HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

TRENDS IN THE DEVELOPMENT OF AUTOMATED COMMAND AND CONTROL SYSTEMS FOR AIR DEFENSE ASSETS

Sirojitdinov Erkin Salimovich
PhD, Associate Professor
Military Institute of Information and
Communication Technologies and Communications
Email: whitehorsepapas2@gmail.com

doi:**https://doi.org/10.5281/zenodo.23168444**

Abstract. This article examines major trends in the development of automated command and control systems for air-defense assets, with emphasis on architecture, data integration, decision support, interoperability, cyber resilience, human-machine teaming, and institutional requirements. The study uses a structured qualitative review of open official documents and peer-reviewed or professionally reviewed publications, combining evidence from NATO and allied institutions with official sources from the Republic of Uzbekistan. The results indicate a transition from platform-centric and vertically integrated Command and Control toward federated, modular, data-centric systems-of-systems. The article concludes that successful modernization depends less on acquiring isolated technologies than on establishing interoperable standards, high-quality data governance, secure communications, rigorous testing and evaluation, and a phased human-centered transformation model. The analysis remains at the strategic and systems-engineering level and does not address operational vulnerabilities or tactical employment procedures.

Keywords: automated command and control; air defense; integrated air and missile defense; Command and Control; artificial intelligence; sensor fusion; interoperability; data-centric architecture; cyber resilience; Uzbekistan.

Annotatsiya. Ushbu maqolada havo hujumidan mudofaa vositalarini avtomatlashtirilgan boshqarish tizimlarining rivojlanishidagi asosiy tendensiyalar arxitektura, ma’lumotlarni integratsiyalash, qaror qabul qilishni qo‘llab-quvvatlash, o‘zaro muvofiqlik, kiberbarqarorlik, inson va mashina hamkorligi hamda institutsional talablar nuqtai nazaridan tahlil qilingan. Tadqiqot ochiq rasmiy hujjatlar, taqrizdan o‘tgan ilmiy maqolalar va professional nashrlarning tizimli sifat tahliliga asoslangan bo‘lib, unda NATO va ittifoqdosh tashkilotlar materiallari O‘zbekiston Respublikasining rasmiy manbalari bilan uyg‘unlashtirilgan. Tadqiqot natijalari havo hujumidan mudofaa sohasidagi boshqaruv tizimlari platformaga yo‘naltirilgan va vertikal integratsiyalashgan modeldan federativ, modulli, ma’lumotlarga asoslangan hamda o‘zaro bog‘langan tizimlar majmuasi modeliga o‘tayotganini ko‘rsatadi. Maqolada muvaffaqiyatli modernizatsiya alohida texnologiyalarni xarid

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

qilishdan ko‘ra, o‘zaro muvofiq standartlarni joriy etish, ma’lumotlarni samarali boshqarish, xavfsiz aloqa infratuzilmasini shakllantirish, tizimlarni qat’iy sinov va baholashdan o‘tkazish hamda inson omiliga yo‘naltirilgan bosqichma-bosqich transformatsiya modelini amalga oshirishga ko‘proq bog‘liq ekanligi asoslangan. Tahlil strategik va tizimli muhandislik darajasida olib borilgan bo‘lib, operatsion zaifliklar yoki taktik qo‘llash tartib-taomillarini qamrab olmaydi.

Kalit so‘zlar: avtomatlashtirilgan boshqaruv; havo hujumidan mudofaa; integratsiyalashgan havo va raketaga qarshi mudofaa; qo‘mondonlik va boshqaruv; sun’iy intellekt; sensor ma’lumotlarini birlashtirish; o‘zaro muvofiqlik; ma’lumotlarga asoslangan arxitektura; kiberbarqarorlik; O‘zbekiston.

Аннотация. В данной статье рассматриваются основные тенденции развития автоматизированных систем управления средствами противовоздушной обороны с акцентом на архитектуру систем, интеграцию данных, поддержку принятия решений, оперативную совместимость, киберустойчивость, взаимодействие человека и машины, а также институциональные требования. Исследование основано на структурированном качественном анализе открытых официальных документов, рецензируемых научных публикаций и профессиональных источников, объединяющем материалы НАТО и союзных организаций с официальными источниками Республики Узбекистан. Результаты исследования свидетельствуют о переходе от платформо-ориентированных и вертикально интегрированных систем управления к федеративным, модульным, ориентированным на данные комплексам взаимосвязанных систем. В статье обосновано, что успешная модернизация зависит не столько от приобретения отдельных технологий, сколько от внедрения совместимых стандартов, эффективного управления данными, обеспечения защищённой связи, проведения строгих испытаний и оценки систем, а также реализации поэтапной модели трансформации, ориентированной на эффективное взаимодействие человека и автоматизированных средств. Анализ выполнен на стратегическом и системно-инженерном уровнях и не затрагивает вопросы эксплуатационных уязвимостей или процедур тактического применения.

