Military Environmental Security under Radiation and Chemical Threats

https://doi.org/10.31713/MCIT.2025.129

Ramil Akhundov
Professor at National Defence University
Baku, Azerbaijan
mr.axundov1@gmail.com

Islam Islamov
Professor at Baku Engineering University
Baku, Azerbaijan
isislamov@beu.edu.az

Abstract - **Radiation and chemical hazards pose persistent, often invisible risks to personnel, civilians, infrastructure, and ecosystems in both peacetime and combat operations. This article presents an integrated concept for a military environmental security system that treats sensing, risk assessment, and decision support as a single end to end capability. We synthesize a threat model for radiological and chemical releases, derive quantitative detection and response objectives, and propose a layered architecture spanning tactical sensors, resilient communications, governed data management, streaming analytics, and role specific decision support. The concept targets compression of the detect to act timeline, reduction of uncertainty, and preservation of legal traceability. A consolidated section summarizes design choices, including k out of n resilience, calibration traceability, and anti spoofing safeguards. A notional case outlines performance metrics such as alarm latency, source localization accuracy, and contour forecast error. The approach converts fragmented practices into a repeatable and auditable function that strengthens force protection and reduces ecological harm. The framework supports phased adoption, after action learning, and alignment with national environmental and public health requirements.**

Keywords - ***environmental security, armed forces, radiation safety, chemical safety, CBRN, risk assessment, dispersion modeling, decision support***

I. INTRODUCTION

Military operations intersect with the environment in complex ways that amplify risks to personnel, civilians, infrastructure, and ecosystems. Among these risks, radiation and chemical hazards are uniquely severe because they can spread invisibly, persist across time, and overwhelm conventional incident response. Modern armed forces must therefore treat environmental security as a mission function that protects combat power, supports operational continuity, and upholds national and international obligations [1-8, 40].

Existing arrangements for radiation, chemical, and biological defense provide essential capabilities such as reconnaissance, detection, decontamination, medical support, and protective equipment. However, these capabilities often operate as fragmented lines of effort with limited data integration, heterogeneous measurement quality, and delayed decision cycles. The result is an operational gap between sensing and action that can increase exposure time, complicate maneuver, and magnify ecological damage during both routine activities and high-tempo operations [9-15, 22-24].

This article addresses that gap by framing environmental security in the armed forces as a system problem. We define a military environmental security system as a layered, interoperable architecture that couples multi-source monitoring with risk assessment and decision support at strategic, operational, and tactical levels. The system integrates fixed and mobile sensors, unmanned platforms, secure communications, streaming analytics, dispersion modeling, and command interfaces that translate environmental signals into prioritized actions for commanders and specialized units [25-30].

The contributions are threefold. First, we formalize a threat model for radiation and chemical hazards in peacetime and wartime, including sources, pathways, and exposure scenarios that inform requirements for monitoring and control [31, 38, 39]. Second, we propose a conceptual architecture with clearly defined data flows, performance objectives, and reliability constraints that align with military command-and-control processes. Third, we present a risk-based method for thresholding alarms, allocating reconnaissance assets, and orchestrating protective measures, illustrated through a case scenario and quantitative effectiveness metrics.

By treating environmental security as an integrated capability rather than a collection of tools, armed forces can shorten detection-to-decision time, reduce false alarms, optimize resource use, and limit both human and ecological harm [32-35]. The following sections review related work, detail the threat model and requirements, and develop the proposed architecture and methods.

II. BACKGROUND AND RELATED WORK

Research on environmental security in the armed forces sits at the intersection of CBRN defense, environmental monitoring, and command-and-control engineering. Classical CBRN doctrine concentrates on detection, individual and collective protection, decontamination, medical countermeasures, and reconnaissance [36, 37]. These functions are well established, yet much of the literature treats them as separate capability lines rather than as a single integrated system that continuously measures, assesses, and informs command decisions.

