TRANSFORMING SECURITY AND DEFENSE FORCE OPERATIONS IN MODERN CONFLICTS

Vasyl Shkoliarenko

[A] Candidate of Technical Sciences, Senior Research Fellow, e-mail: vasyl1970@yahoo.com, ORCID ID: https://orcid.org/0000-0001-8274-2232

Yevheniy Bereznyak Military Academy, Kyiv, Ukraine

Received: June 21, 2026 | Revised: June 29, 2026 | Accepted: June 30, 2026

UDC 355.40:355.45:004.8

DOI: https://doi.org/10.33445/psssj.2026.7.2.6

Abstract

The article examines the operations of the security and defense forces as a complex object of scientific research in the field of national security. It is determined that modern operations are multidimensional in nature and combine military, intelligence, information, cybernetic, analytical and humanitarian components. The features of the operations of the security and defense forces in new-type wars are analyzed, which are characterized by network-centric approaches to management, the use of digital platforms, information and psychological influence, cyber operations and decision-making support systems. The concepts of "operations of the security and defense forces" and "operations of the security and defense forces in new-type wars" as an integrated system of military and non-military actions aimed at ensuring the national security of the state are substantiated. Special attention is paid to intelligence operations, which are considered as a system of organized activities for the collection, analysis, forecasting and dissemination of information about threats to national security. The role of intelligence exchange, the use of OSINT, predictive intelligence and artificial intelligence technologies in modern operations of security and defense forces is investigated. It is determined that the effectiveness of modern operations largely depends on the level of integration of information and analytical systems, the speed of data processing and interagency coordination. The essence of information and intellectual operations as important elements of the modern system for ensuring national security is revealed. It is established that the implementation of AI, machine learning and Big Data technologies contributes to the formation of a new model of management of security and defense force operations, focused on proactive response to threats, risk forecasting and ensuring information advantage. The need for further development of theoretical and methodological approaches to the study of security and defense force operations in the context of modern hybrid threats is emphasized.

Key words: National Security; Operations; Intelligence; Information Operations; Intellectual Operations; Artificial Intelligence; Cybersecurity; Hybrid Threats.

Introduction

The contemporary security environment is characterized by an unprecedented increase in the complexity of threats, driven by the simultaneous evolution of military, informational, cyber, economic, and cognitive forms of confrontation. Armed conflicts of the twenty-first century have become increasingly multidimensional, combining conventional military operations with information and psychological operations, cyberattacks, economic coercion, special operations, artificial intelligence (AI), and advanced decision-support systems. Under these conditions, the traditional understanding of military operations no longer adequately reflects the nature and dynamics of contemporary warfare (Afolabi & Bodunde, 2020; Gasanov et al., 2024).

This issue has become particularly significant following the large-scale Russian aggression against Ukraine, which has demonstrated a fundamentally new model of warfare. Modern security and defense force operations are conducted in a multi-domain environment, integrating military, intelligence, information, cyber, space, and cognitive dimensions into a unified operational framework. Consequently, the effectiveness of such operations depends not only on military capabilities or technological superiority but also on the ability to integrate heterogeneous information flows, ensure interagency coordination, rapidly process intelligence, and support timely and evidence-based decision-making (Ignatiev et al., 2025; Gasanov et al., 2024).

Simultaneously, the rapid advancement of digital technologies, artificial intelligence, machine learning, Big Data, decision-support systems, autonomous platforms, and Open-Source Intelligence (OSINT) has profoundly transformed the planning and execution of security and defense operations. In leading countries, these technologies are increasingly recognized as critical enablers of information superiority, strategic forecasting, accelerated command and control, and adaptive responses to hybrid threats (Gill & Phythian, 2018; Kerr, 2023; Mille, 2022).

Although a substantial body of research has examined various aspects of modern security and defense activities, most studies focus on individual components, such as military operations, intelligence, cybersecurity, information operations, or artificial intelligence applications. Considerably less attention has been devoted to a comprehensive understanding of security and defense force operations as an integrated system that combines these functional domains within a unified conceptual framework. Furthermore, the existing literature lacks a common conceptual approach to the classification, structure, and interrelationships of contemporary operations, limiting the development of a coherent theoretical foundation for future research.

The purpose of this review article is to critically analyze contemporary scholarly approaches to the study of security and defense force operations, to systematize existing concepts describing their transformation under conditions of hybrid warfare, digitalization, and artificial intelligence adoption, and to identify the principal research trends, conceptual gaps, and promising directions for future studies in this field.

