FEBRUARY 2026

How Russia Is Reshaping Command and Control for AI-Enabled Warfare

AUTHOR
Kateryna Bondar

A Report of the CSIS Wadhwani AI Center

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

Contents

FEBRUARY 2026

How Russia Is Reshaping Command and Control for AI-Enabled Warfare

By Kateryna Bondar

Executive Summary

This paper examines how Russia is transforming its command and control (C2) architecture under wartime pressure, how these changes shape the country's incremental move toward battlefield-required software solutions, and what lessons U.S. policymakers can learn from Russia's experiences. Focusing on both strategic ambitions and battlefield practice, the takeaways below summarize how automated C2 systems, unmanned platform management software, and emerging AI applications are being developed, adapted, and scaled within Russia's military ecosystem.

1. **Russia is no longer prioritizing the construction of a single, comprehensive automated C2 architecture comparable to Western joint concepts; instead, it is reallocating effort toward tactical, task-specific software, driven by battlefield necessity.** Prolonged, high-intensity combat in Ukraine exposed the limits of centralized, system-wide C2 modernization and elevated the importance of accelerating the tactical kill chain. The emergence of systems such as the "Svod" Tactical Situational Awareness Complex and other integrated reconnaissance-strike tools reflects a pragmatic shift in which operational control of unmanned systems and real-time battlefield management now deliver greater military value than achieving end-to-end C2 integration.
2. **Because unmanned systems now conduct up to 80 percent of Russian fire missions, the center of gravity in C2 innovation has shifted toward software that manages drones and integrates them with artillery and other fire units.** Civilian engineers and volunteer developers have focused on closing this gap by building tools that provide situational awareness, automate fire correction, and link unmanned aircraft systems (UAS) operators directly to firing units. Russia's "Glaz/Groza" software complex demonstrates this trend, functioning as a unified

reconnaissance-strike workflow that converts drone footage into targeting data and compresses the time from detection to impact from hours to minutes.

3. **The Russian military assesses its AI capabilities for visual and audio data processing as relatively mature, placing computer vision, sensor fusion, and signal analysis at technology readiness level (TRL) 6–9, while natural-language processing remains at an early, experimental stage, TRL 1–3.** This disparity reflects a deliberate prioritization of AI applications that deliver immediate battlefield utility—such as target recognition, guidance, and autonomous terminal functions for unmanned systems—and where abundant data and combat validation are available. By contrast, text analysis AI, which underpins document processing and higher-level C2 decision support, remains constrained by immature architectures, limited certified software, and organizational barriers, slowing progress toward fully AI-enabled command workflows.
4. **Within Russian C2 systems, AI is primarily envisioned as a support function rather than a replacement for human decisionmaking.** Russian military doctrine assigns AI two core roles: enhancing the processing and interpretation of sensor data and providing predictive decision support through forecasting, scenario generation, and recommendations for commanders. Across strategic and tactical levels, AI is intended to augment situational awareness and analytical capacity, while formal authority and responsibility for decisions remain firmly with human commanders.
5. **Russia began its C2 digitalization effort by building a dense layer of standards governing terminology, system architecture, hardware-software integration, and information management.** This standardization drive, coupled with the transition to the domestically controlled Astra Linux operating system, reflects an attempt to create a unified technical foundation capable of supporting data integration, interoperability, and future AI insertion across the command hierarchy. While this framework provides structural coherence, it has not, on its own, resolved deeper institutional and methodological constraints that continue to limit system-wide C2 integration.
6. **To enable AI-driven tactical software, the Russian military launched a systematic data collection effort in 2025 focused on unmanned operations and strike outcomes.** The emerging data infrastructure aggregates UAS video feeds, operator telemetry, strike effects, and individual pilot performance metrics, each linked to unique personal identifiers. These datasets serve multiple functions simultaneously: operational analysis, training evaluation, and the creation of labeled data for AI model development, establishing a feedback loop that ties battlefield performance directly to software refinement.
7. **Despite efforts to reduce dependence on foreign commercial technologies, Russia's military AI development remains heavily reliant on open-weight models and civilian software ecosystems.** The transition from tools such as AlpineQuest and Discord toward domestic alternatives like ZOV Maps and Astra-based platforms reflects a push for security and sovereignty at the application layer. At the same time, Russian developers actively adapt open-weight and commercially available AI models, including Mistral, Qwen, LLaMA, YOLO, and related architectures, for military use, embedding them into on-premise, tightly controlled

environments. This hybrid approach allows Russia to mitigate sanctions and accelerate AI adoption without building foundational models from scratch.

