International Journal of Safety and Security Engineering
Vol. 16, No. 2, February, 2026, pp. 403-412
Journal homepage: http://iieta.org/journals/ijsse

National Security and New Technologies: The Impact of Digitalization, Innovation, and Artificial Intelligence on the Effectiveness of Security and Defense Forces

Orest Kachurovskyi[1*], Andrii Buzarov[2], Yevhenii Taran[3], Oleksandr Mynko[4], Andriy Sogorin[5]

[1] Department of Political Science and Philosophy Named after Serhii Konoval, B. D. Havrylyshyn Education and Research Institute of International Relations, Western Ukrainian National University, Ternopil 46009, Ukraine
[2] Kuras Institute of Political and Ethnic Studies of the National Academy of Sciences of Ukraine, Kyiv 01011, Ukraine
[3] Global and National Security Department, Taras Shevchenko National University of Kyiv, Kyiv 04050, Ukraine
[4] Department of State Security, Kyiv Institute of the National Guard of Ukraine, Kyiv 03179, Ukraine
[5] Department of Fire Training, Kyiv Institute of the National Guard of Ukraine, Kyiv 03179, Ukraine

Corresponding Author Email: oma132@ukr.net

https://doi.org/10.18280/ijsse.160215

Received: 2 November 2025
Revised: 1 January 2026
Accepted: 10 January 2026
Available online: 28 February 2026

Keywords:
national security, digitalization, defense innovation, cybersecurity, defense technologies

ABSTRACT

The aim of this study was to analyse the impact of digitalisation, innovation and AI on the effectiveness of security and defence forces. The methodology is based on a combined approach: an analytical review of scientific literature, official reports and open data, as well as case studies. The main methods for processing materials are qualitative. The results of the study showed that the key technologies that increase operational and strategic effectiveness are AI systems for intelligence and data analysis, combat and reconnaissance drones, digital troop management platforms, automated situational awareness systems and cyber defence. The study of individual cases showed that these technologies help reduce decision-making time, increase the accuracy of operations, and reduce personnel losses. At the same time, several barriers were identified – technical, personnel, ethical, and security, that affect the pace and quality of digital solution implementation. The conclusions pointed to the integration of modern technologies into national security systems to increase their resilience and adaptability in the face of constant changes in the security environment. The practical significance of the study lies in the formulation of recommendations for optimising the processes of digital transformation in the defence sector.

1. INTRODUCTION

In the 21st century, technology has become essential for national security. Digitalization, innovation, and Artificial Intelligence (AI) have changed the daily lives of humanity and are fundamentally transforming the functioning of the security and defense sector [1]. In a world of hybrid wars, cyber threats, information attacks, and precision weapons, the effectiveness of national security increasingly depends on the technological capabilities of the state. The introduction of AI into command-and-control systems, real-time analysis of large data sets, autonomous platforms, and cyber defense all contribute to the creation of a new security architecture [2]. Modern scientific research has indicated the transformation of the security sector under the influence of technological progress [3]. Modern analytical works have pointed to the important role of cybersecurity in national strategy [4]. Several studies have also examined the potential of AI in the field of intelligence, threat monitoring, and automated decision-making [5]. At the same time, most work focuses on Western countries with a high level of technical readiness [6, 7]. Studies of the experience of countries at war remain limited.

In this article, AI is defined as a set of computing systems capable of performing analytical, predictive, and support functions in the decision-making process in the field of security and defense. In practical terms, it refers to intelligence analysis, cyber defense, autonomous systems, and intelligent command support tools. Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) in the study is understood as an integrated architecture of command, control, communications, computer systems, intelligence, surveillance, and reconnaissance that provides the collection, exchange, and use of information to improve situational awareness and operational effectiveness.

A vivid example of a large-scale technological transformation in the field of defense is Ukraine, which, after the start of armed aggression by the Russian Federation in 2014, and especially after the full-scale invasion in 2022, became one of the first training grounds for the combat use of modern digital solutions [8, 9]. In conditions of limited resources, but with a high level of mobilization of society and the IT sector, Ukraine is introducing innovations in the field of drones, satellite reconnaissance, digital command and control of troops, the creation of cyber commands and the use of AI in intelligence analytics. This context makes the Ukrainian

experience particularly valuable for studying the impact of new technologies on national security.

However, despite the obvious successes, the introduction of new technologies into the security sector is associated with several challenges in particular, scientific literature highlights the lack of financial and human resources, the lack of legislative regulation, ethical dilemmas associated with autonomous weapons and the aggravation of cyber threats [10]. Additionally, the role of AI and digital technologies in changing the strategy and effectiveness of security and defense forces has not yet been sufficiently studied in the scientific field [11]. Especially little attention is paid to cases when such transformations occur during active military operations [12]. This article attempts to fill these gaps and carry out a systematic study of the role of innovative technologies in the development of the security sector.

Despite the significant amount of research devoted to the digitalization of the security and defense sector, the existing scientific literature has a number of significant limitations. Most of the works focus mainly on the technological aspects of the implementation of AI or on the analysis of individual innovative systems in countries with a high level of technological readiness. At the same time, much less attention is paid to a comprehensive analysis of the impact of digital technologies on the organizational transformation of the security sector, changing management models and the formation of new strategies for responding to threats.

In addition, scientific literature has not sufficiently studied the experience of states that are forced to implement innovative security technologies in conditions of active military operations and limited resources. Most of the existing research considers the digitalization of the defense sector in conditions of relative stability, while the processes of rapid technological adaptation during war remain insufficiently conceptualized.

Thus, the scientific gap of this study lies in the lack of a systematic comparative analysis of the impact of digitalization, innovative technologies and AI on the transformation of the security sector in conditions of modern conflicts. The number of works that combine the analysis of the Ukrainian experience of military digitalization with international examples of the development of digital security strategies is particularly limited.

Accordingly, the goal of the article is to conduct an analysis of the role of digitalization, innovative technologies and AI in the development of security and defense forces in the face of modern threats.

