Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas

Eureka Journal of Education & Learning Technologies (EJELT)

ISSN 2760-4918 (Online) Volume 2, Issue 11, November 2026

This article/work is licensed under CC by 4.0 Attribution

https://eurekaoa.com/index.php/2

DESIGN AND EVALUATION OF AN INTERDISCIPLINARY TRAINING MODULE ON AI AND UAV SECURITY

Batirov Dilshod Bakhramovich
Senior Lecturer of the Military Security and
Defense University of the Republic of Uzbekistan

Abstract

The article addresses the development of an integrated training module aimed at forming a holistic set of knowledge, practical skills, and security culture in artificial intelligence (AI) and unmanned aerial vehicle (UAV) security within military professional education, as well as evaluating its pedagogical effectiveness. The methodological basis of the study is a mixed-methods design employing pedagogical design, expert evaluation, a formative pedagogical experiment, and statistical analysis. The author concludes that integrated teaching of AI and UAV security requires combining technical, organizational, and pedagogical approaches, and provides practical recommendations for implementing the module in military education practice.

Keywords: military professional education, artificial intelligence, UAV security, integrated training module, cybersecurity, security culture, interdisciplinary integration, pedagogical design, cyber range, pedagogical experiment.

Introduction

In the first quarter of the 21st century, the global military sphere has entered a new stage of technological revolution. Artificial intelligence (AI), autonomous control systems, unmanned aerial vehicles (UAVs), robotic platforms, and big data analytics are fundamentally transforming the character of military

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
Eureka Journal of Education & Learning Technologies (EJELT)
ISSN 2760-4918 (Online) Volume 2, Issue 11, November 2026
This article/work is licensed under CC by 4.0 Attribution
https://eurekaoa.com/index.php/2

operations. According to international studies and expert estimates, more than 80 countries worldwide are currently working on the use or development of UAV technologies for military purposes, while AI-based decision-making systems are being actively introduced into intelligence, surveillance, target acquisition, and logistics processes [1].

This transformation places new demands on the military education system. Traditionally organized military professional training is no longer sufficient, because a modern officer and specialist must know not only how to operate weapons and equipment, but also how to ensure the security of digital systems, understand the limitations and risks of AI tools, and counter cyber threats. This requires revisiting the content of military education, strengthening interdisciplinary integration, and developing practice-oriented training models [2].

In recent years, systematic reforms have been carried out in the Republic of Uzbekistan in the field of military education and defence. On the basis of presidential decrees and government resolutions, military higher education institutions were granted the status of institutes, a unified management vertical was formed, and the University of Military Security and Defence was established. The key directions of these reforms are as follows:

Modernization of curricula. Advanced training modules in foreign languages, information technology, fundamentals of artificial intelligence, and cybersecurity are being introduced for cadets.

Training of UAV specialists. The system for training unmanned aerial vehicle operators, engineers, and robotics specialists is being improved, and a unified certification procedure is being formed in this area.

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
Eureka Journal of Education & Learning Technologies (EJELT)
ISSN 2760-4918 (Online) Volume 2, Issue 11, November 2026
This article/work is licensed under CC by 4.0 Attribution
https://eurekaoa.com/index.php/2

Development of digital infrastructure. Plans have been set to establish an artificial intelligence technology department, a cybersecurity laboratory, and satellite communication units within the Ministry of Defence.

Expansion of international cooperation. Joint training programmes and professional development courses on AI and UAVs are being organized in cooperation with leading foreign military education institutions.

These reforms have turned AI and UAV security issues into a priority area of military professional education. However, a holistic educational and methodological framework in this area has not yet been fully formed.

The integration of AI and UAV technologies into military education gives rise to a number of risks. In the scientific literature, these risks are grouped as follows:

Technical and cybersecurity risks: adversarial attacks targeting AI models (adversarial ML), model corruption, and data poisoning; vulnerabilities in UAV telemetry and control channels, attacks on GPS/GNSS navigation systems (spoofing, jamming); vulnerabilities in communication protocols, insufficient authentication and encryption; vulnerability of autonomous systems to control disruptions.