Russia's approach to AI-enabled command and control reflects a decisive shift away from abstract, large-scale modernization concepts and toward solving concrete battlefield problems. Rather than pursuing a fully integrated, end-to-end C2 architecture, Russia has focused on tactical, task-specific software that directly accelerates the kill chain and improves the effectiveness of unmanned systems where operational payoff is immediate and measurable. Its investment in AI follows the same pragmatic logic—prioritizing computer vision, sensor fusion, and signal processing applications that have proven mature under combat conditions, while treating more ambitious uses of AI, such as text analysis and higher-level decision support, as secondary and experimental.

> *Russia is not chasing technological elegance or conceptual completeness but rather applying AI selectively and ruthlessly in service of battlefield effectiveness.*

Where Russia's own AI capabilities remain underdeveloped, particularly in natural-language processing, it compensates not by attempting to build frontier models, but by adapting open-weight architectures developed elsewhere. By leveraging U.S., Chinese, and European advances and embedding them into controlled, military-specific environments, Russia accelerates adoption while avoiding the cost and risk of foundational model development. These choices show a broader pattern: Russia is not chasing technological elegance or conceptual completeness but rather applying AI selectively and ruthlessly in service of battlefield effectiveness.

Introduction

This white paper is the first in a series examining how Russia is moving toward AI-enabled autonomy in military operations. The paper establishes the C2 layer as the foundational substrate of this transformation, arguing that autonomy in unmanned systems, decision support, and battlefield management cannot be understood without first analyzing how Russia conceptualizes, builds, and adapts its automated command infrastructure under wartime conditions.

This paper focuses on Russia's long-running effort to create an automated C2 system for forces and weapons (ACCS)—a concept that, in Russian military thinking, represents a fully digital, end-to-end environment linking sensors, commanders, and weapons into a single decision-execution loop. While this vision closely parallels Western concepts such as Joint All-Domain Command and Control (JADC2), the Russian path has been shaped by different institutional constraints, technological dependencies, and, most recently, the operational pressures of the war in Ukraine. As a result, Russia's approach has evolved from attempts to field comprehensive, centralized systems toward a more fragmented, but pragmatically effective, ecosystem of task-specific software, many of which are optimized for unmanned systems and rapid kill-chain acceleration.

The analysis proceeds from the strategic to the tactical level. It begins by outlining how ACCS is defined in Russian doctrine and professional military literature, tracing its origins, architecture, and the standardization framework the Ministry of Defence has built to support long-term C2 modernization. It assesses the actual state of progress at the strategic level and then shifts to the tactical level, where wartime necessity has driven experimentation with new battlefield management tools, especially for unmanned systems, and where Russia's most tangible advances in automated C2 have occurred.

The analysis also examines the role of AI in Russian C2 systems and assesses its current state of development and implementation at different levels of command, from strategic decision support concepts embedded in automated control architectures to tactical applications that process sensor data, manage unmanned systems, and accelerate battlefield decision cycles.

RESEARCH APPROACH AND SOURCES

This analysis is based on open-source research and does not rely on classified information. The source base comprises Russian primary materials, including official military journals published by the General Staff and affiliated defense research institutions, which provide insight into doctrinal thinking, technical priorities, and the formal conceptualization of automation, C2, and AI within the Russian Armed Forces.

In parallel, the research systematically monitored and analyzed more than 150 Russian Telegram channels and closed or semi-closed groups associated with civilian engineers, volunteer technologists, and military-affiliated developers supporting the Russian war effort. These communities offer granular, near real-time visibility into how specific systems evolve, what technical problems developers encounter, and how they adapt to constraints.