Main research questions:

1. What technologies are used for the operational and strategic effectiveness of security forces?
2. What barriers exist in the implementation of AI and digital solutions in the defense sector?
3. What conclusions can be drawn based on the analysis of Ukrainian experience and international experience in modernizing the security sector in wartime?

2. METHODS

The study used a qualitative, exploratory design that included an analytical review, a comparative case study methodology, and conceptual modeling. The study aimed to investigate the impact of digitalization, innovation, and AI on the effectiveness and organizational transformation of the national security and defense sectors under various threat conditions, including active military conflict.

The analytical approach consists of a review of scientific literature, analytical reports, official documents, national strategies, and open sources related to the use of digital technologies, innovations, and AI in the national security sector. This approach made it possible to identify the main trends and challenges of the digital transformation of the defense sector. Case studies were used for the purpose of in-depth analysis of specific examples related to the implementation of digital technologies in the security and defense sector.

The choice of these approaches is due to the need to combine a broad conceptual framework (through an analytical review) with the consideration of practical examples (through case studies). In this way, not only the potential but also the real challenges of implementing technologies in the security sector were assessed.

2.1 Data sources

Various sources related to academic and official data are used for the study:

1. Academic sources. Consist of peer-reviewed scientific articles, analytical reviews of monographs. The main databases are Scopus, Web of Science, Google Scholar. Time range of inclusion of sources: 2019-2025, selected to analyze only relevant scientific literature.
2. Official reports and documents. Included publications of the Ministry of Defense of Ukraine, the General Staff of the Armed Forces of Ukraine, the Center for Countering Disinformation, as well as international organizations - NATO, DARPA, RAND Corporation.
3. Open sources and analytics. Analyzed reports of cybersecurity companies, reviews of the use of drones, AI and satellite technologies.

The selection of cases is based on the following criteria:

1. Relevance to the topic. Selected cases should indicate the practical impact of digital technologies on the operational or strategic effectiveness of security forces.
2. Data availability. Priority is given to cases for which there are open or official sources that allow for qualitative analysis.
3. Geographic diversity. The analysis covered not only the Ukrainian case but also examples from other countries. This will allow identifying universal and contextual characteristics of technology implementation.
4. Innovation. The cases reflected innovative approaches (implementation of autonomous systems, use of AI in intelligence, or creation of cyber armies).
5. Dynamics of change. Priority is given to cases that demonstrate the rapid evolution of technologies in war conditions.

Accordingly, case studies were used to analyze specific examples of the application of digital technologies and AI in the security sector:

Case 1 (Ukraine) – use of AI in the field of cyber defense in Ukraine; application of drones and automated control systems [13-15].

Case 2. (The United States) (DARPA) – use of AI in combat scenario analysis systems (Mosaic Warfare, AI-driven targeting, Project Maven) [16].

Case 3. (Israel) – integration of AI into intelligence, threat prediction and targeting, use of AI in real time during operations against Hamas [17].

Case 4. (Estonia) – use of AI-based intelligence technologies. National Cyber Defense Strategy and Cyber Command model, as an example of digital integration into the defense system in conditions of constant threat from Russia [18].

Given the limited availability of classified operational metrics, the study relies on quantitative proxies, including deployment rates, budget allocation trends, participation in cyber training, and documented AI deployment programs. These metrics do not measure combat effectiveness directly but provide a reliable approximation of digital maturity and institutional capacity.

2.2 Data analysis

Two complementary methodological approaches are used to interpret the collected data: qualitative content analysis and comparative case analysis. Qualitative analysis made it possible to analyze the content of strategic documents, government reports, expert publications, scientific literature and media sources related to digitalization and the use of innovative technologies in the field of security and defense. The main goal of this analysis was to identify common narratives, priority areas of development, and barriers to the implementation of digital solutions. The analysis is carried out according to the following thematic categories: 1. Technological goal. 2. Functional strategies. 3. Institutional challenges. 4. Socio-ethical aspects. Such analysis made it possible to indicate the systematic nature of digital transformations, as well as their impact on the overall capacity of the national security system.

The second paragraph's important method was a comparative analysis of four cases: Ukraine, Estonia, the United States and Israel. To ensure the relevance of the comparison, a single analytical matrix is used, which covers the following criteria: technology implementation goals, level of innovation integration, achieved efficiency, problems. This made it possible to identify common and distinctive features on the path to attracting innovative technologies and point out typical challenges.

To systematize the comparison of different cases, the study introduced an original analytical tool, the Digital Security Maturity Framework (DSMF). The framework operationalized qualitative findings into 5 analytical dimensions, allowing comparisons across cases and time periods, and avoiding the limitations of direct quantitative indexing in the security field.

2.3 Ethical aspects

The research is based mainly on open sources, official materials, and peer-reviewed scientific articles. All these sources are public, transparent, and do not infringe on the rights of third parties.

Attention is paid to academic integrity. The analysis process strictly adheres to the principles of no manipulation or selective use of data. Norms governing the depiction of military actions and dual-use technologies are also observed so as not to create risks to national security or public order. The analysis of sensitive topics is presented neutrally and without sensationalism, while respecting the responsibility for public discourse.

3. RESULTS

3.1 Analytical review: Digitalization trends in the security and defense sector

Digital transformation in the security and defense sector is a global process that involves the use of various innovative technologies – from AI and autonomous systems to high-precision cybersecurity tools [19]. The increasing complexity of hybrid threats, the development of network-centric warfare approaches, and the need for rapid adaptation to dynamic challenges have led to high demand for technologies that can improve the effectiveness of command, intelligence, logistics, and defense planning. In this sense, digitalization processes play the role of technological modernizations and are a key factor in the transformation of strategic thinking in the field of national security.

One of the leading trends is the widespread implementation of AI in military command and decision-making processes. In leading countries worldwide (the United States, Israel, the United Kingdom), AI is used for intelligence analysis, threat forecasting, and risk scenario modelling [16, 20]. Deep learning algorithms enable automated processing of large volumes of data from satellite imagery, drone videos, and open sources. Such systems allow for the identification of hidden patterns of hostile activity. This, in turn, increases the speed and accuracy of threat response. Specifically, within the framework of the US Department of Defense's Maven project, neural network models are actively used for real-time object recognition in images [21].