Literature Review

Research on contemporary security and defense force operations has expanded considerably over the past decade, reflecting the increasing complexity of the global security environment and the emergence of hybrid forms of warfare. Existing studies can be broadly grouped into five interconnected research streams: (1) conceptual approaches to modern warfare and security operations; (2) intelligence and intelligence-led operations; (3) information and cyber operations; (4) artificial intelligence and digital transformation in defense; and (5) integrated approaches to security governance. Although these areas have developed rapidly, they remain fragmented, and no universally accepted conceptual framework for security and defense force operations has yet been established (Afolabi, M., & Bodunde, O., 2020; Sarjito, A., 2024a).

The first stream focuses on the transformation of warfare and military operations under conditions of technological innovation and hybrid threats. Contemporary researchers emphasize that modern conflicts extend beyond the traditional battlefield by incorporating cyber, informational, economic, political, and cognitive dimensions. Consequently, military operations are increasingly viewed as multi-domain and network-centric activities requiring continuous coordination across diverse operational environments. Studies by Gasanov et al. (2024) and Ignatiev et al. (2025), Pokrajčić (2025) demonstrate that technological superiority, information dominance, and adaptive command-and-control systems have become decisive factors in achieving operational effectiveness. However, these studies primarily examine military operations and provide limited discussion of their integration with intelligence, information, and civilian security activities.

A second research direction concerns intelligence studies. Intelligence is no longer regarded solely as the collection of information but as an integrated analytical process that supports strategic, operational, and tactical decision-making. Gill and Phythian (2018), Mille (2022), and Kerr (2023) argue that contemporary intelligence combines information collection, analysis, forecasting, and strategic assessment within a multidisciplinary framework. Recent studies have further expanded this perspective by emphasizing predictive intelligence, scenario planning, and intelligence-driven decision-making (Sarjito, 2024; Dahl & Strachan-Morris, 2024). Nevertheless, most publications investigate intelligence as an independent discipline rather than as a structural component of broader security and defense force operations.

The third body of literature examines information operations, cyber operations, and strategic communications. Researchers increasingly recognize that information has become both an operational resource and an operational domain. Contemporary conflicts demonstrate that cyberattacks, disinformation campaigns, psychological influence, and strategic communications may significantly affect military outcomes without the direct application of kinetic force. Although numerous studies analyze individual aspects of information warfare and cybersecurity, relatively few investigate their integration into comprehensive operational planning or their interaction with intelligence and military capabilities (Maloku et al., 2022).

A rapidly growing research area addresses the application of artificial intelligence, machine learning, Big Data analytics, and decision-support systems in national security. Zamfirescu (2024), Caballero and Jenkins (2025), Khan and Khan (2025), and Pandey et al. (2024) demonstrate that AI technologies significantly enhance intelligence analysis, cyber defense, operational planning, and command-and-control processes. Similarly, AI-driven OSINT has substantially expanded the capability to detect emerging threats and support strategic decision-making (Kolade et al., 2025). Despite these advances, the literature also identifies significant ethical, legal, and governance challenges associated with algorithmic transparency, accountability, bias, and human oversight (Bellaby, 2026). Current research therefore reflects a growing consensus that technological superiority alone cannot ensure operational effectiveness without appropriate institutional, legal, and ethical frameworks.

Another important direction of research concerns integrated security governance and interagency coordination. Modern security challenges increasingly require cooperation among military organizations, intelligence agencies, law-enforcement institutions, governmental authorities, and international partners. Recent studies argue that effective security management depends on the integration of heterogeneous information systems, shared situational awareness, and interoperable decision-support mechanisms. Nevertheless, these publications mainly address organizational and institutional issues rather than developing an integrated theoretical understanding of security and defense force operations (Maloku et al., 2022; Willis & Jefferson 2025).

The review of contemporary literature reveals several important research gaps. First, existing studies predominantly analyze military, intelligence, cyber, information, or AI-enabled operations separately, while relatively little attention is paid to their systemic interaction within a unified operational framework. Second, there is no generally accepted conceptual definition of security and defense force operations that adequately reflect their multidimensional character in the context of hybrid warfare and digital transformation. Third, limited efforts have been devoted to synthesizing the rapidly expanding body of interdisciplinary knowledge into a coherent theoretical model capable of supporting further research and practical doctrine development.

Accordingly, this review addresses these gaps by critically synthesizing contemporary theoretical approaches, identifying common trends and conceptual differences, and proposing an integrated perspective on security and defense force operations as a multidimensional system operating across military, intelligence, information, cyber, technological, and cognitive domains.

