Journal of Kryvyi Rih National University

Vol. 23, No. 2, 2025

ISSN 2306-5451
e-ISSN 2519-2736

Journal homepage: https://journal-knu.com.ua/en

Article's History: Received: 21.04.2025 Revised: 18.09.2025 Accepted: 24.12.2025 Published: 28.12.2025

UDC 355.48:004

DOI: 10.31721/2306-5451-2025-2-23-89-103

Information and analytical support for the management of threat risks during combat operations

Andrii Kovtun*

PhD in Technical Sciences, Senior Lecturer
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
03056, 37 Beresteiskyi Ave., Kyiv, Ukraine
https://orcid.org/0000-0003-4490-0484

Olena Zemlyanska

Senior Lecturer
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
03056, 37 Beresteiskyi Ave., Kyiv, Ukraine
https://orcid.org/0000-0002-9608-3677

Natalya Prakhovnik

PhD in Technical Sciences, Associate Professor
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
03056, 37 Beresteiskyi Ave., Kyiv, Ukraine
https://orcid.org/0000-0003-0821-2166

Oksana Ilchuk

PhD in Technical Sciences, Senior Lecturer
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
03056, 37 Beresteiskyi Ave., Kyiv, Ukraine
https://orcid.org/0000-0001-6352-5320

Abstract. The purpose of the study was to identify the features of constructing and applying analytical systems in the processes of assessing and minimising wartime risks. The methodology was based on structural-functional, comparative and system-analytical methods. It was established that the identification of threats during combat operations is based on the integration of multi-source data and covers four interrelated types of risks – physical, man-made, information and psychological. Physical risks are associated with the destruction of critical infrastructure, in particular during the defence of Kyiv in 2022 and shelling in the Gaza Strip in 2023; man-made consequences, such as the breach of the Kakhovka dam in 2023 and damage to the Zaporizhzhia Nuclear Power Plant, caused flooding of more than 600 km^2 and required round-the-clock monitoring by the International Atomic Energy Agency. In 2022-2024, more than 20,000 cyberattacks were recorded, and hybrid threats, combining physical, cyber and psychological impacts, destabilise the state and society. It was found that the key response instrument is an information and analytical system with a multi-level architecture for collecting, processing and visualising data, which uses Big Data, Machine Learning and predictive modelling to assess risks and support real-time decision-making. A comparison of Ukraine, Gaza, and Burundi showed different stages of development of an information and analytical system: in Ukraine, the system provides response within "hours to a

Suggested Citation:
Kovtun, A., Zemlyanska, O., Prakhovnik, N., & Ilchuk, O. (2025). Information and analytical support for the management of threat risks during combat operations. *Journal of Kryvyi Rih National University*, 23(2), 89-103. doi: 10.31721/2306-5451-2025-2-23-89-103.

*Corresponding author

day" and integrates data from various sources. In Gaza, the system has a humanitarian nature, updating daily data on more than 4,500 destroyed facilities; in Burundi, it uses an infrastructure resilience index with a lag of several days and weekly risk correction. The most effective is a hybrid model that combines international standards and national resources, ensuring rapid response and long-term resilience in post-conflict conditions. The practical significance lies in the possibility of using the results by state, analytical and humanitarian structures for faster response and infrastructure protection during combat operations

Keywords: physical destruction; predictive modelling; situational awareness; infrastructure resilience; cyberattacks; psychological impact; humanitarian analytics

Introduction

In the conditions of modern 21st-century hybrid conflicts and high-technology military operations, the information component of security becomes decisive. Armed conflicts are characterised not only by physical destruction, but also by a systemic struggle for data, analytics, and control over information flows. Under these conditions, the effectiveness of the state's response to wartime risks increasingly depends on the quality of information and analytical support for risk management, which encompasses the processes of data collection, processing, forecasting and decision-making. In particular, combat operations in Ukraine have demonstrated the need to create integrated risk-analysis systems capable of synchronising military, civilian and humanitarian approaches.

In academic discourse, the issues of information and analytical systems (IAS) for risk management are considered in the context of conflict forecasting, digital technologies, Artificial Intelligence (AI) and automated decision-making systems. The study by E.G. Rød *et al*. (2024) proved that conflict early-warning systems demonstrate the highest effectiveness when the systems combine quantitative indicators of violence (number of incidents, victims, population displacement) with qualitative characteristics of political dynamics and local context. It is precisely the multi-level structure of data collection and regular updating of indicators that makes it possible to identify signs of escalation in a timely manner. This confirms the need to integrate different types of data (social, spatial, event-based) into a single analytical risk-management system. The results obtained in the study by Y. Wang *et al*. (2025) showed that the automatic detection of war-damaged buildings on the basis of high-resolution satellite imagery makes it possible to identify the scale of damage and the spatial distribution of destruction in conflict zones with high accuracy. The use of deep-learning algorithms to analyse remote-sensing data provides the possibility of prompt identification of new pockets of destruction that pose a risk to the civilian population, and can be used to confirm facts of violations of international humanitarian law. This demonstrates the potential of IAS in applying remote-monitoring technologies to improve the accuracy of threat assessment and support decision-making in crisis conditions.

The study of analytical approaches to forecasting conflict risks showed that modern statistical models are capable of reflecting not only the current dynamics of violence, but also predicting its recurrence over time. According to the study by R. Browning *et al*. (2024), the application of Bayesian Hawkes processes provides accurate detection of temporal clusters of violence and increases the reliability of forecasts by considering event inertia. Such an approach forms the basis for improving information and analytical risk-management systems, which must respond promptly to changes in the dynamics of combat operations. Further development of the technological direction of information analysis is demonstrated by the results of the study by A. Beger *et al*. (2021), who proved that the effectiveness of machine-learning models in forecasting armed conflicts depends not so much on the complexity of algorithms as on the quality of initial indicators and the system's ability to update data in real time. This emphasises that information and analytical systems must be adaptive, integrate streaming data from various sources and maintain stability of risk assessment even in the dynamic environment of military operations.

In the ethical and legal context of AI use in armed conflicts, A. Brenneis (2024) found that the main threat to the legitimacy of dual-use analytical systems is the lack of mechanisms for distributed responsibility between developers, operators and state structures. Automating risk assessment without ethical oversight creates the risk of erroneous decisions, in particular under conditions of uncertainty in combat data, which reinforces the concept of information and analytical security, proving that IAS must include ethical protocols for data control. Z. Małodobry *et al*. (2024) proved that integrating AI into weapons systems increases the speed of decision-making, but at the same time increases the risks of uncontrolled use of algorithms without human verification. The effectiveness of such systems depends on the level of analytical verification that prevents autonomous errors in combat conditions. This means that technological effectiveness must be accompanied by a reliable risk-management mechanism. In the socio-cognitive dimension of information security, A. Sinha *et al*. (2024) proved that information flows during war have a direct impact on the psychological stability of

society. This conclusion complements the concept of humanitarian-oriented IAS, as it shows that risk management must include monitoring of information and psychological threats.

