Governance**

The third result of the study demonstrates that the transformation of contemporary warfare has fundamentally changed the architecture of strategic and operational planning. The experience of Ukraine confirms that modern armed conflicts can no longer be managed through isolated military planning within individual operational domains. Instead, effective strategic planning increasingly depends on the ability to integrate military and non-military instruments into a unified governance system capable of responding simultaneously to kinetic, hybrid, cyber, informational, economic, and geopolitical threats.

Unlike conventional military conflicts, where operational planning primarily focused on the coordination of land, air, and maritime forces, Russia's full-scale aggression has created an operational environment characterised by the continuous interaction of multiple domains. Military operations are conducted simultaneously with cyberattacks against critical infrastructure, disinformation campaigns, attacks on energy systems, economic coercion, diplomatic pressure, space-enabled intelligence, and attempts to destabilise public institutions. Consequently, operational success increasingly depends on synchronising activities across all these interconnected domains rather than achieving superiority within a single battlespace.

The Ukrainian experience demonstrates that strategic planning must therefore encompass not only the traditional operational domains of land, maritime, and air, but also cyber, space, information, critical infrastructure protection, and border security. These domains are no longer independent sectors of national security but function as interconnected elements of a comprehensive security ecosystem in which disruptions within one domain rapidly generate cascading effects across others. For example, cyberattacks against energy infrastructure may directly affect military logistics, communications, transportation

systems, and civilian resilience, illustrating the necessity of integrated planning mechanisms.

This transformation corresponds to the concept of multi-domain operations (MDO) developed by Semenenko et al. (2024), who argue that future military operations require simultaneous planning, coordination, and execution across all operational environments. According to their approach, multidomain operations are not merely a combination of different military branches but represent a fundamentally new operational philosophy based on the integration of military capabilities with information superiority, cyber operations, electronic warfare, intelligence, and technological innovation. The Ukrainian experience provides practical evidence supporting this concept, demonstrating that operational effectiveness increasingly depends upon synchronised decision-making across multiple domains rather than sequential planning conducted within separate institutional structures.

An important component of this transformation is the growing strategic importance of cyber defence. Prior to the full-scale invasion, cyber capabilities were frequently perceived as technical support functions primarily responsible for protecting information systems. However, Ukraine's wartime experience has demonstrated that cyberspace constitutes an independent operational domain directly influencing military operations, public administration, economic stability, critical infrastructure, and international cooperation. Consequently, cyber capabilities have evolved from auxiliary technical functions into one of the central components of strategic planning.

The recommendations proposed by Horbatiuk et al. (2025) concerning the development of Ukraine's prospective Cyber Forces clearly illustrate this evolution. Their application of the DOTMLPFI capability framework demonstrates that cyber defence requires the simultaneous development of doctrine, organisational structures, specialised personnel, education and training systems, technological resources, infrastructure, leadership, and interoperability with allied partners. Such an approach confirms that cyber capability development is fundamentally a governance challenge rather than solely a technological one. Effective cyber resilience therefore depends on institutional coordination between military organisations, governmental agencies, intelligence services, academic institutions, private technology companies, and international partners.

The multidomain nature of contemporary security challenges also significantly increases the strategic importance of border security. Ukraine's experience has demonstrated that national borders represent not merely geographical boundaries but complex operational spaces where military, intelligence, law enforcement, migration, customs, cyber, and diplomatic activities intersect. The protection of borders increasingly requires

continuous coordination between military operations and civilian governance, particularly under conditions of hybrid warfare involving sabotage, illegal migration, disinformation, organised crime, and transnational security threats.

Kurashkevych & Tushko (2025) demonstrate that capability-based operational planning for border security units in NATO member and partner states increasingly relies on strategic forecasting, capability assessment, interoperability, and flexible operational management. These principles are progressively being incorporated into Ukraine's border security reforms, enabling greater compatibility with NATO operational standards while simultaneously improving institutional adaptability under wartime conditions. The Ukrainian case therefore illustrates that border security planning should be integrated into the broader strategic planning architecture rather than managed as a separate administrative function.

