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

Eureka Journal of Artificial Intelligence and Data Innovation (EJAIDI)

ISSN 2760-5000 (Online) Volume 2, Issue 10, October 2026
This article/work is licensed under CC by 4.0 Attribution
https://eurekaoa.com/index.php/11

ARTIFICIAL INTELLIGENCE AND AUTONOMOUS PATROL DRONES IN BORDER SECURITY

Abduolimov Ikboljon Ilkhomjonovich
Senior Lecturer, Military Security and Defense
University of the Republic of Uzbekistan

Abstract:
This article comprehensively analyzes the role of artificial intelligence (AI) technologies and autonomous patrol unmanned aerial vehicles (UAVs) in the state border protection and control system. The limitations of traditional border security mechanisms are highlighted, and the architecture of autonomous drones—including modern neural networks, computer vision systems, SLAM navigation algorithms, and thermal visualization—is scientifically substantiated. Furthermore, the principles of autonomous drone movement in conditions of limited GPS signals or electronic warfare, data encryption, and cybersecurity issues are examined. Practical recommendations have been developed based on international scientific experiences (IEEE Xplore data and GEOINT integration) and the practice of digitalizing border security in the Republic of Uzbekistan.

Keywords: artificial intelligence, autonomous patrol drones, border security, neural networks, computer vision, thermal visualization, SLAM navigation, GEOINT.

Introduction

In the 21st century, the global security architecture is undergoing severe changes, and threats such as transnational crime, illegal migration, arms trafficking, and drug smuggling are becoming increasingly complex. In such circumstances,

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
Eureka Journal of Artificial Intelligence and Data Innovation (EJAIDI)
ISSN 2760-5000 (Online) Volume 2, Issue 10, October 2026
This article/work is licensed under CC by 4.0 Attribution
https://eurekaoa.com/index.php/11

ensuring the inviolability of their borders is of strategic importance for sovereign states. Traditional border security systems–stationary surveillance posts, visual monitoring towers, and foot patrol groups–cannot always ensure absolute effectiveness because they rely heavily on the human factor (fatigue, negligence, extreme weather conditions) [1].

Establishing continuous control through human resources in remote areas with complex geographical relief (high mountain ranges, deserts, swamps, and dense forests) incurs high economic costs and human risks. Therefore, in recent years, the rapid introduction of autonomous patrol drones equipped with artificial intelligence (AI) into the practice of military and law enforcement agencies has become an urgent task. The integration of drones with AI algorithms transforms them from mere remotely controlled cameras into intelligent patrol systems capable of making autonomous decisions.

Throughout history, protecting and ensuring the inviolability of thousands of kilometers of extended state border sections has relied primarily on classical approaches–namely, human resources, stationary engineering structures, and visual control posts. However, 21st-century threats and the technological advancement of transnational crime clearly demonstrate the vulnerability of traditional systems in certain situations [2].

Fundamental problems of the traditional border security architecture:

Infrastructure shortage and logistical barriers: The absence or extreme limitation of power grids, centralized water supply, stationary communication towers, and asphalted transport roads in border sections located in remote desert, semi-desert, high-mountain, and swampy areas makes the construction and maintenance of permanent bases economically extremely costly and technically complex. Maintaining and continuously supplying personnel in these remote areas, where air temperatures change sharply, roads become covered with snow in winter, or overheat intensely in summer, requires large logistical resources.

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
OPEN ACCESS JOURNALS

Eureka Journal of Artificial Intelligence and Data Innovation (EJAIDI)

ISSN 2760-5000 (Online) Volume 2, Issue 10, October 2026
This article/work is licensed under CC by 4.0 Attribution
https://eurekaoa.com/index.php/11

"Blind spots" caused by geographical and topographic factors: The complexity of the natural relief–deep gorges, canyons, dense forest massives, and desert dunes–significantly limits the field of view of traditional stationary surveillance cameras and optical posts. Since stationary towers can only operate within a certain radius, the vast distances between them and relief shadows create natural "blind spots" Violators and smugglers strive to bypass the protection system by moving precisely through these zones [3].

Resource consumption, human factor, and psychological stress: Organizing border service relying on human resources demands constant physical and mental strain from military servicemen. Serving long-term foot patrols in extreme climatic conditions (severe cold, scorching heat, strong winds, and storms) negatively affects the health of personnel. Due to fatigue, inattention, and subjective factors, the human eye may miss important movements, which can cause unexpected gaps in the security system. Furthermore, maintaining and rotating thousands of personnel in remote areas for extended periods imposes a major financial burden on the state budget [4].

