ROMANIAN
MILITARY
THINKING

INTEGRATING ARTIFICIAL INTELLIGENCE INTO OPERATIONAL RESEARCH – NEW HORIZONS FOR NATIONAL SECURITY –

Associate Professor Florentina Loredana DRAGOMIR, PhD
"Carol I" National Defence University
DOI: 10.55535/RMT.2025.1.08

The article analyzes the role of artificial intelligence (AI) and operational research in national security, highlighting their contributions to optimizing decision-making processes and risk management. AI facilitates rapid data analysis, threat forecasting, and automated crisis responses, while operational research improves resource allocation and conflict management. This paper presents the integration of advanced operations research and artificial intelligence (AI) techniques in drone operations, highlighting how these fields contribute to the optimization of flight operations. It explores the use of optimization algorithms for route planning and management of drone fleets, as well as the implementation of AI for their autonomization, improving efficiency, performance, and cost of operations. The article highlights this interconnectedness that transforms operational processes, providing intelligent and scalable solutions.

Keywords: operational research; artificial intelligence; vulnerabilities; national security; algorithms;

INTRODUCTION

In the digital age, national security has evolved significantly, given that threats no longer come only from traditional armed conflicts, but also from complex and often invisible areas, such as cyber attacks, information warfare and natural disasters managed through advanced technologies. The concept of *national security* has now expanded to include not only the physical defence of a nation, but also the protection of critical infrastructure, sensitive data and economic and political integrity. As technologies rapidly advance, national security is becoming increasingly dependent on the use of IT solutions and artificial intelligence (AI), which can analyse and anticipate emerging threats much more effectively than traditional methods.

The concept of "national security" has now expanded to include not only the physical defence of a nation, but also the protection of critical infrastructure, sensitive data and economic and political integrity. As technologies rapidly advance, national security is becoming increasingly dependent on the use of IT solutions and artificial intelligence.

This progress is influencing international relations and global cooperation structures, intensifying competition between world powers. The USA and the EU are consolidating their position as normative leaders in the field, while China and Russia are seeking to integrate AI in a sustainable and secure way to enhance their military, economic and strategic capabilities. At the same time, states are faced with the challenge of preventing unacceptable risks to critical infrastructure and essential digital systems in a globalized world. Any military activity involves organizing forces and coordinating them according to time, space and strategic objectives. The combat power of a dominant component influences the entire combined force, and operational success depends on effective organization and leadership. A major challenge is the accessibility of artificial intelligence technologies, which can be quickly adapted to improve security or to counteract previous versions. In this context, a deep understanding of the capabilities of all actors involved, of the intentions of the adversaries and of the specifics of the operational environment is essential. Also crucial is the analysis of the interdependence between the different areas and dimensions of the conflict. Given the complexity of military activities, from logistics to direct combat engagements,

a careful assessment of the main challenges and conditions for ensuring the security of the armed forces is necessary, especially in the context of the increasing lethality of modern weapons and combat systems.

Operational research and artificial intelligence play an essential role in this context, transforming the way strategic decisions are made in national security. Operational research, through mathematical models and advanced simulations, allows for the analysis and optimization of resources in a more efficient way, thus helping to manage complex situations and plan more precise responses to threats. In parallel, artificial intelligence is bringing about a significant change, through its ability to process large volumes of data in an extremely short time, to identify hidden patterns and to anticipate risks, helping decision-makers to respond quickly and effectively to various scenarios.

National security operations research is an essential branch of decision science that uses mathematical and statistical techniques to analyse and optimize processes and resources for strategic and operational purposes. This operational research is applicable in a wide range of areas of national security, including defence, intelligence, crisis management, and critical infrastructure protection.

The objective of this article is to analyse modern methods used to optimize national security, focusing on operational research and artificial intelligence technologies as fundamental tools in improving the decision-making process. It presents how these innovative techniques are implemented to protect national interests, ensuring that nations are prepared to respond effectively to a wide range of threats using drones.

OPERATIONAL RESEARCH METHODS IN DRONE OPERATIONS

National security operations research is an essential branch of decision science that uses mathematical and statistical techniques to analyse and optimize processes and resources for strategic and operational purposes. This operational research is applicable in a wide range of areas of national security, including defence, intelligence, crisis management, and critical infrastructure protection.