Another significant development concerns the emergence of integrated deterrence as an overarching strategic planning concept. Masitoh et al. (2025), analysing the implementation of the 2022 United States National Defence Strategy, argue that contemporary deterrence extends well beyond conventional military capabilities. Integrated deterrence combines military power with diplomatic engagement, economic instruments, technological innovation, intelligence cooperation, cyber capabilities, strategic communications, and alliance networks to influence adversaries across multiple operational domains simultaneously.

Ukraine's wartime experience strongly supports this approach. Effective resistance against Russian aggression has depended not only on military operations conducted by the Armed Forces of Ukraine but also on international sanctions, diplomatic support, intelligence sharing, technological assistance, cyber cooperation, strategic communications, humanitarian assistance, and the resilience of national institutions. Consequently, operational planning increasingly integrates instruments that were previously managed within separate governmental sectors.

These developments reflect a broader transition toward whole-of-government and whole-of-society approaches to national security governance. Rather than assigning responsibility for security exclusively to military institutions, strategic planning increasingly incorporates public administration, local governments, emergency management agencies, intelligence services, critical infrastructure operators, private industry, civil society organisations, research institutions, and international partners into a unified governance framework. Such integration substantially increases institutional adaptability while strengthening national resilience against multidimensional threats.

The findings of the present study therefore suggest that multidomain operations should not be understood solely as a military innovation but rather as an institutional transformation of strategic governance. Existing studies have primarily analysed multidomain operations (Semenenko et al., 2024), cyber capability development (Horbatiuk et al., 2025), border security planning (Kurashkevych & Tushko, 2025), and integrated deterrence (Masitoh et al., 2025) as relatively independent research areas. However, the Ukrainian experience demonstrates that these dimensions constitute interconnected components of a comprehensive strategic planning architecture operating across military, governmental, technological, and societal domains.

This integrated perspective is particularly relevant for states facing persistent military aggression, hybrid threats, transnational organised crime, terrorism, cyberattacks, or unstable border environments. Countries with elevated security risks require planning systems capable of synchronising diverse operational domains through adaptive governance mechanisms rather than relying upon coordination among isolated security institutions. The Ukrainian case provides empirical evidence that integrated security governance significantly enhances strategic flexibility, institutional resilience, and operational effectiveness under conditions of prolonged multidomain conflict.

The conducted analysis demonstrates that contemporary multi-domain operations require integrated security governance rather than coordination among isolated defence institutions. Ukraine's experience confirms that strategic planning should synchronise military operations, cyber defence, border security, critical infrastructure protection, strategic communications, and international cooperation within a unified adaptive governance framework. This transdisciplinary model offers transferable lessons for states exposed to complex and multidimensional security risks, where operational success increasingly depends on institutional integration across the entire national security ecosystem rather than on the effectiveness of individual security sectors.

• **Strategic Resource Management and Whole-of-Society Security**

The fourth result of the study concerns the transformation of strategic resource management under conditions of prolonged high-intensity warfare. The transdisciplinary analysis demonstrates that Ukraine's experience has fundamentally altered the understanding of resources within strategic planning. While traditional defence planning largely regarded financial, material, and logistical resources as supporting elements of military operations, the realities of full-scale war have shown that resource management constitutes an integral component of strategic governance. Consequently, strategic planning and resource

planning have become mutually dependent processes that evolve simultaneously throughout the conflict.

This transformation reflects the increasing complexity of the contemporary security environment, where military effectiveness depends not only on combat capabilities but also on the resilience of economic systems, industrial production, transportation networks, energy infrastructure, digital technologies, human capital, and institutional capacity. Under such conditions, strategic planning can no longer focus exclusively on operational objectives but must simultaneously ensure the long-term sustainability of the national resource base supporting security and defence activities.

The Ukrainian experience demonstrates that resource planning extends beyond the allocation of military budgets or procurement of defence equipment. Instead, it requires continuous coordination among governmental institutions, local authorities, defence industries, international donors, humanitarian organisations, and private enterprises. This broader perspective transforms resource management from a predominantly logistical function into a strategic governance mechanism responsible for balancing immediate operational requirements with long-term national resilience.