Ключевые слова: автоматизированное управление; противовоздушная оборона; интегрированная противовоздушная и противоракетная оборона; командование и управление; искусственный интеллект; объединение данных датчиков; оперативная совместимость; архитектура, ориентированная на данные; киберустойчивость; Узбекистан.

INTRODUCTION

Air-defense command and control has evolved from a primarily hierarchical function—receiving radar reports, forming an air picture, issuing orders and coordinating individual weapon units—into a networked information-management problem in which heterogeneous sensors, decision nodes, communications systems and defensive effectors must operate as a coherent whole. The change is driven by the diversity, speed and scale of contemporary aerial threats, including small unmanned

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

aircraft, cruise and ballistic missiles and other complex air vehicles. NATO's 2025 Integrated Air and Missile Defence (IAMD) Policy explicitly describes the air domain as increasingly contested and identifies coherent use of sensors and C3I, multi-domain interoperability, speed, agility, resilience and survivability as central requirements [9].

The central technological problem is no longer merely the automation of individual command-post functions. It is the creation of a trusted digital environment in which data can be collected, correlated, shared and converted into decision-relevant information with sufficient speed and reliability. NATO accordingly defines its IAMD structure through interconnected national and Alliance sensors, command-and-control assets and weapon systems, while its current digital transformation agenda emphasizes data-centric architecture, secure access to trusted data and interoperability across domains [7], [10].

This transformation has important organizational consequences. Automated Command and Control systems increasingly combine software-defined services, distributed computing, common data models, secure tactical and strategic communications, modelling and simulation, and AI-assisted analytics. Yet automation does not remove the need for human judgment. Rather, the design challenge is to allocate tasks appropriately between people and machines, preserve accountability, provide explainable recommendations and ensure that operators can continue to function under degraded information or communications conditions. NATO's revised AI strategy therefore couples accelerated adoption with principles of lawfulness, responsibility and accountability, explainability and traceability, reliability, governability and bias mitigation [8].

The topic is also relevant to Uzbekistan. The Defence Doctrine of the Republic of Uzbekistan calls for the introduction of modern information and communication technologies into the management system of the state military organization [16]. More recent official initiatives go further: in 2025 an international scientific-practical conference in Uzbekistan focused specifically on the role of automated command systems in troop management, and in May 2026 national authorities announced measures to further develop automated command-and-control systems, artificial intelligence, cybersecurity structures, satellite communications and specialized military education [4], [15].

The aim of this article is to identify and systematize the principal development trends in automated Command and Control systems for air-defense assets and to assess their implications for future capability development, with particular attention to lessons relevant to Uzbekistan. The research questions are: (1) Which architectural and technological trends are most consistently supported by current authoritative sources? (2) How are AI, data-centricity and interoperability changing the role of automated Command and Control? (3) Which organizational, cybersecurity and human-factor conditions determine whether these technologies produce dependable operational value? and (4) Which development priorities are most relevant for a phased national modernization pathway?

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

LITERATURE REVIEW

From automated command posts to integrated air and missile defense

Classical automated command systems were designed largely around defined echelons, dedicated sensor channels and specific weapon complexes. Their principal advantages were faster transmission of reports, standardized processing, reduced manual workload and more consistent execution of command procedures. However, vertically integrated architectures tend to create "stovepipes": a sensor, command post and weapon system may work effectively as a package but exchange limited information with systems outside that package. Contemporary IAMD concepts challenge this model by treating the defense enterprise as a network of interconnected capabilities rather than a collection of independent batteries or platforms.

NATO's public description of NATINAMDS illustrates this systems perspective: national and NATO capabilities are connected through a command structure, and integration depends on procedural, technical and human interoperability. The 2025 policy identifies four functional areas—air surveillance; battle management, command, control, communications and information (BMC3I); active air and missile defence; and passive air and missile defence—and stresses coordination among them [9]. In this conception, Command and Control is not simply a command-post application but the connective layer that converts distributed sensing and defensive resources into a coherent capability.