Finally, this report includes analysis of official Russian media, government publications, and public statements by senior leadership, including President Vladimir Putin, Defence Minister Andrei Belousov, and other senior officials, to assess how the Kremlin frames technological priorities, projects progress, and signals shifts in strategic direction through formal communication.

Russian Command and Control in Transition Toward Autonomy

In Russian military doctrine and professional discourse, the push toward automation and a fully digital operating environment is framed as the creation of "automated command and control system for forces and weapons," commonly referred to as the Automated Command and Control System (ACCS). According to Russian military thinking, ACCS is a set of integrated automated control and information systems, complexes of equipment for automation, software-hardware complexes, and remote automated workstations distributed across the command hierarchy.[1] Though the definition may appear somewhat complex, this concept most closely aligns with the United States' JADC2.

This section examines the evolution of Russia's efforts to develop all-encompassing, automated C2 systems and its subsequent shift toward smaller, functional software solutions deployable on the battlefield. It assesses the current state of progress in developing these systems, traces their origins, and

1 Б.Б. Ишечкин, В.Б. Ишечкин, С.В. Евтихов [B.B. Ishchekin, V.B. Ishchekin, and S.V. Evtikhov], "Перспективы применения искусственного интеллекта в управлении войсками" [Prospects for the Application of Artificial Intelligence in Command and Control of Troops], Военная Мысль [*Military Thought*], no. 8 (2023): 84–79.

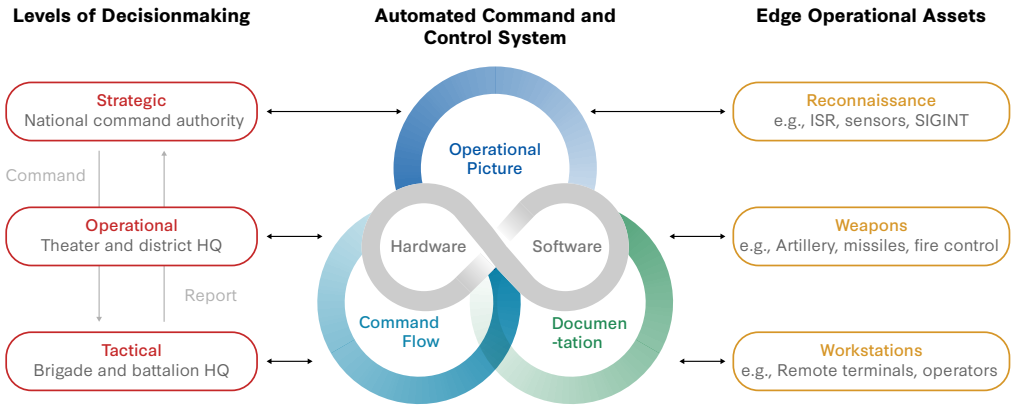
analyzes the role of civilian and commercial technologies, including AI, in shaping their development and operational use.

ASSESSING RUSSIA'S ADVANCEMENT IN AUTOMATED C2 TECHNOLOGIES AT A STRATEGIC LEVEL

As shown in Figure 1, ACCS is a system of systems in which command structures, operational headquarters, reconnaissance assets, and weapons platforms are interconnected within a single integrated environment for decisionmaking and execution. The central purpose of such a meta-system, as described in Russian military literature, is to increase the effectiveness of force employment by automating core command processes, namely

- continuous collection, processing, and visual display of data outlining the operational picture at the level of operators' workstations;
- receipt, evaluation, and transmission of combat orders, alerts, identification signals, and targeting instructions; and
- real-time documentation, storage, and processing of operational information and combat documentation as actions unfold.

Figure 1: Automated Command and Control System (ACCS) Architecture



Note: ISR = intelligence, surveillance, and reconnaissance; SIGINT = signals intelligence.

Source: CSIS analysis.