In the practical context of the Ukrainian experience, V. Goncharuk (2024a) showed that Ukraine's defence sector is actively forming a "smart defence" model, where military and civilian analytical technologies are combined. The application of Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) platforms, Open-Source Intelligence (OSINT) data and commercial AI creates a new level of situational awareness on the battlefield. This confirms Ukraine's capacity to develop its own model of information and analytical risk management that already meets international standards. As evidenced by the results of the study by K. Sporyshev *et al*. (2024), the main limitation of Ukraine's security systems remains the fragmentation of analytical data and the lack of centralised inter-agency integration. Only the implementation of a unified analytical architecture will make it possible to increase the effectiveness of decision-making in crisis situations, which highlights the need to create an inter-agency IAS capable of co-ordinating military, civilian and humanitarian actions. The Ukrainian experience of integrating analytical systems into combat management, studied by M. Onderco (2025), influenced the development of NATO approaches to regulating military AI. This practice became the basis for developing allied principles of transparency and accountability in automated decisions, demonstrating the interconnection between national and international levels of risk management in defence analytics.

Despite significant academic progress in studying information and analytical support for risk management, from technological solutions to ethical and humanitarian aspects, a number of unresolved issues remain. In particular, the systemic integration of analytical, legal and humanitarian components into a single risk-management model has been insufficiently studied. In addition, the Ukrainian experience of practical implementation of such systems in real wartime conditions has not yet received comprehensive academic interpretation. Therefore, the purpose of the study was to clarify the main mechanisms of operation and interaction of information and analytical structures in the process of managing risks of a military nature. To achieve the purpose, the following tasks were set: to analyse the types of threats and risks that arise during combat operations in order to determine the impact on the effectiveness of managerial decisions; to assess the structure, principles, and tools of functioning of information and analytical systems in international and Ukrainian practice in order to determine patterns of development and effectiveness of IAS in different phases of conflict.

Materials and Methods

To systematise the types of threats arising during armed conflicts and to determine the relationship with risk-management processes, structural-functional and content-analytical methods were used. Scientific sources were used that covered the main categories of risks: physical (Collins & Spencer, 2025), physical/humanitarian, man-made (Rapid environmental assessment…, 2023), man-made/radiological (International Atomic Energy Agency, 2024), information/cyber threats, information/cognitive, psychological (Rizk & Cordey, 2023), complex/hybrid. Classification was carried out according to the following criteria for selecting risks: the nature of impact (physical, man-made, information or psychological), the source of formation (direct consequence of combat operations or secondary effects (environmental, technological, cognitive)), the scale of impact (local, national or transnational level of threat), social and humanitarian consequences (impact on the civilian population, critical infrastructure and the moral resilience of society), the degree of integration (the ability of a threat to combine several types of risks, forming hybrid or complex models of danger). The task of this stage was to form a systemic structure of threats that reflects the multi-level nature, from physical destruction to information and psychological impacts, which created the basis for further risk modelling and the construction of an IAS for security management during combat operations.

In order to study the practical application of IAS in the military, environmental, man-made and humanitarian spheres, a comparative-analytical approach and the case method were used. The analysis was carried out through a comparative study of foreign and national examples that reflect real mechanisms of IAS functioning on the basis of official reports and analytical studies: AI-based military analytics (Robinson *et al.*, 2023), monitoring of the combat situation (Goncharuk, 2024a, 2024b), assessment of critical infrastructure resilience through sensor and geospatial monitoring, environmental monitoring of the consequences of the destruction of the Kakhovka Hydroelectric Power Plant (HPP) (Rapid environmental assessment…, 2023), a digital system for monitoring the safety of the Zaporizhzhia Nuclear Power Plant (ZNPP) in a combat zone (International Atomic Energy Agency, 2024), a national cyber-defence platform with Big Data analytics, a humanitarian IAS for spatial analysis of destruction in the Gaza Strip, a digital humanitarian monitoring system for assessing information and cyber risks in conflict zones (Rizk & Cordey, 2023; International Committee of the Red Cross, n.d.). The task of this stage was to identify patterns of IAS functioning in real armed-conflict conditions, and to determine which technological and analytical tools ensure the effectiveness in forecasting risks and supporting decisions.

In addition, to analyse the regulatory and legal regulation of the functioning of risk-management systems during combat operations, a comparative-legal method was applied in order to determine the legal foundations for forming and integrating IAS in the sphere of national and collective security. The analysis covered the provisions of Law of Ukraine No. 2469-VIII (2018), Law of Ukraine No. 389-VIII (2015) and Law of Ukraine No. 2163-VIII (2017), which define the operational model of risk management within the state, regulate the powers of state authorities, the procedure for response and the protection of critical infrastructure and cyberspace. At the global level, Charter of the United Nations and Statute of the International Court of Justice (1945), Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) (1978) and Convention on Cybercrime (2001) were used. These documents define global standards of humanitarian and cybersecurity law, aimed at unifying the principles of collective security and controlling compliance with international law norms. The task was to form an integrated legal basis for the functioning of IAS that combines national implementation mechanisms with international security and response standards.

For a comparative analysis of risk-management algorithms during combat operations, a comparative approach was applied, implemented through analytical and structural methods to determine the logic of functioning of IAS within a single management cycle – collection→analysis→assessment→response→-control. The selection of this cycle is determined by its universality, since it corresponds to foreign risk-management standards ISO 31000:2018 (2018) and the principles defined in Sendai Framework for Disaster Risk Reduction 2015-2030 (2015). This model reflects the complete management process, from the receipt of data to decision-making and subsequent correction of actions, and ensures the integration of technical, legal and humanitarian components within the security system. To reflect the practical implementation of the stages of the risk-management cycle in global and Ukrainian practice, an analytical method was used based on empirical examples of IAS functioning that cover all stages of the cycle. The task was to identify practical mechanisms of risk management in different conflict conditions and to assess the degree of alignment of Ukrainian IAS with foreign security standards.

For an in-depth analysis of the effectiveness of IAS in different types of conflicts, a structural method was applied, which involved selecting three representative cases – Ukraine (International Atomic Energy Agency, 2024), the Gaza Strip and Burundi. The selection of these cases was determined by the need to cover the full spectrum of phases of the conflict cycle, from active combat operations (Ukraine) to humanitarian response (Gaza Strip) and post-conflict stabilisation (Burundi). This approach made it possible to trace the evolution of IAS functions in different environments and security conditions. The criteria for selecting cases were: phase of conflict, type of IAS (military, humanitarian, recovery), level of technical integration, presence of international participation and availability of analytical data. The task of this stage was to identify patterns of development and effectiveness of IAS depending on the phase of conflict, the degree of technological integration and the level of interaction between national and international security structures.

Results

Identification of threats and the formation of a risk management system during combat operations. Identification of threats during combat operations is a key stage of risk management, which ensures the detection and assessment of hazards through the synthesis of data from intelligence, satellite monitoring, sensors, OSINT, cyberspace and social indicators. Within the systemic approach, all threats that arise during combat operations are divided into four basic groups. Physical risks are associated with the direct impact of military factors – the casualties among personnel, the destruction of infrastructure, transport and energy hubs, and the use of explosives. The characteristics are formed through the processing of spatio-temporal data, topographical models and field observations (Aviv & Ferri, 2023).

Man-made risks arise as a result of secondary effects of war – accidents at industrial facilities, damage to energy supply systems, water supply, nuclear or chemical installations. The identification is based on the integration of environmental monitoring data, engineering systems and technical sensors, which makes it possible to forecast cascading consequences of destruction. Information risks cover threats to cybersecurity, disinformation campaigns and data distortion that affect the decision-making process. To assess these risks, algorithms for big-data analysis, network traffic monitoring and models for verifying source credibility are used. Psychological risks are associated with the condition of military personnel, the civilian population and governance structures under stressful conditions. Such risks are identified on the basis of the analysis of social communications, behavioural indicators, medical and sociological data. Integrating psychological parameters into the overall risk model makes it possible to timely recognise signs of destabilisation or moral exhaustion (de Bruin *et al.*, 2022). Table 1 presents a classification of threats that characterise key types of risks in modern combat conditions.