The United States' Integrated Battle Command System (IBCS) is another publicly documented example of the architectural shift. Open sources describe it as an effort to connect sensors and effectors that were not originally designed to work together, replacing platform-specific control arrangements with an integrated command-and-control environment [1], [17]. The important analytical point is not any particular system configuration, but the broader move toward "any appropriate sensor–shared picture–available effector" logic enabled by common interfaces and networked Command and Control.

Data fusion and the common operational picture

Air-defense Command and Control depends on the quality of the operational picture. Multiple sensors may observe the same object with different accuracy, update rates, classifications and levels of confidence. Automated fusion therefore has to correlate observations, manage duplicate tracks, reconcile uncertainty and present a coherent representation to operators. NATO's 2025 policy explicitly identifies capable surveillance data fusion and analysis—including potential use of AI and machine learning—as critical to producing a coherent and accurate battlespace picture [9].

The literature increasingly treats data itself as a strategic resource. NATO's Data Exploitation Framework calls for data governance, standardization, connectivity, open data architecture and AI-enabled analytics; the 2025 Data Strategy further emphasizes a secure data-sharing ecosystem and data-centric reference architecture [6], [10]. This shifts modernization priorities from purchasing isolated applications toward managing data definitions, metadata, quality, access controls, interfaces

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

and lifecycle governance across organizations.

Artificial intelligence and decision support

Academic literature on intelligent air-defense Command and Control commonly groups AI applications into information processing, situation cognition, decision-option generation, human-machine interaction and effectiveness assessment. Li et al. [2], for example, identify these areas as key technologies for intelligent air-defense and anti-missile command and control. Experimental research has also explored deep reinforcement learning and related methods for decision support in stylized air-defense problems [18]. These studies demonstrate the research potential of AI but should not be interpreted as evidence that fully autonomous command is mature or appropriate for real-world deployment.

Official policy is more cautious and operationally useful. NATO's revised AI strategy emphasizes AI-ready quality data, testing/evaluation/verification/validation (TEV&V), interoperability and responsible-use principles. This suggests that near-term value is likely to come from bounded decision-support functions—classification assistance, anomaly detection, information prioritization, forecasting, resource-status analysis and operator workload reduction—rather than unqualified delegation of command authority to algorithms [8].

Open architecture, federation and interoperability

Open architecture is becoming a central design principle because air-defense systems have long service lives while sensors, communications and software evolve rapidly. In 2025, the NATO Communications and Information Agency (NCIA) described a federated systems-of-systems approach based on open standards, modular components, published interfaces, common data models and shared services. Such an approach allows services to be developed and upgraded more independently while maintaining interoperability [13].

MITRE's 2024 study on coalition air and missile defense similarly argues that integration should not require every participant to adopt one monolithic system. A federated model can preserve national requirements and sovereignty while allowing timely information exchange across heterogeneous national Command and Control and defensive systems [3]. This is particularly relevant for states that must modernize incrementally and integrate legacy assets rather than replace an entire defense architecture at once.

Cyber resilience, electronic contestation and continuity of command

Greater connectivity increases both capability and dependence. A data-centric Command and Control architecture must therefore be designed for disruption. NATO's IAMD policy calls for resilience by design against kinetic and non-kinetic disruption, including cyberattack and electromagnetic warfare [9]. The implication for engineering is that availability, integrity, authentication, segmentation, recovery, redundancy and degraded-mode operation are not secondary cybersecurity features; they are core performance attributes of the command system.

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

Uzbekistan's recent digitalization agenda also reflects this linkage. Official reporting in 2026 noted an Information Security Monitoring Center within the Ministry of Defense and proposed additional AI and cybersecurity structures alongside further development of automated Command and Control and satellite communications [5]. This indicates that national modernization is increasingly being framed as an integrated digital, communications and cyber-resilience problem.

METHODOLOGY

This study applies a structured qualitative literature review and comparative policy analysis. The unit of analysis is the development trend—not a specific weapon system. Sources were selected according to four criteria: authority, relevance, recency and verifiability. Priority was given to official documents from NATO, NCIA, the Government and President of Uzbekistan, and publicly accessible institutional material; peer-reviewed academic publications and established research organizations were used to supplement official policy evidence.