Work on radiation and chemical monitoring in military contexts has focused on sensor technologies and deployment patterns. Studies describe fixed posts on key facilities, mobile platforms on ground vehicles, and airborne surveys using manned aviation and unmanned aircraft systems. Typical attention centers on sensitivity, selectivity, calibration drift, false alarm rates, and ruggedization. Fewer publications address data quality assurance in field conditions, traceability of measurements, or the fusion of heterogeneous sensor streams.

A second body of work examines environmental data integration and situational awareness. Proposed architectures range from ad hoc data loggers to enterprise service buses that ingest telemetry into centralized repositories. Stream processing frameworks and edge analytics have been explored to reduce latency and bandwidth use [38]. However, many reported implementations stop at visualization and alerting dashboards and do not close the loop with resource allocation, mission planning, or after-action learning.

Modeling and prediction studies contribute dispersion models for radionuclides and toxic industrial chemicals under varying meteorology and terrain. These models are used for contour forecasting, hazard zoning, and route planning [39]. Recent efforts combine model outputs with geospatial intelligence to generate exposure maps and evacuation recommendations. The persistent challenge is the reconciliation of model uncertainty with noisy field observations, especially under contested electromagnetic environments and rapidly changing weather.

Standards and guidance documents provide requirements for instrument performance, sampling, reporting, and interoperability. They support comparability across units and coalitions and help align military practice with national environmental and public health regulations. At the same time, the standards landscape is fragmented across agencies and mission sets, which complicates end-to-end system design and lifecycle management.

Across these threads, recurring gaps are visible. Data are often siloed by platform or unit with limited cross-domain fusion [40]. Detection thresholds are not consistently tied to operational risk and mission objectives. Decision timelines are elongated by manual steps between sensing, modeling, and command approval. Cybersecurity and resilience to spoofing or jamming are addressed unevenly. Finally, rigorous, quantitatively defined performance metrics are rare, which limits comparative evaluation and evidence-based modernization.

This article builds on the prior art by treating environmental security as a layered system that integrates monitoring, risk assessment, and decision support across strategic, operational, and tactical echelons. The next section formalizes a threat model and derives system requirements that unify sensor performance, data quality, modeling fidelity, and command responsiveness.

III. Threat Model and Requirements

The system is designed to protect military personnel, civilians in areas of deployment and operations, critical military infrastructure, weapons and equipment, logistics nodes, and adjacent ecosystems. The impact of threats is assessed through degradation of combat capability, disruption of operations, medical casualties, noncompliance with exposure limits for people and the environment, and long term ecological damage.

Sources of danger include radiation and chemical releases of both intentional and technological origin. Radiation scenarios cover dispersal of radionuclides due to damage to reactors and storage sites, use of radiological devices, residues of depleted uranium, compromise of medical and industrial sources, and re entrainment of deposited fallout through wind lofting or vehicle movement. Chemical scenarios include warfare agents and toxic industrial chemicals released at fixed facilities or during transport, as well as secondary combustion products when depots, refineries, and combined logistics hubs are struck. These hazards are relevant in peacetime at garrisons and training ranges, during deployment and maneuver, in urban terrain, and during strikes on dual use facilities.

Primary exposure pathways are inhalation, ingestion, dermal contact, and external gamma neutron irradiation. Observable indicators for detection include dose rate and particle flux fields, spectrometry, concentrations in air, water, and soil, along with early medical indicators. Pollutant transport and dose formation depend on meteorology, terrain, and urban geometry, which requires accounting for local conditions when interpreting data.

Active adversary countermeasures are assumed, including concealment, delayed releases, source decoys, sensor data spoofing, GPS interference, and electronic attack. Communications may be bandwidth limited and unstable, weather may be volatile, and power and maintenance constraints affect readiness and availability of measurement assets. Under these conditions the system must provide resilience, traceability, and verifiability of data.

Risk is formulated using a probabilistic consequence approach. For each scenario the probability within a planning horizon is evaluated, exposure is computed as a function of concentration fields and duration with allowance for protection level, and consequences aggregate effects on personnel, mission, and environment. Alarm and control thresholds are set on the integrated risk indicator and on early predictors such as the expected exceedance of operational exposure limits.