Table 1. Taxonomy of threats in the modern conflict environment of the 21st century

Threat category	Description of the essence of the risk	Example
Physical	Destruction of civilian and critical infrastructure, civilian deaths, disruption of logistics	During the defence of Kyiv (February-March 2022), the city's infrastructure became an arena of combat. The destruction of bridges, energy lines and residential buildings complicated the coordination of civil defence
Physical/ humanitarian	Mass destruction of civilian facilities, leading to humanitarian crises	Analysis of satellite data showed the destruction of more than 4,500 critical infrastructure facilities (hospitals, schools, water mains) during the first 6 weeks of the 2023 campaign; the consequences – lack of water and medical services
Man-made	Secondary disasters caused by the destruction of industrial or energy facilities	A dam breach in June 2023 led to flooding of more than 600 km^2, loss of drinking-water sources, destruction of the Dnipro ecosystems and population displacement
Man-made/ radiological	Loss of control over nuclear or energy facilities, accident risks	Military presence near ZNPP is accompanied by damage to power lines, threats to staff safety and the shutdown of reactor cooling systems
Information/ cyber threats	Attacks on control systems, disinformation, data manipulation	In 2022-2024, an increase in the intensity of cyberattacks on government resources and energy networks was recorded; malicious AI-based algorithms were used
Information/ cognitive	Use of AI and big data for military intelligence and targeting	AI systems for metadata analysis create risks of erroneous target identification and violations of IHL norms
Psychological	Psycho-emotional pressure on military personnel and civilians, influence of information campaigns	An excessive number of shocking digital messages on social media during combat operations creates a state of panic and "digital fatigue" among the civilian population
Complex/hybrid	Combination of physical, cyber and psychological impacts to destabilise the state	Co-ordinated strikes on energy systems, port infrastructure and telecommunications, combining physical destruction with cyber activity to undermine stability

Source: compiled by the authors based on J. Rizk & S. Cordey (2023), Rapid environmental assessment of Kakhovka Dam Breach Ukraine, 2023 (2023), Y. Asi *et al.* (2024), International Atomic Energy Agency (2024), A. King (2024), L. Collins & J. Spencer (2025), O. Semenenko *et al.* (2025), W. Skomra & K. Wojtasik (2025)

The nature of threats is complex and interdependent, since physical destruction causes man-made disasters, while information and psychological impacts amplify the scale of humanitarian consequences. Physical threats form the primary level of risk and are associated with the destruction of critical infrastructure facilities, transport communications and life-support systems. Events such as the defence of Kyiv in 2022 or the massive bombardment in the Gaza Strip in 2023 show that dense urban development and a high level of technological saturation significantly complicate humanitarian response. Man-made risks arise as a result of loss of control over energy or industrial facilities. The destruction of the Kakhovka HPP and the threat of radiological incidents at the Zaporizhzhia NPP indicate the need to integrate environmental monitoring and critical infrastructure analytics into a single risk-management system. Information and cyber threats act as risk multipliers, as these threats can influence operational decisions, communication between security structures and public trust in official sources. The increase in cyberattacks on Ukraine's state systems and the use of AI algorithms in military intelligence demonstrate that the information space is becoming an independent theatre of hostilities. The psychological dimension of threats manifests through mass information pressure, which generates emotional exhaustion, fear, and disorientation of the population. Digital platforms increasingly become channels of psychological influence, which disrupts the balance between the right to information and the protection of mental health during war. Complex or hybrid threats combine physical attacks, cyber interference and information campaigns, creating the effect of multi-level destabilisation. Such actions have a strategic goal – undermining trust in state institutions, disorganising logistics and the erosion of societal morale. The process of threat identification is not only a stage of information collection, but also the basis of information and analytical support for risk management during combat operations (Iskoujina *et al.*, 2024).

Regulatory and legal support is the basis for creating effective risk-management systems under conditions of combat operations. It defines the rules of information exchange, the powers of state authorities and the limits of using analytical technologies. National regulations create a single legal framework for the functioning of the security sector, risk management and cyber defence. Law of Ukraine No. 2469-VIII (2018) defines the system of state administration in the field of security, the principles of forecasting and assessing threats, as well as the role of information and analytical structures under the National Security and Defence Council of Ukraine (NSDC) and the Security Service of Ukraine (SSU). Law of Ukraine No. 389-VIII (2015)

regulates the actions of state authorities under conditions of armed conflict, the procedure for informing the population, the interaction of security structures and ensuring the resilience of critical infrastructure. Law of Ukraine No. 2163-VIII (2017) forms the national cyber defence system, establishes the principles of exchanging incident data and responding to cyber threats, which is a component of analytical monitoring during war. Together, these laws regulate the legal, organisational and informational aspects of risk management and create the basis for the functioning of national information and analytical systems.

International documents set the legal framework for collective security and humanitarian control over actions during war. Charter of the United Nations and Statute of the International Court of Justice (1945) defines the principles of collective security, the right to self-defence and mechanisms for preventing threats to peace. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) (1978) establishes the obligation of parties to assess risks to the civilian population and minimise the consequences of combat operations. Convention on Cybercrime (2001) regulates international co-operation in countering cyber threats, in particular during armed conflicts. Taken together, these acts form an integrated legal basis that combines national and international mechanisms for risk management of threats and the protection of information systems. The difference between Ukrainian regulatory acts and international legal documents lies in the level of regulation, the scale of operation and the purpose of application. National acts form the internal security system, define the powers of state authorities, the procedure for response during war and the protection of critical infrastructure and cyberspace. The purpose is to create an operational model of risk management within the state. International documents set the normative framework of global and humanitarian security, regulate the responsibility of parties in war, the protection of civilians and co-operation in the field of cyber defence to unify international standards and control compliance with humanitarian law. National acts ensure internal risk management, while international acts provide external co-ordination and legal guarantees in the sphere of collective security.

IAS is a key element of risk management of threats during combat operations. Its main function is to collect, process, synthesise and visualise data that characterise the situational environment, the level of danger and possible scenarios of events. The architecture of IAS ensures the integration of information flows of different nature, from operational intelligence data to technical measurements and open data. The system architecture is built on a multi-level principle. At the primary level, data are aggregated from various sources – intelligence, satellite observations, sensor networks, communication systems, OSINT platforms and internal databases of state structures. The second level includes data-processing centres where cleansing, credibility verification, format standardisation and preliminary classification of information are performed. The third level is represented by analytical modules that provide the calculation of risk indicators, the formation of threat scenarios and support for the decision-making process (Robinson *et al.*, 2023).

The methods of information processing in IAS are based on a combination of classical and modern approaches to data analysis. The key technologies are Big Data analytics, which allow work with large volumes of unstructured information, and Machine Learning, which is used to identify patterns and forecast risk dynamics. Automated analysis algorithms are applied to determine relationships between events, objects, and threat factors. An important component is predictive modelling, which makes it possible to form scenarios of situation development and assess the effectiveness of potential decisions. The final level of IAS provides visualisation of analysis results in the form of interactive maps, monitoring dashboards and reports for operational management. Thanks to this, a single analytical space is created, in which data from different sources and levels are combined, providing support for strategic and tactical decisions in real time. IAS acts not only as an information-collection tool, but also as a comprehensive mechanism for predicting and preventing risks that combines technological, analytical and managerial components of the security system.