Materials and methods

This study was conducted as a review article aimed at systematizing, critically analyzing, and synthesizing contemporary scholarly approaches to understanding security and defense force operations within the context of the evolving security environment. The methodological foundation of the study is based on an interdisciplinary approach integrating concepts from national security studies, military science, management theory, intelligence studies, cybersecurity, information science, and artificial intelligence research (Sarjito, 2024c).

The study draws upon a broad range of scholarly sources, including monographs, peer-reviewed journal articles, analytical reports published by international organizations, official security and defense policy documents, and recent academic studies published primarily between 2018 and 2026. The selected literature addresses the transformation of modern warfare, multi-domain operations, intelligence activities, information and cyber operations, artificial intelligence, Big Data technologies, decision-support systems, and the digital transformation of the security and defense sector.

The research was conducted in several interrelated stages. The first stage involved the identification and selection of relevant scientific literature according to the objectives of the study. During the second stage, the selected publications were classified into major thematic areas in order to identify the principal schools of thought, conceptual approaches, and emerging trends in the study of security and defense force operations. The third stage consisted of a critical analysis of the selected literature aimed at identifying common theoretical assumptions, conceptual differences, controversial issues, and existing research gaps. The final stage integrated the findings into a coherent conceptual framework reflecting the contemporary understanding of security and defense force operations as a multidimensional object of scientific inquiry.

To achieve the research objective, a combination of complementary scientific methods was employed. Bibliographic analysis was used to determine the current state of research and identify major trends in the field. Content analysis facilitated the systematization of key concepts, categories, and research themes. Comparative analysis was applied to examine different conceptual approaches to contemporary operations, their structure, and functional characteristics. The method of synthesis enabled the integration of findings from individual studies into a unified body of knowledge, while the systems approach allowed security and defense force operations to be examined as a complex open system comprising military, intelligence, information, cyber, technological, and humanitarian components.

Unlike most existing review studies, the present research focuses not only on describing individual areas of contemporary security and defense operations but also on their conceptual integration. This approach makes it possible to identify the major trends in the transformation of security and defense force operations, reveal existing research gaps, and establish a coherent theoretical foundation for future studies in the fields of national security and defense.

Results

Evolution of Scientific Approaches to Security and Defense Force Operations

The concept of security and defense force operations has undergone a profound transformation over the past several decades. During the second half of the twentieth century, military operations were predominantly interpreted as coordinated combat actions aimed at defeating an adversary through the application of military force. Their planning and execution focused primarily on kinetic effects, territorial control, and the destruction of enemy forces. Intelligence, logistics, information support, and political decision-making were generally regarded as supporting functions rather than integral operational components.

The changing character of armed conflicts at the beginning of the twenty-first century

substantially altered this traditional perspective. Military campaigns in Iraq and Afghanistan, the rapid expansion of cyberspace, the increasing role of non-state actors, and the emergence of hybrid threats demonstrated that military superiority alone is insufficient to achieve strategic objectives. Contemporary operations increasingly involve the coordinated employment of military, intelligence, cyber, information, diplomatic, economic, and legal instruments of national power within a unified operational framework.

This transformation has been reflected in the evolution of military doctrine. NATO introduced the concept of comprehensive and integrated operations, emphasizing cooperation among military forces, governmental institutions, international organizations, and civil society. Simultaneously, the concept of Multi-Domain Operations (MDO) emerged, recognizing that future operations must be planned and executed simultaneously across the land, maritime, air, space, cyber, and information domains. Under this approach, superiority is achieved through the synchronized integration of capabilities rather than through dominance within a single operational domain.

Another significant development has been the growing role of intelligence as a core operational function. Intelligence has evolved from a supporting activity into a continuous process encompassing information collection, data fusion, predictive analysis, threat assessment, and decision support. The widespread adoption of artificial intelligence, machine learning, and advanced analytics has further accelerated this transformation by enabling commanders to process vast amounts of heterogeneous information and rapidly adapt operational plans to changing battlefield conditions.

The digitalization of defense systems has also fundamentally changed the understanding of operational effectiveness. Modern operations increasingly depend on information superiority, resilient communication networks, real-time situational awareness, and the interoperability of command-and-control systems. Consequently, information has become not only a resource but also a strategic operational asset capable of influencing both military actions and political decision-making.

Despite these developments, scientific literature continues to exhibit considerable conceptual fragmentation. Military science, intelligence studies, cybersecurity, information operations, strategic communications, and artificial intelligence are often examined as separate research domains, employing different terminology and theoretical perspectives. As a result, there is still no universally accepted definition of security and defense force operations that adequately captures their multidimensional nature and the complex interactions among their military, intelligence, informational, technological, and organizational components.