An important contribution to understanding this transformation is provided by Petrukha et al. (2025), who argue that strategic management of financial and material resources within security and defence projects increasingly depends upon the interaction of three mutually reinforcing components: operational management, administrative coordination, and long-term strategic investment. Operational management ensures the timely allocation of resources required for current military activities, while administrative coordination synchronises financial, organisational, and procurement processes across multiple institutions. Long-term strategic investments, in turn, strengthen defence capabilities by supporting technological modernisation, infrastructure development, industrial capacity, innovation, and institutional sustainability. These three dimensions collectively determine the efficiency of strategic resource management under conditions of prolonged conflict.

The Ukrainian case demonstrates that the effectiveness of resource planning cannot be measured solely by the volume of available financial or material assets. Rather, it depends on the capacity of governance institutions to rapidly redistribute resources according to changing operational priorities while simultaneously preserving strategic reserves and ensuring the continuity of critical public services. Resource resilience therefore emerges as a dynamic institutional capability that enables governments to maintain operational effectiveness despite continuous disruption caused by military operations,

economic instability, cyberattacks, or damage to critical infrastructure.

Another significant lesson concerns the growing role of public-private partnerships in strengthening national security. Modern conflicts increasingly require governments to mobilise capabilities that extend far beyond the resources directly controlled by defence institutions. Private enterprises, technology companies, transport operators, energy providers, financial institutions, volunteer organisations, humanitarian actors, and research institutions all contribute essential capabilities supporting national resilience.

The study by Dragan et al. (2025) demonstrates that wartime cooperation between governmental institutions, private companies, and civil society has become one of the defining characteristics of Ukraine's security governance model. Public-private partnerships have supported military logistics, humanitarian assistance, reconstruction of critical infrastructure, technological innovation, cyber resilience, emergency response, and the continuity of essential public services. These findings indicate that the effectiveness of strategic planning increasingly depends upon institutional cooperation across organisational boundaries rather than upon the exclusive capacity of governmental agencies.

The growing importance of institutional integration is further reflected in the concept of Total Defence, developed by Roelsgaard et al. (2026). Their comparative analysis conceptualises national defence as an inter-organisational governance system that integrates military organisations, civilian authorities, private enterprises, and civil society into a unified security architecture. The Total Defence concept emphasises that resilience against contemporary security threats depends upon coordinated planning, shared responsibilities, institutional interoperability, and continuous cooperation across the entire society rather than upon military preparedness alone.

The Ukrainian experience strongly supports this analytical perspective. Since the beginning of the full-scale invasion, the protection of national security has relied upon coordinated interaction among the Armed Forces, central and local government authorities, emergency services, intelligence agencies, defence industries, volunteer networks, local communities, educational institutions, research organisations, and international partners. Consequently, strategic planning has expanded beyond the traditional defence sector and increasingly incorporates public administration, economic governance, digital infrastructure, social resilience, and international cooperation into a single planning framework.

This evolution also reflects the broader transition toward whole-of-government and whole-of-society approaches to national security governance. Within this framework,

responsibility for national security is distributed across multiple institutions whose activities are coordinated through integrated strategic planning rather than through isolated sectoral policies. Such an approach strengthens institutional adaptability while reducing vulnerabilities arising from organisational fragmentation and resource competition.

The findings of this study therefore suggest that strategic resource management should be conceptualised as a governance capability rather than merely a logistical function. Previous studies have examined financial management (Petrukha et al., 2025), public-private partnerships (Dragan et al., 2025), and Total Defence (Roelsgaard Obling et al., 2026) from different disciplinary perspectives. However, the Ukrainian experience demonstrates that these elements constitute interconnected components of a unified strategic planning system. Resource allocation, institutional cooperation, technological development, and societal resilience collectively determine the capacity of the state to sustain long-term defence efforts under conditions of persistent multidomain conflict.

This integrated understanding is particularly relevant for countries facing elevated military, hybrid, terrorist, or transnational security risks. States operating under conditions of prolonged instability require resource management systems capable of simultaneously supporting operational readiness, institutional resilience, economic sustainability, and societal cohesion. The Ukrainian model illustrates that strategic planning becomes substantially more effective when resource governance is integrated with broader national security objectives rather than treated as a separate administrative process.

The conducted analysis demonstrates that resource resilience should be understood as an integrated governance capability rather than exclusively as logistical support. Ukraine's wartime experience confirms that effective strategic planning requires the synchronisation of financial management, material resources, institutional coordination, public-private partnerships, critical infrastructure protection, and societal resilience within a unified whole-of-government and whole-of-society framework. This integrated model provides practical lessons for states seeking to strengthen the sustainability of their security and defence systems under conditions of prolonged uncertainty and complex security threats.