Detection and estimation objectives are quantitative. The minimally discernible gamma dose rate should be no greater than 0.05 μSv per hour against field background. For priority toxic industrial chemicals the system must detect at levels at or below eight hour occupational limits or AEGL 1 within the first ten minutes from onset. Source localization error for unmanned aerial surveys should not exceed 300 meters, achieved within twenty minutes of the first signal. Median forecast of contamination contours should provide a root mean square error no greater than 500 meters at a range of about three kilometers with updates every thirty minutes.

Time requirements target compression of the detect to act cycle. Time to a first credible alarm from sensor capture to fused alert should be no more than two minutes. The interval from alarm to a recommended action for command and CBRN units including sheltering, route change, and reconnaissance tasking should be no more than five minutes. The common operational picture should refresh at intervals no longer than sixty seconds.

Functional requirements cover continuous multimodal monitoring by fixed stations, mobile teams, and unmanned aerial payloads, along with opportunistic collection from onboard platforms. The system must provide streaming validation, bias correction, spectral classification, and anomaly detection with uncertainty estimation. Modeling must support transport calculations, dose projections, and countermeasure what if analysis in both batch and streaming modes. Decision support must implement risk oriented alerts, prioritization of tasks for CBRN reconnaissance, recommendations on protective postures, and geofenced warnings. After incidents the system automatically compiles a ground truth base for recalibration of models and tracking of performance indicators.

Data quality is ensured by calibrations traceable to national standards, shift based field checks, automatic drift detection, and complete metadata. Each record stores coordinates with positioning accuracy, precise time, instrument state, uncertainty estimate, and operator identifier, and full data lineage is preserved for audit and legal reporting.

Reliability requirements include availability of key services of at least 0.995 over thirty days, sensor to display latency no more than five seconds for critical events, a steady state fused alert false alarm rate no more than one per system per day, mean time to repair frontline sensors no more than two hours, and graceful degradation based on a k out of n principle when channels fail. Communications must function under degraded and denied conditions with traffic prioritization and store and forward modes, interoperate with command systems and CBRN units through open secure data models and interfaces, and maintain time coherence across all nodes with holdover when satellite synchronization is lost.

Cybersecurity and anti spoofing are provided through mutual authentication and integrity checks for telemetry, algorithms for detecting synthetic spectra and artificial plumes, replay detection, and radio frequency monitoring for jamming indicators with automatic fallback to reserve modes. Human machine interfaces are tailored to the roles of commanders, staff, medics, and reconnaissance units, provide clear recommendations and uncertainty visualization, and simulator tools allow rehearsal of plume, sensor network, and communications scenarios to validate standard procedures. Compliance is maintained with national limits on permissible exposures, environmental reporting requirements, and principles of data minimization for medical streams.

In sum, the threat model and the set of quantitative and procedural requirements define the design envelope of the proposed architecture. The next section translates these requirements into a layered system with explicit data flows, time and reliability budgets, and integration rules for command processes.

IV. CONCEPTUAL ARCHITECTURE OF THE MILITARY ENVIRONMENTAL SECURITY SYSTEM

The proposed system is a layered, interoperable architecture that couples continuous monitoring with risk assessment and decision support across strategic, operational, and tactical echelons. Its purpose is to transform heterogeneous environmental signals into timely, actionable recommendations for commanders and specialized CBRN units while maintaining auditability, resilience, and legal compliance. Conceptually, the architecture follows a left-to-right flow from sensing to command action, and a top-to-bottom hierarchy from enterprise policy to frontline execution. For clarity, Fig. 1 depicts the components and principal data paths.