Data privacy and legal risks: protection of personal data of cadets and service members; risk of leakage of classified and official-use information; legal limits on data processing in AI systems; intellectual property and liability issues.

Pedagogical and psychological risks: formation of cognitive dependence on AI tools; decline in critical thinking; excessive trust in AI recommendations (automation bias); insufficient formation of security culture.

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
Eureka Journal of Education & Learning Technologies (EJELT)
ISSN 2760-4918 (Online) Volume 2, Issue 11, November 2026
This article/work is licensed under CC by 4.0 Attribution
https://eurekaoa.com/index.php/2

Ethical and normative risks: explainability of AI systems and distribution of liability; ethical limits of using AI for military purposes; spread of deepfake and disinformation tools.

These risks acquire particular importance in the military environment, because the cost of error is measured not only materially, but also in human life and operational effectiveness. Therefore, training in AI and UAV security must become an integral component of military professional education.

In current military education practice, AI and UAV security are often taught within separate disciplines: AI knowledge is delivered within computer science or information technology subjects; UAV security is taught within technical disciplines or special training courses; cybersecurity is offered as a separate course. This fragmented approach gives rise to the following shortcomings:

Content gaps — cadets do not fully grasp the interrelationship between AI and UAVs, for example, the possibilities of identifying UAV threats using AI.

Lack of holistic security thinking — interdisciplinary skills and the ability to make decisions in complex situations are formed weakly.

Low practical orientation — theoretical knowledge is not sufficiently linked to real service situations.

Insufficient formation of security culture — cadets' skills in anticipating risks and understanding responsibility do not develop consistently.

International experience shows that combining technologies such as AI and VR within a single instructional design helps to deepen understanding of complex phenomena. Accordingly, teaching AI and UAV security in an integrated manner is also pedagogically appropriate.

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
Eureka Journal of Education & Learning Technologies (EJELT)
ISSN 2760-4918 (Online) Volume 2, Issue 11, November 2026
This article/work is licensed under CC by 4.0 Attribution
https://eurekaoa.com/index.php/2

Scientific literature on the topic is developing in several directions.

Research in the area of AI and cybersecurity examines the detection of cyberattacks using AI, defence methods against adversarial ML attacks, statistical signs of data poisoning, and the explainability of AI systems. These works thoroughly cover the technical aspects of AI security, but pay little attention to pedagogical application.

Research in UAV security focuses on the security of UAV telemetry and control channels, threats to navigation systems, authentication protocols, and encryption methods. In this area too, technical solutions prevail, while educational and methodological aspects remain insufficiently developed.

In the area of integrating technologies into military education, Kjeksrud et al. (2026) demonstrated the pedagogical possibilities of combining AI and virtual reality in military education. Kurdubova (2024) emphasizes the need to take into account information and military security requirements when integrating neural network technologies into military education. Sapayev (2026) analyses simulation-based teaching methods based on digital technologies and AI. However, these works do not consider AI and UAV security as a single integrated module [2, 3].

In the area of national military education reforms, sources exist on Uzbekistan's military education reforms and the strategic importance of AI and cybersecurity, but the methodological model for teaching AI and UAV security in an integrated manner has not yet been developed.

Conclusions from the literature review: while existing studies adequately cover the technical aspects of AI and UAV security, the pedagogical model for teaching them in a holistic, integrated, and practice-oriented form within military professional education remains insufficiently developed. This gap determines the scientific relevance of the present study.

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
Eureka Journal of Education & Learning Technologies (EJELT)
ISSN 2760-4918 (Online) Volume 2, Issue 11, November 2026
This article/work is licensed under CC by 4.0 Attribution
https://eurekaoa.com/index.php/2

The research problem is the insufficient methodological support for delivering knowledge and skills in AI and UAV security in a holistic, practice-oriented form that meets security requirements within military professional education [4].