The review focused primarily on materials published or updated between 2021 and 2026, while older normative documents were retained when still legally or conceptually relevant. The Uzbek Defence Doctrine of 2018 was included because it remains an important public policy basis for the use of modern information and communication technologies in military management. Search concepts included "air command and control," "integrated air and missile defence," "automated command system," "data-centric Command and Control," "sensor fusion," "AI decision support," "interoperability," "open architecture," "cyber resilience," and Uzbek/Russian equivalents related to automated troop management and defence digitalization.

After source collection, statements were coded into thematic categories: (A) architecture; (B) sensing and data fusion; (C) data governance; (D) AI and decision support; (E) interoperability; (F) communications and resilience; (G) human-machine teaming; (H) modelling, simulation and testing; and (I) education and institutional capacity. A trend was considered "strongly supported" when it appeared consistently across multiple authoritative sources and was reflected in current capability programs or policy documents. The comparative component then assessed whether recent Uzbek official initiatives correspond to the same categories.

The method has limitations. Public sources cannot reveal classified system performance, detailed operational procedures or vulnerabilities; academic demonstrations may use simplified assumptions; and official policy documents express intended direction rather than guaranteed implementation. Consequently, the article makes no claims about classified capabilities or combat effectiveness. Its conclusions concern observable development directions, governance requirements and systems-engineering implications.

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

RESULTS AND DISCUSSION

Trend 1: transition to federated, modular systems-of-systems

The strongest architectural trend is the replacement of tightly coupled platform-centric Command and Control by federated systems-of-systems. This does not mean that every component becomes technically identical. Instead, heterogeneous components exchange standardized information through defined interfaces and shared services. The architecture separates, as far as practical, the lifecycle of applications from the lifecycle of individual sensors or defensive platforms.

This direction is visible in NATO's eAirC2 transformation. In July 2026, NCIA announced contracts for the first implementation phase of a modern, data-centric Air Command and Control environment built around open standards and a common data foundation. The stated goals include secure operational information exchange, improved situational awareness, faster decision-making and easier integration of future capabilities [14]. Together with the 2025 open-architecture discussions, this provides concrete evidence that modularity and federation have moved from general aspiration to active program design.

Trend 2: data-centric command and control

The second trend is a conceptual shift from application-centric automation to data-centric Command and Control. In older designs, information is often locked inside a particular application or command echelon. In data-centric designs, trusted data are treated as a shared strategic asset that authorized services can discover and use under governance rules. NATO's Data Exploitation Framework, Digital Transformation Implementation Strategy and Data Strategy all reinforce this principle [6], [7], [10].

Trend 3: multi-sensor fusion and distributed situational awareness

Modern air-defense Command and Control increasingly depends on combining observations from multiple sensor types and locations. The purpose is not simply to display more tracks, but to improve confidence, continuity and context. NATO identifies persistent surveillance, networked active and passive sensors, space-derived information and advanced fusion/analysis as components of modern IAMD situational awareness [9].

Trend 4: AI as bounded, testable decision support

AI is likely to become pervasive in automated Command and Control, but the evidence supports a bounded-assistance model rather than an assumption of unrestricted autonomy. High-value applications include filtering large data volumes, identifying anomalies, supporting classification, recommending priorities, forecasting system states, retrieving relevant knowledge and assisting staff work. These functions can shorten the cognitive path between observation and decision while leaving command responsibility with authorized personnel.

Three constraints are decisive. First, AI quality depends on representative, governed and secure data. Second, performance must be tested under realistic and degraded conditions, including distribution shifts and incomplete data. Third, human-machine interfaces must communicate

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

confidence, uncertainty and rationale sufficiently for responsible use. NATO's revised AI strategy explicitly emphasizes quality data, responsible-use principles, AI-ready personnel and TEV&V infrastructure, making governance inseparable from technical adoption [8].

Trend 5: multi-domain and coalition interoperability

Air defense is increasingly embedded in a broader multi-domain information environment. Relevant information may originate from air, land, maritime, space or cyber sources, and defensive actions may require coordination across services and national boundaries. NATO therefore treats interoperability as procedural, technical and human, not merely as a communications protocol [9].

Trend 6: resilience by design and distributed Command and Control

Automation creates a paradox: greater integration can improve speed and coordination, yet excessive centralization can create dependence on a small number of nodes or communications paths. Current policy therefore combines centralized direction with decentralized execution and emphasizes redundancy and reconfigurability. NATO's 2025 IAMD policy explicitly calls for complementarity between centralized control and decentralized execution, as well as the ability to reconfigure networks and resources as conditions change [9].