The practical application of IAS in the military, environmental, man-made and humanitarian spheres demonstrate the key role in ensuring situational awareness, forecasting risks and co-ordinating response during conflicts. One of the most representative examples is the RAND Corporation study (Robinson *et al.*, 2023), which created an experimental machine-learning analytical system to forecast combat risks in Ukraine. The system processed operational reports, topographical parameters and the temporal dynamics of combat operations, which made it possible to form scenarios of event development with high accuracy. The report of the International Centre for Defence and Security (International Centre for Defence and Security, (2024), confirmed the criticality of using IAS with AI elements for monitoring the combat situation and analysing satellite data. Through these systems, a real-time situational awareness environment is created that combines intelligence data, OSINT flows and geospatial analytics. As an example of a practical approach to assessing the resilience of Ukraine's critical infrastructure, a case is presented in which the "resilience index" model developed by the ETH Zürich Centre for Security Studies (Aebi *et al.*, 2024) was applied. The model is based on the integration of sensor, geo-analytical and infrastructure data and reflects the overall ability of energy, transport, and

communication systems to maintain functioning during crisis impacts and recover after damage. Such a description of the principles for assessing the index ensures transparency and reproducibility of results, as it allows the indicator to be interpreted not only as a numerical value, but as a comprehensive criterion of system resilience. The use of IAS in this context contributes to assessing the ability of critical infrastructures to withstand cascading attacks and recover effectively after these attacks.

After the destruction of the Kakhovka HPP, the United Nations Environment Programme (Rapid environmental assessment…, 2023) introduced an environmental rapid-response IAS that combined satellite imagery, field reports and mathematical models of water spread. The system provided the first comprehensive assessments of environmental damage within 72 hours after the event, demonstrating the effectiveness of IAS in crisis monitoring. The International Atomic Energy Agency (International Atomic Energy Agency, 2024) created a digital IAS to monitor the safety of the Zaporizhzhia NPP. The system provides round-the-clock data collection on reactor parameters, the state of energy supply and the physical protection of the facility, performing functions of international control in a combat zone. The Ukrainian experience reflects the activities of CERT-UA, which operated as a state cyber-defence IAS in 2022-2024 (Semenenko *et al.*, 2025). The platform combines Big Data analytics, anomaly detection and forecasting of intrusion indicators; thanks to it, more than 20,000 attempted cyberattacks on Ukraine's state structures were recorded. International humanitarian analytics is also based on IAS: the Conflict and Health team created a geoinformation system for monitoring destruction in the Gaza Strip (October-November 2023). The IAS made it possible to identify more than 4,500 destroyed civilian infrastructure facilities, including hospitals and water mains, enabling humanitarian planning on the basis of spatial data (Asi *et al.*, 2024). International Committee of the Red Cross (n.d.) developed a digital risk-assessment platform that analyses cyberattack, personal data leaks and information manipulation in conflict zones. This system became a benchmark for balancing information security and humanitarian principles during combat operations.

The generalisation of the presented cases indicates that IAS in the sphere of security and humanitarian response share common features that determine the effectiveness in contemporary 21st-century conflicts. Such systems are characterised by multi-source data collection, which provides for the combination of intelligence data, satellite imagery, OSINT resources and field observations for comprehensive situation analysis. The automation of analytics through the use of machine-learning algorithms and predictive modelling is significant, as it increases the accuracy of risk assessment and the speed of decision-making. IAS are also characterised by modularity and adaptability, which makes it possible to scale these systems for the needs of military, environmental or humanitarian missions. In addition, systems have a clear humanitarian-legal orientation, as norms of international humanitarian law are integrated into the work, regulating the processing, use and dissemination of data. IAS emerge as a key element of risk management in wartime conditions, combining technological, legal and humanitarian dimensions of security management.

Information and analytical risk-management systems during combat operations in global and Ukrainian contexts. Within the system of information and analytical security support during combat operations, risk management is based on the principle of a continuous decision cycle: collection→analysis→assessment→response→control. This cycle ensures dynamic adaptation to environmental changes, the integration of technical, legal and humanitarian aspects, and also makes it possible to create a coherent algorithm of interaction between security actors – military, civilian, environmental and humanitarian structures (Bondar, 2025). Table 2 illustrates the risk-management algorithm during combat operations in a comparison format of international and Ukrainian experience.

Table 2. Risk-management algorithm during combat operations in foreign and Ukrainian practice

Stage of the risk-management cycle	Example from international practice (implemented by international organisations)	Example of Ukrainian practice (national level)	Results
Information collection	After the destruction, an international UN environmental mission in Ukraine, which after the destruction of the Kakhovka HPP applied the global Rapid Environmental Assessment system (satellites, sensors, field data). An International Atomic Energy Agency (IAEA) mission for round-the-clock monitoring of the state of the ZNPP	CERT-UA – a state system for collecting and analysing cyberattacks in real time. The State Emergency Service of Ukraine (SES) – a sensor system for monitoring hazardous territories	International IAS demonstrate the effectiveness of global standards for data collection, while Ukrainian systems provide operational response at the local level

Table 2. Continued

Stage of the risk-management cycle	Example from international practice (implemented by international organisations)	Example of Ukrainian practice (national level)	Results
Data analysis	A machine-learning analytical model for forecasting risks in conflicts, tested on data from Eastern Ukraine (an example of global AI analytics)	Ukraine's integrated C4ISR system – a combination of AI satellite intelligence, OSINT data and commercial technologies (Starlink, Palantir, DJI). The system provides real-time analytical data processing for threat forecasting and decision-making	International studies create analytical standards that Ukraine implements in its own resilience and forecasting systems
Risk assessment	An international humanitarian organisation developed a digital-risk assessment IAS in conflict zones, including in Ukraine, and the legal foundations for assessing humanitarian risks	The C4ISR system is used to assess risks in the planning of operations and the protection of civilian infrastructure; it integrates legal and humanitarian assessment criteria	Analytical AI and C4ISR systems can be applied not only in the military sphere but also in the humanitarian sphere of risk management
Response	Creation of an international platform for co-ordinating actions on security and humanitarian support for Ukraine	The Ministry of Internal Affairs (MIA) of Ukraine ("DiiaBezpeka") – an integrated system for public alerting and co-ordinating response. The SES – national response plans for man-made and environmental incidents	International organisations provide response methodology, while Ukraine is an example of rapid implementation of these approaches in national IAS
Control and adjustment	The IAEA international mission carries out ongoing monitoring of ZNPP safety and adjusts protection procedures. Monitoring of digital risks and the effectiveness of humanitarian measures	The SES and the Ministry of Infrastructure (2023-2024) – monitoring the restoration of facilities after attacks and verifying analytical forecasts	Effective control requires feedback between international observers and national structures for continuous updating of IAS models

Notes: In the table, "international practice" refers to the activities of such institutions (United Nations Environment Programme (UNEP), International Atomic Energy Agency (IAEA), International Committee of the Red Cross (ICRC)) and reflects not the place of implementation, but the methodological basis of the systems applied in Ukraine. This makes it possible to consider the given examples as global risk-management models tested under real combat conditions