At the tactical edge the system employs a mixed sensor constellation. Fixed posts cover key facilities and training ranges to provide stable baselines and early warning. Mobile teams carry spectrometric and chemical detectors for hotspot confirmation and sampling under protective protocols. Unmanned aerial systems host wide-area payloads for plume mapping, source localization, and terrain-aware surveys. Vehicle-mounted opportunistic sensors extend coverage along patrol routes. Each device stamps measurements with time, position, instrument state, and uncertainty, then publishes compact records through a gateway. Local edge processors perform quality checks, calibration drift tests, spectral classification, and first-pass anomaly detection to reduce noise and bandwidth demand.

Communications form the second layer. The network supports prioritized telemetry and control channels over a mix of radios, cellular links, and line-of-sight relays. Store-and-forward modes preserve continuity during outages. Time synchronization is maintained with GNSS and disciplined holdover to keep clocks aligned when satellites are denied. Traffic shaping ensures that critical alerts preempt routine data, and encryption with mutual authentication protects integrity and origin of messages.

The data management layer ingests validated records into a streaming bus that feeds two stores. A hot store keeps recent telemetry in memory for sub-minute queries and dashboards. A durable store maintains versioned measurements, calibration metadata, and provenance for audit and training of models. Data lineage is preserved end to end so that any visualized map, metric, or decision recommendation can be traced back to raw observations and instrument states. This layer also houses schemas and open interfaces that allow exchange with command-

and-control systems, medical surveillance, and public environmental authorities when coordination is required.

Analytics and modeling provide the computational heart of the system. Stream processors fuse multi-source observations, estimate background fields, and compute confidence intervals. Dispersion engines run in two modes. In streaming mode they update predicted concentration and dose contours at fixed intervals using the latest meteorological nowcasts. In on-demand mode they execute what-if analyses for candidate countermeasures such as evacuation routes, sheltering policies, or reconnaissance tasking. Source term estimation reconciles model predictions with field readings to reduce bias. The analytics tier produces risk indicators that align with operational thresholds defined in the threat model and emits machine-readable recommendations.

Decision support bridges analytics with the command process. A rules and optimization service translates risk indicators into proposed actions for each role. Commanders receive a concise summary of the situation, uncertainty bounds, and a set of recommended measures that include protective posture, route adjustments, tasking of reconnaissance assets, and geofenced warnings. Reconnaissance teams receive targeted waypoints with expected information gain and safe approach corridors that account for wind, terrain, and current exposure. Medical staff receive projected casualty envelopes and triage guidance synchronized with logistics constraints. All recommendations are timestamped, versioned, and reversible, which allows after-action review and incremental learning.

Human-machine interfaces are role-tailored yet share a common operational picture. The main view displays contours of predicted and observed contamination, confidence bands, sensor health, and communications status. A timeline shows the detect-to-act chain with clock budgets for each stage so that staff can immediately see where delays occur. Drill-down panels reveal spectra, calibration checks, and raw counts for expert verification. A training mode replays historical incidents and simulated scenarios to rehearse procedures and validate standard operating protocols without touching the live system.

Reliability and resilience are engineered into each tier. The edge layer supports k-out-of-n coverage so that loss of individual sensors reduces precision but does not blind the system. Communications fail gracefully with automatic switchover to reserve links and deferred delivery during blackouts. Core services are deployed in redundant clusters with health checks and rolling updates to maintain availability targets. Every component exports metrics for latency, loss, and false alarm rates so that the system can enforce service level objectives in real time.

Cybersecurity is treated as a continuous process rather than a perimeter feature. All telemetry is signed and checked for integrity. Behavioral analytics flag spoofed spectra, synthetic plumes, and replayed packets. Radio frequency monitors detect jamming and geolocation degradation, triggering fallbacks such as inertial dead reckoning for time and position. Access controls follow least privilege, and all administrative actions are recorded for accountability.

Governance completes the architecture. A policy service encodes exposure limits, reporting rules, and sharing agreements so that the system can automatically enforce national standards and produce legally admissible records. Model management supports versioning, validation, and rollback of analytical components. After each incident or exercise, the learning pipeline absorbs ground truth, recalibrates models, and updates thresholds to improve performance over time.