Trend 7: digital engineering, modelling, simulation and continuous testing

As Command and Control becomes software-intensive, modernization cannot rely only on periodic field trials. Digital engineering, modelling and simulation support requirements analysis, interface validation, operator training and assessment of alternative architectures before physical integration. NATO Allied Command Transformation explicitly treats experimentation, wargaming, modelling and simulation as enablers of digital transformation and capability development [12].

Trend 8: human-centered automation and workforce transformation

Automated Command and Control is frequently discussed as a technology program, but authoritative sources consistently identify people and processes as co-equal pillars. NATO's digital transformation strategy defines transformation across people, processes and technology, while its AI strategy highlights workforce retraining and deeper integration of technical expertise into military operations [8], [12].

Uzbekistan: alignment with global development directions

Uzbekistan's public policy trajectory shows increasing convergence with the global trends identified above. The 2018 Defence Doctrine established a policy basis for introducing modern information and communication technologies into the military management system. In December 2025, a dedicated international scientific-practical conference at the Military Institute of Information and Communication Technologies and Communications examined the role and status of automated control systems in troop management, indicating an institutional research focus on the subject [16], [4].

Table 1. Synthesis of trends

Development trend	Primary driver	Expected Command and Control effect	Key implementation condition

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

Federated open architecture	Heterogeneous/legacy systems and rapid technology change	Faster integration and upgrade cycles	Stable interfaces, standards, configuration governance
Data-centric Command and Control	Need for shared, reusable information	Common operational picture and analytics	Data quality, metadata, access control, provenance
Multi-sensor fusion	Diverse and distributed sensing	More coherent situational awareness	Time synchronization, uncertainty management
AI-enabled decision support	Information volume and decision tempo	Prioritization and cognitive assistance	TEV&V, explainability, human accountability
Multi-domain interoperability	Cross-service and coalition operations	Wider information sharing and coordination	Technical, procedural and human interoperability
Resilient/distributed Command and Control	Cyber/EW and physical disruption	Continuity under degraded conditions	Redundancy, segmentation, graceful degradation
Digital engineering & simulation	Software complexity and integration risk	Earlier verification and faster iteration	Representative test environments and scenarios
Workforce transformation	New digital roles and human-machine teaming	Effective and responsible use of automation	Training, doctrine, technical career development

In May 2026, official announcements described a broader next stage of military digitalization. Measures included further development of automated command-and-control systems, expansion of robotic and autonomous systems research, creation or strengthening of AI and cybersecurity structures, a satellite communications center, and organizational posts responsible for digitalization, AI and cybersecurity. The same announcement emphasized development of national AI models and qualified personnel [15], [5].

CONCLUSION AND RECOMMENDATIONS

The development of automated command and control systems for air-defense assets is best understood as a transition from isolated automation toward a resilient digital ecosystem. The defining characteristic of the emerging model is not a single algorithm or command-post product but the ability to combine heterogeneous sensors, information services, decision-support tools and defensive resources through governed data and interoperable interfaces. NATO policy and current Air Command and Control programs provide strong evidence for this shift toward federated, open, modular and data-centric architectures.

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

AI will be an important accelerator, particularly for information processing and decision support, but its value depends on data quality, testing, cybersecurity, explainability and human accountability. Similarly, increased connectivity must be balanced by resilience: future Command and Control should be designed to reconfigure, degrade gracefully and preserve essential command functions when communications or services are disrupted. The modernization problem is therefore simultaneously technical, organizational and educational.

For Uzbekistan, the direction established by the Defence Doctrine and reinforced by 2025–2026 official initiatives is broadly consistent with global development trends. The most productive next step is to convert individual digitalization projects into a coherent capability architecture in which communications, automated Command and Control, AI, cybersecurity, research infrastructure and military education are governed as parts of one long-term transformation program.

Recommendations

- Adopt a national reference architecture for defense Command and Control based on modularity, open interfaces, common data models and controlled federation, so that modernization can proceed incrementally without creating new information silos.
- Create a formal defense data-governance framework covering data ownership, quality, metadata, provenance, classification, access, retention and exchange. AI projects should be treated as downstream consumers of this trusted data foundation.
- Prioritize multi-sensor information integration and common situational awareness at the architecture level. Evaluation metrics should include data quality, continuity, confidence and operator comprehension—not only processing speed.
- Introduce AI first in bounded decision-support and staff-assistance functions where performance can be measured and human responsibility is clear. Establish national procedures for testing, evaluation, verification and validation of AI-enabled defense software.
- Engineer cyber resilience and continuity from the beginning: secure-by-design development, segmentation, identity and access management, redundancy, backup communications, recovery procedures and realistic exercises should be mandatory requirements.
- Establish an integration and simulation laboratory for automated Command and Control where legacy and new systems can be tested through representative interfaces and scenarios before field introduction. Use digital engineering to reduce integration risk and support lifecycle upgrades.
- Develop human capital in parallel with technology: create advanced curricula for Command and Control systems engineering, data engineering, AI assurance, cybersecurity, human-machine interaction and software lifecycle management, while maintaining strong operator training for degraded modes.
- Use phased capability development with measurable maturity gates. Each phase should demonstrate interoperability, resilience, usability and maintainability before additional automation is introduced.