The scientific hypothesis is that if the educational content on AI and UAV security is structured as a holistic three-block module based on the principles of interdisciplinary integration, and is enriched with practical scenarios and cyber range exercises, the level of cadets' knowledge, practical skills, and security culture will increase significantly compared to the control group.

The study was organized on the basis of a mixed-methods design. The rationale for choosing this approach is that evaluating the effectiveness of a training module on AI and UAV security requires both quantitative data (knowledge test, rubric scores, statistical indicators) and qualitative data (expert conclusions, observation results, focus group discussions).

The study was carried out in four stages:

Preparatory stage – analysis of scientific literature on the topic, study of existing curricula, and formulation of the risk taxonomy.

Design stage – development of the didactic model of the integrated module, preparation of educational and methodological support, and expert evaluation.

Experimental stage – testing the module in the experimental group, comparative study with the control group, and data collection.

Analytical stage – analysis of quantitative and qualitative data, formulation of conclusions, and development of practical recommendations.

The following theoretical approaches were relied upon in designing the module:

Systemic approach – AI and UAV security was considered as a holistic system, and its components were analysed in their interrelation.

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
Eureka Journal of Education & Learning Technologies (EJELT)
ISSN 2760-4918 (Online) Volume 2, Issue 11, November 2026
This article/work is licensed under CC by 4.0 Attribution
https://eurekaoa.com/index.php/2

Principle of interdisciplinary integration – technical, legal, organizational, and pedagogical knowledge was combined into a single educational content.

Competence-based approach – learning outcomes were defined in terms of knowledge, skills, and security culture components.

The study involved **94 cadets** studying in the relevant field at a military education institution. They were divided into two groups:

- **Experimental group (n = 48):** received training under the integrated module.
- **Control group (n = 46):** were taught under the traditional, discipline-separated curriculum.

The sample size was determined on the basis of power analysis: with a medium effect size d = 0.5, statistical power of 0.80, and significance level α = 0.05, at least 42 participants per group are required (G*Power 3.1 software). The actual sample exceeds this minimum.

The groups were equalized in terms of baseline training level: entry knowledge test results (experimental group M = 54.2; SD = 9.8; control group M = 53.7; SD = 10.1), previous academic performance indicators, and basic technical training level were compared. At the initial stage, no statistically significant difference was found between the groups according to the independent-samples t-test ($t(92) = 0.24$; $p = 0.811$; $d = 0.05$).

The content and methodological quality of the module were evaluated by **7 experts**: 3 Doctors of Pedagogical Sciences (military pedagogy); 2 Candidates of Pedagogical Sciences (pedagogy of information security); 2 practising specialists (cybersecurity and UAV control systems). The experts rated the module content, the accuracy of interdisciplinary connections, practical orientation, and the adequacy of assessment criteria on a 5-point scale. The consistency of expert ratings was checked using Kendall's W coefficient ($W = 0.78$; $p < 0.01$), which indicates that expert conclusions were sufficiently consistent.

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
Eureka Journal of Education & Learning Technologies (EJELT)
ISSN 2760-4918 (Online) Volume 2, Issue 11, November 2026
This article/work is licensed under CC by 4.0 Attribution
https://eurekaoa.com/index.php/2

Knowledge test. The test consists of 40 items covering the levels of knowledge, comprehension, application, and analysis. The internal consistency of the test was assessed using Cronbach's alpha: $\alpha = 0.87$ (high reliability). Content validity was confirmed by 5 experts (CVI = 0.91). Test-retest reliability (2-week interval) was $r = 0.84$.

Practical skills rubric. The rubric consists of 5 criteria: threat identification, vulnerability assessment, selection of protective measures, justification of decisions, and awareness of responsibility. Each criterion is assessed on a 1–5 scale. The internal consistency of the rubric was $\alpha = 0.83$; inter-rater reliability between two independent raters was Cohen's kappa = 0.79.