• **Ukraine's Strategic Experience as an International Model for High-Risk States**

The fifth result of the study synthesises the findings of the previous sections into a comprehensive transdisciplinary analytical framework for strategic planning in states exposed to elevated security risks. The conducted analysis demonstrates that Ukraine's experience extends beyond the national context and offers broader conceptual and

practical implications for the evolution of contemporary security governance. Rather than representing an isolated case of wartime adaptation, Ukraine provides an empirical example of how strategic planning can be transformed into an adaptive governance system capable of operating under conditions of prolonged multidomain conflict, continuous uncertainty, and rapidly evolving threats.

Recent scholarship consistently demonstrates that Russia's full-scale invasion of Ukraine has fundamentally reshaped the European security architecture and accelerated profound institutional changes within the Euro-Atlantic security system. Cardwell & Moret (2023) argue that the war has reinforced the European Union's role as a geopolitical actor through the expansion of sanctions policy and regional strategic leadership. Similarly, Fiott (2023) concludes that the conflict has become a catalyst for deeper European defence integration by strengthening common defence initiatives and increasing cooperation among Member States. Helwig (2023) further demonstrates that the war substantially advanced the concept of European strategic autonomy by encouraging the European Union to enhance its capacity for independent security action. Genini (2025) likewise argues that the Common Foreign and Security Policy has undergone significant transformation, reflecting the need for more coherent and integrated responses to large-scale military aggression.

These developments indicate that Ukraine's wartime experience has influenced not only national defence reforms but also broader international approaches to security governance. The practical lessons generated during the war increasingly inform discussions concerning strategic planning, resilience, capability development, institutional cooperation, and crisis management within European and transatlantic security communities.

One of the most significant findings of this study is that Ukraine should no longer be viewed exclusively as a recipient of international military, financial, or humanitarian assistance. Instead, the Ukrainian experience has become an important source of strategic innovation influencing contemporary security thinking. Wartime adaptations developed under exceptionally demanding operational conditions have generated practical knowledge regarding multidomain operations, institutional resilience, integrated governance, cyber defence, capability development, strategic resource management, and whole-of-society security. These innovations increasingly contribute to the international exchange of best practices and provide valuable reference points for countries confronting comparable security challenges.

The international significance of Ukraine's experience is further reinforced by ongoing debates concerning the future architecture of European security. Evangelista (2024) demonstrates that discussions surrounding post-war

security guarantees for Ukraine, including proposals related to extended deterrence and long-term security commitments, have broader implications for European and international security arrangements. In parallel, Masitoh et al. (2025) show that the concept of integrated deterrence has expanded strategic planning beyond traditional military capabilities by incorporating diplomatic, economic, technological, cyber, and alliance-based instruments into a unified strategic framework. Ukraine's wartime experience provides practical evidence of how such multidimensional approaches can be implemented under conditions of active military conflict.

The broader geopolitical consequences of the war are also reflected in the emergence of Ukraine as a key contributor to European security. Kotlyar & Lymar (2025) characterise Ukraine as a strategic shield for Europe, emphasising that the country's resistance has become an essential factor shaping regional stability and the future development of international security institutions. This perspective supports the argument that Ukraine increasingly participates in defining new principles of collective security rather than merely adapting to externally developed security models.

Building upon the empirical findings presented in the previous sections, this study proposes a Transdisciplinary Strategic Planning Framework for High-Risk States. Unlike existing analytical approaches that examine strategic security analysis, capability development, multidomain operations, resource management, institutional coordination, or international cooperation separately, the proposed framework integrates these dimensions into a unified adaptive governance model.

First, it conceptualises strategic planning as a genuinely transdisciplinary governance process that connects military planning with public administration, cyber security, resource governance, institutional resilience, and international cooperation. Second, it systematises Ukraine's wartime experience into transferable institutional lessons that may support strategic planning reforms in countries facing military aggression, hybrid threats, terrorism, organised transnational crime, border instability, or other complex security risks. Third, it integrates previously fragmented research directions into a coherent analytical model capable of supporting decision-making under conditions of prolonged multidomain conflict and persistent uncertainty.