The objective necessity of digital transformation: The only and most effective scientific and practical way to eliminate the aforementioned fundamental problems is to gradually abandon traditional approaches and implement digital transformation. Modern military-scientific approaches necessitate the introduction of the "Smart Border" concept, which integrates automated aerial platforms (autonomous drones), IoT (Internet of Things) sensors, and artificial intelligence analysis centers into a single network.

This system makes it possible to establish absolute control in remote areas on a 24/7 basis, detect potential threats at an early stage, and rationally allocate available material and technical resources while minimizing the human factor [5].

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
Eureka Journal of Artificial Intelligence and Data Innovation (EJAIDI)
ISSN 2760-5000 (Online) Volume 2, Issue 10, October 2026
This article/work is licensed under CC by 4.0 Attribution
https://eurekaoa.com/index.php/11

Autonomous drones designed to ensure border security differ fundamentally from ordinary civil or commercial quadcopters in their engineering-technical parameters, durability, and functional capabilities. Such specialized platforms are designed to operate continuously even under extreme weather conditions, strong winds, and enemy electronic-technical impacts, and their architecture relies on the following key engineering solutions:

VTOL Aerodynamic Structure: Sharp, changing strong wind flows in mountainous areas, narrow gorges, and air vortices in desert regions drastically disrupt the stability of ordinary drones. Therefore, hybrid platforms based on the VTOL (Vertical Take-Off and Landing) principle are used for border patrol. These systems combine the advantages of a vertical flight rotor and a fixed-wing construction: they can take off vertically from any remote border post without a special runway and move in the air at high speed (100–150 km/h) like a fixed-wing airplane, covering long distances.

Energy Sources and Flight Autonomy: The limited capacity of traditional lithium-polymer (LiPo) batteries (typically 30–50 minutes) is insufficient for the continuous monitoring of vast border lines. Modern tactical drones are being equipped with advanced energy sources to extend flight duration up to 12–24 hours:

Hydrogen Fuel Cells: Possessing higher energy storage density compared to traditional batteries, ensuring long-term patrol flights.

Hybrid internal combustion engines and solar panels: Enabling flights over long distances while carrying heavy loads by combining fuel and electricity [6].

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
OPEN ACCESS JOURNALS

Eureka Journal of Artificial Intelligence and Data Innovation (EJAIDI)

ISSN 2760-5000 (Online) Volume 2, Issue 10, October 2026
This article/work is licensed under CC by 4.0 Attribution
https://eurekaoa.com/index.php/11

Multisensor Suites and Search Modules: Sensor modules, serving as the main "eyes" of the drone, are specialized in collecting data across various spectra:

Optical zoom cameras: Stabilized gimbal cameras with ultra-high resolution (4K/8K) and powerful optical zoom (30x–40x) capabilities allow for the precise identification of suspicious objects, vehicles, and even human silhouettes at a distance of several kilometers during the day.

Thermal (heat-recording) cameras: Uncooled microbolometer sensors used to reveal the body temperature of individuals or thermal traces of moving equipment hidden in cold seasons, at night, in thick fog, or among dense bushes guarantee round-the-clock continuous monitoring.

LiDAR (Laser Imaging, Detection and Ranging): As an active sensing technology, it creates ultra-precise 3D relief maps of the area where the drone is operating. LiDAR automatically detects tree branches, power transmission lines, and obstacles in darkness or poor visibility conditions, preventing collisions [7].
In ensuring border security and conducting modern military-tactical operations, the reliability of unmanned aerial vehicles largely depends on their navigation stability. Under normal conditions, drones rely on Global Navigation Satellite Systems (GNSS/GPS) to determine their position and navigate along designated routes. However, in the modern border environment and potential conflict zones, the deployment of electronic warfare (EW) tools by the adversary is widespread, attempting to deprive drones of control by artificially jamming or spoofing GPS signals. To ensure that autonomous patrol drones successfully perform their missions in extreme conditions where GPS communication is lost or unreliable, the following advanced technologies are applied:

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
OPEN ACCESS JOURNALS

Eureka Journal of Artificial Intelligence and Data Innovation (EJAIDI)

ISSN 2760-5000 (Online) Volume 2, Issue 10, October 2026
This article/work is licensed under CC by 4.0 Attribution
https://eurekaoa.com/index.php/11

SLAM (Simultaneous Localization and Mapping): Even in cases where GPS signals are completely disabled or suppressed by the enemy, SLAM technology enables the drone to navigate completely independently. The drone continuously scans the environment using on-board LiDAR sensors, optical cameras, and inertial measurement units (IMU). Based on the acquired data, the on-board computing system autonomously creates a real-time digital map of the unknown area (Mapping) and precisely calculates its current coordinates within that map (Localization). As a result, the UAV, disconnected from external satellite communication, continues its flight along the pre-programmed strategic route without any deviations and safely returns to its base [8].