The definition of operational research is closely related to the systematic analysis of complex processes to find optimal or near-optimal solutions under conditions of uncertainty and limited resources. It relies on mathematical, statistical, and computational methods to model and analyse situations involving multiple choices, usually under conditions of risk and uncertainty. In the context of national security, operational research is used to evaluate the effectiveness of different scenarios and to support the development of strategies to respond quickly

and effectively to national or international crises. A fundamental aspect of operational research is the use of mathematical models and algorithms for risk analysis and resource allocation. As in the field of national security, risks can come from multiple sources, such as armed conflicts, cyber attacks, natural disasters, or terrorism. Optimization models, simulation models and forecasting models are used to analyse these risks, assess their impact on security and determine the most effective possible responses. Resource optimization algorithms can help to efficiently allocate equipment and personnel in emergency situations, ensuring that resources are used efficiently and that reaction time is minimized. Conflict simulation models can be used to analyse different war scenarios and to evaluate the effectiveness of defence tactics and strategy. They can contribute to the development of more effective defence plans that minimize losses and maximize success in the face of a threat. In intelligence, operational research can be used to optimize information collection and analysis, identifying the most important sources of information and allocating resources effectively to prevent and combat threats. Data analysis algorithms can help detect patterns and anticipate adversary behaviour, thus contributing to strategic decision-making based on relevant and accurate information. In terms of crisis management, operational research can inform the planning and coordination of rapid responses. For example, in the case of a terrorist attack or a natural disaster, operational research can be used to assess available resources and determine the most efficient ways to allocate them, so as to minimize damage and loss of life. Resource distribution optimization models can be applied to ensure that aid is delivered quickly and equitably to those who need it. Also, during a crisis, simulation models of the evolution of events can help authorities anticipate the development of the situation and adapt strategies in real time to respond to emerging challenges. Drones are experiencing a continuous development. They are not a myth of national security; they have become a necessity. Unmanned Aircraft Systems have also been deployed in all military services, ranging from man-portable micro-UAVs (Unmanned Aircraft) to medium-sized tactical systems and large unmanned aircraft. The continued development of this technology, together with improvements in sensors, batteries, and navigation systems, will open up new possibilities for use

Conflict simulation models can be used to analyse different war scenarios and to evaluate the effectiveness of defence tactics and strategy. They can contribute to the development of more effective defence plans that minimize losses and maximize success in the face of a threat.

and improved performance. Today's security environment is characterized by significant changes not only in terms of the relevance of regional and global actors but also in the characteristics of the environment in which confrontations take place, as well as in terms of the objectives for optimal management of the problem. As a result, Romania is obliged to adapt to the geopolitical and geostrategic conditions in the wider Black Sea region. Operational research adds value to Unmanned Aircraft Systems by optimizing cost and efficiency, features that are based on advanced optimizations such as linear programming, Monte Carlo simulation, and a wide range of genetic algorithms (Dragomir, 2017-i). These various genetic algorithms, combined with artificial intelligence, solve tasks of high complexity in the area of energy reduction, route optimization, and drone fleet coordination. The expectation theory underpins transport time optimization and optimal management of aircraft resources, being thus logistically useful (Dragomir, 2017-j). Reduced energy consumption facilitates rigorous flight planning for the inspection of critical infrastructures such as power lines, dams, bridges, and points of economic interest in a minimum time.

Today's security environment is characterized by significant changes not only in terms of the relevance of regional and global actors but also in the characteristics of the environment in which confrontations take place, as well as in terms of the objectives for optimal management of the problem. As a result, Romania is obliged to adapt to the geopolitical and geostrategic conditions in the wider Black Sea region.