The analysis conducted in this review indicates that contemporary security and defense force operations should be understood as an integrated system of coordinated activities carried out across multiple operational domains through the synchronized employment of military, intelligence, cyber, information, technological, and organizational capabilities in order to achieve strategic, operational, and tactical security objectives. Such an understanding provides a broader conceptual foundation for analyzing the transformation of modern conflicts and creates a basis for integrating emerging technologies into future operational doctrines.

Classification and Functional Structure of Contemporary Security and Defense Force Operations

The review of contemporary scientific literature demonstrates that security and defense force operations can no longer be interpreted exclusively as military activities. The evolution of modern conflicts has fundamentally transformed the operational environment, requiring the simultaneous integration of military, intelligence, information, cyber, technological, economic, and cognitive capabilities. Consequently, security and defense force operations should be viewed as a multidimensional system composed of interrelated operational domains rather than as a collection of independent functional activities.

Based on the synthesis of existing scientific approaches, the principal functional components

of contemporary security and defense force operations are summarized in Table 1.

Table 1: Functional Components of Contemporary Security and Defense Force Operations

Operations Component	Main Content	Key Technologies	Main Purpose
Military Operations	application of defense forces and assets	autonomous systems, digital platforms	neutralization of military threats
Intelligence Operations	collection and analysis of information	OSINT, predictive intelligence, AI	information superiority
Information Operations	information and psychological influence	strategic communications, media technologies	influence on the information environment
Intelligent Operations	analytical and predictive support	Big Data, ML, AI	decision-making support
Cyber Operations	protection and attacks in cyberspace	cyber intelligence, automated systems	protection of information infrastructure

Source: Compiled by the author.

The first category comprises **military operations**, which remain the principal instrument for achieving operational and strategic objectives through the employment of armed force. These operations include conventional combat, special operations, stabilization activities, peace support operations, deterrence, and multidomain military campaigns. Their effectiveness increasingly depends on the integration of intelligence, cyber capabilities, and information superiority rather than solely on kinetic power.

The second category includes **intelligence operations**, which provide continuous situational awareness and decision support across all levels of command. Modern intelligence encompasses strategic, operational, and tactical intelligence; human intelligence (HUMINT); signals intelligence (SIGINT); geospatial intelligence (GEOINT); measurement and signature intelligence (MASINT); open-source intelligence (OSINT); and all-source intelligence fusion. Recent technological developments have significantly expanded predictive intelligence through artificial intelligence, automated data processing, and advanced analytical models.

Table 2: Main types of intelligence operations

Type of Intelligence Operations	Main Activities	Main Tools and Technologies	Key Purpose
Military Intelligence	Collection of information on military forces, weapons, deployment, and enemy intentions	satellite monitoring, UAVs, technical surveillance systems	providing military command with operational information
Strategic Intelligence	Analysis of long-term threats and geopolitical processes	analytical systems, forecasting, scenario modeling	support for strategic security planning
Operational Intelligence	Collection of information to support specific operations	agent activities, technical intelligence, OSINT	support for operational decision making
Cyber Intelligence	Detection of cyber threats and analysis of adversary cyber activities	SIEM systems, AI, cyber monitoring, network traffic analysis	protection of information infrastructure and prevention of cyber threats
OSINT (Open Source Intelligence)	Analysis of open-source information	Big Data, AI-driven OSINT, social media, media monitoring	early threat detection and information analysis

Type of Intelligence Operations	Main Activities	Main Tools and Technologies	Key Purpose
Predictive Intelligence	Forecasting the development of threats and crisis situations	machine learning, predictive models, data analytics	proactive response to future challenges
POPINT (Population Intelligence)	Analysis of social processes, population behavior, and the humanitarian environment	social analytics, information monitoring, AI	assessment of social risks and information influence
Information and Analytical Intelligence	Integration and analysis of data from various sources	analytical platforms, decision support systems	formation of a unified security information space
Counterintelligence Operations	Detection and neutralization of foreign intelligence activities and internal threats	operational-search measures, cyber defense, analytical systems	protection of national interests and state security

Source: Compiled by the author.

The classification presented in Table 2 illustrates the diversity of intelligence activities that support contemporary security and defense operations. Beyond intelligence, modern operational systems also incorporate information, cyber, and technology-enabled functions.

A third category consists of **information and influence operations**, aimed at shaping perceptions, influencing decision-making, protecting national information space, and countering hostile information activities. These operations combine strategic communications, military public affairs, psychological operations, counter-disinformation measures, electronic warfare, and cognitive influence activities. Contemporary conflicts demonstrate that dominance in the information environment often determines operational success before kinetic engagement begins.