The practical relevance of this framework extends beyond the European context. Although the institutional and geopolitical circumstances of individual states differ considerably, many countries in Latin America, including Ecuador, increasingly confront complex security environments characterised by organised transnational crime, illicit trafficking, cyber threats, attacks on critical infrastructure, border insecurity, and growing interdependence between internal and external security challenges. While

these threats differ from interstate warfare, they similarly require adaptive strategic planning, institutional interoperability, integrated resource management, and coordinated action across military, civilian, law enforcement, and societal actors. In this regard, Ukraine's experience should not be interpreted as a model for replication but rather as a source of transferable strategic principles that can be adapted to different national contexts according to specific institutional capacities and security priorities.

The findings demonstrate that Ukraine should increasingly be regarded not only as an object of international assistance but also as a subject of strategic transformation within the evolving international security order. Ukraine's wartime experience contributes to the development of new approaches to strategic planning, resilience, multidomain operations, institutional coordination, and international cooperation, thereby positioning the country as an important source of normative and practical innovation for states facing elevated contemporary security risks. The proposed Transdisciplinary Strategic Planning Framework provides an integrated analytical model that may support future security governance reforms and strengthen strategic planning capacities in diverse high-risk environments.

The findings of this study contribute to the growing body of research on strategic planning, defence governance, and security management by proposing a transdisciplinary framework that integrates previously fragmented dimensions of security planning into a coherent analytical model. While recent studies have significantly advanced understanding of capability-based planning, multidomain operations, strategic resilience, and European security transformation, the present research demonstrates that these concepts should not be treated as independent analytical domains but rather as interconnected components of a single adaptive strategic planning system.

The first contribution of the proposed framework concerns the conceptualisation of strategic planning as an integrated governance system. Existing studies have primarily examined military planning, public administration, cyber security, resource governance, or societal resilience within their respective disciplinary boundaries. For example, capability-based planning has been analysed predominantly from the perspective of defence management (Kurashkevych & Tushko, 2025; Lutsyk et al., 2023), while multidomain operations have largely been discussed within military operational theory (Semenenko et al., 2024). Similarly, research on public-private partnerships (Dragan et al., 2025), Total Defence (Roelsgaard Obting et al., 2026), and strategic resource management (Petrukha et al., 2025) has generally focused on institutional cooperation without fully integrating these dimensions into the broader strategic planning process. The framework proposed in this study addresses this fragmentation by conceptualising strategic planning as a continuous governance

process linking military planning with public administration, cyber security, strategic resource management, institutional resilience, and international cooperation.

The second contribution relates to the systematisation of Ukraine's wartime experience into transferable institutional lessons. The literature increasingly recognises Ukraine as an important source of innovation in defence governance and strategic adaptation (Fedorchak, 2024; Reznikova et al., 2024). However, many existing studies remain focused on specific aspects of the war, including strategic culture, resilience, capability development, or operational adaptation. The present research extends these perspectives by demonstrating that Ukraine's experience represents a comprehensive model of adaptive strategic governance rather than a collection of isolated military innovations. This distinction is particularly important because many contemporary security challenges – including hybrid threats, cyberattacks, organised transnational crime, attacks on critical infrastructure, and border instability – require integrated institutional responses that extend beyond conventional military planning.

Accordingly, the proposed framework has practical relevance for states facing diverse high-risk security environments. Although countries differ considerably in their geopolitical position, institutional capacity, and threat profiles, many confront increasing levels of uncertainty generated by hybrid threats, transnational organised crime, terrorism, cyber insecurity, irregular migration, and strategic competition. In this context, Ukraine's experience should not be interpreted as a model to be replicated mechanically. Rather, it offers transferable governance principles – including adaptive planning, capability development, multidomain coordination, institutional interoperability, and whole-of-government cooperation – that can be tailored to different political, legal, and organisational contexts. This consideration is particularly relevant for Latin American countries, where security challenges often combine internal and external dimensions and require coordinated action across military, civilian, law enforcement, and governmental institutions.