Tasks and resources are allocated through task and resource selection algorithms, knowing which drones are best suited for particular missions. Drones and drone swarms are provided with algorithms inspired by the collective behaviours of insects to coordinate the movements of large groups of drones, which is beneficial in search and rescue operations or military applications. Using these advanced optimization methods, drones can work together efficiently, avoiding collisions and maximizing spatial coverage in reconnaissance operations or synchronized attacks. Stochastic models represent that part of operational research that helps to make average decisions under risk and uncertainty, and military environments share this aspect (Dragomir, 2017-d). They are used to assess the likelihood of certain scenarios, such as the unfolding of attacks or the occurrence of threats (Dragomir, 2017-b). By analysing risks and possible outcomes, these models allow drones to plan appropriate responses (Dragomir, 2017-c). Network flow modelling and linear programming techniques are often used for resource allocation and complex logistics planning to ensure efficient supply during military operations, especially in conflict-restricted areas (Dragomir, 2017-h). In support of low-cost resupply decisions, multi-criteria analysis comes with the evaluation of alternatives based on several criteria when planning operations or allocating resources according to factors such as cost, risk, or efficiency (Dragomir, 2017-g). To get the clearest possible picture of the risks and opportunities associated with each decision, operational research comes up with the technique of Monte Carlo simulations, in which military scenarios are modelled in order to analyse the effectiveness of the air defence system against drone attacks (Dragomir, 2017). Game theory supplements the war scenario with optimal conflict strategies. In the case of drones, cyber conflicts are often modelled because, by anticipating the adversary's actions, appropriate defence responses can be developed (Yang, Liu, 2022). Based on this analysis, prevention and response strategies are developed.

Game theory supplements the war scenario with optimal conflict strategies. In the case of drones, cyber conflicts are often modelled because, by anticipating the adversary's actions, appropriate defence responses can be developed.

ARTIFICIAL INTELLIGENCE ALGORITHMS ON BOARD THE UAS

The specialized literature describes the equipping of force structures with unmanned aircraft systems (UAS) intended to collect data and information of military interest. *Table 1* centralizes the categories of AI algorithms and associates them with the area of applicability of the software present on board a UAS, thus making a correlation with the degree of usefulness of the drone.

Table 1: Categories of AI algorithms used on board UAS
(author's adaptation based on Kour, Jha, 2023)

Algorithm category	Method/algorithm	Applicability
Navigation and Route Planning Algorithms	Algorithms A and Dijkstra	Use to find the shortest routes between points of interest, avoiding obstacles.
	RERT (Rapidly-Exploring Random Tree) and ORERT (Optimized RERT)	Algorithms used for route planning in complex and dynamic environments.

Algorithm category	Method/algorithm	Applicability
Obstacle Avoidance Algorithms	DWA (Dynamic Window Approach)	Algorithm that plans short-term movements to avoid collisions with moving obstacles.
	Potential Field Method	It creates a *"force field"* around obstacles, allowing the UAV to navigate around them.
Computational recognition algorithms and object recognition	Convolutional Neural Networks (CNN)	Used to detect and classify objects in images and video captured by UAVs.
	YOLO (You Only Look Once) and SSD (Single Shot Multibook Detector)	Real-time object detection algorithms for applications such as surveillance and monitoring.
Data Fusion Algorithms	Kalman Filters and Particle Filters	Used to combine data from multiple sources (e.g., GPS, IMU, cameras) for an accurate estimation of the UAV's position and motion.
	SLAM (Simultaneous Localization and Mapping)	Algorithms that allow UAVs to build maps of their environment and localize themselves at the same time.
Machine learning and reinforcement learning algorithms	Deep Q-Learning is Proximal Policy Optimization (PPO)	Reinforcement learning algorithms used to improve autonomous flight performance through experience and exploration.
	Classification and regression algorithms	Use to analyse and interpret collected data, such as identifying suitable landing terrains or estimating environmental parameters.

Algorithm category	Method/algorithm	Applicability
Control and stabilization algorithms	Proportional-Integral-Derivative (PID) Control	Used for stabilization and flight control of UAVs.
	Predictive Control Model (PCM)	Advanced control algorithm that optimizes UAV movements to meet dynamic and environmental constraints.
Speech recognition and processing algorithms	Recursive Neural Networks (RNN)	Voice command recognition.
	Long Short-Term Memory (LSTM)	Interaction with human operators.
Cybersecurity and data protection algorithms	AI-based intrusion detection systems	Algorithms that monitor and identify abnormal or malicious activities in UAS networks.
	Advanced cryptography	Using AI to improve encryption techniques and protect data transmitted between UAVs and control stations.
Multi-sensor fusion algorithms	Fusion algorithms based on neural networks	Combining data from different sensors (optical, thermal, LIDAR) to create a more complete and accurate understanding of the environment.
	Deep learning techniques	Used to improve the interpretation and fusion of data from various sources.