At the same time, AI plays a significant role in the field of military logistics. Using predictive analytics algorithms, it is possible to optimize supply routes, anticipate disruptions in logistics chains, and automate resource management processes [21]. As a result, the burden on personnel is reduced, and resilience to external destabilizing factors is increased. Such capabilities are already being actively used by the armed forces of NATO member countries [22]. Countries with a developed cyber strategy are implementing multi-layered defense architectures consisting of behavioral analysis modules, cryptographic protection, and intelligent traffic filters.

At the same time, in Ukraine, starting in 2022, the accelerated formation of a resilient cybersecurity system is taking place [13]. Within the framework of government initiatives and public-private partnerships, systems are being developed and implemented that combine machine learning algorithms with behavioral analytics tools. One such platform is "Morana," which is focused on monitoring, detecting, and locating cyberattacks on critical infrastructure in combat conditions [23].

A separate and increasingly important direction of digitalization is innovation in the field of autonomous systems, which includes robotics, unmanned aerial vehicles (UAVs), and ground autonomous platforms. Technological development in this segment opens possibilities for creating high-autonomy systems capable of performing reconnaissance, target designation, target engagement, or evacuation tasks. Specifically, Israel is actively using autonomous systems on its borders to detect and intercept sabotage groups, combining drones with sensor networks and AI. The US is implementing the concept of "swarm" drones, which can operate as a coordinated system with decentralized control. Thus, the examples presented cover various

technological aspects: from AI used for automated video data analysis, to combat drones and robotic systems, as well as cybersecurity infrastructures (X-Road, Guardtime KSI). Each of these technologies performs a critically important function – from ensuring operational advantage on the battlefield to guaranteeing the cyber resilience of government institutions. Table 1 provides examples of key digital technologies used in selected countries.

Table 1. Digital technologies in security (by country)

Technology/System Name, Country	Technology Type	Purpose	Comment / Feature
Morana, Ukraine	Cyber Defense, AI	Detection and neutralization of cyberattacks	Uses machine learning elements
Delta, Ukraine	Combat IT Platform [24]	Coordination of actions on the battlefield, surveillance	Integration with UAVs and GIS
Shablja, Ukraine	AI Analytics [25]	Processing intelligence from various sources	Used in military intelligence
MQ-9 Reaper, United States	Drone (Strike)	Reconnaissance, targeted destruction	Used in combat zones around the world
Project Maven, United States	AI	Automatic analysis of drone video	Uses computer vision
Palantir Gotham, United States	Analytics / AI	Visualization and analysis of data for the army	Integrates with intelligence services
HAROP, Israel	Kamikaze Drone	Destroying targets with autonomous guidance	Often used in conflicts in the Middle East
IRON DOME AI Upgrade, Israel	Air Defense + AI	Optimization of missile interception	Introduction of neural network algorithms
Elbit Skylark I-LEX	Tactical UAV	Aerial reconnaissance	High maneuverability, real-time use
X-Road, Estonia	Cyber Defense Infrastructure	Secure data exchange between institutions	A key component of state cybersecurity
SIEM (Guardtime KSI), Estonia	Cyber Defense, Blockchain	Registration of changes in databases	Based on blockchain; ensures data integrity
NATO CCDCOE Simulators, Estonia	Cyber Training	Simulation of attacks, training of specialists	NATO Center of Excellence

Note: Ukr: Ukraine; Est.: Estonia; GIS: Geographic Information System; SIEM: Security Information and Event Management; KSI: Keyless Signature Infrastructure; CCDCOE: Cooperative Cyber Defence Centre of Excellence.

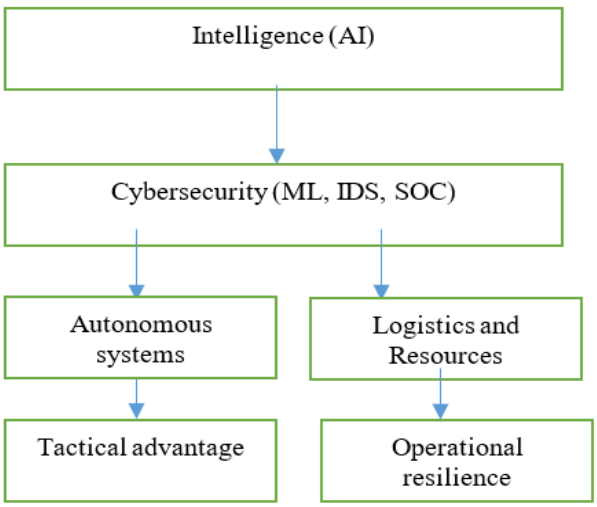

Figure 1. The connection between AI, cybersecurity, autonomous systems, logistics, and tactical management

Thus, they demonstrate various technological innovations: the use of AI for automated video data analysis (Project Maven, Palantir Gotham), combat drones and robotic systems (MQ-9 Reaper, HAROP, Elbit Skylark), as well as cybersecurity infrastructures (X-Road, Guardtime KSI). Ukrainian experience in this field is also noteworthy. The "Army of Drones" initiative involves the comprehensive use of UAVs for reconnaissance, target engagement, and securing tactical advantage on the battlefield. A significant portion of such systems have computer vision modules integrated with neural network-based enemy object recognition platforms. Autonomous ground platforms are also being developed for evacuating the wounded or transporting cargo, which reduces the risk to personnel. Thus, the digitalization of the security and defense sector is not purely a technological process. Figure 1 visually illustrates the relationship between AI, cybersecurity, autonomous systems, logistics, and tactical management.

Therefore, the use of AI in military and security structures demonstrates the potential to optimize decision-making and increase operational flexibility, which is an important condition for adapting to modern technological and strategic challenges.