The fourth category includes **cyber operations**, which have evolved into an independent operational domain. Cyber operations involve both defensive and offensive activities designed to protect critical information infrastructure, ensure the resilience of command-and-control systems, disrupt adversary information networks, and support military operations in other domains. Their strategic importance continues to increase as modern armed forces become increasingly dependent on digital technologies.

The fifth category comprises **technology-enabled operations**, representing one of the fastest-growing areas of contemporary security studies. Artificial intelligence, autonomous systems, robotics, unmanned platforms, Big Data analytics, cloud computing, digital twins, and decision-support systems are increasingly integrated into operational planning, intelligence processing, logistics, command and control, and battlefield management. These technologies improve operational speed, enhance decision quality, and increase adaptability in highly dynamic operational environments.

An increasingly important category is represented by **integrated interagency operations**, which combine the capabilities of armed forces, intelligence agencies, law-enforcement institutions, emergency services, governmental authorities, private organizations, and international partners. Such operations are particularly characteristic of hybrid conflicts, crisis response, counterterrorism, civil protection, border security, and resilience-building activities. Their effectiveness depends on institutional interoperability, information sharing, and coordinated decision-making across multiple organizations.

The analysis further indicates that these categories cannot be considered independent operational activities. Rather, they constitute mutually reinforcing components of an integrated operational system. Military operations require continuous intelligence support; intelligence depends on cyber capabilities and advanced analytical technologies; information operations rely on intelligence

products and strategic communications; and all operational domains increasingly depend on artificial intelligence and digital infrastructures. This growing interdependence represents one of the defining characteristics of contemporary security and defense force operations.

Consequently, the traditional domain-oriented understanding of operations should be replaced by a capability-oriented perspective in which operational effectiveness emerges from the synchronized integration of diverse functional capabilities. Such an approach provides a more comprehensive theoretical basis for analyzing modern conflicts and supports the development of adaptive operational doctrines capable of responding to rapidly evolving security challenges.

A Conceptual Model of Contemporary Security and Defense Force Operations

The analysis of contemporary scientific literature indicates that existing studies primarily describe individual components of security and defense activities without adequately explaining their systemic relationships. Military operations, intelligence activities, cyber operations, information operations, and emerging technologies are frequently examined as separate research domains, resulting in conceptual fragmentation and limiting the development of an integrated understanding of contemporary operations.

The relationships among the principal functional components identified in this review are summarized in the conceptual model presented in Figure 1. The model illustrates the interaction between strategic governance, intelligence, decision-making, operational execution, and organizational learning, while emphasizing the cross-cutting role of artificial intelligence and digital technologies across the entire operational cycle.

To address this limitation, this review proposes a conceptual model in which security and defense force operations are considered a multidimensional adaptive system integrating functional capabilities rather than independent operational domains. Within this model, operational effectiveness is determined not by the performance of individual components but by the quality of their interaction, coordination, and synchronization throughout the operational cycle.

The conceptual architecture proposed in this study is presented in Figure 1. Unlike existing doctrinal representations that primarily emphasize operational domains, the proposed framework illustrates the continuous interaction between strategic governance, intelligence, decision-making, operational execution, and organizational learning. It also highlights the cross-functional role of artificial intelligence and digital technologies, which enhance every stage of the operational cycle rather than constituting an independent operational domain.

Figure 1: Conceptual Model of Contemporary Security and Defense Force Operations
Source: Compiled by the author.

As illustrated in Figure 1, operational effectiveness emerges from the dynamic interaction among the five functional layers rather than from the performance of any individual component. Continuous feedback enables organizational learning and capability adaptation, ensuring that security and defense organizations remain responsive to rapidly evolving operational environments.

The proposed model consists of five interconnected layers.

The **strategic layer** defines political objectives, national security priorities, legal frameworks, resource allocation, and strategic planning. This layer determines the desired operational effects and establishes the institutional environment within which security and defense operations are conducted.

The **information and intelligence layer** provides continuous situational awareness through the collection, processing, fusion, analysis, and dissemination of information obtained from multiple intelligence disciplines. Artificial intelligence, machine learning, predictive analytics, and open-source intelligence significantly enhance this layer by improving information processing speed and supporting evidence-based decision-making.

The **decision-making layer** transforms intelligence products into operational decisions. It integrates military planning, risk assessment, operational analysis, scenario development, and command-and-control processes. Modern decision-support systems enable commanders to evaluate multiple courses of action simultaneously, increasing operational flexibility under conditions of uncertainty.

