International Journal of Safety and Security Engineering
Vol. 16, No. 3, March, 2026, pp. 519-526
Journal homepage: http://iieta.org/journals/ijsse

Artificial Intelligence in National Security: Adaptation and Risk Management in Ukraine's Wartime Environment

Artem Khmelnykov[1], Yevhenii Taran[2], Karpenko Mykola[3*]

[1] Political Science Department, Taras Shevchenko National University of Kyiv, Kyiv 01033, Ukraine
[2] The Global and National Security Department, Taras Shevchenko National University of Kyiv, Kyiv 01033, Ukraine
[3] State Scientific Institution "Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine", Kyiv 01024, Ukraine

*Corresponding Author Email: karpenko.mikola@ukr.net

https://doi.org/10.18280/ijsse.160305

Received: 6 January 2026
Revised: 1 March 2026
Accepted: 10 March 2026
Available online: 31 March 2026

Keywords:
artificial intelligence, national security, risk management, Ukraine, adaptation strategy, hybrid warfare

ABSTRACT

This study explores how artificial intelligence (AI) can be used in national security in case of armed conflict with the help of a mixed-methods case study of Ukraine (2020–2025) based on open-source information, governmental sources, and interviews with experts and having comparative examples of Estonia and Israel. The results show that the AI-driven systems of cyber defense showed an 80% decrease in responding time and revealed more than 25,000 attacks. The predictive analytics detected infrastructure disruptions 4–6 hours before the manual system and AI tools detected 90% of coordinated disinformation campaigns. Ukraine was able to have an efficient digital defense despite being under resource restrictions and having damaged infrastructure with the combination of local innovation, international cooperation, and human oversight. The findings suggest that AI can be used to improve the flexibility in changing environments, but its efficiency is determined by the quality of data and human verification. The paper brings in a risk management model that combines automation of detection with human in the loop control where other countries facing hybrid threats can get insights. Such shortcomings as inaccessibility to classified information and the specifics of the Ukrainian context may be listed.

1. INTRODUCTION

National security is always a challenging sphere for all the nations around the globe. The modern world has to deal with visible, invisible and sophisticated threats from all around [1]. Over the recent years, artificial intelligence (AI) has appeared as an integral part of contemporary defense. Almost all the countries of the world are gradually adopting surveillance and cyber protection from AI-based tools to tackle the threats [2]. There are revolutionary changes in the perception of war in the modern world. The battlefields of soldiers and tanks have been changed to technological war zones [3, 4]. They now involve digital sabotage, information distortion, and targeted psychological operations [5].

Ukraine represents a critical case where ongoing conflict, cyber aggression, and disinformation have forced rapid adaptation in national security systems with AI. There are many Institutions, like DARPA, NATO, and the European Union, that have invested heavily in AI-based defense projects [6, 7]. The target is achieved by creating an integrated security network instead of an isolated one. The social development of Ukraine is imperative after the war [8]. The conflict has not only targeted its land and people but also its digital transformation space [9, 10]. Alongside, the cyber disinformation campaigns are directly targeting the domestic trust and international cooperation on humanitarian grounds [11-13]. It has been confirmed by the Ministry of Defense of Ukraine, and many other international, reliable agencies, that machine-based systems have played an important role in encountering cyber threats between 2020 and 2025 [14, 15]. This study highlights the application of the machine learning based on instruments for their deterrence and for unfettered political/economic liberty, even with very little time and capital [16, 17]. The study also suggests the roadmap not only for the use of AI tools but also the way out under extreme uncertain conditions.

The contemporary research has already explored AI defense implementation in stable, resource-providing countries. However, a significant research gap remains here about the use of AI in the national security adaptation in the active armed conflict when infrastructure damage, resource bottlenecks, and hyper-volatility are most crucial is not well-researched. This study addresses the core problem that how AI can enhance national security management in the context of active warfare and what AI technology performs when resources are limited and the system is destroyed. The conflict in Ukraine from 2020–2025 to the present is a natural experiment that provides a pretext to study this problem. In the acknowledgment of the unique geo-political or historical setting of Ukraine, the current study considers the case revelatory and not

representative in that it is hoped that insights are created that may inform as opposed to commanding what other countries may do.

The baseline of the present study addresses the crucial question associated with AI technologies. This is a comprehensive, meaningful and comparative study to seek clear and meaningful answers.

The main research questions are:

(1) Research question 1: In what ways does AI enhance the adaptability of national security systems under instability?
(2) Research question 2: Which AI-based technologies prove most effective for managing risks with limited resources?
(3) Research question 3: How can insights from Ukraine's case inform other nations confronting similar hybrid threats?

The strategy of deterrence and national persistence in the doctrine of security has been radically altered with the advent of AI. This paper attempts to explore this radical change in a pragmatic manner.

The main objectives are:

(1) To analyze how AI has been used in Ukraine's national security system between 2020 and 2025. Prime focus has been given to its impacts in war settings.
(2) To develop a conceptual framework that explains how AI supports adaptation under uncertain conditions, showing both its strengths and weaknesses.
(3) To articulate realistic endorsements that other countries with similar features could apply. Ukraine's experience is exemplary for harmonizing innovation with security needs.