3.2 Comparative analysis of digital strategy cases in the security sector

While the previous section outlined the key technological trends shaping the digital transformation of the security sector, the following comparative analysis focuses on how these technologies are implemented within different national security strategies. The cases of Ukraine, the United States, Israel, and Estonia illustrate distinct institutional approaches to integrating digital technologies, AI, and cyber capabilities into defense systems. Specifically, Ukraine is focusing its digital efforts on countering hybrid and cyber threats, utilizing open platforms, engaging private developers, and adapting Western solutions to the conditions of high-intensity warfare. The Morana platform has become an example of a domestic cybersecurity solution that combines log analytics, anomaly detection, and rapid scaling.

At the same time, the US is demonstrating a strategy of full-scale digital transformation using drones (MQ-9 Reaper), satellite intelligence, and AI analytics at the strategic level.

The integration of digital tools at all levels of defense is accompanied by high levels of funding and standardization based on NATO approaches.

Israel uses models of digital point advantage. The use of autonomous kamikaze drones (Harop) in combination with AI guidance provides precision and speed of strikes, which is critical in the face of terrorist threats. A key feature is the synergy between the military-industrial complex and the high-tech sector [24].

Despite its small size, Estonia is a pioneer in the digitalization of the state. Her unique experience in cybersecurity, built after the 2007 cyberattacks, became the foundation for creating a cyber doctrine that includes digital resilience, simulated attacks, and continuous updating of national response systems. Centralized institutions such as the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) highlight its leadership in the field of cyber defense within the European context (Table 2).

Table 2. Comparative analysis of digital strategies in the security sector

Parameter	Ukraine	United States	Israel	Estonia
Industry of implementation	Cyber Defense, AI Analytics	Autonomous systems, satellite intelligence	Preventive drones, autonomous guidance	Cyber defense, digital resilience
Technologies	Morana, Open Source Log Analysis	MQ-9, AI-intelligence, distributed sensors	Harop, edge AI, target recognition	X-Road, SIEM systems, cyber simulators
Institutional model	Flexible, Decentralized	Centralized, hierarchical	Hybrid: private-public	Centralized with NATO coordination
Context of application	Full-Scale War, Russian Attacks	Foreign operations, global strategy	Border conflicts, terrorist threat	Persistent hybrid threat, strategic stability
Key challenges	Policy Fragmentation, Staffing Shortage	- 45% losses	Legal issues, escalation risks	Reliance on partnerships, low resources

Note: SIEM: Security Information and Event Management; NATO: North Atlantic Treaty Organization.

Table 3. Quantitative proxy indicators of digital and AI integration in the security sector (open sources)

Indicator	Country	Recorded Value	What Exactly does it Measure?	Source (Type)
Number of AI autonomous guidance kits for UAVs	Ukraine	33,000 units	Scale of practical implementation of AI in combat systems	Reuters, Defense Contracts
Contract volume for AI solutions for drones	Ukraine / United States	≈ 50 million USD	Level of institutional investment in autonomous technologies	Reuters
Maximum distance of autonomous tracking of a target	Ukraine	up to 1 km	Technical capability of AI guidance in EW conditions	Reuters
Share of counter-UAV technologies developed by startups	Israel	about 50%	Level of integration of the private AI sector into defense	Reuters
Number of defense startups whose solutions are used in war	Israel	over 25	Depth of the innovation ecosystem in the security sector	Reuters
Participants in Locked Shields cyber exercises (2024)	Estonia (NATO CCDCOE)	≈ 4,000 specialists	Scale of preparation for cyber operations	NATO CCDCOE
Number of simulated systems in Locked Shields	Estonia	over 5,500 systems	Complexity and realism of cyber threats	NATO CCDCOE
Target identification accuracy in the "human + AI" model	United States (DoD tests)	➢ 95%	Human-in-the-loop effect in military analytics	DoD / Air & Space Forces
Identification accuracy: human without AI	United States	≈ 85%	Baseline without AI support	DoD
Identification accuracy: AI without human	United States	≈ 44%	Limitations of full autonomy	DoD

Sources: [26, 27]

Note: UAV: Unmanned Aerial Vehicle; EW: Electronic Warfare; NATO: North Atlantic Treaty Organization; CCDCOE: Cooperative Cyber Defence Centre of Excellence; DoD: Department of Defense.

Despite the obvious advantages of digitalization in the defense sector, its implementation is accompanied by several significant challenges that are both technical and socio-political in nature. These challenges vary depending on a country's level of digital maturity, geopolitical position, available resources, and national strategic priorities. The analysis of the selected cases allows us to identify several common and specific problems. Specifically, the integration of AI systems, drones, and cloud platforms opens opportunities for cyberattacks, sabotage, information leaks, or manipulation of algorithms. Furthermore, there are situations where digital solutions are often not compatible with traditional military command structures. Compatibility issues, lack of standardization, and outdated software can hinder the effective deployment of innovations. In Estonia, this challenge was successfully addressed thanks to a centralized digital architecture, but in Ukraine, there is often fragmentation between individual IT solutions in different departments. Modern countries are also facing a need for highly skilled IT professionals who can develop, maintain, and analyze digital systems. AI, autonomous weapons systems, biometric surveillance – all these technologies pose challenges to international humanitarian law and national legislation. The use of autonomous drones or algorithms for strike decisions raises discussions about accountability, transparency, and humanity.