The **operational execution layer** encompasses the coordinated implementation of military, intelligence, cyber, information, electronic warfare, and interagency activities. Rather than operating independently, these capabilities function as mutually supporting elements designed to achieve common operational objectives through synchronized action across multiple domains.

The **assessment and adaptation layer** provides continuous monitoring of operational performance, evaluates mission outcomes, identifies emerging threats, and generates feedback for

subsequent planning cycles. Lessons learned, operational experience, and adaptive organizational learning constitute essential components of this layer, ensuring the continuous improvement of future operations.

The interaction among these five layers forms a continuous adaptive cycle rather than a linear sequence of activities. Information collected during operational execution immediately influences intelligence assessments, operational decisions, strategic planning, and future capability development. Consequently, contemporary security and defense force operations should be understood as dynamic systems capable of continuous adaptation to rapidly changing operational environments.

Artificial intelligence represents a cross-cutting enabling capability rather than an independent operational domain within the proposed model. AI technologies support intelligence analysis, operational planning, predictive modeling, cyber defense, logistics, autonomous systems, and decision support across all layers of the operational cycle. Their value lies in strengthening human decision-making rather than replacing human judgment, particularly in complex security environments characterized by uncertainty and rapidly evolving threats.

The proposed conceptual model integrates fragmented scientific perspectives into a unified theoretical framework. It demonstrates that operational effectiveness depends on the synchronization of strategic governance, intelligence, decision-making, operational execution, and continuous organizational learning. Such an integrated perspective may serve as a theoretical foundation for future research, doctrine development, capability-based planning, and the digital transformation of security and defense institutions.

Discussion

The findings of this review confirm that the scientific understanding of security and defense force operations has evolved significantly during the last two decades. Whereas earlier studies primarily interpreted operations through the prism of conventional military activities, contemporary research increasingly recognizes their multidimensional character, integrating military, intelligence, cyber, informational, technological, and cognitive components. This evolution reflects the changing nature of security threats and the growing importance of information superiority, digital transformation, and interagency cooperation (Sarjito, 2024b; Gasanov et al.,2024; Ignatiev et al.,2025).

The proposed conceptual model is consistent with the general direction of contemporary military thought while extending existing theoretical approaches. The concept of Multi-Domain Operations (MDO) emphasizes the synchronized employment of capabilities across the land, maritime, air, space, cyber, and information domains. Similarly, NATO's comprehensive approach highlights cooperation among military, governmental, and civilian actors in achieving common security objectives. However, both approaches are primarily doctrine-oriented and focus on operational planning and capability employment.

Unlike these concepts, the model proposed in this study adopts a broader systems perspective. Rather than concentrating exclusively on operational domains, it conceptualizes security and defense force operations as an adaptive system composed of interconnected functional layers, including strategic governance, intelligence, decision-making, operational execution, and continuous organizational learning. This perspective better reflects the increasing interdependence between technological innovation, intelligence support, command-and-control processes, and operational effectiveness.

To better position the proposed framework within the existing body of knowledge, Table 3 compares its principal characteristics with the dominant theoretical approaches discussed in the literature. The comparison demonstrates that the proposed model extends previous concepts by integrating strategic governance, intelligence, digital technologies, organizational learning, and adaptive capability development into a single analytical framework.

Table 3: Comparative Characteristics of Existing Approaches to Security and Defense Force Operations

Characteristic	Traditional Military Operations	Joint Operations	Multi-Domain Operations	Intelligence-Led Operations	Proposed Conceptual Model
Primary objective	Defeat the enemy through military force	Synchronize military services	Synchronize effects across operational domains	Support decision-making through intelligence	Integrate all security and defense capabilities
Operational domains	Land, sea, air	Military domains	Land, maritime, air, space, cyber, information	Intelligence environment	Military, intelligence, cyber, information, technological, organizational, cognitive
Role of intelligence	Supporting	Supporting	Integrated	Central	Integrating mechanism
Information operations	Auxiliary	Supporting	Operational domain	Intelligence support	Core operational capability
Cyber capabilities	Limited	Supporting	Independent domain	Intelligence support	Integrated operational capability
Artificial intelligence	Minimal	Limited	Decision-support tool	Intelligence analytics	Cross-functional enabling capability
Decision-making	Commander-centered	Joint command	Network-enabled	Intelligence-driven	AI-supported adaptive decision-making
Organizational approach	Hierarchical	Joint force integration	Domain integration	Intelligence-centered	Adaptive systems approach
Feedback mechanism	Limited	Operational assessment	Continuous operational assessment	Intelligence cycle	Continuous learning and capability development
Principal contribution	Combat effectiveness	Service interoperability	Cross-domain synchronization	Intelligence superiority	Holistic integration of all operational capabilities

Source: Compiled by the author.