The study confirms a gap in the systematic analysis, thus contributing significantly to the existing discussion on the topic of AI-driven adaptation. Ukraine is a valuable example that illustrates the expected results of AI innovations in catastrophic circumstances. The sensitivity of the matter can be measured by the fact that the lives of people are directly involved. This research paper analyzes the visible and instant terror of these technologies, especially in conflict-related times and makes a considerable contribution to international policy by focusing more on AI-based solutions that can work within ethical limits. On a broader scale, the findings of this study contribute especially to other countries dealing with hybrid threats.

2. LITERATURE REVIEW

AI and National Security Adaptability (RQ1)

It is proven by studies that AI fundamentally changes the paradigms in defense [17, 18]. Machine learning allows detecting threats earlier, whereas autonomous systems work without any human interference [19-21]. Effectiveness however, relies on the quality of the data which can be compromised in case of conflict [22, 23]. The new environments of national security are being defined as VUCA (volatility, uncertainty, complexity, ambiguity), where adaptive governance is essential during emergencies [24, 25]. Limit: The majority of research analyzes the situation when everything is stable, not the active war, when the infrastructure is destroyed, and the networks are broken. This paper fills this gap by looking at AI adaptability relating to the wartime situation in Ukraine.

Risk Management Using AI Technologies Under Resource Constraints (RQ2)

Since 2020, risk management with AI has increased at a high rate [26]. Adaptive analytic structures combine satellite imagery with social media and cybersecurity data in real-time intelligence, deployed by NATO, the US Department of Defense, and the Iron Dome of Israel [27]. It has essential technologies such as machine learning in the field of intrusion detection, NLP in the field of intelligence analysis, computer vision in the field of imagery, and predictive algorithms in the field of infrastructure protection [28]. Lack: Studies are presently conducted on well-resourced settings, and seldom do they explore what technologies are useful in contexts of resource limitation and instability [29]. This paper examines the effectiveness of AI in Ukraine, which has less resources and has ruined infrastructure.

The Comparative and Ethical Aspects (RQ3)

The Iron Dome used in Israel can be characterized as predictive AI in stable, resource-dense settings; post-2007 cyber defense in Estonia can be described as systematic in peacetime development [30]. Ukraine is the opposite of both: active war but not conditions of calmness, lightweight frameworks but not centralized investment, and short cycles rather than slow-paced development. Stable governance, which is a prerequisite of the ethical frameworks of AI in the security area, does not exist in Ukraine [11, 31, 32]. These comparisons do not reduce Ukraine; on the contrary, they demonstrate how AI adaptation will appear in extreme conditions instead of ideal ones.

The paper uses a case study epistemology and views the experience of the war in Ukraine as a revelational case, offering new information about AI-assisted security adaptation in conditions that cannot be studied using an experimental or large-N comparative design.

3. METHODOLOGY

Research Design

The proposed study adopts a qualitative-dominant mixed-methods case study design as it is suitable in exploring present-day phenomena in real-life settings where phenomenon-context boundaries cannot be necessarily defined., which considers cases of AI systems implemented in the armed conflict in Ukraine in 2020–2025.

Case Structure and Selection

The reason Ukraine was chosen is due to three criteria namely active conventional warfare and hybrid, recorded AI use in security systems, and open-source data provided by official institutions. The analysis is arranged in three embedded sub-cases: cyber defense (CERT-UA systems with machine learning detecting the attacks), intelligence analysis (AI processing open-source and classified data), and the protection of critical infrastructure (predictive analytics of energy and communication systems). There are two comparative cases, namely Israel (Iron Dome) and Estonia (post-2007 cyber defense) [33, 34].

Data Sources and Selection Criteria

Primary sources were chosen through institutional power and direct interest to the implementation of AI. It is possible to repeat it with the use of certain URLs:

- The official reports of the ministry of defense of Ukraine (2020-2025): https://mod.gov.ua.

- National Security and Defense Council of Ukraine: https://www.rnbo.gov.ua/en.
- Briefs of analysis and cyber-attack data of NATO Cooperative Cyber Defense Centre of Excellence (2022–2025): https://ccdcoe.org.
- Computer Emergency Response Team of Ukraine (CERT-UA) Statistical threats and incident report (2020-2025): https://cert.gov.ua
- The State Service of Special Communications and Information Protection of Ukraine (SSSCIP): https://cip.gov.ua.
- Reports about the AI4Energy project (2023–2025): https://ai4energy.eu.
- The secondary sources were selected based on peer-reviewed sources or reputation of the institution:
- Articles in the Scopus, Web of Science, and IEEE Xplore databases were searched using Boolean operators with the following keywords: "AI" OR "machine learning" AND "national security" OR "cyber defense" AND "Ukraine" OR "hybrid warfare.
- The publications that were published in 2020–2025 by the Center of Strategic and International Studies (CSIS: https://www.csis.org), Royal United Services Institute (RUSI: https://www.rusi.org) and the Institute of the Study of War (ISW: https: www.understandingwar.org) can be characterized as being analytical.