While AI brings a high degree of autonomy and functionality to UASs, its implementation must be accompanied by stringent cybersecurity measures and extensive testing to reduce vulnerabilities.

While AI brings a high degree of autonomy and functionality to UASs, its implementation must be accompanied by stringent cybersecurity measures and extensive testing to reduce vulnerabilities (Dragomir, 2017-a; Garling, Nilson, 2022; Li, Zheng, 2021). Investments in robust systems and continuous monitoring processes are essential

to maximize AI benefits and minimize associated risks (Mor, 2019; Tan, Yao, 2023; Zhang, Chen, 2023). Adversaries can exploit AI networks through adversarial attacks, in which they introduce data designed to trick the system (e.g., subtly altered images to avoid detection) thus registering attacks on neural networks (Dragomir, 2017-f; Han, Jiang, 2020; Yang, Nang, 2023). If AI algorithms are not configured to unexpected situations, such as there is over-reliance on autonomy, UASs can make decisions that compromise the mission (Dragomir, 2017-e; Kour, Jha, 2023; Martin, Wang, 2021). As vulnerabilities, we can list delays in processing critical information, manipulation of training data by injecting corrupted data into the learning process through cyber-attacks, and spoofing (Nguyen, Patel, 2020; Zhang, Chen, 2023; Aitech, 2020). GPS spoofing or jamming attacks can severely affect the autonomous navigation of a UAS, leading to course deviation or even crash. Communication vulnerabilities between the drone and the control station can be exploited to take control of the UAS.

Over the past few decades, technology has advanced at a rapid pace, and autonomous systems, such as Lethal Autonomous Weapons Systems (LAWS) and some categories of drones, have been developed to make rapid decisions on the battlefield, without the direct intervention of a human operator.

THE NEED FOR REGULATION AND INTERNATIONAL COOPERATION IN THE USE OF EMERGING TECHNOLOGIES

The use of artificial intelligence in the field of national security raises a number of ethical issues and dilemmas that are difficult to manage, with a significant impact on fundamental human rights and on the way armed conflicts are managed. One of the greatest ethical concerns is related to autonomous decisions in armed conflicts. Over the past few decades, technology has advanced at a rapid pace, and autonomous systems, such as Lethal Autonomous Weapons Systems (LAWS) and some categories of drones, have been developed to make rapid decisions on the battlefield, without the direct intervention of a human operator. It may seem effective in managing some conflicts, but it raises fundamental questions related to the responsibility and control over the actions of automated systems. Moreover, these weapons can be used in ways that violate international humanitarian law, which regulates the use of force in armed conflicts and protects civilians and prisoners of war. Thus, the use of AI in this context raises not only concerns about efficiency, but also about morality and human rights. Another significant ethical dilemma arises from the use

of AI for mass surveillance and monitoring of citizens using drones. Advanced technologies such as facial recognition, behavioural analysis and communication processing allow governments to monitor almost every aspect of their citizens' daily lives, from their physical movements to their online interactions. While such technologies can be useful in combating crime or terrorism, they create a surveillance society, in which privacy is compromised and the state can exercise excessive control over individual behaviour and choices. As artificial intelligence becomes an increasingly central tool in national security strategies, it becomes obvious that the creation of clear and effective regulatory frameworks is essential to prevent the misuse of this technology and to ensure a balance between security needs and respect for the fundamental rights of citizens. International organizations such as the UN have begun to address this issue, but there are still gaps in international law regarding the use of lethal autonomous weapons in armed conflicts. Autonomous weapons, which can make decisions to attack without human intervention, pose a significant risk, as there is no clear legal framework to regulate their use and establish responsibility in case of errors or abuse. It is necessary to develop treaties and agreements at a global level that strictly regulate the use of these weapons, to prevent possible abuses and to ensure that their use respects the principles of international humanitarian law. Another important point is international collaboration against cyberattacks, which represent a major threat in the digital age. States must cooperate internationally not only to combat cyberattacks, which can target critical infrastructure, but also to prevent the use of AI by terrorist groups or hostile states. Cyber threats do not respect borders and can have serious consequences for national and international security. It is essential for states to establish mechanisms for international cooperation, which include information sharing, coordination of responses and the application of clear sanctions for cyberattacks. Global monitoring systems must also be created to detect and prevent misuse of emerging technologies. Finally, to ensure the responsible use of AI in national security, it is crucial that governments and international organizations should establish mechanisms for transparency and accountability. They must include oversight and audit measures to verify how AI is used for security purposes, ensuring