In practical terms the architecture turns environmental security from a collection of tools into an integrated capability. Sensors feed trustworthy data, communications carry it with priority and protection, data services preserve its lineage, analytics convert it into risk-aware predictions, and decision support aligns recommended actions with command intent. Fig. 1 summarizes these relationships and the clock budgets between stages, preparing the ground for the methods and implementation details presented in the next section.

VI. UNIFIED CONCEPT AND REQUIREMENTS FOR THE ENVIRONMENTAL SECURITY SYSTEM

Environmental security in the armed forces should be treated as a cross-cutting operational function that reduces risks to personnel, civilians, weapons and infrastructure, while minimizing long-term damage to ecosystems. The key threats arise from radiation and chemical scenarios of both intentional and technogenic origin. They manifest in peacetime at training ranges and garrisons, during deployment and maneuver, in urban environments, and when dual-use facilities are struck. Primary exposure pathways include inhalation, ingestion, dermal contact, and external irradiation. Meteorology, terrain, and urban morphology shape dispersion and dose, which requires locally adaptive monitoring and modeling. An adversary may conceal sources, spoof sensor data, and disrupt navigation and radio communications. Therefore, the system must provide resilience, traceability of measurements, and verifiability of decisions.

Table I. Risk Matrix for Radiological and Chemical Events (with recommended actions)

Probability \ Severity	S1 (Minor)	S2 (Moderate)	S3 (Serious)	S4 (Severe)	S5 (Critical)
P1 (Rare)	Monitor background; log	Increase sampling; verify calibration	Task recon team; prepare shelter-in-place	Temporary movement restrictions	Immediate C2 notification; pre-alert medical
P2 (Unlikely)	Monitor & trend	Local warning; check meteorology	UAS recon; confirm source term	Shelter-in-place; reroute logistics	Raise protective posture; standby decon
P3 (Possible)	Heightened monitoring	Local cordon; sensor QC	Evacuate non-essentials; start modeling	Task CBRN recon; increase PPE level	Partial evacuation; prepare medica triage
P4 (Likely)	Issue local warning	Shelter-in-place	Route changes; establish ICP	Evacuation sectors; geofenced alerts	Full response; decon corridors medical surge
P5 (Almost certain)	rend review & audit	Immediate cordon	Rapid source localization	Deploy countermeasures	Maximum protective posture; interagency coordination

Current practice shows gaps caused by fragmented sensing channels, heterogeneous data quality, manual handoffs between measurement, modeling, and command actions, as well as uneven attention to cyber threats. To close these gaps, environmental security should be designed as a multilayer system that integrates observation, risk assessment, and decision support at strategic, operational, and tactical levels. At the tactical edge, fixed posts, mobile teams, and unmanned aerial payloads operate as complementary assets. Up front, field checks, calibration-drift detection, first-pass spectral classification, and anomaly filtering are performed. Communications provide prioritization of critical telemetry, encryption, and store-and-forward modes for intermittent links. The stream of validated records enters a fast analytics memory tier and a durable repository with preserved provenance, which enables reproduction of any contamination maps and command recommendations.

The analytics loop fuses heterogeneous observations, estimates background fields, runs transport calculations, and produces forecast contours with regular updates, as well as scenario analysis for countermeasure selection. The decision service converts risk indicators into concrete actions for commanders, reconnaissance units, and medical staff. Commanders receive concise summaries with uncertainty bounds and recommended measures; reconnaissance receives routes with expected information gain and safe corridors; medical personnel receive estimates of potential casualties and triage guidance. Interfaces share a common operational picture and allow drill-down to raw spectra and instrument status. Reliability is ensured by component redundancy, target availability levels, and k-out-of-n degradation when sensors or links fail. Cybersecurity is implemented through mutual authentication, integrity control, behavioral analytics for spoofing indicators, and radio monitoring for jamming.