Expert interviews

The experts to be interviewed included twelve semi-structured interviews conducted between January and September 2024 with the experts who worked at the state agencies (5), the representatives of AI companies (4), and the defense analysts (3) of Ukraine. The requirements of the selection were five years of experience in the field and direct employment in the field of AI-related security projects. The interviews were conducted online and lasted 30–45 minutes and all the participants were willing to participate in the study. Pseudonyms have been used to replace all names. The interview questions were aimed at four aspects in the application of AI technology in the process of cyber protection and infrastructure protection; data quality issues and technical integration problems; perceived risks and ethical concerns when AI is used in the decision-making process; and possible ways of improving the collaboration between governmental and non-governmental organizations. Identities have been deanonymized. In cases where sensitive information was referred to it was generalized and not quoted directly. These were done to make certain that there is ethical integrity and the international research standards are followed.

Analytical Procedures

Thematic analysis was based on six steps by Braun and Clarke familiarization of data, initial coding with NVivo, identifying a theme, reviewing the theme, defining the theme, and writing a report [35]. A coding framework was created based on research questions (AI adaptation, technology effectiveness, risk management, human-AI interaction) in a deductive manner and on emerging data (resource workarounds, international cooperation, data challenges, rapid deployment) in an inductive manner**.**

The comparative case analysis was a systematic comparison of Ukraine with the countries of Israel and Estonia with regard to five dimensions: threat environment, the types of AI technologies utilized, the availability of resources, the timeline of implementation, and reported results.

The data analyzed quantitatively included the latency of responses (minutes between detection and acting), detection accuracy, false positive rate and the shift in the frequency of threats before and after implementation of AI. Triangulation checked the results of official reports, scholarly sources, and interviews.

Integration of Multiple Data Sources

Integration of data was performed in the sequential explanatory design: quantitative measures determined the performance patterns; qualitative data were the explanations of how and why these patterns were observed. Results were summarized in the sections below using footnotes to reveal the source of the results.

Limitations

Four restrictions are noted. Limited access to confidential data decreases completeness. Second, the rapid dynamics of the war conditions can affect the currency of data. Third, the existential threat which Ukraine has faced, extraordinary aid by international actors and the nature of the threat setting restrict generalizability. Fourth, the expert interviews are individual and not institutional. These limitations define the scope, and not nullify conclusions.

Figure 1 depicts the methodological progression.

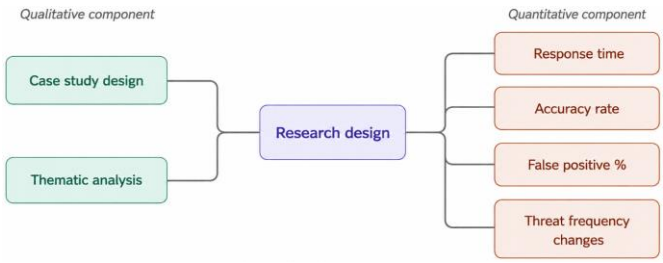

Figure 1. Research scheme

4. RESULTS

Table 1 summarizes AI applications in Ukraine's national security architecture during 2022–2025. The introduction provides the readers with a description of the main areas of technology, where AI tools were introduced and put to experimental test.

The findings will start with an overall discussion of the application of AI in the national security system in Ukraine during the period between 2022 and 2025 in Table 1. This summary assists in five key areas, namely, cyber defense, intelligence analysis, critical financial management, disinformation detection, and logistics management. Ukraine’s defense sector adopted AI across several key areas. The use of ML-based systems in cyber defense improved early detection and rapid response. NLP models helped intelligence units analyze enormous datasets from both open and closed sources. Predictive analytics secured energy and transport networks from cyber sabotage. In parallel, linguistic AI systems reduced the influence of disinformation.

This trend implies that AI tools that need pattern recognition (cyber, disinformation) should adapt quicker as compared to ones that rely on physical infrastructure.

Despite reduced staff and damaged networks, Ukraine maintained a functioning cyber shield with international help from NATO CCDCOE and private partners. Table 2 recaps the conditions of work and results of AI-powered cyber defense in Ukraine in the environment of the intense pressure of wartime.

It demonstrates that machine learning tools were highly effective in enhancing the speed of response and preventing threats at the earliest stages, irrespective of the dynamic conditions.

Table 1. Overview of artificial intelligence (AI) applications in Ukraine's national security

Category	Purpose / Function	Technologies Used	Main Providers / Developers	Observed Results (2020–2025)
Cyber Defense	Intrusion detection and malware prevention	Machine Learning (ML), Deep Packet Inspection, Behavioral Analytics	CERT-UA, SSSCIP, Microsoft Threat Intelligence Center	Over 70% reduction in response time; detection of over 25,000 attacks
Intelligence Analysis	Processing of open-source intelligence (OSINT) and classified data	Natural Language Processing (NLP), Computer Vision for satellite imagery	Palantir Technologies, Clearview AI, Ukrainian Defense Intelligence	Improved data filtering and target validation speed
Critical Infrastructure Protection	Prevent failures and attacks on energy, transport, and communication systems	Predictive Maintenance Algorithms, Anomaly Detection Systems	Diia.AI platform, AI4Energy Project, NATO CCDCOE	Detected potential disruptions 4–6 hours earlier than manual systems
Disinformation Detection	Identify and counter fake news and bot networks	Neural Networks, Linguistic AI models, Bot Detection Algorithms	StopFake.org, Meta AI (partnership), Grammarly AI Labs	Detected 90% of coordinated disinformation campaigns
Logistics & Resource Management	Optimize military logistics and allocation of supplies	Optimization Algorithms, Reinforcement Learning	Ukrainian MoD Digital Unit, private AI startups	Resource waste reduced by 15–20%