The third contribution concerns the integration of previously fragmented research streams into a unified analytical framework suitable for prolonged multidomain conflict. Previous scholarship has substantially advanced understanding of European defence integration (Fiott, 2023; Genini, 2025; Helwig, 2023), strategic deterrence (Masitoh et al., 2025), sanctions and geopolitical leadership (Cardwell & Moret, 2023), and post-war security guarantees (Evangelista, 2024). Nevertheless, these studies generally address different levels of analysis, from international security architecture to operational planning, without proposing a comprehensive model connecting strategic governance, institutional adaptation, operational capabilities, resource management, and international

partnerships. The transdisciplinary framework developed in this study contributes by integrating these dimensions into a single adaptive planning architecture capable of supporting decision-making under conditions of prolonged uncertainty and multidomain threats.

The findings also contribute to the evolving debate on resilience in contemporary security governance. Rather than viewing resilience solely as the capacity to withstand external shocks, the Ukrainian experience suggests that resilience should be understood as the institutional ability to learn, adapt, reorganise resources, and continuously revise strategic priorities. This interpretation expands the understanding of resilience beyond military endurance and incorporates organisational learning, technological innovation, interagency cooperation, and societal participation as essential components of strategic planning. Consequently, adaptive governance emerges as a critical determinant of long-term security effectiveness.

Another important implication concerns the changing role of Ukraine within the international security system. The analysis supports the growing scholarly argument that the country should no longer be perceived exclusively as a beneficiary of external assistance but increasingly as a contributor to the evolution of strategic thinking in Europe and beyond. Wartime innovations in multidomain operations, capability development, cyber defence, civil resilience, and institutional coordination have generated valuable practical knowledge that informs contemporary debates on security governance, NATO interoperability, European defence integration, and integrated deterrence. In this sense, Ukraine functions not only as a testing ground for new security solutions but also as a source of strategic learning with broader international relevance.

Despite these contributions, several limitations of the study should be acknowledged. First, the proposed framework is primarily based on the analysis of Ukraine's experience during the ongoing full-scale war and therefore reflects conditions associated with high-intensity interstate conflict. While many of its principles are transferable, their practical application may require adaptation to different political systems, institutional arrangements, and security environments. Second, the framework has been developed through a qualitative synthesis of contemporary research and conceptual analysis. Future studies could strengthen its empirical validation through comparative case studies, expert surveys, scenario-based simulations, or quantitative assessments of strategic planning effectiveness across different countries. Third, the rapidly evolving international security environment suggests that strategic planning models should remain flexible and open to further refinement as new operational experiences and technological developments emerge.

Overall, the findings extend existing scholarship on capability-based planning, multidomain operations, Total Defence, and the transformation of European security by demonstrating that effective strategic planning increasingly depends on adaptive governance rather than exclusively on military superiority. The proposed Transdisciplinary Strategic Planning Framework therefore provides both a theoretical contribution to the study of strategic governance and a practical analytical tool for policymakers seeking to strengthen national security systems under conditions of persistent uncertainty, multidomain threats, and rapidly changing geopolitical realities.

CONCLUSIONS

This study examined the transformation of strategic planning through a transdisciplinary analysis of Ukraine's experience during the full-scale war. The findings demonstrate that contemporary security challenges have fundamentally redefined the principles of strategic planning by requiring a transition from conventional military planning toward integrated governance systems capable of operating in environments characterised by multidomain conflicts, persistent uncertainty, hybrid threats, and continuous technological change. Under these conditions, strategic planning can no longer be understood solely as a military function but as a comprehensive governance process that coordinates political, institutional, economic, technological, and societal capabilities.

The principal scientific contribution of this research is the development of the Transdisciplinary Strategic Planning Framework for High-Risk States, which integrates six complementary dimensions: strategic security environment analysis, capability-based and risk-oriented planning, multidomain operational planning, strategic resource governance, whole-of-government and whole-of-society institutional coordination, and international interoperability through strategic partnerships. Rather than analysing these dimensions independently, the proposed framework conceptualises them as interconnected components of a single adaptive governance system that strengthens strategic decision-making, institutional resilience, and operational effectiveness under conditions of prolonged conflict.

The proposed framework also contributes to closing important gaps identified in the contemporary literature by integrating defence planning, public governance, cyber-security, institutional resilience, strategic resource management, and international cooperation within a unified analytical model. Through this integration, Ukraine's wartime experience is transformed into a set of transferable strategic principles that may support institutional reforms in countries confronted with military aggression, hybrid warfare, organised transnational crime, terrorism, cyber threats, border instability, and other multidimensional security risks.