Source: compiled by the authors based on International Committee of the Red Cross (n.d.), Law of Ukraine No. 389-VIII (2015), Law of Ukraine No. 2163-VIII (2017), Law of Ukraine No. 2469-VIII (2018), Special meeting of the Permanent Council (1368th Plenary Meeting) (2022), Rapid environmental assessment of Kakhovka Dam Breach Ukraine, 2023 (2023), E. Robinson *et al*. (2023), J. Rizk & S. Cordey (2023), International Atomic Energy Agency (2024), S. Aebi et al. (2024), V. Goncharuk (2024b), O. Semenenko *et al*. (2025), K. Bondar (2025)

Effective response to threats during combat operations requires the combination of international and national IAS. Foreign organisations form methodological and technological standards that are used in global risk-management practice. The activity in Ukraine is an example of applying international principles on a real battlefield, where the effectiveness of integrating satellite, sensor and analytical data for operational response to physical, man-made and humanitarian risks is tested. In turn, the Ukrainian risk-management system is gradually acquiring the features of a comprehensive IAS, combining the tools of CERT-UA, "DiiaBezpeka", the SES and the Ministry of Infrastructure. These structures ensure data collection, analytics, response, and control at the national level, which corresponds to the basic stages of the risk-management cycle. Ukraine effectively serves as an example of adapting international standards to the conditions of hybrid war, where legal, technical and humanitarian solutions are implemented simultaneously. The risk-management model in combat conditions is an integrated system in which analytics, law and humanitarian principles interact within a single information environment. Table 3 presents the characteristics of conflict conditions, the structure of IAS, its level of effectiveness and key results of the functioning of Ukraine, the Gaza Strip and Burundi depending on the type of conflict environment. The comparison made it possible to trace how differences in scale, technological support and humanitarian orientation affect the performance of monitoring and response systems.

Table 3. IAS of risk management in conditions of different conflict environments

Country/region	Characteristics of the conflict	Structure/type of IAS	Effectiveness of monitoring and response	Key results/conclusions
Ukraine	Full-scale war, a complex of physical, man-made, cyber and humanitarian threats	A national IAS with a multi-agent structure: SES, CERT-UA, MIA "DiiaBezpeka", Ministry of Infrastructure. Integration with international UNEP and IAEA missions	High level of technical integration; partial automation of data collection, operational response (hours to a day)	A model of a multi-level IAS combining military, environmental and humanitarian modules has been formed. It requires improvement of legal co-ordination between agencies
Gaza (part of the Palestinian territories)	A high-density urban conflict, mass destruction of civilian infrastructure in 2023	A geo-analytical IAS of spatial analysis – integration of satellite imagery, cartographic databases and field observations (United Nations (UN), World Health Organisation (WHO), Conflict and Health)	High accuracy of data georeferencing; limited response speed due to lack of field channels; humanitarian data are updated daily	More than 4,500 destroyed critical infrastructure facilities were identified; an interactive map of humanitarian risks was created and is used by the UN
Burundi (post-conflict context, East Africa)	Post-conflict destabilisation, risks of hybrid threats for energy and transport	An IAS for assessing the resilience index – multi-scenario modelling of the resilience of critical facilities; satellite and sensor monitoring	Medium level of technical integration; data are collected with a delay of several days; risk adjustment is carried out weekly	The system proved effective in forecasting man-made risks, but has a limited humanitarian component; it requires connection to global IAS

Notes: the indicator "operational response (hours to a day)" provides an averaged time interval between the detection of a threat and the primary response of the IAS system at the national level. This quantitative characteristic reflects the speed of co-ordinating actions between analytical centres, the SES and departmental structures during crisis events, which is consistent with rapid monitoring and response practices recorded in Rapid environmental assessment of Kakhovka Dam Breach Ukraine, 2023 (2023), International Atomic Energy Agency (2024), O. Semenenko *et al*. (2025), where the time limits of primary response varied from several hours to one day depending on the type of event

Source: compiled by the authors based on Charter of the United Nations and Statute of the International Court of Justice (1945), Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) (1978), Law of Ukraine No. 2163-VIII (2017), Law of Ukraine No. 2469-VIII (2018), Rapid environmental assessment of Kakhovka Dam Breach Ukraine, 2023 (2023), E. Robinson *et al*. (2023), S. Aebi *et al*. (2024), V. Goncharuk (2024b), Y. Asi *et al*. (2024), G. Irankunda et al. (2024), International Atomic Energy Agency (2024), V. Goncharuk (2024b), O. Semenenko *et al*. (2025)

Ukraine has the most comprehensive and technologically advanced model of IAS, combining national and international institutions (SES, CERT-UA, MIA, UNEP, IAEA). Its strength is integration and multichannel data (from satellites to field sensors), which ensures a high level of situational awareness. At the same time, problems of institutional synchronisation remain, i.e., the need for better co-ordination between different state agencies, especially during cross-sectoral response. The Gaza Strip demonstrates a different type of effectiveness – a humanitarian-analytical orientation. Here, the IAS functions as a geo-analytical system that explains the destruction of civilian infrastructure in detail and assesses humanitarian consequences. High accuracy of spatial analysis makes this system exemplary for humanitarian monitoring; however, its operational speed is limited by the deficit of field resources and low resilience of data transmission channels. Burundi, by contrast, represents a post-conflict scenario – the stage of transition from response to stabilisation. The IAS here is used to assess the resilience index of critical infrastructure (energy, transport, water supply), i.e., to forecast secondary risks and support reconstruction processes. Its effectiveness lies in long-term planning, but the system is still limited in its humanitarian component and is not integrated into global analytical networks.

The comparison of these three cases makes it possible to trace the evolution of IAS in different phases of conflict development. In the active phase of war, as in the case of Ukraine, IAS serves as a means of operational response, ensuring rapid decision-making and co-ordination of actions on the basis of multi-source data. In the humanitarian phase of conflict, represented by the Gaza Strip, the system acquires functions of humanitarian control aimed at documenting the consequences of destruction and supporting international reporting processes. Meanwhile, in the post-conflict phase, characteristic of Burundi, IAS is transformed into a mechanism for restoring the resilience of critical infrastructure and preventing secondary threats. The

most effective is the hybrid model that combines international methodology with national analytical capabilities of the state. Such integration ensures the creation of an adaptive, multi-level monitoring system capable not only of responding quickly to risks, but also of supporting long-term security and humanitarian resilience in a post-conflict environment.

The level of integration of IAS across different security sectors directly affects response speed and the systems' capacity to recover. The use of information and analytical systems contributes to minimising wartime risks by ensuring not only threat assessment, but also the actual reduction of the consequences through operational response, automated data analysis and the integration of information flows in real time. Examples of the practical functioning of such systems demonstrate a cause-and-effect relationship between the technological capabilities of IAS and the reduction in the scale of risks. In particular, the C4ISR system makes it possible to reduce decision-making time, increase accuracy and synchronisation of combat operations, which directly reduces the level of losses and the risk of destabilisation (Bondar, 2025). In the cyber sphere, CERT-UA ensures rapid detection and neutralisation of attacks, preventing the escalation (Semenenko *et al.*, 2025). In the environmental dimension, it reduced the response time to the destruction of the Kakhovka HPP to 72 hours, minimising the humanitarian and environmental consequences of the event (Rapid environmental assessment…, 2023). The IAEA's permanent IAS mission at the ZNPP (International Atomic Energy Agency, 2024) is an example of continuous monitoring that reduces the risks of radiological incidents through round-the-clock analysis and warning of deviations on a 24/7 basis. Taken together, the above examples confirmed that the implementation of IAS is an effective tool for minimising wartime, cyber and man-made risks. Thus, IAS have proven the effectiveness not only as a risk-assessment tool, but also as a factor in the real reduction through data integration, response automation and inter-agency co-ordination. The further development creates the basis for increasing the resilience of state and humanitarian institutions in complex security environments.