3.3 Quantitative indicators of digital transformation of the security sector

In contrast to the qualitative analysis presented in the previous sections, this subsection introduces quantitative proxy indicators that reflect the scale of digital transformation in the security sector. These indicators provide an approximate but informative assessment of technological adoption in the absence of classified operational data. According to official reports of international news agencies, in 2024–2025 Ukraine will receive tens of thousands of AI-guidance sets for strike drones under contracts supported by the US Department of Defense. These systems will provide autonomous tracking of the target at the final stage of the flight and increased resistance to radio-electronic interference. At the same time, experimental studies conducted by the US Department of Defense have shown that the highest accuracy rates are achieved not in fully autonomous systems, but in "human + AI" models. According to the results of controlled tests, the combination of analytics with AI-tips provided over 95% accuracy in object identification. At the same time, the indicators for a person or algorithm separately are lower. Therefore, in the absence of open combat statistics, the scale of implementation, funding volumes and results of experimental tests allow us to draw a reasonable conclusion about the real impact of digital technologies and AI on increasing the operational capabilities of security forces. At the same time, in Israel, where the technology sector is integrated into national defense, a significant part of modern counter-drone systems comes from private startups. It is estimated that about 50% of such technologies are used in combat conditions thanks to support and government contracts. Estonia, for its part, hosts one of the world's largest cyber exercises, Locked Shields, which annually brings together several thousand specialists from dozens of countries to practice protecting critical digital infrastructure. In 2024, the exercise brought together about 4,000 experts and simulated the protection of more than 5,500 virtual systems, demonstrating the high level of preparation of allies for complex cyber operations (see Table 3).

To systematize the comparative analysis and increase the analytical consistency of the study, the author's framework for assessing the digital readiness of the security sector (DSMF) is proposed.

This framework is based on 5 key dimensions, each of which is assessed on a conditional scale from 0 to 5, where 0 means the absence of systemic implementation, and 5 - a high level of institutional and operational maturity. These dimensions include: the level of integration of AI, cyber resilience, institutional coordination, legal and ethical governance, as well as cooperation between the public and private sectors. This approach made it possible to identify national models of digital transformation of the security sector even in the absence of open combat performance indicators and minimizes the risk of incorrect quantitative generalizations.

The application of the Digital Security Maturity Framework in this study allows us to identify common patterns of digital transformation and differences due to the state of war, institutional structure or level of development of the innovation ecosystem. Thus, the framework acts as an analytical tool that combines qualitative case analysis with a comparative logic for assessing digital maturity.

Description of criteria

AI integration level – the degree of use of AI in intelligence, management, cyber defense and autonomous systems.

Cyber resilience — the ability of the system to resist, localize and recover from cyber-attacks.

Institutional coordination – the level of coordination between military, government and security institutions.

Legal & ethical governance – the presence of regulatory frameworks and mechanisms for controlling the use of AI.

Public–private cooperation – the intensity of involvement of the private IT sector and startups in defense solutions.

In Ukraine, high AI adaptation and unique public–private cooperation is noticeable, but fragmented institutional coordination and an incomplete legal framework were also noticeable. This is due to the conditions of war.

At the same time, in the United States, maximum systematicity, institutional maturity and standardization are noticeable, which is visible in the assessments.

In Israel, there is an extremely strong AI integration and startup ecosystem, but limited formalization of ethical governance.

At the same time, Estonia has become a benchmark for cyber resilience and legal governance, but there is less deep military AI integration (see Figure 2).

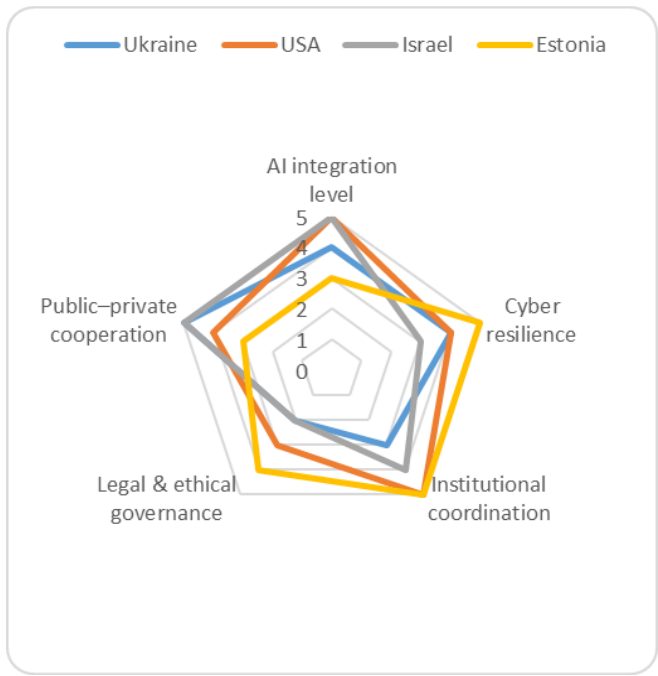

Figure 2. Digital Security Maturity Framework (DSMF)

Thus, digitalization and AI have influenced changes in approaches to organizing the security sector at both the tactical management level and the strategic planning level. According to the results obtained, technology plays an increasingly decisive role in modern armed conflicts, not a secondary one. In the face of high threat dynamics, digital solutions provide the army with the ability to adapt, respond flexibly, accurately predict risks, and reduce personnel losses.

4. DISCUSSION

The analyzed cases showed that the greatest potential for improving operational and strategic effectiveness lies in AI systems for reconnaissance and analysis, combat and

reconnaissance drones, digital troop management platforms, automated situational awareness systems (C4ISR), and cybersecurity platforms. Ukraine is using comprehensive solutions like Delta, the Israeli army is employing AI systems for real-time decision-making (Gospel AI system), and the United States is utilizing integrated cloud environments for sharing tactical information (e.g., JADC2). In all cases, technology accelerates the "observe – orient – decide – act" (OODA) loop. Such a system is particularly important in the context of hybrid warfare. These findings correlate with the results of the study by other researchers [28], which showed that national AI strategies enhance the resilience of security systems and enable multidimensional strategic planning. In turn, other scientists have pointed out that the third wave of digital governance is based on the integration of big data analytics and machine learning to improve the accuracy and effectiveness of public administration, particularly in the security sector. Das and Sandhane's study also confirm the effectiveness of using AI in detecting and preventing cyber threats, which is directly relevant to ensuring cybersecurity in the context of a military conflict [28]. According to the findings of Soare [29] and Benouachane [30] the successful implementation of digital defense solutions requires not only technological modernization but also adaptation of the organizational structure and political will. The Ukrainian experience presented in this work has demonstrated that even under limited resources, defense digitalization is possible if effective management, partner support, and a strategic vision are combined. Thus, empirical cases confirm that digital platforms and AI technologies are becoming fundamental elements of modern security [31]. According to the results obtained, the key advantages of digital technologies are the automation of intelligence data collection, processing, and analysis, which significantly reduces decision-making time and improves their quality. For digital communication systems, the main advantages relate to accelerating information exchange, reducing the risk of data loss, and increasing the transparency of management processes [32]. At the same time, other scientists emphasized that the use of innovations involves reducing the burden on personnel, lowering losses, and increasing the accuracy of operations [33, 34].