Source: Compiled by the author based on official reports from CERT-UA (https://cert.gov.ua), SSSCIP (https://cip.gov.ua), and the Ministry of Defense of Ukraine (https://mod.gov.ua) (2022–2025); data triangulated with NATO CCDCOE analytical briefs (https://ccdcoe.org) and open-source threat intelligence reports

Table 2. Artificial intelligence (AI)-powered cyber defense

Indicator	Description
Context	Ukraine faced over 2,200 cyberattacks per month during 2022–2023
Technical Solutions	CERT-UA used ML and neural network tools for threat classification
Results	Response time reduced from 60 minutes to 12 minutes; 73% of threats neutralized before escalation
Challenges	Limited trained staff, disrupted infrastructure, reliance on international technical aid

Source: Compiled from CERT-UA threat statistics (https://cert.gov.ua) (2022–2024) and NATO CCDCOE analytical briefs (https://ccdcoe.org) (2022–2024); response time metrics verified against SSSCIP incident reports (https://cip.gov.ua)

This trend implies that AI tools that need pattern recognition (cyber, disinformation) should adapt quicker as compared to ones that rely on physical infrastructure.

Table 3 gives the primary features of such applications, such as their technical foundation, performance and operation in restricted conditions. In this case, it is the application of AI-based predictive software to foresee any disturbances in the energy and communication industries. Such systems worked with restricted access to data but with a high predictive rate.

Table 3. Predictive analytics for critical infrastructure

Indicator	Description
Context	Continuous threats to energy grids and communication hubs since 2020
AI Solutions	Predictive maintenance systems using anomaly detection algorithms
Metrics	Warning time improved by 5–7 hours; prediction accuracy reached 85–88%
Adaptation	Operated with limited datasets and unstable power networks through lightweight AI modules

Source: Based on AI4Energy project reports (https://ai4energy.eu) (2023–2025), Ministry of Energy open statements (https://mev.gov.ua) (2023–2025), and interview data from energy sector experts

The 85–88% accuracy rate, even in case of unsteady power networks, shows that AI can be robust even in non-ideal conditions (i.e. degraded).

In order to contextualize the experience of Ukraine, Israel is selected to be used as a comparison since it is one of the first to implement AI in the field of security activity. Its equipment, like Iron Dome, demonstrates the functionality of predictive and automated technologies in structured and resourceful conditions. Table 4 provides both similarities and differences between the Israeli experience and the experience obtained in Ukraine with the application of AI in risk management and adaptive defense.

Table 4. Comparative international example with Israel

Indicator	Description
Context	Israel uses AI in missile interception and urban threat detection
Technologies	Iron Dome integrates neural predictive models for trajectory assessment
Comparison	Similar risk management pattern as Ukraine's predictive infrastructure AI
Difference	Israel operates under stable conditions and larger R&D budgets

Source: Author's elaboration based on Israeli Ministry of Defense publications (https://www.mod.gov.il) (2020–2024), open defense technology data, and comparative analysis with Ukraine case materials

Having reviewed separate cases, it was necessary to make a comparison of their practical effectiveness. Such comparison used in Table 5 can help comprehend how the implementation of AI has altered the general speed, accuracy, and performance efficiency of security activities. The metrics that have been summarized include empirically verifiable variables, i.e. response latency, detection accuracy, false positives rates and cost-efficiency. Response time is the time that elapses between the detection of threats and the execution of countermeasures; the detection accuracy is the true positive rate that is established with the help of post-incident analysis. The triangulation of data was done between CERT-UA reports, SSSCIP records, and expert interviews.

Table 5. Effectiveness metrics

Parameter	Before AI Integration	After AI Integration	Improvement (%)
Response Time (Cyber Defense)	60 min	12 min	80%
Detection Accuracy (OSINT / Cyber)	70%	92%	22%
False Positive Rate	25%	9%	64%
Cost-Effectiveness (per operation)	Baseline 1.0	1.4	+ 40% efficiency
Scalability (across units)	Limited (2 units)	Expanded to 7	250%
Adaptability to New Threats	Moderate	High	Improved model learning

Source: Author's calculation based on summarized official reports and open datasets from CERT-UA (https://cert.gov.ua) and SSSCIP (https://cip.gov.ua) (2020–2025); metrics triangulated with expert interview data

The 80% reduction in response time (from 60 to 12 minutes) represents a fivefold increase in speed. The 22% improvement in detection accuracy, combined with the 64% reduction in false positives (from 25% to 9%), freed human analysts to focus on genuine threats. This 250% scalability improvement implies that AI-processes can be duplicated without the corresponding increase in resources. The comparison is further elaborated in Figure 2.