Discussion

The study results showed that IAS implements a combination of risk-modelling algorithms with multi-level data processing (aggregation, cleansing, analytical modules and scenario forecasting). This was consistent with the conclusions of D. Granata & M. Rak (2024), who carried out a systematic comparison of automated threat-modelling tools in an open environment. The authors proved that combining modular systems makes it possible to ensure scalability and adaptability to new hazard scenarios. The analytical architecture of the IAS in the present study has similar features, as it includes scenario forecasting and machine processing of big data. The consistency of the results demonstrates that risk management systems require a flexible software core capable of synchronising heterogeneous information flows. This confirms the scientific basis for developing national systems using open threat-modelling standards.

The study results revealed that the IAS model provides for the use of machine-learning technologies to analyse risk dynamics and build scenarios for the development of combat events. This is consistent with the study by M. Murphy *et al.* (2024), which demonstrated the potential of AI models in forecasting armed conflicts. The authors showed that combining social, topographical and temporal parameters makes it possible to achieve high accuracy in predicting violent events. This corresponds to the present study in the description of the RAND Corporation analytical system, which uses similar approaches to processing operational data. Predictive modelling is an effective tool for strategic planning under conditions of uncertainty, which confirms the expediency of implementing IAS with AI modules for operational risk management during combat operations. In the study by C. Scher & J. Van Den Hoek (2025), the application of InSAR technologies for remote monitoring of destroyed buildings in the Gaza Strip during the 2023 war was considered. The authors showed that interferometric analysis of satellite imagery makes it possible to quantify the scale of destruction, track structural changes in the urban environment and create detailed maps of damage to civilian infrastructure. The combination of geospatial analytics and radar-data processing algorithms expands the possibilities of accurate humanitarian monitoring of conflict zones. This corresponded to the results of this study, since the IAS model also provides for the use of satellite and sensor data to analyse physical and humanitarian risks. Integrating InSAR methods into the structure of IAS contributes to increasing the objectivity of documenting the consequences of combat operations. Both studies confirmed the shift of humanitarian analytics from descriptive assessments to high-technology monitoring based on open satellite data and automated analysis of spatial changes.

The study results demonstrate that the effectiveness of IAS is largely associated with the use of machine-learning technologies to forecast risks in cyberspace. This is consistent with the study by N. Mohamed (2025), which provided a comprehensive review of contemporary Machine Learning Approaches (ML) approaches of the 21st century in the field of cybersecurity. The author emphasised that adaptive models based on deep learning make it possible to identify new attack patterns that are inaccessible to traditional systems. In this study, a similar concept is implemented through the description of an IAS capable of forming risk scenarios on the basis of continuous analysis of streaming data. Both approaches indicate that hybrid

war requires the integration of ML analytics into the process of making security decisions, which points to the expediency of transitioning from reactive to self-learning cyber-defence systems.

In the work by S.-A. Mitoulis *et al*. (2023), a conflict-resilience framework, was developed for assessing and restoring critical infrastructure in armed conflicts. The authors showed that the resilience of infrastructural systems depends on the ability to integrate data on the condition of engineering assets, energy networks and transport hubs into a single analytical model. The combination of geo-monitoring, structural analysis and scenario forecasting of the consequences of destruction makes it possible to determine the resilience index of assets in the dynamics of combat operations. This correlates with the results of this study, since the IAS model is also based on the integration of sensor and satellite data to forecast cascading effects of man-made destruction. The resilience of critical infrastructure cannot be achieved solely through engineering solutions – a multi-level analytical system is needed that takes legal, humanitarian and environmental criteria into account. This confirms the global trend towards forming integrated risk-management systems oriented towards improving infrastructure resilience indicators.

The study results showed that cyber-defence IAS achieve maximum effectiveness under conditions of integrating heterogeneous data streams and predictive threat analysis. This was evidenced by the work of S. Ainslie *et al*. (2023), which conducted a systematic review of the development of the Cyber-Threat Intelligence (CTI) concept as a key element of cybersecurity management. The authors analysed approaches to collecting, correlating and interpreting cyber data, developing a scientific and practical programme for improving decision-making processes in the field of information protection. An effective CTI system should move from reactive response to proactive risk forecasting, using machine-learning algorithms, big-data analytics and real-time threat visualisation. In the IAS of this study, similar mechanisms of multi-source information collection are implemented – network traffic, sensor data and OSINT streams – for the prompt detection of cyber threats. Both studies emphasised the need to standardise data formats and create integrated platforms for sharing analytics between governmental, private and international structures. Implementing CTI approaches in the national security system is a key factor in increasing the effectiveness of cyber defence under conditions of hybrid war.

A. Habbal *et al*. (2024) proposed a theoretical and practical framework, Artificial Intelligence Trust, Risk, and Security Management (AI TRiSM), aimed at increasing the reliability and ethicality of the use of artificial intelligence systems in critical domains. Uncontrolled use of machine-learning algorithms in military, security and humanitarian environments can generate cognitive risks associated with erroneous decisions, data distortion and loss of user trust. At the centre of the AI TRiSM model are three core principles – trust, clarity, and controllability – which determine the safe functioning of AI in high-risk scenarios. This was consistent with the study results regarding similar problems – the possibility of erroneous target identification, ethical dilemmas in decision-making and the risk of violating humanitarian norms under the influence of automated algorithms; the technical sophistication of AI does not guarantee safety without legal and ethical oversight. Integration of AI trust policies into national and international security systems is necessary, which will ensure a balance between technological effectiveness and humanitarian responsibility.

The study results revealed that satellite and geospatial data are a basic tool for detecting the consequences of combat operations in real time. This corresponded to the work of V. Sticher *et al*. (2023), who demonstrated the capabilities of remote conflict monitoring using high-resolution imagery and automated analysis. The authors showed that such technologies make it possible to identify zones of destruction even without physical access to territories. IAS, in the present study, uses satellite and sensor data to build spatio-temporal models of destruction and support the risk-assessment process in combat zones. Satellite analytics is becoming a fundamental element of situational awareness systems, combining military, environmental and humanitarian aspects of risk management. Thus, IAS is an effective risk-management tool in military, man-made, cyber and humanitarian environments. IAS confirmed the ability to integrate heterogeneous data – from geospatial and sensor to cognitive and informational – into a single analytical architecture that provides forecasting, situational awareness and real-time decision support.

Conclusions

The study results showed that contemporary 21st-century combat operations form a multidimensional chain of threats in which physical, man-made, informational and psychological factors interact in a cascading manner. Physical and humanitarian risks manifest in mass destruction of infrastructure and crises of population provision, while man-made and radiation-related risks are associated with damage to industrial and energy facilities, which leads to environmental catastrophes. Informational, cyber and cognitive impacts use artificial intelligence technologies for disinformation and manipulation, while hybrid threats combine physical, cyber and psychological factors with the aim of destabilising the state. IAS provide situational awareness and risk forecasting during combat operations. Damage to energy and industrial facilities forms secondary risks that, within the first 72 hours, determine the scale of environmental and humanitarian consequences, as recorded by the United Nations Environment Programme

after the destruction of the Kakhovka HPP. The effectiveness of risk management depends on the level of integration of IAS into national and international structures, and the regulatory framework of Ukraine regulates activities in the field of security, cyber defence and critical infrastructure resilience, aligning with collective and humanitarian security norms.