These advantages are confirmed in articles that highlight the role of AI in active network defense, as these systems can detect threats based on anomalies in real-time. Benouachane's research is developing in a similar direction, outlining the relationship between autonomous platforms and new challenges in the fields of ethics and international law [34]. Despite the advantages, the study also revealed a few challenges that align with the findings of other researchers. For example, Dunleavy & Margetts, in their concept of the "third wave of digital governance," emphasize the need to restructure bureaucratic structures and retrain personnel to ensure the effective implementation of AI [34]. This resonates with Ukrainian realities, where the digital modernization of the defense sector is often hampered by a lack of personnel, the absence of a centralized strategy, and dependence on foreign solutions.

Additionally, other scholars have pointed out that the modern European space faces a dilemma between national digital sovereignty strategies and global markets, which creates legal gaps and institutional contradictions. In this sense, Israel's experience, which integrates AI at all levels of defense while considering its own specificities, demonstrates a more balanced implementation model compared to the EU or Ukraine [35, 36]. Thus, these barriers remain significant. Other works point to challenges such as inadequate infrastructure and limited access to quality data [37, 38]. Specifically, as the authors note, AI technologies in a defense context often promise more than they can realistically deliver, creating the illusion of digital sovereignty [39-41]. A comparison with current research indicates that without proper regulatory support, digital transformation in the security sector may remain fragmented [42-44]. The authors stated that digitalization requires not only technical implementation but also institutional adaptation, political will, and a legal framework [45-47]. The same emphasis is observed in the Estonian case: despite successful digital initiatives (such as X-Road or KSI Blockchain), their effectiveness is ensured by a well-thought-out national strategy [48, 49].

However, studying has several limitations. Firstly, access to sensitive information in the security sector is limited, which has affected the completeness of the analysis. Additionally, the specifics of the cases are different. Each case combined political, economic, and military aspects, making a complete comparison difficult. For example, the Estonian strategy is systematic, while the Ukrainian one is fragmented due to the war and resource limitations. As a result, some findings may be local in nature and not representative of broader regional trends.

Before cross-comparisons and maturity assessments, the data revealed a pronounced temporal dimension to the digital security transformation. The pace and trajectory of digitalization vary across the cases analyzed and are strongly dependent on critical security shocks, persistent threat exposure, and institutional learning capacity.

5. CONCLUSIONS

The current level of digitalization, the use of deep innovations, and AI systems have significantly transformed existing approaches to ensuring national security. The experiences of the proposed cases from Ukraine, the United States, Israel, and Estonia demonstrated how technology can play a leading role in both strategic planning processes and at the tactical level of combat operations. A noticeable positive effect of digitalization has been demonstrated in areas such as intelligence, Big Data analysis, troop management, logistical movement, and cyber defense against hacker attacks.

First and foremost, the introduction of AI systems into military management allows for a reduction in decision-making time (sometimes even by 50%); an increase in threat detection accuracy (up to 80%); the automation of intelligence gathering; and a flexible response to hybrid and asymmetric challenges. Further attention is needed for the process of training highly qualified personnel; adapting management structures; and the legal justification of the problems of autonomous use of force. The analysis of specific cases showed that Ukraine has a high efficiency in adapting open technologies under wartime conditions (Morana, Delta), but there is a problem with ensuring and fragmenting IT systems.

Based on the results obtained, the most relevant recommendations for Ukraine are to further increase investments in training and preparing personnel in the fields of AI, machine learning, and cybersecurity. This process will require the development of an appropriate strategy. There is a need to further strengthen public-private cooperation in the

field of autonomous weapons development, and to deepen cooperation with NATO and EU partners. It is recommended to create state programs that stimulate the introduction of innovative technologies in the defense sector.

In times of war and existential threats, societies tend to unite around issues of defense. The technological modernization of the armed forces and the security system emerge as a crucial factor of national mobilization and cohesion.

The conducted study on digitalization and the introduction of innovations in the sphere of national security demonstrates that technological modernization of the defense sector constitutes an essential condition for national consolidation. The Ukrainian experience has confirmed the capacity of society to mobilize resources for the implementation of advanced technologies in the military domain, which has had a direct impact on the level of moral and political cohesion during the full-scale invasion.

Thus, national consolidation is driven not only by political or cultural factors, but also by the technological modernization of the security sector, which becomes both a condition for survival and a catalyst for the further development of the state.

To ensure transparency and reliability in the use of AI technologies in the defense sector, future research should focus on developing comprehensive performance assessment models. Such models should combine quantitative performance indicators (accuracy, completeness, response time) with qualitative criteria, including compliance with ethical standards, ease of implementation in operational processes, and resistance to hostile influences.