ROMANIAN MILITARY THINKING

Autonomous weapons, which can make decisions to attack without human intervention, pose a significant risk, as there is no clear legal framework to regulate their use and establish responsibility in case of errors or abuse. It is necessary to develop treaties and agreements at a global level that strictly regulate the use of these weapons, to prevent possible abuses and to ensure that their use respects the principles of international humanitarian law.

that it complies with ethical and legal norms. It is important that any decision based on AI should be explainable and subject to external scrutiny, to prevent errors and abuses. Clear standards of accountability for decisions made by automated systems must also be established, so that there could be no ambiguity about who is responsible in the event of failure. Appropriate regulation of the use of AI in the field of national security to prevent risks and abuses, as well as to ensure that these technologies are used in a responsible and ethical manner, international collaboration and compliance with global legal norms are essential to building a balanced global security framework that protects both national interests and fundamental human rights.

CONCLUSIONS

Artificial intelligence contributes to automating processes, analysing data in a faster and more efficient way, and predicting risks, all of which having a significant impact on national security.

Artificial intelligence and operational research are essential pillars in optimizing national security and supporting strategic decisions in the face of increasingly complex and diversified threats. AI contributes to automating processes, analysing data in a faster and more efficient way, and predicting risks, all of which having a significant impact on national security. Operational research, with a focus on mathematical models and resource optimization, also underpins the efficient allocation of resources in crisis situations and risk management, being a tool for analysing and making strategic decisions in the fields of defence, intelligence, and crisis management. In this context, combining the two fields brings considerable benefits.

The directives aimed at integrating AI into national defence strategies are multiple and promise to revolutionize the way in which states protect their national security. These directions include the development of autonomous defence systems capable of responding in real time to emerging threats, improving cyber monitoring and protection, and optimizing the planning and coordination of military operations through advanced data analysis. In addition, the integration of AI can support the process of detecting and preventing terrorist attacks or combating cybercrime through algorithms that can identify unusual patterns and signal possible risks. As technology evolves, AI will become increasingly present within security structures, with the potential to address the increasingly complex challenges of this era. Integrating operational research with artificial intelligence opens new perspectives for drone autonomy. Predictive modelling and machine learning enable rapid adaptation to environmental conditions and optimization of decisions in real time. It makes drone applications more versatile and efficient, from emergency deliveries to natural disaster management.

In conclusion, operational research is an indispensable foundation for maximizing the potential of drones, helping to make them essential tools for a variety of domains. Operational research combined with artificial intelligence continues to revolutionize the field of military security, ensuring a faster and more effective response to modern threats.

BIBLIOGRAPHICAL REFERENCES:

1. Aitech (2020, December/January). *Artificial intelligence efforts for military drones.* Avionics – digital ed., https://interactive.aviationtoday.com, retrieved on 12 January 2025.
2. Dragomir, F. (2017-a). *Artificial Intelligence Techniques Cybersecurity*, in *Proceedings of International Scientific Conference Strategies XXI*, vol. 3, pp. 147-152.
3. Dragomir, F. (2017-b). *Application of the method of covering zeros in decision-making foundations, International Scientific Conference Strategies XXI. The Complex and Dynamic Nature of the Security Environment*, pp. 342-347.
4. Dragomir, F. (2017-c). *Effectiveness of the use of forces and means of fighting*, ib., pp. 342-352.
5. Dragomir, F., Alexandrescu, G. (2017-d). *The axiomatic character of decision,* in *Bulletin of "Carol I" National Defence University*, Vol. 6, pp. 16-22.
6. Dragomir, F. (2017), Dragomir, F. (2017-e). *Modelling of decisional problems*, in *Bulletin of "Carol I" National Defence University*, vol. 1, pp. 72-75.
7. Dragomir, F. (2017-f), *Applications of Artificial Intelligence in Decision-Making*, in *Bulletin of "Carol I" National Defence University*, vol. 4, pp. 56-61.
8. Dragomir, F. (2017-g). *Eficacitatea unui sistem de întreținere a pierderilor*, in *Analele – Seria de științe militare*, vol. 9, pp. 97-105.
9. Dragomir, F. (2017-h). *Mathematical Models Specific to the Military Domain*, in *Strategic Impact*, no. 64, pp. 62-67.
10. Dragomir, F. (2017-i). *Aplicații de programare liniară*, in *Buletinul Universității Naționale de Apărare "Carol I"*, vol. 4, pp. 59-64.
11. Dragomir, F. (2017-j). *Efficiency action soldier using theory graphs*, in *Bulletin of "Carol I" National Defence University*, vol. 2, pp. 48-55.