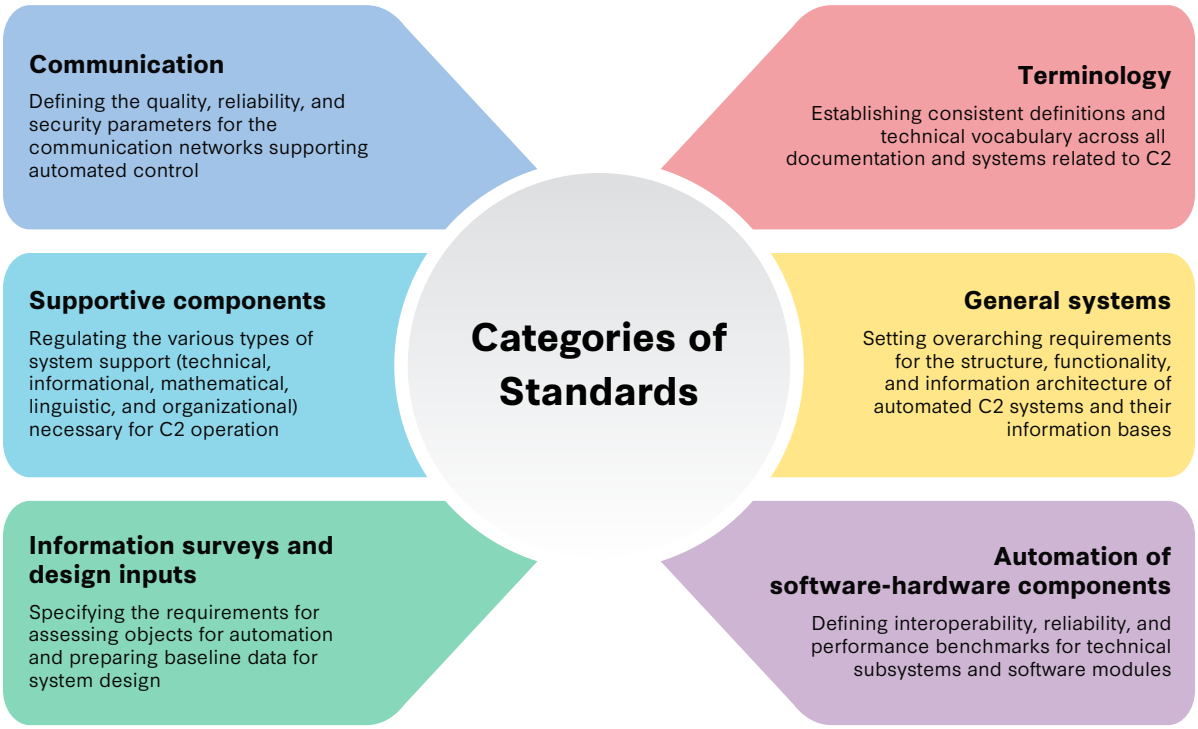
The ACCS concept emphasizes the seamless fusion of technical systems and workflows to integrate decisionmaking with execution. Its central objective is to minimize the temporal gaps between target detection, situational assessment, command issuance, and the application of force. The model aspires to establish a unified, interoperable, and secure digital environment that connects all tiers of the C2 structure, from tactical units to strategic leadership.

Publicly available data provides limited insight into the actual progress achieved in developing this concept. Nevertheless, military and technical literature indicates that Russia's efforts to build the ACCS began in the early 2000s, with an initial emphasis on standardization. Over the subsequent two decades, the Russian Ministry of Defence has pursued a comprehensive approach to formalize and

standardize the evolution of its automated C2 systems. This approach has centered on developing a coherent classification framework for C2 systems, delineating them by functional purpose and hierarchical level, and harmonizing technical, informative, and organizational parameters across all stages of their life cycle.[2]

To institutionalize these developments, the Ministry of Defence has introduced a set of state military standards regulating the design, production, maintenance, and integration of automated C2 systems, as shown in Figure 2. These standards encompass terminology, system architecture, software-hardware integration, information management, and communication protocols. Together, they provide the regulatory backbone of Russia's C2 modernization program, establishing a coherent technical foundation that supports interoperability, data integrity, and the gradual incorporation of AI and autonomous capabilities into military decisionmaking.