Security culture questionnaire. The questionnaire consists of 24 items covering 4 subscales: attitude to security, awareness, risk anticipation, and responsibility. The internal consistency of the questionnaire was $\alpha = 0.89$; factorial validity was checked by confirmatory factor analysis (CFI = 0.94; RMSEA = 0.06).
Qualitative data were summarized using content analysis. The following additional theoretical approaches were also applied: **Practice-oriented education** – through scenario-based exercises and cyber range tasks, the learning environment was brought closer to real service situations. **Constructivist learning theory** – cadets' active participation, independent solution of problem situations, and reflection were encouraged. **Security culture theory** – alongside technical knowledge, values, responsibility, and risk anticipation skills were formed. Cadets of the relevant field at a military education institution participated in the study. The sample was formed on the basis of convenience and purposive sampling, since the study was conducted within a specific educational field. Participants were divided into two groups:
Experimental group – received training under the integrated module.

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
Eureka Journal of Education & Learning Technologies (EJELT)
ISSN 2760-4918 (Online) Volume 2, Issue 11, November 2026
This article/work is licensed under CC by 4.0 Attribution
https://eurekaoa.com/index.php/2

Control group – were taught under the traditional, discipline-separated curriculum.

The groups were equalized in terms of baseline training level: entry knowledge test results, previous academic performance indicators, and basic technical training level were compared. No statistically significant difference was found between the groups at the initial stage, which allowed subsequent results to be compared.

The module was designed as three interconnected blocks (**Table 1**).

Table 1 – Blocks of the integrated training module, content areas, and main learning outcomes

Block	Content area	Main learning outcomes
Block 1. Fundamentals of AI and cybersecurity	Machine learning concepts, threats to AI systems, adversarial ML, data privacy	Identify and describe AI security risks
Block 2. UAV security	Telemetry and control channels, navigation threats, authentication, encryption	Assess vulnerabilities of UAV communication and control systems
Block 3. Integration and practical decisions	Identifying UAV threats using AI, responding to cyber incidents, scenario exercises	Make decisions in complex security situations

The didactic model of the module was built on a three-stage learning trajectory:

1. Stage 1: Technical proficiency. Cadets are introduced to the basic concepts of AI and UAV security, types of threats, and protection methods.

2. Stage 2: Operational integration. Skills are formed in identifying UAV threats using AI tools, assessing communication channel vulnerabilities, and making security decisions.

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
Eureka Journal of Education & Learning Technologies (EJELT)
ISSN 2760-4918 (Online) Volume 2, Issue 11, November 2026
This article/work is licensed under CC by 4.0 Attribution
https://eurekaoa.com/index.php/2

3. Stage 3: Resilience and critical thinking. Through complex scenarios, cyber incident response exercises, and group discussions, cadets' ability to make independent decisions is developed [5, 6].

Each stage includes lecture, practical session, independent work, and assessment components. Learning outcomes are aligned with the cognitive levels of Bloom's taxonomy: **remember → understand → apply → analyse → evaluate → create.**

Block 1. Fundamentals of AI and cybersecurity. Content: machine learning concepts, fundamentals of neural networks, taxonomy of threats to AI systems, adversarial ML attacks, data poisoning, model robustness, data privacy, AI ethics and explainability. Practical sessions: analysing vulnerabilities of an AI model; working with adversarial examples; designing a data protection policy. Expected outcomes: identify and describe AI security risks; select protective measures.

Block 2. UAV security. Content: UAV architecture, telemetry and control channels, GPS/GNSS navigation systems, spoofing and jamming threats, authentication protocols, encryption methods, drone identification, blocking unauthorized access. Practical sessions: analysing telemetry traffic; assessing communication channel vulnerabilities; applying encryption settings. Expected outcomes: assess vulnerabilities of UAV communication and control systems; apply protective measures.

Block 3. Integration and practical decisions. Content: identifying UAV threats using AI, cyber incident response plan, scenario exercises, group decision-making, security culture. Practical sessions: solving a complex cyber incident scenario; identifying anomalies using AI tools; planning response measures. Expected outcomes: make decisions in complex security situations; demonstrate security culture.

