MACHINE LEARNING DECISION SUPPORT IN DEFENSE SYSTEMS

Ibidun C.A.[1], Nasirov E.V.[2], Akhundov R.G.[2], Hashimov E.G.[2,3]
Sol Plaatje University, Kimberley, South Africa
National Defense University, Baku, Azerbaijan
Azerbaijan Technical University, Baku, Azerbaijan

This article examines machine learning based decision support in defense systems through an integrated analytical framework that combines effectiveness measurement, threat resilience, and auditable governance. The study is motivated by the growing use of machine learning in cybersecurity, military logistics, and autonomous decision-making, where operational value depends not only on predictive accuracy but also on timeliness, stability under adversarial pressure, resource efficiency, and accountability. In defense settings, a technically accurate model cannot be considered operationally sufficient if it is vulnerable to false alarms, delayed reactions, manipulation of input data, or opaque decision logic. The aim of the study is therefore to develop a unified methodological structure in which machine learning solutions can be evaluated as operational decision mechanisms rather than as isolated technical models.

The methodology treats the defense system as a multi-component decision environment functioning under antagonistic conditions. A generalized objective function is introduced in which achieved operational benefit is balanced against risk and resource-economic cost. Within this structure, a unified set of EFG indicators is defined for the three main application domains. In cybersecurity, the key indicators include detection probability, false alarm rate, and response delay. In logistics, the framework evaluates on-time delivery probability, route resilience, and inventory balance. In autonomous decision mechanisms, the emphasis is placed on explainability, thresholds for human oversight, and constraints related to civilian risk. These indicators are normalized and linked to scenario-based evaluation, allowing structured comparison across nominal and adversarial regimes.

A central feature of the proposed framework is that machine learning performance is tested not only under ordinary operating conditions but also under deliberate adversarial influences such as data poisoning, adversarial examples, and sensor deception. For each scenario, the degradation trajectory of effectiveness indicators is assessed separately. The article shows that aggregate measures may conceal critical weaknesses in subordinate threat classes and that operational assessment should therefore be performed by sub-scenarios rather than by average values alone. The discussion further demonstrates that false alarms in cybersecurity create a dual burden by simultaneously increasing operational risk and resource consumption, while resilience gains in logistics often produce nonlinear cost escalation rather than proportional benefit.

The study also argues that auditability must be embedded directly into the decision cycle. Decision traces, input data, applied rules, and critical threshold crossings should be recorded systematically, and transfer to human oversight must

function as an internal control mechanism rather than as an external procedural formality. The overall conclusion is that machine learning can become a justified and effective instrument in defense systems only when three conditions are satisfied simultaneously: effectiveness is standardized through measurable EFG indicators, resilience is tested across adversarial scenarios, and governance is supported by audit, explainability, and human oversight. Under these conditions, machine learning based solutions acquire operational credibility and become suitable for real defense applications.

References

1. Ibrahimov B.G. Information security research special-purpose telecommunication systems using machine learning technology. *In* Problems of informatization. 2024. 1, 87-88.
2. Islamov, I., et al. Big data analytics and machine learning for predicting radiation and chemical threats in the military sphere. *Collection of Scientific Papers «SCIENTIA»*, (September 26, 2025; Kraków, Poland), 30–38.
3. Dergachov K., et al. AI based physical and cyber defense for energy grids and transportation systems. *In* Problems of informatization. 2025. Vol. 1., section 1,2. p.75-78
4. Krikun, V.L., et al. Accelerating decision making and operational efficiency through C4ISR architecture / Problems of informatization. 2025, Vol. 2., section 3,7. p.120-121
5. Radovanović M. et al. Application of the new hybrid model LMAW-G-EDAS multi-criteria decision-making when choosing an assault rifle for the needs of the army //Journal of decision analytics and intelligent computing. – 2024. – Т. 4. – №. 1. – С. 16-31.
6. Akhundov R.G., Hashimov E.G. Enhancing the physical protection of critical facilities through the integration of physical process models and machine learning. Grail of Science, № 61 (January 2026). P.722-731.
7. Huseynov B.S. et al. Multisensor detection architectures on UAV platforms: methodology, indicators and implementation in Azerbaijan / Problems of informatization. 2025, Vol. 2., section 3,7. -p.p.132-134
8. Muradov S.A., Huseynov B.S., Akhundov R.G., Hashimov E.G. System-level methods for enhancing UAV flight safety and resource efficiency / Problems of informatization. 2025, Vol. 2., section 3,7. p.124-126
9. Bayramov A. A. et al. SMART control system of systems for dynamic objects group //Bulgarska Voenna Misal.–2018. – 2018.
10. Hashimov E., Khaligov G. The issue of training of the neural network for drone detection //Advanced Information Systems. – 2024. – Т. 8. – №. 3. – С. 53-58.
11. Teymurov M., et al. Multi-criteria optimization of UAV routes through integration of a risk map and communication quality. *In* Current issues of science, prospects and challenges: Collection of Scientific Papers «SCIENTIA». Sydney, Australia. 2026. P.107-116
12. Hashimov, E.G. et al. (2016). Terrain orthophotoplanes making for military objects revealing. *National security and military sciences*, *2*(4), 14-20.
13. Nasibov, Y.A. et al. (2019). Modelling of the rationally deployment of observing systems. *Сучасні інформаційні системи*, (3,№ 2), 10-13.
14. Hashimov, E.G. (2017). GIS technology and terrain orthophotomap making for military application. *Journal of Defense Resources Management*, *8*(2), 81-90.