From a practical perspective, the findings indicate that Ukraine should increasingly be recognised not only as a recipient of international assistance but also as a source of strategic innovation. The country's experience demonstrates how institutional learning, adaptive governance, civil-military cooperation, technological innovation, and international partnerships collectively strengthen national resilience during prolonged crises. Although differences in political systems, institutional capacity, and geopolitical contexts prevent the direct transfer of specific policies, the adaptive principles identified in this study provide a flexible conceptual foundation that can be adjusted to the strategic needs of states facing elevated security risks in different regions of the world.

Beyond its practical implications, this research advances the theoretical understanding of strategic planning by positioning it as a transdisciplinary field that extends beyond the traditional boundaries of military science. The analysis shows that strategic effectiveness increasingly depends on the interaction between governance structures, organisational learning, technological capabilities, institutional resilience, sustainable resource management, and international cooperation. Consequently, future strategic planning models should integrate knowledge from multiple disciplines while maintaining the flexibility required to respond to rapidly evolving security environments.

Future research should empirically validate the proposed framework through comparative analyses involving different categories of high-risk states and assess its applicability across diverse institutional and geopolitical settings. Additional studies should examine how emerging technologies, including artificial intelligence, autonomous systems, advanced cyber capabilities, quantum technologies, and data-driven decision-support systems, may reshape strategic planning and security governance. Comparative research on regional security organisations, multinational defence cooperation, and public-private partnerships would also contribute to refining and expanding the proposed framework.

Overall, this study demonstrates that the future effectiveness of strategic planning in the security and defence sector will depend less on the accumulation of military capabilities alone and more on the capacity of states to integrate governance, technological innovation, institutional resilience, strategic resource management, societal participation, and international cooperation into a coherent and adaptive planning system. In an increasingly uncertain international environment, this transdisciplinary perspective provides a robust conceptual foundation for strengthening national resilience, improving strategic decision-making, and enhancing the long-term effectiveness of security and defence policies.

REFERENCES

- Cardwell, P. J., & Moret, E. (2023). The EU, sanctions and regional leadership. *European Security*, 32(1), 1–21. <https://doi.org/10.1080/09662839.2022.2085997>
- Dragan, I., Panfilova, T., Chistiakova, I., & Tatarinov, R. (2025). Public-private partnerships in national security: A case study in the context of the war in Ukraine (2022–2024). *Clio. Revista de Historia, Ciencias Humanas y Pensamiento Crítico*, 5(9), 599–631. <https://doi.org/10.5281/zenodo.14566958>
- Evangelista, M. (2024). A nuclear umbrella for Ukraine? Precedents and possibilities for postwar European security. *International Security*, 48(3), 7–50. https://doi.org/10.1162/isec_a_00476
- Fedorchak, V. (2024). *The Russia–Ukraine war: Towards resilient fighting power*. Routledge.
- Fiott, D. (2023). In every crisis an opportunity? European Union integration in defence and the war on Ukraine. *Journal of European Integration*, 45(3), 447–462. <https://doi.org/10.1080/07036337.2023.2183395>
- Genini, D. (2025). How the war in Ukraine has transformed the EU's Common Foreign and Security Policy. *Yearbook of European Law*. <https://doi.org/10.1093/yel/yeaf003>
- Götz, E., & Staun, J. (2022). Why Russia attacked Ukraine: Strategic culture and radicalized narratives. *Contemporary Security Policy*, 43(3), 482–497. <https://doi.org/10.1080/13523260.2022.2082633>
- Helwig, N. (2023). EU strategic autonomy after the Russian invasion of Ukraine: Europe's capacity to act in times of war. *JCMS: Journal of Common Market Studies*, 61(S1), 57–67. <https://doi.org/10.1111/jcms.13527>
- Horbatiuk, V., Horhulenko, V., Horhulenko, V., Dobrovolskiy, Y., & Samsonenko, M. (2025). Recommendations on the implementation of defence planning measures for acquiring and developing capabilities by the prospective cyber forces of the Armed Forces of Ukraine based on the DOTMLPFI. *International Scientific Journal Military Science*, 3(2), 137–150. <https://doi.org/10.62524/msj.2025.3.2.10>
- Ignatiev, A., Burlakov, S., Terletsii, A., & Skryl, S. (2025). Assessing modern challenges and threats affecting national security by full-scale military operations. *DIXI*, 27(2), 1–14. <https://doi.org/10.16925/2357-5891.2025.02.02>
- Ketners, K. (2025). Adaptation of state security to modern military operations and terrorist risks in the world. *Space and Culture, India*, 13(1), 1–5. <https://doi.org/10.20896/e3p2jm77>