The risk-management algorithm during combat operations covers the stages of collection, analysis, assessment, response and control, implemented through the integration of international and national IAS. Ukraine adapts global standards to its own conditions, ensuring operational response, threat forecasting and increased resilience of security infrastructure. IAS that combines satellite, sensor, intelligence and open data reduce response time and increase the reliability of assessments through automated processing of big data. The Ukrainian IAS, formed on the basis of the State Emergency Service of Ukraine, CERT-UA, the Ministry of Internal Affairs ("DiiaBezpeka") and the Ministry of Infrastructure, recorded over 20,000 cyberattacks in 2022-2024, which confirms the effectiveness of using Big Data and machine learning in defence analytics. Global IAS, such as the IAEA and UN humanitarian environmental systems (in particular in the Gaza Strip), demonstrate stability and high functionality in crisis conditions. The Ukrainian system is distinguished by the highest level of technological integration and operational responsiveness, combining satellite observations, sensor networks, OSINT and analytical algorithms. A hybrid model of IAS that combines international standards with national resources creates a continuous risk-management cycle (collection→analysis→assessment→response→-control), ensuring operational response within hours-days and strategic resilience in post-conflict environments. A limitation of the study is its theoretical nature and the incompleteness of data in open sources. Future research should be directed towards deepening the empirical base by expanding data sources and using field observations, improving methods of collecting, processing and verifying information, and increasing the accuracy of real-time threat identification through the integration of analytical and predictive models.

Acknowledgements

None.

Funding

None.

Conflict of Interest

None.

References

[1] Aebi, S., Hauri, A., & Kamberaj, J. (2024). *Critical infrastructure resilience in Ukraine: energy, transportation, and communication*. Zurich: Centre for Security Studies. doi: 10.3929/ethz-b-000662463.

[2] Ainslie, S., Thompson, D., Maynard, S., & Ahmad, A. (2023). Cyber-threat intelligence for security decision-making: A review and research agenda for practice. *Computers & Security*, 132, article number 103352. doi: 10.1016/j.cose.2023.103352.

[3] Asi, Y., *et al*. (2024). "Nowhere and no one is safe": Spatial analysis of damage to critical civilian infrastructure in the Gaza Strip during the first phase of the Israeli military campaign, 7 October to 22 November 2023. *Conflict and Health*, 18, article number 24. doi: 10.1186/s13031-024-00580-x.

[4] Aviv, I., & Ferri, U. (2023). Russian-Ukraine armed conflict: Lessons learned on the digital ecosystem. *International Journal of Critical Infrastructure Protection*, 43, article number 100637. doi: 10.1016/j.ijcip.2023.100637.

[5] Beger, A., Morgan, R.K., & Ward, M.D. (2021). Reassessing the role of theory and machine learning in forecasting civil conflict. *Journal of Conflict Resolution*, 65(7-8), 1405-1426. doi: 10.1177/0022002720982358.

[6] Bondar, K. (2025). *How Ukraine's war is reshaping C4ISR for the modern battlefield*. Hague: The Hague Centre for Strategic Studies (HCSS).

[7] Brenneis, A. (2024). Assessing dual use risks in AI research: Necessity, challenges and mitigation strategies. *Research Ethics*, 21(2), 302-330. doi: 10.1177/17470161241267782.

[8] Browning, R., Patten, H., Rousseau, J., & Mengersen, K. (2024). Bayesian spatiotemporal modelling of political violence and conflict events using discrete-time Hawkes processes. *ArXiv*. doi: 10.48550/arXiv.2408.14940.

[9] Charter of the United Nations and Statute of the International Court of Justice. (1945, June). Retrieved from https://treaties.un.org/doc/publication/ctc/uncharter.pdf.

[10] Collins, L., & Spencer, J. (2025). *Case study #12 – Kyiv*. Retrieved from https://mwi.westpoint.edu/urban-warfare-project-case-study-12-battle-of-kyiv/.

[11] Convention on Cybercrime. (2001, November). Retrieved from https://rm.coe.int/1680081561.

[12] de Bruin, S.P., Hoch, J.M., von Uexkull, N., Buhaug, H., Demmers, J., Visser, H., & Wanders, N. (2022). Projecting long-term armed conflict risk: An underappreciated field of inquiry? *Global Environmental Change*, 72, article number 102423. doi: 10.1016/j.gloenvcha.2021.102423.

[13] Goncharuk, V. (2024a). Survival of the smartest? Defense AI in Ukraine. In H. Borchert, T. Schütz & J. Verbovszky (Eds.), *The very long game: 25 case studies on the global state of defense AI* (pp. 375-395). Cham: Springer. doi: 10.1007/978-3-031-58649-1_17.