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
Eureka Journal of Education & Learning Technologies (EJELT)
ISSN 2760-4918 (Online) Volume 2, Issue 11, November 2026
This article/work is licensed under CC by 4.0 Attribution
https://eurekaoa.com/index.php/2

The following educational and methodological materials were prepared for the module: lecture texts and presentations; instructions for practical sessions; a set of scenario-based tasks; a description of cyber range exercises; assessment rubrics and criteria; independent work assignments; a methodological guide for instructors.

To assess theoretical knowledge of AI and UAV security, a test was applied before and after. The test items covered the levels of knowledge, comprehension, application, and analysis. A rubric was developed to assess security decisions in scenario-based exercises. Criteria: threat identification, vulnerability assessment, selection of protective measures, justification of decisions, awareness of responsibility. A questionnaire was used to measure cadets' attitude to security, awareness, risk anticipation skills, and sense of responsibility. An expert sheet was used to assess module content, methodological quality, accuracy of interdisciplinary connections, and practical orientation. During practical sessions, cadets' activity, group work skills, and decision-making processes were observed. Assessment was carried out on the basis of a three-component system (**Table 2**).

Table 2 – Assessment components, their weights, and assessment methods

Component	Weight	Assessment method
Theoretical knowledge	30%	Knowledge test
Practical skills	40%	Rubric-based assessment
Security culture	30%	Questionnaire and observation

Results for each component were compared before and after.

Stages of the pedagogical experiment

Entry stage (pre-test). In both groups, the baseline level of knowledge, skills, and security culture was measured. *Formative stage.* The experimental group received training under the integrated module; the control group was taught under the traditional programme. *Final stage (post-test).* In both groups, a final

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
Eureka Journal of Education & Learning Technologies (EJELT)
ISSN 2760-4918 (Online) Volume 2, Issue 11, November 2026
This article/work is licensed under CC by 4.0 Attribution
https://eurekaoa.com/index.php/2

knowledge test, practical rubric, and questionnaire were conducted. *Delayed assessment.* Where possible, knowledge retention was assessed some time after the module was completed.

Quantitative data were analysed using descriptive statistics — mean, standard deviation, median, percentage indicators; comparative analysis — appropriate statistical criteria were used to assess the difference between groups (t-test under parametric conditions, an alternative under nonparametric conditions); dynamic analysis — changes between pre- and post-indicators were assessed; and effect size — calculated to assess the practical significance of the pedagogical impact.

Qualitative data were summarized using content analysis: expert conclusions, observation results, and focus group discussions were coded by theme.

The study observed the following ethical principles: voluntariness of participants, confidentiality of data, anonymity, objective presentation of results, and compliance with the requirements of the military institution. Classified information was not used for research purposes.

The experts rated the content integrity, accuracy of interdisciplinary connections, and practical orientation of the module highly. A particularly noted aspect was the integration of AI and UAV security into a single learning trajectory, which reduces content gaps compared with traditional separated instruction. The experts noted that the three-block structure of the module is logically consistent for achieving the learning outcomes.

Observation and focus group discussions showed that the integrated format strengthens cadets' ability to see interdisciplinary connections, increases motivation, and creates a learning environment closer to real service situations. At the same time, some cadets noted the complexity of technical material and limited time resources.

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
Eureka Journal of Education & Learning Technologies (EJELT)
ISSN 2760-4918 (Online) Volume 2, Issue 11, November 2026
This article/work is licensed under CC by 4.0 Attribution
https://eurekaoa.com/index.php/2

Knowledge dynamics. In the experimental group, knowledge test results increased significantly at the end of the module. The control group also showed growth, but the average result in the experimental group was statistically significantly higher. The experimental group showed a particular advantage in questions related to analysing AI and UAV threats in an integrated manner. This confirms the positive effect of the integrated approach on holistic knowledge acquisition.