- Kotlyar, Y., & Lyman, M. (2025). Ukraine as a shield for Europe: The Russian invasion and the reshaping of international security. *Acta de Historia & Politica: Saeculum XXI*, 10, 75–86. <https://doi.org/10.26693/ahpsxxi2025.10.075>
- Kurashkevych, A., & Tushko, D. (2025). Analysis of foreign experience in capability-based operational planning of border security units of NATO member and partner countries. *Naukovyi Visnyk Kyivskoho Instytutu Natsionalnoi Hvardii Ukrainy*, 2, 88–94. <https://doi.org/10.59226/2786-6920.2.2025.88-94>
- Lutsyk, Y., Parkhomenko, P., Demeniev, O., & Alimov, D. (2023). Analysis of the defence planning system based on capabilities taking into account the leading experience of NATO member states. *Modern Economics*, 41, 73–78. [https://doi.org/10.31521/modecon.v41\(2023\)-11](https://doi.org/10.31521/modecon.v41(2023)-11)
- Masitoh, Y. T., Perwita, A. A. B., & Rudy, E. (2025). Integrated deterrence in practice: The 2022 United States National Defence Strategy towards the Russia–Ukraine war. *International Journal of Humanities, Education, and Social Sciences*, 3(3), 1030–1048. <https://doi.org/10.58578/ijhess.v3i3.7317>
- Pashchenko, Y. M., & Ivashchenko, S. (2023). Concepts and principles of risk management in the Ministry of Defence of Ukraine and the Armed Forces of Ukraine. *Uzhhorod National University Herald. Series: Law*, 2(77), 102–107. <https://doi.org/10.24144/2307-3322.2023.77.2.17>
- Petrukha, N. M., Petrukha, S. V., Tiurmenko, Y. M., & Kononenko, I. M. (2025). Strategic management of financial and material resources in security and defence projects. *The Problems of Economy*, 63(1), 81–89. <https://doi.org/10.32983/2222-0712-2025-1-81-89>
- Reznikova, O. (2022). Strategic analysis of Ukraine's security environment. *Strategic Panorama*, Special Issue, 45–53. <https://doi.org/10.53679/2616-9460.specialissue.2022.05>
- Reznikova, O., Hryhorenko, O., & Myronenko, V. (2024). Transformation of the strategic culture of Ukraine under the influence of the Russian threat. *Politologija*, 116(4), 59–108. <https://doi.org/10.15388/Polit.2024.116.2>
- Roelsgaard Obling, A., Berndtsson, J., & Gilje Ostensen, A. (2026). Conceptualising total defence: Inter-organisational structures in a comparative perspective. *European Security*. Advance online publication. <https://doi.org/10.1080/09662839.2026.2620708>
- Rohulia, A., Taran, Y., Tymoshenko, O., Bereziuk, V., & Nianko, V. (2025). Ensuring security in crisis: Risk mitigation strategies and response planning. *Journal of Information Systems Engineering and Management*, 10(12s). <https://doi.org/10.52783/jisem.v10i12s.1861>
- Semenenko, O., Koval, V., Vodchyts, O., & Dobrovolskyi, Y. (2024). A multidomain operation: A modern view of the forms and methods of military operations adapting to the environment of transforming challenges and threats. *International Scientific Journal Military Science*, 2(1), 17–34. <https://doi.org/10.62524/msj.2024.2.1.02>

Conflicts of Interest:

The authors declare no conflicts of interest.

Author Contributions:

Tetiana Bielska, Vasyl Shkoliarenko: Conceptualization, data curation, formal analysis, investigation, methodology, supervision, validation, visualization, original draft writing, and writing, review, and editing.

Ethical statement:

The study was based on the analysis of documentary sources and publicly available data, and therefore did not involve the direct participation of human subjects. No personally identifiable information was handled.