Figure 2: Categories of Standards for Russia's Automated C2



Source: A.A. Протасов et al. [A.A. Protasov et al.], "Актуальные вопросы стандартизации автоматизированных систем управления войсками (силами)" [Current Issues in the Standardization of Automated Command and Control Systems for Troops (Forces)], Военная Мысль [*Military Thought*], no. 3 (2025): 48–59; and CSIS analysis.

An important step toward technical standardization and technological sovereignty has been the Russian military's **shift** from Microsoft Windows to a domestic operating system, **Astra Linux**. A software company **RusBITech began** developing the system in 2008, and the Ministry of Defence formally **adopted** it as the unified operating platform for automated C2 systems in 2013. Built on **open-source**

2 А.А. Протасов, В.Н. Козичев, В.А. Двойченков, and А.А. Комиссаров [A.A. Protasov, V.N. Kozichev, V.A. Dvoichenkov, and A.A. Komissarov], "Актуальные вопросы стандартизации автоматизированных систем управления войсками (силами)" [Current Issues in the Standardization of Automated Command and Control Systems for Troops (Forces)], Военная Мысль [*Military Thought*] no. 3 (2025): 48–59.

Linux, Astra Linux allows full access to and control over source code, enabling customization for military security requirements that were not possible with closed-source Western software. The Astra Linux Special Edition is now marketed as a single system deployed across C2 systems, servers, and onboard equipment and weapon systems that integrates with secure government **document** and **geospatial systems** and that supports domestic processors such as Elbrus and Baikal, reducing reliance on foreign software and hardware.

These actions—standardization efforts and the introduction of locally developed software—suggest that the Ministry of Defence has sought to consolidate military digital infrastructure around a secure, domestically controlled digital infrastructure. These measures were taken to reduce external technological dependencies and ensure that critical military and administrative systems operate in a unified, certified environment aligned with national security requirements.

This effort points to an attempt to establish a foundational layer for automated C2 through standardization and the adoption of a single operating environment. At the same time, the absence of a fully deployed, end-to-end ACCS at the tactical level and the continued reliance of frontline units on volunteer-developed and commercial tools, indicate limited success in translating this foundational work into a functioning, large-scale automated C2 system.

Russia's development of an integrated ACCS remains constrained by deep-seated methodological and institutional barriers. One central problem is that the Ministry of Defence continues to rely on Soviet-era, state-owned research and development (R&D) institutes whose engineering cultures, processes, and incentives are optimized for traditional hardware-centric programs. These institutions perform well when producing familiar legacy systems such as missiles, electronic warfare (EW) complexes, and other conventional platforms, but they lack the talent base, methodology, and organizational agility required for modern software, data-centric architectures, and AI-enabled capabilities. They also cannot match the speed, flexibility, and iterative innovation cycles characteristic of private technology companies.

Additional inefficiencies compound this problem and, in many cases, stem directly from it. One of the most persistent issues is the poor quality and delayed delivery of foundational data to system developers. As a result, design and modernization work often begins without complete, consistent, or timely information on operational needs, integration pathways, or user requirements.

This information gap originates in outdated procedures for conducting "informational surveys," the preliminary phase in which necessary data on system requirements and operating conditions is collected and analyzed before software development begins. Russia's methods, which still rely heavily on paper-based questionnaires and on collecting inputs from a wide array of stakeholders, create significant aggregation and synthesis challenges, diverge from modern data collection and storage practices, and fail to match the complexity of contemporary digital architectures or the demands of network-centric warfare.

Compounding the problem is fragmented institutional responsibility. Data collection and ownership are dispersed among multiple organizations with poorly defined accountability, resulting in duplication, delays, and inconsistent datasets across military and industrial actors.

Finally, the regulatory base itself remains partly obsolete. Existing standards fail to address emerging requirements for interoperability, cybersecurity, and data governance, and do not clearly define the structure or documentation of survey and design processes.