The system is oriented toward measurable goals. Time to a credible alarm is cut to the order of minutes, the interval from alarm to recommended action fits within five minutes, and the common operating picture refreshes up to once per minute. For radiation and chemical hazards, controlled thresholds are set for sensitivity, source-localization accuracy, and contour forecast error. After incidents and exercises, a ground-truth corpus is compiled to retrain models and refine thresholds, closing the loop for continuous improvement.

In this way the concept transforms environmental security from a set of disparate tools into an integrated risk-management capability. The combination of trustworthy measurements, protected and prioritized communications, governed analytics, and disciplined decision-making reduces exposure, avoids false alarms, conserves resources, and diminishes both sanitary and ecological harm while preserving legal admissibility of records and interagency interoperability.

VII.CONCLUSION

This work frames environmental security for the armed forces as an integrated, mission-enabling capability rather than a loose collection of tools. We synthesized the threat landscape for radiation and chemical hazards, specified quantitative detection and response targets, and articulated a layered architecture that links sensing, secure communications, governed data management, streaming analytics, and role-tailored decision support. In doing so, the approach compresses the detect-to-act timeline, reduces uncertainty, and improves protection of personnel, civilians, and ecosystems while maintaining legal traceability and interoperability with command systems. The consolidated concept emphasizes measurable performance (sensitivity, localization accuracy, forecast error, alert latency) and continuous learning through after-action truth capture. Limitations include dependence on communications resilience, model fidelity under rapidly changing meteorology, and the need for rigorous cyber hardening and operator training. Future work should validate the architecture in field exercises with contested electromagnetic conditions, refine source-term estimation and uncertainty quantification, and develop doctrine and KPIs for operational integration across strategic, operational, and tactical echelons. Implemented systematically, the proposed system turns environmental risk management into a repeatable, auditable core function of military readiness.

REFERENCES

[1] R. Akhundov, “Modern developments in the field of weapons of mass destruction and defence against them,” in Problems of Informatization: Proc. 12th Int. Sci. and Tech. Conf., vol. 3, pp. 132–133, 2024.

[2] R. Q. Axundov, “Azərbaycan Ordusunda radiasiya, kimyəvi və bioloji kəşfiyyatın xüsusiyyətləri,” in 4-cü Sənaye İnqilabı və İqtisadiyyatın Rəqəmsallaşdırılması: Beynəlxalq Elmi Konfransın Materialları, pp. 104–108, 2023.

[3] R. Q. Axundov, “Azərbaycan Ordusunda ekoloji təhlükəsizliyin təşkili və təkmilləşdirilməsi,” Hərbi Bilik, no. 4, pp. 7–15, 2024.

[4] S. Babayev et al., “Prospects for the application of nanotechnology in the military sector,” in Problems of Informatization: Proc. 12th Int. Sci. and Tech. Conf., vol. 3, pp. 14–15, 2024.

[5] R. Akhundov and I. Islamov, “Implementation of new technologies for cleaning and neutralizing radiological and chemical contaminants in military environments,” Матеріали конференцій МЦНД, (30.05.2025; Київ, Україна), pp. 321–329, 2025.

[6] R. Akhundov and I. Islam, “Ensuring environmental safety in military activities considering radiological and chemical protection,” Collection of Scientific Papers «SCIENTIA», (May 23, 2025; New York, USA), pp. 175–182, 2025.

[7] E. V. Mammadov et al., “Development of multilayered protection systems against chemical, radiological, and biological hazards for military personnel,” in Current Directions of Development of Information and Communication Technologies and Control Tools, vol. 1, pp. 112–113, 2025.

[8] R. Akhundov, “Establishing a global system for radiation and chemical security monitoring: importance and opportunities for international cooperation,” Collection of Scientific Papers «ΛΌГOΣ», (July 4, 2025; Zurich, Switzerland), pp. 121–127, 2025.

[9] A. H. Hasanov et al., “Scientific and technological progress or environmental safety,” in Problems of Informatization: Proc. 12th Int. Sci. and Tech. Conf., vol. 3, pp. 22–23, 2024.