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

REFERENCES

1. Center for Strategic and International Studies (CSIS) Missile Defense Project. (2021). Integrated Air and Missile Defense Battle Command System (IBCS). Missile Threat. https://missilethreat.csis.org/defsys/ibcs/
2. Li, T., Wang, G., Guo, X., Fu, Q., & Wu, M. (2024). Research on the development of air defense and anti-missile intelligent command and control. Tactical Missile Technology, 2024(4), 115–122. https://doi.org/10.16358/j.issn.1009-1300.20240041
3. McFeely, A., Giachinta, R., Milner, T., Coons, R., Adams, M., McCarthy, M., & Butners, D. (2024). Coalition Air and Missile Defense: Integration and Interoperability. MITRE.
4. Ministry of Digital Technologies of the Republic of Uzbekistan. (2025, December 19). “Qo‘shinlar boshqaruvini amalga oshirishda avtomatlashtirilgan boshqaruv tizimini qo‘llashning o‘rni va nufuzi” mavzusida xalqaro ilmiy-amaliy konferensiya bo‘lib o‘tdi. https://digital.gov.uz/oz/mudofaa/news/view/112197
5. Ministry of Digital Technologies of the Republic of Uzbekistan. (2026). Military education and army digitalization to be taken to a new level. https://www.digital.gov.uz/en/news/view/162785
6. NATO. (2022). Summary of NATO’s Data Exploitation Framework Strategic Plan. https://www.nato.int/en/news-and-events/articles/news/2022/11/23/summary-of-natos-data-exploitation-framework-strategic-plan
7. NATO. (2024a). NATO’s Digital Transformation Implementation Strategy. https://www.nato.int/cps/en/natohq/official_texts_229801.htm
8. NATO. (2024b). Summary of NATO’s revised Artificial Intelligence (AI) strategy. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy
9. NATO. (2025a). NATO Integrated Air and Missile Defence Policy. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/02/13/nato-integrated-air-and-missile-defence-policy
10. NATO. (2025b). Data Strategy for the Alliance. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/05/05/data-strategy-for-the-alliance
11. NATO Allied Command Transformation. (2024). The Integrated Air and Missile Defence Centre of Excellence: A Cornerstone of NATO’s Security. https://www.act.nato.int/article/iamd-coe-2024/
12. NATO Allied Command Transformation. (2026). Digital Transformation. https://www.act.nato.int/activities/digital-transformation/
13. NATO Communications and Information Agency (NCIA). (2025, November 6). NCIA leads discussion on Command and Control Open Architecture at Air and Missile Defence

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

Technology Conference. https://www.ncia.nato.int/newsroom/news/ncia-leads-discussion-on-command-and-control-open-architecture-at-air-and-missile-defence-technology-conference

14. NATO Communications and Information Agency (NCIA). (2026, July 7). NATO accelerates transformation of Air Command and Control with key contract awards. https://www.ncia.nato.int/newsroom/news/nato-accelerates-transformation-of-air-command-and-control-with-key-contract-awards
15. President of the Republic of Uzbekistan. (2026, May 7). Military education and digitalization of the army to be elevated to a new level. https://www.president.uz/en/lists/view/9184
16. Republic of Uzbekistan. (2018). Law No. ZRU-458 "On the Defence Doctrine of the Republic of Uzbekistan." LexUZ. https://www.lex.uz/uz/acts/3495906
17. U.S. Army. (2026, February 19). IBCS and the future of offensive and defensive integrated fires. https://www.army.mil/article/290087/ibcs_and_the_future_of_offensive_and_defensive_integrated_fires
18. Zhao, et al. (2023). Deep reinforcement learning-based air defense decision-making using potential games. Advanced Intelligent Systems. https://doi.org/10.1002/aisy.202300151