Practical skills. In scenario-based exercises, the experimental group cadets showed high results in identifying UAV threats using AI, assessing communication channel vulnerabilities, and responding to cyber incidents. The difference between the groups in rubric scores confirms the advantage of the integrated module in forming practical skills. It was observed that cadets moved towards taking technical, organizational, and legal aspects into account together when justifying their decisions.

Security culture. According to the questionnaire results, indicators of compliance with security rules, risk anticipation, and awareness of responsibility improved in the experimental group. Cadets noted that they had moved towards perceiving AI and UAV technologies not only as tools but as systems subject to security requirements.

Qualitative results. Observation and focus group discussions showed that the integrated format strengthens cadets' ability to see interdisciplinary connections, increases motivation, and creates a learning environment closer to real service situations. At the same time, some cadets noted the complexity of technical material and limited time resources.

The results of the study demonstrate the pedagogical appropriateness of teaching AI and UAV security in an integrated manner within military professional

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
Eureka Journal of Education & Learning Technologies (EJELT)
ISSN 2760-4918 (Online) Volume 2, Issue 11, November 2026
This article/work is licensed under CC by 4.0 Attribution
https://eurekaoa.com/index.php/2

education. This conclusion is consistent with the idea of "holistic instructional design" advanced in international studies.

Secondly, the results confirm that education on AI and UAV security should not be limited to technical knowledge alone. Forming cadets' security culture, critical thinking, and sense of responsibility remains an important component of the module.

Thirdly, the integrated module is directly aligned with the priority directions of Uzbekistan's military education reforms — deepening AI, digital technologies, and cybersecurity.

Limitations: the sample is limited to a single institution, the duration of the experiment is relatively short, and there is no possibility to assess long-term impact.

Practical recommendations: incorporate the module into the curriculum as an interdisciplinary course or module; enrich practical sessions with cyber ranges and simulation environments; develop a methodological guide for instructors.

CONCLUSION

1. Holistic teaching of AI and UAV security serves to deepen cadets' knowledge acquisition and enhance their ability to apply it in practice.
2. The integrated module yields positive results in forming security culture.
3. The effectiveness of the module is achieved by ensuring the unity of technical, organizational, and pedagogical approaches.

It is recommended to introduce the integrated training module into military education practice and to continuously improve it.

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas

Eureka Journal of Education & Learning Technologies (EJELT)

ISSN 2760-4918 (Online) Volume 2, Issue 11, November 2026
This article/work is licensed under CC by 4.0 Attribution
https://eurekaoa.com/index.php/2

References:

1. Курдубова, В. В. Интеграция нейросетевых технологий в систему военного образования с учётом требований информационной и военной безопасности / В. В. Курдубова // Цифровизация в системе образования: передовой опыт и практика внедрения : материалы VII Всероссийской научно-практической конференции. – Ростов, 2026. – С. 593–595.
2. Sapayev, I. N. Harbiy ta’lim tizimida raqamli texnologiyalar va AI asosida simulyatsion o‘qitish metodlari / I. N. Sapayev // ILM FAN YANGILIKLARI KONFERENSIYASI: to‘plam. – Andijon : [b. i.], 2026. – B. 122.
3. Uzbekistan Shifts Defense to AI, Drones, and Satellite Communications [Electronic resource] // ixbt.uz. – 2026. – URL: https://ixbt.uz –Фccessed: 18.11.2026)
4. Uzbekistan to establish AI, satellite communications and cyber units in the military [Electronic resource] // Daryo. – 2026. – URL: https://daryo.uz (accessed: 18.11.2026).
5. Kjeksrud, S. Making Hybrid War Teachable and Learnable: Combining Artificial Intelligence and Virtual Reality in Military Education / S. Kjeksrud, S. A. Engdal, L. M. Hokstad, S. Grassini, P. H. F. Lindqvist // Scandinavian Journal of Military Studies. – 2026. – Vol. 9, № 1. – P. 62–81. – DOI: 10.31374/sjms.414.
6. Curriculum framework: AI and UAS integration in military education [Electronic resource] // MIlAK. – 2025. – URL: https://milak.edu – Accessed: 18.11.2026.