The comparison confirms that previous concepts generally focus on specific operational dimensions, such as military force employment, joint interoperability, multidomain synchronization, or intelligence support. By contrast, the proposed model conceptualizes security and defense force operations as an adaptive system in which operational effectiveness results from the coordinated interaction of multiple functional capabilities.

The review also demonstrates that artificial intelligence is transforming virtually every stage of the operational cycle. Most previous studies examine AI applications within specific domains, such as intelligence analysis, cyber defense, logistics, autonomous systems, or operational planning. The proposed framework instead considers artificial intelligence as a cross-functional enabling capability that enhances information processing, supports evidence-based decision-making,

improves operational adaptability, and accelerates organizational learning across the entire security and defense system.

Another important contribution concerns the integration of intelligence into the operational architecture. Existing literature frequently analyzes intelligence as an independent discipline or as a supporting function for military operations. The present study argues that intelligence should instead be regarded as a central integrating mechanism linking strategic planning, operational execution, information activities, and continuous assessment. Such an interpretation reflects contemporary operational realities in which timely intelligence increasingly determines operational success.

The proposed model may also support capability-based planning and the digital transformation of defense institutions. Its layered architecture facilitates the identification of capability gaps, supports the prioritization of technological investments, and provides a conceptual basis for integrating artificial intelligence, advanced analytics, autonomous systems, and decision-support technologies into future operational concepts. Consequently, the model has potential practical value for defense planners, military educational institutions, and organizations responsible for force development.

Nevertheless, several limitations should be acknowledged. As a review study, the proposed framework is conceptual rather than empirical and has not yet been validated through quantitative analysis or operational case studies. Future research should evaluate the applicability of the model using evidence from recent military conflicts, multinational operations, and national security institutions. Comparative assessments involving NATO member states and partner countries could further refine the proposed framework and strengthen its practical relevance.

Overall, the findings indicate that contemporary security and defense force operations should no longer be interpreted as isolated military activities. Instead, they represent adaptive, technology-enabled, intelligence-driven systems operating across multiple functional domains. This integrated understanding provides a stronger theoretical foundation for future research and contributes to the continuing development of security and defense studies.

Conclusions

This review has demonstrated that contemporary security and defense force operations have evolved beyond the traditional understanding of military activities into complex, multidimensional systems integrating military, intelligence, cyber, information, technological, and interagency capabilities. The transformation of the security environment, characterized by hybrid threats, rapid technological advancement, and increasing uncertainty, requires a systemic approach that ensures the coordinated employment of these capabilities throughout the operational cycle.

The analysis of contemporary scientific literature revealed that existing theoretical approaches—including Joint Operations, Multi-Domain Operations, Intelligence-Led Operations, and capability-based concepts—have significantly contributed to the understanding of modern operations. However, these approaches remain primarily focused on individual operational dimensions and do not provide a comprehensive framework that integrates strategic governance, intelligence, operational decision-making, technological innovation, operational execution, and organizational learning within a unified conceptual architecture.

The principal scientific contribution of this study is the development of a conceptual model of contemporary security and defense force operations that conceptualizes operations as an adaptive, intelligence-driven system composed of five interrelated functional layers: strategic governance, information and intelligence, decision-making, operational execution, and assessment and adaptation. Unlike existing doctrinal models, the proposed framework emphasizes the continuous interaction among these layers and identifies artificial intelligence and digital technologies as cross-functional enablers that strengthen every stage of the operational process.

The proposed model provides a theoretical foundation for future studies in security and defense management, capability-based planning, digital transformation, and military innovation. It may also support the development of operational doctrines, decision-support systems, military education, and organizational modernization within national security institutions.

Future research should focus on validating the proposed conceptual framework through empirical case studies, comparative analyses of national security systems, and the examination of recent military conflicts. Additional studies may also investigate the integration of artificial intelligence, autonomous systems, advanced analytics, and human–machine collaboration into adaptive security and defense ecosystems capable of responding effectively to emerging multidomain threats.

Funding

This study received no specific financial support.

Competing interests

The authors declare that they have no competing interests.

Use of Artificial Intelligence

Artificial intelligence was used for language editing, translation, and technical verification of the manuscript.