Visual Odometry: Another important method for stabilizing navigation in a GPS-free environment is visual odometry algorithms. Through its bottom and front cameras, the drone analyzes the optical characteristics of the earth's surface (relief contours, rocks, vegetation cover, roads, and natural landmarks) as a sequence of frames. Visual analysis algorithms compare frame-to-frame changes to calculate the drone's speed, direction, and traveled distance with high precision. Using AI-based landscape recognition algorithms, the UAV accurately finds its geographical trajectory without erring even in remote desert or mountain gorges where GPS is absent, guaranteeing flight safety.

Information collected through unmanned aerial vehicles in the process of ensuring state border security constitutes classified information of strategic importance and a state secret. As autonomous patrol drones operate in airspace, they maintain continuous radio communication and data exchange with ground control posts. This means that these systems may be vulnerable to cyberattacks, information interception, or unauthorized control attempts. Therefore, the architecture of autonomous drones must rely on the following strict cybersecurity and protection protocols:

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
Eureka Journal of Artificial Intelligence and Data Innovation (EJAIDI)
ISSN 2760-5000 (Online) Volume 2, Issue 10, October 2026
This article/work is licensed under CC by 4.0 Attribution
https://eurekaoa.com/index.php/11

Encrypted Communication Channels: All telemetry data, high-resolution video imagery, and control commands transmitted between the drone and the ground command post are encrypted using ultra-strong cryptographic algorithms (e.g., AES-256 – Advanced Encryption Standard). This absolutely guarantees that even if the adversary intercepts the transmission stream using specialized radio frequency scanners, they will not be able to read or decrypt the data. Furthermore, data packets are transmitted through dynamically changing secure VPN tunnels [9].

Resistance to Electronic Warfare (EW) and Frequency Hopping: In modern conflicts and border areas, enemy forces may deploy specialized electronic suppression equipment (jammers). To counter attempts to disrupt the drone's control and navigation frequencies, FHSS (Frequency Hopping Spread Spectrum) technology is applied. Using this technology, the drone and control post change their communication frequency hundreds of times per second, preventing enemy radio-technical means from blocking the signal or depriving the drone of control [10].

Software Protection and Anti-Hijack Mechanisms: The drone's internal microprocessors and operating system must be protected from external cyberattacks, remote introduction of malware, or attempts to force the drone to land. On-board systems only accept trusted software updates with a digital signature. If an attempt to remotely hijack the drone is detected, an automated security protocol activates, immediately switching the drone to an autonomous Return-to-Home mode back to its initial base.

The process of integrating autonomous patrol drones and artificial intelligence technologies into border security is one of the rapidly studied and scientifically substantiated directions on a global scale. Work carried out by the global

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
Eureka Journal of Artificial Intelligence and Data Innovation (EJAIDI)
ISSN 2760-5000 (Online) Volume 2, Issue 10, October 2026
This article/work is licensed under CC by 4.0 Attribution
https://eurekaoa.com/index.php/11

scientific community and leading research centers determines achievements in this field:

Research in IEEE Xplore and Scientific Databases: Research published in international scientific journals and prestigious databases such as IEEE Xplore has demonstrated in practice the high effectiveness of UAV-GEOINT (UAV-Geospatial Intelligence) platforms incorporating LiDAR technology, high-resolution RGB visualization, GIS spatial analysis, and AI-based object detection systems. Using these platforms, real-time generation of 3D relief models in remote and mountainous areas, highly reliable target recognition, and a manifold reduction in the time required to deliver intelligence data to the command post have been achieved.

GEOINT (Geospatial Intelligence) Integration and Decision Support: International practice shows that modern border security is not limited to the flight of a single drone. It synthesizes streams coming from satellite data, ground stationary sensors, radar stations, and autonomous drones into a single GEOINT center [5]. This allows military analysts to evaluate any changes in remote areas within a broad space-time context, predict the movement trajectories of transnational criminals, and direct rapid reaction forces in the shortest possible time.