Overall, Russia's difficulties in advancing its automated C2 systems are rooted less in technological constraints than in methodological and organizational shortcomings that undermine coherence, timeliness, and system integration across the defense establishment.

ASSESSING RUSSIA'S ADVANCEMENT IN AUTOMATED C2 TECHNOLOGIES AT A TACTICAL LEVEL

Russia's **announcement** of the "Svod" Tactical Situational Awareness Complex in August 2025 triggered a noticeable wave of discussion among military analysts, largely because it signals yet another attempt to resolve a long-standing problem inside the Russian Armed Forces: the persistent gap between ambitions for network-centric warfare and the uneven performance of actual C2 systems in combat.

The announcement by Defence Minister Andrei Belousov was particularly striking not merely because Svod is a new system, but also because the system was described as the next major step in Russia's effort to build a coherent digital ecosystem at the tactical level. According to official statements, the system has been under active development **since 2024**, and was expected to begin experimental field deployment in Russian units in the **fall of 2025**, with plans for large-scale production and integration across all operational units to follow. This tight timeline reflects broader institutional pressure to modernize Russia's C2 apparatus amid the ongoing war in Ukraine.

Yet the origins of Svod remain ambiguous. It is unclear whether this is a genuinely new architecture or simply a reconfiguration of earlier projects that never achieved operational maturity. The most relevant precedent system is the **Unified Tactical-Level Control System** (UTLCS), a program that Russian authorities once positioned as their breakthrough in digital C2. UTLCS reportedly was used during the **Kavkaz 2016** exercises and moved into production stage by 2018. Its concept was tied to Russia's declared vision of network-centric warfare—a tactical environment where secure multifunctional radios, onboard computing nodes, and distributed data links would give units a real-time operational picture and enable faster decision cycles.

In practice, however, UTLCS **never lived up** to that promise. Reports from the field suggested substantial technical and organizational failures: unreliable data links, inconsistent integration across units, and limited resistance to EW—each of which undermined Russia's aspiration for seamless digital command. The system became a symbol of the gap between theoretical modernization rhetoric and actual battlefield performance.

Svod is being positioned as a new solution to these old problems. It will only matter, however, if it represents not an incremental upgrade but an entire system that addresses the vulnerabilities exposed in earlier attempts at tactical digitalization. These include the need for survivable communications under heavy EW pressure, interoperable data formats across disparate units, faster processing of battlefield sensor inputs, and user interfaces adapted to real operational conditions rather than laboratory assumptions.

The emergence of Svod should be read less as a single programmatic bet and more as evidence of Russia's capacity to absorb failure and adapt under pressure. Russian military innovation rarely follows public-facing, large-scale presentations or declared breakthroughs. Instead, systems are typically developed with limited visibility, deployed experimentally, and iterated directly through combat use. If lessons from earlier failures such as UTLCS have been internalized, the indicator of success will not be formal announcements but rather a qualitative shift in how Russian units conduct operations—shorter decision cycles, tighter integration between sensors and fires, and more resilient tactical coordination. Whether through Svod or a successor system, such changes would signal that Russia has translated battlefield experience into functional C2 adaptation rather than merely rhetorical modernization.

Evolving C2 for Unmanned Systems

The war in Ukraine has reshaped the priorities and urgency of the problems that Russian military leadership seeks to solve first. Colonel Sergey Ishtuganov, deputy head of the Armed Forces' Unmanned Systems Forces, explained in an interview that UASs now carry out up to 80 percent of all fire missions in the war. Russian forces strike roughly 300 targets each day, including armored vehicles and fortified positions.[3] These figures illustrate both how decisive unmanned systems have become in combat and that the Russian military increasingly ties the success of its operations to how effectively it manages these systems.

Yet, Russian forces operate an increasingly heterogeneous mix of platforms, rely on human-centric control with limited autonomy, use incompatible communication channels, and face constant spectrum congestion—all of which make it difficult to scale unmanned systems, limit interoperability, slow deployment, and disrupt effective C2. Therefore, the Russian Armed Forces now view integration of all types of unmanned platforms, the codification of combat lessons, and the establishment of an automated, unified combat management architecture as an essential and top priority.