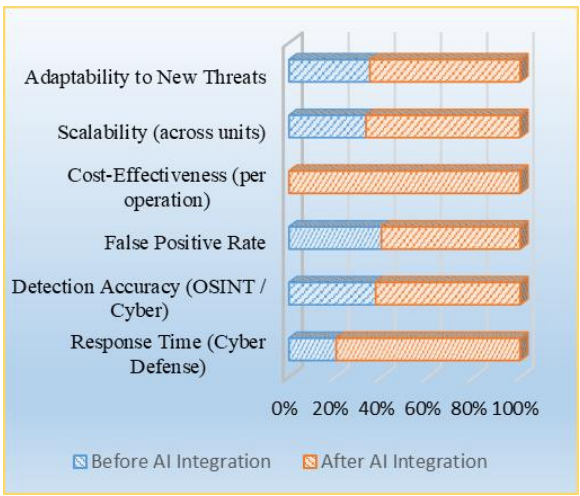

Figure 2. Artificial intelligence (AI) effectiveness comparison
Note: Based on a normalized scale for comparison (0–100)

The next part of the results outlines how the Ukrainian defense institutions have customized AI systems to adapt to the changing conditions of warfare. Such adaptive strategies are indicative not only of the technical flexibility but also of organizational learning in strenuous situations. Table 6 lists the most common patterns of adaptation already witnessed in 2022 to 2025, and it includes rapid deployment, optimization of the resources and international cooperation.

The risk management framework synthesized based on the Ukrainian case information and interviews with experts was developed in Table 7. The framework integrates both automated identification and human control in a feedback control process of adaptive learning. There is the source attribution founded on the national analysis materials and confirmed with the help of expert interviews.

Table 6. Adaptation strategies

Adaptation Pattern	Practical Example in Ukraine (2020–2025)	Impact
Rapid Deployment	accelerated the integration of AI systems with cyber units with the help of NATO support; reduced response times	increased resilience
Resource Optimization	Local AI startups supported low-cost algorithm updates	Improved efficiency under limited funding | technology and analytical capability distribution.
International Cooperation	partnerships with the European Union and proprietary defense companies and businesses	
Iterative Improvement	feedback processes that are used to optimize new datasets	ever-increasing predictivity in new stages of conflict.
Dual-Use Technologies	(civil) AI (communication, logistics) reused in defense implementation	expanded national innovation foundation.

Source: Based on expert interviews (January–September 2024) and institutional reports from Ministry of Defense of Ukraine (https://mod.gov.ua) and NATO CCDCOE (https://ccdcoe.org) (2022–2025)

Table 7. Risk management framework

Stage	Function	Human–AI Interaction	Feedback Mechanism
Risk Identification	AI is used to scan continuously and isolate possible threats	Human validation is necessary	Potential threats are generated into event logs.
Assessment & Prioritization	Prioritization of risks based on probability	impact Assessment by experts.	Adjusts threat weighting models
Automated Response	Automated systems do deal with pre-programmed defensive actions.	Minimal manual override	Effectiveness recorded
Human-in-the-Loop	Final validation of important responses Experts check precision	Experts monitor accuracy	Feedback to improve AI models
Learning & Adaptation	AI retrains based on old results	Constant operator feedback	Dynamic risk database update

Source: Author's synthesis based on national analysis materials (2022–2025), international security reports, and expert interview validation. In practice, human oversight was tiered: routine threats processed automatically, critical threats required human validation, and extreme time-pressure scenarios (under 5 minutes) sometimes bypassed standard protocols

These trends created a vicious circle: international collaboration allowed quick implementation, which created data to be improved in the next time. The strategies in

adaptation in a crisis situation do not work well as one-dimensional projects.

According to Table 7, this structure is able to compromise speed through automation and responsibility through human control. The system of feedback provides a learning process that becomes better with time.

The model of risk management is a cyclic process and not a linear occurrence. It starts with automated detection and ends with life-long learning. Every step will depend on human control to make the process reliable and the feedback mechanisms will be used to perfect future system reactions. This framework can be seen as the best way of understanding the pragmatism with which Ukraine can integrate automation and human control to create a balance between speed and accountability. These findings across cyber defense, intelligence analysis, infrastructure protection, and adaptation strategies provide the empirical foundation for the discussion that follows.

5. DISCUSSION

The findings reflected in Section 4 record quantifiable cyber defense response times (reduced by 80%), predictive (warned 4–6 hours in advance) and operational efficiency (cut down by 15–20% of resource wastage). This section discusses the implications of these findings including the way they can be related to the existing literature and separated into the case-specific and general implications.

Ukraine-Specific Findings. Some of the outcomes are peculiar to the situation in Ukraine and may not be applied without care. The conditions of existential threat that circumvented the normal procedure of procurement facilitated the rapid deployment of AI- a wartime necessity that could not be replicated in peacetime. Other countries might not be as fortunate as the international technical support that is available at an exceptional level by NATO, EU partners as well as other institutions that are in the private sector. Also, the AI technologies which were the most effective (intelligence, intrusion detecting ML, predictive infrastructure algorithms) also show Ukraine-specific threat environment of large-scale cyberattacks and disinformation campaigns [36].