[14] Goncharuk, V. (2024b). *Russia's war in Ukraine: Artificial intelligence in defence of Ukraine*. Retrieved from https://icds.ee/en/russias-war-in-ukraine-artificial-intelligence-in-defence-of-ukraine/.
[15] Granata, D., & Rak, M. (2024). Systematic analysis of automated threat modelling techniques: Comparison of open-source tools. *Software Quality Journal*, 32, 125-161. doi: 10.1007/s11219-023-09634-4.
[16] Habbal, A., Ali, M.K., & Abuzaraida, M.A. (2024). Artificial intelligence trust, risk and security management (AI TRiSM): Frameworks, applications, challenges and future research directions. *Expert Systems with Applications*, 240, article number 122442. doi: 10.1016/j.eswa.2023.122442.
[17] International Atomic Energy Agency. (2024). *Two years of IAEA continued presence at the Zaporizhzhya nuclear power plant.* Retrieved from https://surl.li/hhhyvz.
[18] International Committee of the Red Cross. (n.d.). *Protecting civilians against digital threats during armed conflict: Recommendations to states, belligerents, tech companies and humanitarian organizations*. Retrieved from https://surl.li/sltbau.
[19] Irankunda, G., Zhang, W., Fernand, M., & Zhang, J. (2024). Assessing the resilience of critical infrastructure facilities toward a holistic and theoretical approach: A multi-scenario evidence and case study. *Sustainability*, 16(20), article number 8735. doi: 10.3390/su16208735.
[20] Iskoujina, Z., Gnatchenko, Y., & Bernal, P. (2024). Social media as an information warfare tool in the Russia-Ukraine war: A systematic literature review. In *EventCenter for informed democracy & social – cybersecurity (IDeaS) annual conference*. Pittsburgh: Carnegie Mellon Univeristy.
[21] ISO 31000:2018. (2018). *Risk management – guidelines*. Retrieved from https://surl.li/epiiha.
[22] King, A. (2024). Digital targeting: Artificial intelligence, data, and military intelligence. *Journal of Global Security Studies*, 9(2), article number ogae009. doi: 10.1093/jogss/ogae009.
[23] Law of Ukraine No. 2163-VIII "On the Basic Principles of Cybersecurity in Ukraine". (2017, October). Retrieved from https://zakon.rada.gov.ua/laws/show/en/2163-19#Text.
[24] Law of Ukraine No. 2469-VIII "On National Security of Ukraine". (2018, June). Retrieved from https://zakon.rada.gov.ua/laws/show/2469-19#Text.
[25] Law of Ukraine No. 389-VIII "On the Legal Regime of Martial Law". (2015, May). Retrieved from https://zakon.rada.gov.ua/laws/show/389-19.
[26] Małodobry, Z., Nastaj-Sałek, K., Cyrkun, K., & Jakubiec, W. (2024). Application of artificial intelligence in modern weapon systems – opportunities and threats in armed conflicts. *Scientific Journal of Bielsko-Biała School of Finance and Law*, 28(4), 56-60. doi: 10.19192/wsfip.sj4.2024.8.
[27] Mitoulis, S.-A., Argyroudis, S., Panteli, M., Fuggini, C., Valkaniotis, S., Hynes, W., & Linkov, I. (2023). Conflict-resilience framework for critical infrastructure peacebuilding. *Sustainable Cities and Society*, 91, article number 104405. doi: 10.1016/j.scs.2023.104405.
[28] Mohamed, N. (2025). Artificial intelligence and machine learning in cybersecurity: A deep dive into state-of-the-art techniques and future paradigms. *Knowledge and Information Systems*, 67, 6969-7055. doi: 10.1007/s10115-025-02429-y.
[29] Murphy, M., Sharpe, E., & Huang, K. (2024). The promise of machine learning in violent conflict forecasting. *Data & Policy*, 6, article number e35. doi: 10.1017/dap.2024.27.
[30] 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. doi: 10.1080/01402390.2025.2463451.
[31] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I). (1978, December). Retrieved from https://surl.li/wvqnsq.
[32] Rapid environmental assessment of Kakhovka Dam Breach Ukraine, 2023. (2023). Retrieved from https://www.unep.org/resources/report/rapid-environmental-assessment-kakhovka-dam-breach-ukraine-2023.
[33] Rizk, J., & Cordey, S. (2023). *What we don't understand about digital risks in armed conflict and what to do about it*. Retrieved from https://blogs.icrc.org/law-and-policy/2023/07/27/digital-risks-in-armed-conflict/.
[34] Robinson, E., Egel, D., & Bailey, G. (2023). *Machine learning for operational decision-making in competition and conflict: A demonstration using the conflict in eastern Ukraine*. Retrieved from https://surl.li/anhkoj.
[35] Rød, E.G., Gåsste, T., & Hegre, H. (2024). A review and comparison of conflict early warning systems. *International Journal of Forecasting*, 40(1), 96-112. doi: 10.1016/j.ijforecast.2023.01.001.
[36] Scher, C., & Van Den Hoek, J. (2025). Active InSAR monitoring of building damage in Gaza during the Israel-Hamas War. *ArXiv*. doi: 10.48550/arXiv.2506.14730.
[37] Semenenko, O., Palamarchuk, S., Poberezhets, T., Palamarchuk, N., & Mytchenko, S. (2025). Cybersecurity in modern armed conflicts: Threats and responses. *International Journal of Advances in Soft Computing and its Application*, 17(1), 32-48. doi: 10.15849/IJASCA.250330.03.
[38] Sendai Framework for Disaster Risk Reduction 2015-2030. (2015). Retrieved from https://www.undrr.org/publication/sendai-framework-disaster-risk-reduction-2015-2030.

[39] Sinha, A., Rout, B., Mohanty, S., Mishra, S.R., Mohapatra, H., & Dey, S. (2024). Exploring sentiments in the Russia-Ukraine conflict: A comparative analysis of KNN, decision tree, and logistic regression machine learning classifiers. *Procedia Computer Science*, 235, 1068-1076. doi: 10.1016/j.procs.2024.04.101.
[40] Skomra, W., & Wojtasik, K. (2025). Critical infrastructure as a target for hybrid operations: Case studies of attacks against the facilities and systems of CI. *Terrorism – Studies, Analyses, Prevention*, 2025, 13-34. doi: 10.4467/27204383TER.25.013.21516.
[41] Special meeting of the Permanent Council (1368th Plenary Meeting). (2022). Retrieved from https://www.osce.org/files/f/documents/2/5/518964.pdf.
[42] Sporyshev, K., Pasichnyk, A., & Morokhovskyi, M. (2024). Problematic aspects of information and analytical support for the management bodies of Ukraine's security forces. *Security Studies*, 2(4), 78-82. doi: 10.33405/2786-8613/2024/2/4/323379.
[43] Sticher, V., Wegner, J.D., & Pfeifle, B. (2023). Toward the remote monitoring of armed conflicts. *PNAS Nexus*, 2(6), article number pgad181. doi: 10.1093/pnasnexus/pgad181.
[44] Wang, Y., Li, Y., & Zhang, S. (2025). Automatic detection of war-destroyed buildings from high-resolution remote sensing images. *Remote Sensing*, 17(3), article number 509. doi: 10.3390/rs17030509.

Інформаційно-аналітичне забезпечення управління ризиками загроз під час бойових дій

Андрій Ковтун

Кандидат технічних наук, старший викладач
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
03056, просп. Берестейський, 37, м. Київ, Україна
https://orcid.org/0000-0003-4490-0484

Олена Землянська

Старший викладач
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
03056, просп. Берестейський, 37, м. Київ, Україна
https://orcid.org/0000-0002-9608-3677

Наталія Праховнік

Кандидат технічних наук, доцент
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
03056, просп. Берестейський, 37, м. Київ, Україна
https://orcid.org/0000-0003-0821-2166

Оксана Ільчук

Кандидат технічних наук, старший викладач
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
03056, просп. Берестейський, 37, м. Київ, Україна
https://orcid.org/0000-0001-6352-5320

Анотація. Метою дослідження було виявлення особливостей побудови та застосування аналітичних систем у процесах оцінки й мінімізації воєнних ризиків. Методологія базувалась на структурно-функціональному, порівняльному і системно-аналітичних методах. Встановлено, що ідентифікація загроз під час бойових дій ґрунтується на інтеграції багатоджерельних даних і охоплює чотири взаємопов'язані типи ризиків – фізичні, техногенні, інформаційні та психологічні. Фізичні ризики пов'язані з руйнуванням критичної інфраструктури, зокрема під час оборони Києва в 2022 році та обстрілів у секторі Газа в 2023 році, техногенні наслідки, як прорив Каховської дамби у 2023 році й пошкодження Запорізької атомної електричної станції, спричинили затоплення понад 600 км^2 і потребували цілодобового моніторингу Міжнародного агентства з атомної енергії. У 2022-2024 зафіксовано понад 20,000 кібератак, а гібридні загрози, поєднуючи фізичні, кібер- та психологічні впливи, дестабілізують державу й суспільство. Виявлено, що ключовим інструментом реагування є інформаційно-аналітична система з багаторівневою архітектурою збору, обробки й візуалізації даних, що використовує Big Data, Machine Learning і прогнозне моделювання для оцінки ризиків та підтримки рішень у

реальному часі. Порівняння України, Гази та Бурунді показало різні етапи розвитку інформаційно-аналітичної системи: в Україні система забезпечує реагування протягом «години – доби» та інтегрує дані з різних джерел. У Газі система має гуманітарний характер, щоденно оновлюючи дані про понад 4,500 зруйнованих об'єктів, у Бурунді – resilience-індекс інфраструктури з кількаденним лагом і щотижневою корекцією ризиків. Найбільш ефективною є гібридна модель, що поєднує міжнародні стандарти й національні ресурси, забезпечуючи швидке реагування та довгострокову стійкість у постконфліктних умовах. Практична значущість полягає у можливості використання результатів державними, аналітичними та гуманітарними структурами для швидшого реагування та захисту інфраструктури під час бойових дій

Ключові слова: фізичні руйнування; прогнозне моделювання; ситуаційна обізнаність; стійкість інфраструктури; кібератаки; психологічний вплив; гуманітарна аналітика