[10] R. G. Akhundov and E. A. Eldarov, “Special operations forces in modern conflicts,” Вестник науки и образования, no. 6(149), pp. 16–20, 2024.

[11] R. Akhundov, “The environmental impact of military activities,” ResearchGet, 2024. [Online]. Available: ResearchGet. [Accessed: Oct. 4, 2025].

[12] R. Akhundov and I. Islamov, “Innovative technologies for radiation and chemical protection in the armed forces,” Collection of Scientific Papers «ΛΌΓΟΣ», (June 6, 2025; Bologna, Italy), pp. 247–255, 2025.

[13] R. Akhundov and I. Islamov, “Implementation of new technologies for cleaning and neutralizing radiological and chemical contaminants in military environments,” Матеріали конференцій МЦНД, (30.05.2025; Київ, Україна), pp. 321–329, 2025.

[14] R. G. Akhundov and A. M. Talibov, “Environmental safety as a component of national security,” in The Latest Technologies – for the Protection of Airspace: Abstracts of the 20th Int. Sci. Conf. of Kharkiv National University of the Air Force Named After Ivan Kozhedub, Kharkiv, Ukraine, May 2–3, 2024, pp. 25–27.

[15] Р. Г. О. Ахундов, “Построение экспериментальных изотерм адсорбции образцами угленаполненного химзащитного субстрата,” Наука, техника и образование, no. 10(63), pp. 16–20, 2019.

[16] Р. Г. Ахундов, А. Г. Ахмедова, Ш. Д. Даньялов, и И. И. Мустафаев, “Радиационно-стимулированные процессы получения активного угля,” Санкт-Петербург, vol. 25, no. 1, p. 47, 2020.

[17] R. Akhundov and D. Sh., “The use of modified activated coal in sorption of carbon-monoxide,” in Materials of the Int. Sci.-Practical Conf. “Radiation and Chemical Safety Problems”, Baku, Nov. 2019, pp. 161–162.

[18] R. Akhundov, “Ecocide in the Nagorno-Karabakh conflict: an analysis of Armenia’s environmental impact on Azerbaijan,” in Current Directions of Development of Information and Communication Technologies and Control Tools. Abstracts of the 14th Int. Sci. and Tech. Conf., Kharkiv, Ukraine, vol. 2, pp. 95–96, Apr. 2024.

[19] R. Akhundov and I. Islamov, “Operational modes of environmental security systems in the armed forces facing radiation and chemical threats,” Collection of Scientific Papers «SCIENTIA», (Aug. 22, 2025; Bern, Switzerland), pp. 103–111, 2025.

[20] R. Akhundov and I. Islamov, “Innovative technologies for enhancing environmental security in armed forces under radiation and chemical threats,” Матеріали конференцій МЦНД, (15.08.2025; Харків, Україна), pp. 141–150, 2025.

[21] R. Akhundov and I. Islamov, “Comprehensive approach to establishing operational modes of environmental security systems in military forces under radiation and chemical hazards,” Collection of Scientific Papers «SCIENTIA», (Aug. 8, 2025; Liverpool, UK), pp. 108–116, 2025.

[22] R. Akhundov, “Application of innovative technologies for the decontamination and neutralization of radiological and chemical hazards in military environments,” Collection of Scientific Papers «ΛΌΓΟΣ», (Aug. 1, 2025; Seoul, South Korea), pp. 107–115, 2025. doi: 10.36074/logos-01.08.2025.017.

[23] R. Akhundov and I. Islamov, “Exploring the potential, challenges, and future of robots and autonomous systems in warfare,” Матеріали конференцій МЦНД, (18.07.2025; Тернопіль, Україна), pp. 117–126, 2025.

[24] R. Akhundov, “Advancements in monitoring radiation and chemical hazards for military environmental safety,” Матеріали конференцій МЦНД, (04.07.2025; Ужгород, Україна), pp. 89–97, 2025. doi: 10.62731/mcnd-04.07.2025.002.