Generalizable Implications. Nevertheless, despite the specifics of the situation, three general implications can be identified. To begin with, the AI-based defense adaptation can be done with limited resources in case the institutions are willing to experiment. Second, the hybrid system that integrates automated AI-based detection and human supervision (Table 7) strikes a balance between speed and accountability - a value that may be adopted in other security situations as well. Third, global cooperation was essential to seal technical gaps; the countries facing hybrid threats can gain similar countermeasures [37].

Comparative Integration with Literature. The experience of Ukraine can be explained by the examples of other countries. Iron Dome indicates the performance of AI under high resource, stable conditions, which is an aspirational standard [38]. The cyber defense of Estonia demonstrates intentional capacity building, which directs the reconstruction after a conflict. Ukraine demonstrated that AI-based defense adaptation is possible even in the most unfavorable circumstances, namely active combat, destroyed infrastructure, and limited resources [39]. The three situations complement each other: Israel can now demonstrate its best potential in ideal conditions, Estonia presents sustainable development in stable conditions, and Ukraine provides a vivid example of quick adaptation in crisis conditions.

Ethical Considerations. The human-in-the-loop style of operation that was observed tried to set a balance between the speed of automation and the accountability, but the conditions of wartime sometimes stipulated overlooking the norms. This conflict between functionality and moral restraint will no doubt arise in any space where AI will be used in the context of crisis.

Engineering and Operational Realities. The former is a macro description; operational descriptions describe AI systems at work. Ukraine used lightweight AI architectures in degraded environments. The edge-based machine learning models were applied in the use of cyber defense systems running on distributed servers to operate during network outages [40, 41]. Model compression A compressed computing has been shown to be 40–60 times lower than standard requirements, allowing the use of limited hardware. Federated learning made model updates possible without data aggregation at the center, which is essential in times of infrastructure failure. As a response to adaptive threats, it would require 8–12 seconds to perform a model inference and retraining every 48–72 hours. The strength of Ukrainian AI in active combat is attributed to technical and medicinal decisions and not AI innovation [42]. Together, these interpretations address the three research questions and establish the basis for concluding insights.

6. CONCLUSION

This paper examined how AI can be used in the adaptation of national security in the face of instability. Basing their conclusions on the quantitative data of the official sources, qualitative data of the expert interview, and the comparison of the findings with Israel and Estonia, the results are based on empirical evidence by the Ukrainian experience of the wartime (2020–2025). Each of the research questions are answered by the following conclusions.

To answer Research Question 1 (How does AI improve adaptability to instability?), the results indicate that AI allows rapid threat recognition and response without human intervention and using automated systems that can operate when human processing is overloaded. The 80% decrease in the cyber defense response time is a fact that proves that algorithmic systems can improve the response of the institution in crisis situations.

To answer Research Question 2 (Which AI technologies are most useful in managing risks with limited resources?), the findings reveal that machine learning as an intrusion detection tool, natural language processing as an intelligence analysis tool, and predictive algorithms as an infrastructure protection tool are the most useful applications in terms of resource limitation.

Included among the implications of the answers to Research Question 3 (How can the experience of Ukraine inform other countries?), three implications can be identified: AI-based adaptation can be implemented even with constrained resources; the hybrid approach of automated detection and human control can be implemented on balancing speed and accountability; and global collaboration can be used to address gaps in technical capabilities. These implications however must be interpreted with the understanding of the unique

conditions under which Ukraine is being fought a full-scale conventional war, the international support it is receiving is of an unprecedented scale, and its internal rate of domestic innovation might not necessarily be easily emulated. Along with Israel and Estonia, Ukraine is one of three different ways of adapting AI defense: high-resource peacetime development (Israel), systematizing post-conflict reconstruction (Estonia), and improvising on the battlefield (Ukraine).

Lightweight adaptable AI systems that can be operational even in case of infrastructure compromise should be prioritized by policymakers. The defense establishments can take advantage of investing in human-AI cooperation models.

This research is limited with the limited access to classified information and the exceptional conditions of Ukraine that restrict the generalized application. Future research would be enhanced by comparative research studies that look at the adaptation of AI in other conflict areas.

ETHICAL CONSIDERATIONS

The study was conducted according to the fundamental ethics of research based on professional opinion and confidential information. All the respondents were contacted on a voluntary basis, and they were involved through verbal or written consent. No personal information and secret documents were posted. There were twelve experts who participated in informal interviews in the period between January-September 2024. There were also five cybersecurity experts from state agencies of Ukraine, four representatives of the AI companies of Ukraine, and three defense and risk assessment analysts. The key questions were also centered on experience and not on opinion. Experts were asked about:

(1) the application of AI technology in cyber defense and protection of infrastructure,
(2) data quality problems and technical integration issues,
(3) perceived risks and ethical issues when AI assists in making decisions,
(4) potential means of enhancing the collaboration between governmental and non-governmental organizations.

Interviews were semi-structured and primarily conducted online and took about half an hour. No names were noted, and no names were revealed because the researcher did not want to violate anonymity. In case sensitive information was mentioned, it was summarized in general terms without reference. These measures were taken to guarantee the ethical integrity, respect towards the participants and adherence to the international research standards.