REFERENCES

[1] Osimen, G.U., Fulani, O.M., Chidozie, F., Dada, D.O. (2024). The weaponisation of artificial intelligence in modern warfare: Implications for global peace and security. Research Journal in Advanced Humanities, 5(3). https://doi.org/10.58256/g2p9tf63

[2] Gumenyuk, T., Frotveit, M., Bondar, I., Horban, Y., Karakoz, O. (2021). Cultural diplomacy in modern international relations: The influence of digitalization. Journal of Theoretical and Applied Information Technology, 99(7): 1549-1560. https://www.jatit.org/volumes/Vol99No7/7Vol99No7.pdf

[3] Alam, M., Askari, M.U. (2025). Artificial intelligence and national security policy of China: A realist constructivist perspective. Social Science Reviews Archive, 3(1): 2303-2329. https://doi.org/10.70670/sra.v3i1.541

[4] Moggridge, E., Montasari, R. (2022). A critical analysis of the dark web challenges to digital policing. In Artificial Intelligence and National Security, pp. 157-167. https://doi.org/10.1007/978-3-031-06709-9_8

[5] Kanellopoulos, A.N. (2024). Counterintelligence, artificial intelligence and national security: Synergy and challenges. Journal of Politics and Ethics in New Technologies and AI, 3(1): e35617. https://doi.org/10.12681/jpentai.35617

[6] Benzie, A., Montasari, R. (2023). Bias, privacy and mistrust: Considering the ethical challenges of artificial intelligence. In Applications for Artificial Intelligence and Digital Forensics in National Security. Advanced Sciences and Technologies for Security Applications, pp. 1-14. https://doi.org/10.1007/978-3-031-40118-3_1

[7] Khan, A., Imam, I., Azam, A. (2021). Role of artificial intelligence in defence strategy: Implications for global and national security. Strategic Studies, 41(1): 19-40. https://doi.org/10.53532/ss.041.01.0058

[8] Gryshchenko, I.M., Denysova, A.V., Ovsiannikova, O.O., Buha, H.S., Kiselyova, E.I. (2021). Means for control over the activities of public authorities by civic democratic institutions: The conceptual framework analysis. Cuestiones Políticas, 39(69): 796-813. https://doi.org/10.46398/cuestpol.3969.49

[9] Yuryk, O., Holomb, L., Konovalova, L., Vivsyannuk, V., Tsekhmister, Y. (2023). Assessment of the impact of artificial intelligence technologies on the development of Ukrainian medicine in war conditions. International Journal of Chemical and Biochemical Sciences, 24(5): 206-211. https://www.iscientific.org/wp-content/uploads/2023/11/26-ijcbs-23-24-5-26-done.pdf.

[10] Pătrașcu, P. (2021). Emerging technologies and national security: The impact of IoT in critical infrastructures protection and defence sector. Land Forces Academy Review, 26(4): 423-429. https://doi.org/10.2478/raft-2021-0055

[11] Pyati, S.M. (2024). Artificial intelligence (AI) and its threats on human society. Research & Reviews in Biotechnology & Biosciences, 11(2): 1-6. https://doi.org/10.5281/zenodo.14605855

[12] Kalodanis, K., Rizomiliotis, P., Anagnostopoulos, D. (2024). European artificial intelligence act: An AI security approach. Information and Computer Security, 32(3): 265-281. https://doi.org/10.1108/ics-10-2022-0165

[13] Digital Watch Observatory. (2021). National strategy for the development of AI in Ukraine for 2021-2030. https://dig.watch/resource/national-strategy-for-the-development-of-ai-in-ukraine-for-2021-2030.

[14] Fedorov, M. (2023). Ukraine's AI road map seeks to balance innovation and security. Atlantic Council. https://www.atlanticcouncil.org/blogs/ukrainealert/ukraines-ai-road-map-seeks-to-balance-innovation-and-security/.

[15] On the basic principles of cybersecurity in Ukraine. (2017). https://zakon.rada.gov.ua/laws/show/en/2163-19#Text.

[16] Johnson, E.B. (2020). National artificial intelligence initiative act of 2020. https://www.congress.gov/bill/116th-congress/house-bill/6216.

[17] Ministry of Innovation, Science and Technology. (2023). Israel's policy on artificial intelligence regulation and ethics. https://www.gov.il/en/pages/ai_2023.

[18] Riigi Teataja. (2022). Cybersecurity act. https://www.riigiteataja.ee/en/eli/ee/526082022002/consolide/current.

[19] Verordnung über den Aufstieg in den höheren nichttechnischen Verwaltungsdienst über den Masterstudiengang "Intelligence and Security Studies" (MISSAufstV). (2019). https://www.gesetze-im-internet.de/missaufstv/BJNR020200019.html.

[20] Malmio I. (2023). Ethics as an enabler and a constraint – Narratives on technology development and artificial intelligence in military affairs through the case of Project Maven. Technology in Society, 72: 102193. https://doi.org/10.1016/j.techsoc.2022.102193