[25] S. M. Babayev et al., “The impact of new technologies on the progress of military art,” in Proc. Int. Sci. and Practical Conf., vol. 6, pp. 54–56, 2024.

[26] A. Talibov et al., “Environmental safety of nanomaterials application,” in Problems of Informatization: Proc. 12th Int. Sci. and Tech. Conf., vol. 3, pp. 55–56, Baku–Kharkiv–Bielsko-Biala, 2024.

[27] R. Akhundov and E. Hashimov, “The impact of new technologies on enhancing the efficiency of armed,” Матеріалы конференцій МЦНД (13.06.2025; Lutsk, Ukraine), pp. 186–195, 2025.

[28] R. Akhundov and E. Hashimov, “The environmental impact of war: Effects, challenges, and solutions,” Матеріали конференцій МЦНД (27.06.2025; Dnipro, Ukraine), pp. 103–112, 2025.

[29] A. M. Talibov et al., “The use of unmanned aerial vehicles for monitoring chemical and radiation contamination,” in Current Directions of Development of Information and Communication Technologies and Control Tools: Proc. 15th Int. Sci. and Tech. Conf., vol. 4, pp. 88–89, 2025.

[30] A. M. Talibov et al., “Modeling and forecasting radiological and chemical threats in the military sphere,” in Current Directions of Development of Information and Communication Technologies and Control Tools: Proc. 15th Int. Sci. and Tech. Conf., vol. 1, pp. 120–121, 2025.

[31] A. M. Talibov et al., “Application of biotechnology to mitigate the consequences of radiological and chemical contamination,” in Current Directions of Development of Information and Communication Technologies and Control Tools: Proc. 15th Int. Sci. and Tech. Conf., vol. 1, pp. 86–87, 2025.

[32] A. R. Jabrayilov et al., “Development of a comprehensive environmental protection system for military facilities,” Current Directions of Development of Information and Communication Technologies and Control Tools, vol. 4, pp. 82–83, 2025.

[33] A. Jabrayilov et al., “Digital technologies and artificial intelligence in the management of environmental safety in the army,” in Current Directions of Development of Information and Communication Technologies and Control Tools: Proc. 15th Int. Sci. and Tech. Conf., vol. 1, pp. 110–111, 2025.

[34] A. M. Talibov et al., “Training military personnel in radiation and chemical threat protection methods,” in Proc. 15th Int. Sci. and Tech. Conf., vol. 4, pp. 94–95, 2025.

[35] A. R. Jabrayilov et al., “Experience of international cooperation in the field of military environmental safety,” Current Directions of Development of Information and Communication Technologies and Control Tools, vol. 1, pp. 116–117, 2025.

[36] A. R. Jabrayilov et al., “Prospects for creating closed ecological life support systems,” Current Directions of Development of Information and Communication Technologies and Control Tools, vol. 4, pp. 92–93, 2025.

[37] A. R. Jabrayilov et al., “The role of environmental monitoring in ensuring the safety of military units,” Current Directions of Development of Information and Communication Technologies and Control Tools, vol. 1, pp. 128–129, 2025.

[38] A. Talibov et al., “The main anthropogenic sources of atmospheric pollution,” in Problems of Informatization: Proc. 12th Int. Sci. and Tech. Conf., vol. 3, pp. 53–54, Baku–Kharkiv–Bielsko-Biala, 2024.

[39] R. Mammadov et al., “Enhancing special forces management efficiency in modern operations,” in Problems of Informatization: Proc. 12th Int. Sci. and Tech. Conf., vol. 3, pp. 31–32, 2024.

[40] I. Islamov et al, “Integrating environmental security into defense strategy with a focus on radiological and chemical risks,” Strategic directions of science development: Factors of influence and interaction: Collection of scientific papers with materials of the VII International Scientific Conference, Cherkasy, Ukraine, Sept. 26, 2025, pp. 115–125. doi: 10.62731/mcnd-26.09.2025.