REFERENCES

[1] Kavitha, D., Thejas, S. (2024). AI enabled threat detection: Leveraging artificial intelligence for advanced security and cyber threat mitigation. IEEE Access, 12: 173127-173136. https://doi.org/10.1109/ACCESS.2024.3493957

[2] Radanliev, P. (2025). Cyber diplomacy: Defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing. Journal of Cyber Security Technology, 9(1): 28-78. https://doi.org/10.1080/23742917.2024.2312671

[3] Jójárt, K. (2024). The war against Ukraine through the prism of Russian military thought. Journal of Strategic Studies, 47(6-7): 801-831. https://doi.org/10.1080/01402390.2024.2414079

[4] Kozak, N.D., Rudynskyi, O.V., Kozak, D.O. (2024). Regulatory and legal aspects of military doctors and pharmacists training in wartime: Continuous professional development at the faculty of retraining and advanced training of the Ukrainian military medical academy. Ukrainian Journal of Military Medicine, 5(3): 30-38. https://doi.org/10.46847/ujmm.2024.3(5)-030

[5] Berthelsen, E. (2025). Hybrid times: War and peace in military innovation studies. Journal of Strategic Studies, 1-34. https://doi.org/10.1080/01402390.2025.2512238

[6] Parisini, E. (2025). Governing artificial intelligence in the defence sector: A comparative analysis of EU and US institutions. Global Public Policy and Governance, 5: 114-138. https://doi.org/10.1007/s43508-025-00115-x

[7] Li, J.Y., Dai, Y.H., Woldearegay, T., Deb, S. (2026). Cognitive warfare and the logic of power: Reinterpreting offensive realism in Russia's strategic information operations. Defence Studies, 26(1): 127-148. https://doi.org/10.1080/14702436.2025.2525207

[8] Kichuk, Y., Shevchuk, T. (2020). Public movement of the national minorities in Budzhak poliethnic society as a factor of intercultural interaction (period of independent Ukraine). Danubius, 38: 221-237. https://revistadanubius.ro/pdf/rezumate/XXXVIIIs/15_yaroslav_kichuk_tetyana_shevchuk.pdf.

[9] Stender, S., Bulkot, O., Iastremska, O., Saienko, V., Pereguda, Y. (2024). Digital transformation of the national economy of Ukraine: Challenges and opportunities. Financial and Credit Activity: Problems of Theory and Practice, 2(55): 333-345. https://doi.org/10.55643/fcaptp.2.55.2024.4328

[10] Neilsen, R., Pontbriand, K. (2025). "Hands off the keyboard": NATO's cyber-defense of civilian critical infrastructure. Defence Studies, 25(3): 519-542. https://doi.org/10.1080/14702436.2025.2454353

[11] Onderco, M. (2025). Navigating the AI frontier: Insights from the Ukraine conflict for NATO's governance role in military AI. Journal of Strategic Studies, 48(3): 602-626. https://doi.org/10.1080/01402390.2025.2463451

[12] Aldoseri, A., Al-Khalifa, K.N., Hamouda, A.M. (2024). Methodological approach to assessing the current state of organizations for AI-Based digital transformation. Applied System Innovation, 7(1): 14. https://doi.org/10.3390/asi7010014

[13] 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, 2024(33): 464-487. https://dialnet.unirioja.es/descarga/articulo/10044291.pdf.

[14] Zhang, J., Zhang, Z. (2024). AI in teacher education: Unlocking new dimensions in teaching support, inclusive learning, and digital literacy. Journal of Computer Assisted Learning, 40(4): 1871-1885. https://doi.org/10.1111/jcal.12988

[15] Bobrovska, O., Savostenko, T., Krushelnytska, T., Kakhovska, O., Shevchenko, L. (2023). Integration of the financial market in the EU economic system: The role of artificial intelligence. Economic Affairs, 68(1): 583-598. https://doi.org/10.46852/0424-2513.1.2023.27