Global Military-Tactical Standards: Leading countries of the world are testing and introducing fully autonomous, AI-controlled reconnaissance drones into combat duty within their border troops and national guard units. International experience confirms that border systems relying on autonomous drones and AI algorithms, while minimizing the human factor, serve as the most effective strategic tool in minimizing the risks of illegal crossings and smuggling.

In recent years, the Republic of Uzbekistan has paid special attention to digitalizing military-technical capacity and integrating modern intellectual

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
Eureka Journal of Artificial Intelligence and Data Innovation (EJAIDI)
ISSN 2760-5000 (Online) Volume 2, Issue 10, October 2026
This article/work is licensed under CC by 4.0 Attribution
https://eurekaoa.com/index.php/11

technologies to ensure its sovereignty, territorial integrity, and the inviolability of state borders. In our country, which possesses geographically complex border lines, the implementation of autonomous aerial platforms and artificial intelligence systems is being carried out across several practical areas:

Special Units and Modern UAV Fleet: The establishment of combat duty for special units equipped with modern tactical combat unmanned aerial vehicles, including high-technology platforms such as the Bayraktar TB2, within the Border Troops of the State Security Service of the Republic of Uzbekistan, has initiated a qualitatively new stage in border security. Such medium-altitude, long-endurance drones allow for round-the-clock continuous reconnaissance and monitoring in remote and hard-to-reach areas [8].

Digitalization of Infrastructure and Integration: In Uzbekistan's experience, modern UAV systems operate not in isolation, but closely linked with the general border infrastructure. In particular, a unified digital information space has been created by equipping critical sections of state borders with modern video surveillance systems and laying thousands of kilometers of fiber-optic communication lines. Data transmitted by UAVs is delivered through this network to central command posts in real time.

Domestic Manufacturing Potential ("Lochin" Drones): Within the framework of developing the defense industry in our country, relying on our own intellectual and technical capabilities is a priority task. Domestic drones named "Lochin," developed by the Scientific and Production Center under the State Committee for Defense Industry, are adapted for military and special purposes. The establishment of domestic production ensures independence in future spare parts supply, maintenance, and adaptation of the system to national requirements.

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
OPEN ACCESS JOURNALS

Eureka Journal of Artificial Intelligence and Data Innovation (EJAIDI)

ISSN 2760-5000 (Online) Volume 2, Issue 10, October 2026
This article/work is licensed under CC by 4.0 Attribution
https://eurekaoa.com/index.php/11

Formation of the Legal and Regulatory Framework: The system of using UAVs and regulating them legally in Uzbekistan is consistently being improved: Resolutions No. 150 of the Cabinet of Ministers dated May 12, 2016, and No. 658 dated November 15, 2022, granted authorized bodies performing departmental tasks the right to purchase, import, and use UAVs. The documents strictly define legal concepts such as "allocated airspace" and the "airspace of the border strip," which is 25 km wide and adjacent to the state border. Through Article 244-4 introduced into the Criminal Code, criminal liability has been established for the illegal import, storage, and violation of rules for using UAVs, thereby preventing illegal use.

The large-scale implementation of autonomous patrol drones and artificial intelligence technologies in the activities of border troops, alongside significant economic achievements, requires prior assessment and management mechanisms for certain risks:

Reducing Capital Expenditures: Permanently building stationary posts every kilometer of the border and providing them with energy and water networks requires enormous financial costs. Managing a mobile UAV fleet sharply reduces infrastructure costs.

Saving Human Resources: Instead of deploying thousands of servicemen to long-term foot patrols in open areas under severe weather conditions, monitoring the entire territory through small technical groups and autonomous drones allows for the optimization of staff numbers.

Prompt Reaction Time and Efficiency: The time required to direct a rapid response team to the incident point from the moment a violation is detected is reduced severalfold, increasing the probability of preventing violations to the maximum level.

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
OPEN ACCESS JOURNALS

Eureka Journal of Artificial Intelligence and Data Innovation (EJAIDI)

ISSN 2760-5000 (Online) Volume 2, Issue 10, October 2026
This article/work is licensed under CC by 4.0 Attribution
https://eurekaoa.com/index.php/11

Ensuring Personnel Safety: Monitoring the situation from a safe distance without directly exposing servicemen face-to-face to armed transnational groups, smugglers, or extreme natural conditions (strong storms, avalanches, scorching heat) prevents human losses.