References

Afolabi, M., & Bodunde, O. (2020). Concept of security threats and national security. *Readings in Intelligence and Security Studies*, 2, 12–28. https://www.researchgate.net/publication/366543833_Concept_of_Security_Threats_and_National_Security

Anning, S., Fenton, T., Muraszkiewicz, J., & Watson, H. (2022). Operationalising human security in the contemporary operating environment: proposing population intelligence (POPINT). *The Journal of Intelligence, Conflict, and Warfare*, 4(3), 30–61. https://doi.org/10.21810/jicw.v4i3.3802

Bellaby, R. (2026). Managing the ethical risks of AI in intelligence. *AI & Society*. https://doi.org/10.1007/s00146-026-03045-2

Caballero, W., & Jenkins, P. (2025). On large language models in national security applications. *Stat*, 14, e70057. https://doi.org/10.1002/sta4.70057

Gill, P., & Phythian, M. (2018). *Intelligence in an insecure world*. Cambridge: Polity.

Dahl, E.J., & Strachan-Morris, D. (2024). Predictive intelligence for tomorrow's threats. *Journal of Policing, Intelligence and Counter Terrorism*, 19(4), 423–435. https://doi.org/10.1080/18335330.2024.2404834

Hasanov, A., Tahirov, R., & Iskandarov, K. (2024). The future of warfare. Anticipated changes in military trends. *Social Development and Security*, *14*(5), 1-18. https://doi.org/10.33445/sds.2024.14.5.1

Ignatiev, A., Burlakov, S., Terletskii, A., & Skryl, S. (2025). Assessment of modern challenges and threats affecting national security through large-scale military operations. *DIXI*, 27(2), 1–14. https://doi.org/10.16925/2357-5891.2025.02.02

Kerr, A. (2023). Researching national security intelligence: multidisciplinary approaches. *Intelligence and National Security*, 38(5), 838–843. https://doi.org/10.1080/02684527.2023.2170354

Khan, R.N.A., & Khan, A.U. (2025). Artificial intelligence and the national security matrix. *Research Journal for Social Affairs*, 3(4), 139–145. https://doi.org/10.71317/RJSA.003.04.0268

Kolade, T.M., Obioha-Val, O.A., Balogun, A.Y., Gbadebo, M.O., & Olaniyi, O.O. (2025). AI-driven open source intelligence in cyber defense: a double-edged sword for national security. *Asian Journal of Research in Computer Science*, 18(1), 133–153. https://doi.org/10.9734/ajrcos/2025/v18i1554

Maloku, A., Kastrati, S., Gabela, O., & Maloku, E. (2022). Prognostic scientific research in planning and successful management of organizations in the security sector. *Corporate & Business Strategy Review*, 3(2), 138–150. https://doi.org/10.22495/cbsrv3i2art12

Mille, S. (2022). National security intelligence activity: a philosophical analysis. *Intelligence and National Security*, 37(6), 791–808. DOI: https://doi.org/10.1080/02684527.2022.2076329

Pandey, A.K., Chakrovarty, A., & Khandal, V. (2024). Scientometric study of research on AI & ML application in defence technology and military operations. *DESIDOC Journal of Library & Information Technology*, 44(2), 61–68. https://doi.org/10.14429/djlit.44.2.19496

Pokrajčić, I. (2025). Examining the transformation of the US national security system after 2001. *Strategos*, 9(1), 11–32. https://doi.org/10.65243/s.9.1.1

Sarjito, A. (2024a). Enhancing national security: strategic policy development in defense management. *Jurnal Pelita Nusantara: Kajian Ilmu Sosial Multidisiplin*, 2(1), 56–68. https://doi.org/10.59996/jurnalpelitanusantara.v2i1.524

Sarjito, A. (2024b). The impact of intelligence gathering, risk analysis, and scenario planning on defense policy formulation. *International Journal Administration, Business & Organization*, 5(2), 27–46. https://doi.org/10.61242/ijabo.24.396

Sarjito, A. (2024c). Peran intelijen melalui perumusan kebijakan pertahanan negara dalam perang hibrida. *PANDITA: Interdisciplinary Journal of Public Affairs*, 7(1), 74–88. https://doi.org/10.61332/ijpa.v7i1.152

Willis, S., & Jefferson, K.W. (2025). The new power model and United States national defence agility. *Security and Defence Quarterly*, 50(2), 1–12. https://doi.org/10.35467/sdq/202643

Zamfirescu, C. (2024). Strategic decisions in national security: the connectivity between operations research and artificial intelligence. *Journal of Military Technology*, 7(2), 15–18. https://doi.org/10.32754/JMT.2024.2.02