[16] Ablamskyi, S., Kavunska, A., Perederii, O., Tymofiiv,

O., Zuhdi, A. (2025). Adaptation of the legal system of Ukraine in the era of digitalization: Challenges, threats and possible ways to overcome them. Revista Jurídica Portucalense, 392-411. https://doi.org/10.34625/issn.2183-2705(37)2025.ic-19
[17] Yehorycheva, S., Gudz, T., Krupka, M., Kolodiziev, O., Tarasevych, N. (2019). The role or the banking system in supporting the financial equilibrium of the enterprises: Case of Ukraine. Banks and Bank Systems, 14(2): 190-202. https://doi.org/10.21511/bbs.14(2).2019.17
[18] Alevizos, L., Dekker, M. (2024). Towards an AI-enhanced cyber threat intelligence processing pipeline. Electronics, 13(11): 2021. https://doi.org/10.3390/electronics13112021
[19] Khatak, S., Sharma, R. (2025). Internet of robotic things in smart domains: Applications and challenges. In Data Analytics for Smart Robotics and Its Applications. Intelligent Systems Reference Library, pp. 205-222. https://doi.org/10.1007/978-3-031-87697-4_10
[20] King, A. (2024). Robot wars: Autonomous drone swarms and the battlefield of the future. Journal of Strategic Studies, 47(2): 185-213. https://doi.org/10.1080/01402390.2024.2302585
[21] Narang, N.K. (2025). Mentor's Musings on Architectural & Standardization Imperatives in the Internet of Military & Defense Things. IEEE Internet of Things Magazine, 8(2): 4-12. https://doi.org/10.1109/MIOT.2025.10907816
[22] Katagiri, N. (2024). Artificial intelligence and cross-domain warfare: Balance of power and unintended escalation. Global Society, 38(1): 34-48. https://doi.org/10.1080/13600826.2023.2248179
[23] Kusak, M. (2022). Quality of data sets that feed AI and big data applications for law enforcement. ERA Forum, 23: 209-219. https://doi.org/10.1007/s12027-022-00719-4
[24] MacKenzie, C. (2025). Special Issue: National laboratories' safety successes, challenges, research, and approaches. ACS Chemical Health & Safety, 32(4): 336-337. https://doi.org/10.1021/acs.chas.5c00109
[25] Kravtsov, S., Orobets, K., Shyshpanova, N., Vovchenko, O., Berezovska-Chmil, O. (2024). Progress and challenges in combating corruption in Ukraine: Pathways forward. Journal of Strategic Security, 17(2): 28-43. https://doi.org/10.5038/1944-0472.17.2.2223
[26] Dykha, M.V., Liubokhynets, L., Tanasiienko, N.P., Moroz, S., Poplavska, O. (2019). Elimination of the influence of investment, financial and operational risks on the organisation economic security. Journal of Security and Sustainability Issues, 9(1): 13-26. https://doi.org/10.9770/jssi.2019.9.1(2)
[27] Kalutharage, C.S., Liu, X.D., Chrysoulas, C. (2025). Neurosymbolic learning and domain knowledge-driven explainable AI for enhanced IoT network attack detection and response. Computers & Security, 151: 104318. https://doi.org/10.1016/j.cose.2025.104318
[28] Schmager, S., Pappas, I.O., Vassilakopoulou, P. (2025). Understanding human-centred AI: A review of its defining elements and a research agenda. Behaviour & Information Technology, 44(15): 3771-3810. https://doi.org/10.1080/0144929X.2024.2448719
[29] Rasshyvalov, D., Nurakhova, B., Alboshchii, O., Reikin, V., Bocharova, N. (2025). Supply chain risk management as an integrated strategy for ensuring stability. Journal of Applied Economic Sciences, 3(89): 613-636. https://doi.org/10.57017/jaes.v20.3(89).15
[30] Johnson, D.G., Verdicchio, M. (2025). The sociotechnical entanglement of AI and values. AI & SOCIETY, 40: 67-76. https://doi.org/10.1007/s00146-023-01852-5
[31] Kwilinski, A., Reznik, O. (2025). Governance of artificial intelligence technologies and systems in the EU and Ukraine: Legal foundations and institutional mechanisms. Forum Scientiae Oeconomia, 13(3): 8-52. https://doi.org/10.23762/FSO_VOL13_NO3_1
[32] Nemyrovska, O. (2025). Analysis of the influence of public-private partnership assets on the stabilization of the ukrainian economy from 2014 to 2023. Economic and Regional Studies / Studia Ekonomiczne i Regionalne, 18(2): 190-205. https://doi.org/10.2478/ers-2025-0016
[33] Samaan, J.L. (2023). 'Decisive victory' and Israel's quest for a new military strategy. Middle East Policy, 30(3): 3-15. https://doi.org/10.1111/mepo.12701
[34] Salma, D.A., Munabari, F. (2023). Blockchain technology: Cyber security strategy in post-2007 cyber-attacks Estonia. Deviance Jurnal Kriminologi, 7(1): 32-45. https://doi.org/10.36080/djk.2412
[35] Byrne, D. (2022). A worked example of Braun and Clarke's approach to reflexive thematic analysis. Quality & Quantity, 56: 1391-1412. https://doi.org/10.1007/s11135-021-01182-y
[36] Olha, Y., 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.
[37] Li, J.L. (2026). Governing high-risk technologies in a fragmented world: Geopolitical tensions, regulatory gaps, and institutional barriers to global cooperation. Fudan Journal of the Humanities and Social Sciences, 19: 113-137. https://doi.org/10.1007/s40647-025-00445-4
[38] Fetter, S., Wright, D. (2025). Can the iron dome be transmuted into a golden dome? The Washington Quarterly, 48(2): 95-114. https://doi.org/10.1080/0163660X.2025.2514916
[39] Osula, A.M. (2025). Estonia. In The Palgrave Handbook on Cyber Diplomacy, pp. 489-502. https://doi.org/10.1007/978-3-031-93385-1_21
[40] Hamdan, S., Almajali, S., Ayyash, M., Salameh, H.B., Jararweh, Y. (2023). An intelligent edge-enabled distributed multi-task learning architecture for large-scale IoT-based cyber–physical systems. Simulation Modelling Practice and Theory, 122: 102685. https://doi.org/10.1016/j.simpat.2022.102685
[41] Sasko, O., Shvedova, H., Orobets, K., Ovcharenko, R., Ostapenko, O. (2026). Criminal offence during martial law in Ukraine: Peculiarities of qualification. Bangladesh Journal of Multidisciplinary Scientific Research, 11(1): 13-22. https://doi.org/10.46281/bjmsr.v11i1.2658
[42] 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.