Technical Malfunctions and Weather Limitations: Extreme climatic conditions (very strong storms, thick ice formations) can affect drone flights. To overcome this, only highly resilient, certified, military-tested platforms should be used.

Cybersecurity Threats: Strong cryptographic encryption and frequency hopping protocols against attempts to disrupt the drone's control channels must be continuously updated.

he integration of artificial intelligence and autonomous patrol drones into the process of ensuring state border security in remote and geographically complex areas is an inevitable and strategic necessity of modern military-technical progress. The capabilities of drones in independent navigation (SLAM), real-time object recognition using neural networks (YOLO), and thermal visualization fully cover the shortcomings of traditional protection methods, elevating border security to a qualitatively new level.

The achievements realized in the experience of the Republic of Uzbekistan–the introduction of modern tactical UAVs into combat duty, integration with fiber-optic networks, and the strengthening of the legal framework–confirm the absolute correctness of the work in this direction.

To further improve this field and increase efficiency, it is advisable to implement the following scientific and practical recommendations:

Adapting software to local conditions: Improving national software algorithms and enriching deep learning databases to ensure that AI and neural network models operate at high speed even under severely limited computing power.

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
OPEN ACCESS JOURNALS

Eureka Journal of Artificial Intelligence and Data Innovation (EJAIDI)

ISSN 2760-5000 (Online) Volume 2, Issue 10, October 2026
This article/work is licensed under CC by 4.0 Attribution
https://eurekaoa.com/index.php/11

Continuously enhancing operator training: Developing a regular training system in special training centers for border service personnel in piloting autonomous drones, analyzing on-board sensor data, and making prompt decisions in emergency situations.

Strengthening cybersecurity and EW resilience: Continuously modernizing cryptographic protocols to ensure the security of communication channels between drones and control centers, and introducing innovative protection layers that increase resilience against electronic warfare tools.

References

1. Ўзбекистон Республикасининг “Давлат чегараси тўғрисида”ги Қонуни // Ўзбекистон Республикаси Олий Мажлисининг Ахборотномаси. – 1999. – № 5. – 97-модда.
2. Раҳимов, Б. Х. Замонавий ҳарбий-техник тизимлар ва уларни бошқариш асослари / Б. Х. Раҳимов. – Тошкент : Фан ва технология, 2022. – 240 б.
3. Мирзаев, Ш. А. Учuvchisiz uchish apparatlari va sun’iy intellekt texnologiyalarini qo‘llash истиқболлари / Ш. А. Мирзаев, Д. Т. Юсупов // Илмий хабарлар. – 2023. – № 2. – Б. 45–52.
4. Gao, Y. Autonomous Navigation of UAVs in GPS-Denied Environments Using SLAM / Y. Gao, J. Smith // IEEE Transactions on Aerospace and Electronic Systems. – 2023. – Vol. 59, no. 2. – P. 1245–1258.
5. Соболев, А. В. Системы компьютерного зрения и нейросети в робототехнике / А. В. Соболев. – Москва : ДМК Пресс, 2021. – 384 с.
6. Johnson, M. R. Border Security and Smart Surveillance Systems: Trends and Challenges / M. R. Johnson, L. K. Brown // Journal of Defense and Security Studies. – 2024. – Vol. 15, iss. 1. – P. 78–94.

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
OPEN ACCESS JOURNALS

Eureka Journal of Artificial Intelligence and Data Innovation (EJAIDI)

ISSN 2760-5000 (Online) Volume 2, Issue 10, October 2026
This article/work is licensed under CC by 4.0 Attribution
https://eurekaoa.com/index.php/11

7. Тўлаганов, Ҳ. М. Ҳарбий учувчисиз учиш аппаратларининг аэродинамик ва навигация хусусиятлари : автореф. дис. ... тех. фан. д-ра / Тўлаганов Ҳасан Муродович. – Тошкент, 2023. – 36 б.
8. Кузнецов, П. С. Кибербезопасность беспилотных летательных аппаратов и защита каналов связи / П. С. Кузнецов // Защита информации. – 2022. – № 4. – С. 33–39.
9. Корнилов, В. И. Применение беспилотных авиационных систем в мониторинге государственно-граничных территорий / В. И. Корнилов. – Санкт-Петербург : Питер, 2020. – 210 с.
10. Russell, S. Artificial Intelligence: A Modern Approach / S. Russell, P. Norvig. – 4th ed. – Pearson, 2020. – 1152 p.