12. Gärling, P., Nilsson, M. (2022). *Artificial Intelligence Applied to Drone Control: A State of the Art*. In *International Journal of Robotics and Automation*, 37(4), pp. 211-226, https://doi.org/10.1201/9780367334370, retrieved on 2 February 2025.
13. Han, Z., Jiang, L. (2020). *Path planning algorithms for autonomous UAVs in dynamic environments*. In *Journal of Robotics*, 21(4), pp. 372-385, https://doi.org/10.1007/s12838-020-00291-0, retrieved on 22 January 2025.
14. Kour, H., Jha, S. (2023). *Enhancing drone autonomy using AI-powered algorithms*. In *Journal of Aerospace Engineering*, 36(5), pp. 52-63, https://doi.org/10.1061/(ASCE)AS.1943-5525.0000930, retrieved on 11 February 2025.
15. Li, W., Zheng, Z. (2021). *Enhancing UAV swarm tactics with edge AI: Adaptive decision making in changing environments*. MDPI Sensors, 21(13), 4432, https://doi.org/10.3390/s21134432 retrieved on 2 February 2025.
16. Martin, J., Wang, Q. (2021). *UAV swarm intelligence: Recent advances and future trends*. In *Journal of Swarm Intelligence*, 17(3), pp. 334-355, https://doi.org/10.1007/s11721-020-00186-2, retrieved on 22 January 2025.
17. Mor, D. (2019). *Artificial Intelligence efforts for military drones*. Avionics – Digital ed., 22(1), pp. 58-72, https://interactive.aviationtoday.com, retrieved on 17 February 2025.
18. Nguyen, T., Patel, S. (2020). *Research on unmanned aerial vehicle path planning: challenges and opportunities*. Aerospace Systems, 8(2), pp. 28-45, https://doi.org/10.1117/12.2547178, retrieved on 2 February 2025.
19. Patel, R., Thakur, P. (2021). *AI-based algorithms for autonomous drone navigation in real-time environments.* Robotics, 8(5), pp. 112-128, https://doi.org/10.1007/s11432-021-3432-x, retrieved on 22 January 2025.
20. Tan, R., Yao, F. (2023). *Artificial Intelligence in drone applications: Special issue*. In *Journal of Unmanned Systems*, 15(2), pp. 11-35, https://doi.org/10.1007/s40787-023-00192-7, retrieved on 22 January 2025.
21. Tan, X., Li, H. (2022). *Reinforcement learning for UAV path optimization*. In *Journal of Computational Intelligence*, 15(6), pp. 654-671, https://doi.org/10.1007/s10207-022-02059-5, retrieved on 12 January 2025.
22. Yang, H., Liu, X. (2022). *An optimization framework for efficient vision-based autonomous drone navigation*. In *Journal of Robotics*, 38(1), pp. 79-94, https://doi.org/10.1007/s11340-022-00475-x, retrieved on 17 February 2025.
23. Yang, J., Wang, T. (2023). *AI-driven multi-agent systems for autonomous drone swarms: design and control*. In *Artificial Intelligence Review*, 62(3), pp. 2451-2472, https://doi.org/10.1007/s10462-023-10078-w, retrieved on 22 January 2025.

24. Zhang, D., Liu, Y. (2021). *Machine learning in drone navigation and obstacle avoidance*. In *Journal of Artificial Intelligence*, 34(7), pp. 492-506, https://doi.org/10.1109/JAI.2021.3232290, retrieved on 22 January 2025.
25. Zhang, Y., Chen, L. (2023). *Hybrid machine learning and reinforcement learning framework for adaptive UAV obstacle avoidance*. Robotics and Autonomous Systems, 162, 103315, https://doi.org/10.1016/j.robot.2022.103315, retrieved on 2 February 2025.