[21] Sukmono, F.G., Lestari, N.D., Rahman, S.H.A., Ahmad, M.B. (2024). Digital transformation strategy in advertising: A study bibliometric analysis. Komunikator, 16(2): 220-234. https://doi.org/10.18196/jkm.24563
[22] Kormych, L., Krasnopolska, T., Zavhorodnia, Y. (2024). Digital transformation and national security ensuring. Evropsky Politicky a Pravni Diskurz, 11(1): 29-37. https://doi.org/10.46340/eppd.2024.11.1.4
[23] Jaber, A., Fritsch, L. (2022). Towards AI-powered cybersecurity attack modeling with simulation tools: Review of attack simulators. In Advances on P2P, Parallel, Grid, Cloud and Internet Computing, pp. 249-257. https://doi.org/10.1007/978-3-031-19945-5_25
[24] Ministry of Defence of Ukraine. The DELTA combat system has been deployed across all levels of Defence Forces of Ukraine. https://mod.gov.ua/en/news/the-delta-combat-system-has-been-deployed-across-all-levels-of-defence-forces-of-ukraine.
[25] Goncharuk, V. (2024). Survival of the Smartest? Defense AI in Ukraine. DAIO Study 24/22. https://defenseai.eu/wp-content/uploads/2024/02/daio_study2422_survival_of_the_smartest_vitaliy_goncharuk.pdf.
[26] NATO Cooperative Cyber Defence Centre of Excellence. (2024). World's most advanced cyber defence exercise kicks off in Tallinn. https://ccdcoe.org/news/2024/worlds-most-advanced-cyber-defence-exercise-kicks-off-in-tallinn/?utm_source=chatgpt.com.
[27] Ukraine participates in NATO cybersecurity exercise in Estonia. https://english.nv.ua/nation/ukraine-participates-in-nato-cybersecurity-exercise-in-estonia-50413017.html?utm_source=chatgpt.com.
[28] Das, R., Sandhane, R. (2021). Artificial intelligence in cyber security. Journal of Physics: Conference Series, 1964(4): 042072. https://doi.org/10.1088/1742-6596/1964/4/042072
[29] Soare, S.R. (2020). Politics in the machine: The political context of emerging technologies, national security, and great power competition. In Emerging Technologies and International Security, pp. 103-122. https://doi.org/10.4324/9780367808846-9
[30] Benouachane, H. (2024). Cyber security challenges in the era of artificial intelligence and autonomous weapons. In Cyber Security in the Age of Artificial Intelligence and Autonomous Weapons, pp. 24-42. https://doi.org/10.1201/9781003441700-3
[31] Nanni, R., Bizzaro, P.G., Napolitano, M. (2024). The false promise of individual digital sovereignty in Europe: Comparing artificial intelligence and data regulations in China and the European Union. Policy & Internet, 16(4): 711-726. https://doi.org/10.1002/poi3.424
[32] Fatima, S., Desouza, K.C., Dawson, G.S. (2020). National strategic artificial intelligence plans: A multi-dimensional analysis. Economic Analysis and Policy, 67: 178-194. https://doi.org/10.1016/j.eap.2020.07.008
[33] Baltezarević, R. (2023). Impact of artificial intelligence on the global economy. Megatrend Review, 20(3): 13-24. https://doi.org/10.5937/megrev2303013b
[34] Dunleavy, P., Margetts, H. (2025). Data science, artificial intelligence and the third wave of digital era governance. Public Policy and Administration, 40(2): 185-214. https://doi.org/10.1177/09520767231198737
[35] Sharma, A., Garg, K.D. (2024). Cybersecurity challenges, trends, and future directions for smart agriculture. In Intelligent Security Solutions for Cyber-Physical Systems, pp. 246-265. https://doi.org/10.1201/9781003406105-21
[36] Khudov, H., Kostianets, O., Kovalenko, O., Maslenko, O., Solomonenko, Y. (2023). Using Software-Defined radio receivers for determining the coordinates of low-visible aerial objects. Eastern-European Journal of Enterprise Technologies, 4(9 (124)): 61-73. https://doi.org/10.15587/1729-4061.2023.286466
[37] Borchert, H., Schütz, T., Verbovszky, J. (2024). Master and servant: Defense AI in Germany. In The Very Long Game. Contributions to Security and Defence Studies, pp. 195-216. https://doi.org/10.1007/978-3-031-58649-1_9
[38] Reveron, D.S., Mahoney-Norris, K.A. (2018). Information security. In Human and National Security, pp. 181-201. https://doi.org/10.4324/9780429503726-9
[39] Reinhold, T. (2022). Arms control for artificial intelligence. In Armament, Arms Control and Artificial Intelligence. Studies in Peace and Security, pp. 211-226. https://doi.org/10.1007/978-3-031-11043-6_15
[40] Taddeo, M. (2025). Ethical principles for AI in defence. In The Ethics of Artificial Intelligence in Defence, pp. 29-70. https://doi.org/10.1093/oso/9780197745441.003.0002
[41] Bondarenko, S., Bratko, A., Antonov, V., Kolisnichenko, R., Hubanov, O., Mysyk, A. (2022). Improving the state system of strategic planning of national security in the context of informatization of society. Journal of Information Technology Management, 14: 1-24. https://doi.org/10.22059/jitm.2022.88861
[42] Murzagaliev, E.C. (2024). Definition of the concept of a transnational tax crime for ensuring national security and international cooperation in the Eurasian legal space. International Tax Studies, 7(5). https://ssrn.com/abstract=5233520.
[43] Danilyan, O., Dzeban, O., Sepúlveda, J.M., Kalyovskyi, Y., Andrushchenko, O. (2024). Protection of human rights in Ukraine under martial law. Revista Notas Históricas y Geográficas, (33): 464-487.
[44] Danilyan, O., Kalynovskyi, Y.Y., Dzoban, O., Kalynovskyi, Y., Saltanov, M. (2023). Value aspects of the safe existence of social systems in an unstable world. Cogito - Multidisciplinary Research Journal, 2023(4): 60-78. https://www.ceeol.com/search/article-detail?id=1335331.
[45] Hapieieva, O., Martynenko, V., Romanovska, Y., Chyrva, H., Potapiuk, I. (2022). Theoretical and methodological aspects of strategic management of economic security of the state in the conditions of the COVID-19 pandemic: Current problems and vectors of development. Financial and Credit Activity: Problems of Theory and Practice, 1(42): 529-536. https://doi.org/10.55643/fcaptp.1.42.2022.3753
[46] Svoboda, I., Shevchuk, M., Shamsutdinov, O., Lysianskyi, P., Voluiko, O. (2023). Identification of new threats to the national security of the state. Cuestiones Políticas, 41(78): 326-344. https://doi.org/10.46398/cuestpol.4178.23
[47] Suhaimi, S., Ibrahim, N.S., Mohd Zainol, N.A. (2025). The role of youth in strengthening national defense management: Challenges and opportunities in Malaysia.

International Journal of Politics, Public Policy and Social Work, 7(16): 18-26. https://doi.org/10.35631/ijppsw.716002

[48] Lonardo, L. (2021). Power to the people. How open technological innovation is arming tomorrow's terrorists. Terrorism and Political Violence, 33(8): 1820-1821. https://doi.org/10.1080/09546553.2021.2000223

[49] Khudov, H., Baranik, O., Kovalenko, O.V., Yakovenko, Y., Chahan, Y.A. (2022). The information technology for determining vehicle route based on ant colony algorithms. International Journal Emerging Technology and Advanced Engineering, 12(12): 117-128. https://doi.org/10.46338/ijetae1222_13