> *Russian forces operate an increasingly heterogeneous mix of platforms, rely on human-centric control with limited autonomy, use incompatible communication channels, and face constant spectrum congestion.*

By early 2025, however, Russian military scholars openly acknowledged that, despite the urgency, the Ministry of Defence and the emerging unmanned systems branch still had not fielded a fully functional, full-scale UAS management system. The scholars argued that Ukraine had already deployed comparable automated tactical C2 systems—such as Delta, with its integrated UAS control modules—in the field, putting Russian forces roughly 1.5 to 2 years behind Ukraine.[4]

---

3 Н.В. Антошин [N.V. Antoshin], "Вооруженных Силах РФ созданы войска беспилотных систем" [Unmanned Systems Troops Established in the Armed Forces of the Russian Federation] // Красная Звезда [*Red Star*], no. 214, November 13, 2024.

4 S.I. Makarenko and K.V. Kozlov, "Automated control system for unmanned aerial vehicles when they jointly figure out combat missions," *Systems of Control, Communication, and Security* 1 (2025): 131–155 (in Russian), doi:10.24412/2410-9916-2025-1-131-155.

Recognizing the scale of the problem, both military and volunteer civilian engineers have focused on developing software that provides situational awareness, refines fire correction, and enables more integrated control of unmanned systems.

GOVERNMENT-LED EFFORTS TO DEVELOP A COMBAT MANAGEMENT SYSTEM

The Russian military prototypes that do exist, including several ground and air control or sensor integration systems, either largely treat unmanned platforms as remote sensors or provide only narrow functions, and none of them can manage large-scale, heterogeneous UAS operations. As a result, Russian military leaders have realized that they cannot manage the rapidly expanding UAS force by means of legacy control concepts or fragmented, stalled C2 initiatives. Leadership has therefore begun shifting its focus from broad automated C2 concepts, such as ACCS, to a more targeted system built specifically for unmanned systems management.

Russia has not released a full plan, but its direction becomes clear when the fragmented initiatives showcased in state media are viewed in tandem. These signals reveal a consistent push to build new systems and to embed AI-enabled technologies into their architecture. Two sets of actions in particular reveal Russia's larger push for a new, centralized system.

First, the military began collecting large volumes of drone footage and turning it into structured datasets. Precise timelines for the first centralized directives remain unclear, but available reporting indicates that Defence Minister Andrei Belousov **initiated** this effort in mid-2025 by directing the establishment of a unified database to record and analyze enemy losses inflicted by drones. Building such a database required a system capable of automatically recording, aggregating, and processing information from UAS operators, thereby generating data both for operational analysis and for training AI models intended to enhance drone operations effectiveness.

In late August 2025, the Ministry of Defence shared a video of Belousov **inspecting** the command post of the "Center" force grouping. Although most likely part of Russian propaganda efforts, the video provides a glimpse into what the Russian military is working on currently. During the minister's visit, the staff reported that they had fulfilled his directive to create and populate a database capturing effects achieved by UASs. They also demonstrated a software system that automatically aggregated and analyzed operator-reported drone activity. Staff assured Belousov that the system was able to integrate all classes of drones currently in use.

The video showcased an emerging system that not only captures how each drone performs but also how each operator develops over time. Instructors gain access to detailed performance trajectories for every pilot, tracking whether individual skills improve or deteriorate. Each operator's footage is linked to a unique personal identification number assigned to every trainee. This linkage between personal IDs and video streams eliminates opportunities to manipulate results or falsify performance data. All stored material contributes directly to AI training datasets.

Second, the military began developing a battlefield management system designed specifically for drone operations. In September 2025, the Ministry of Defence **convened** a Technical Council on the Development of the Drone Management System to advance efforts aimed at creating a unified system for managing drone missions. The council brought together senior leaders from the military,

research institutes, industrial enterprises, and operational units, with a central focus on improving C2 of unmanned systems across the air, ground, and potentially maritime domains.[5]

The database aggregating detailed records of enemy losses functions both as a training tool and as an analytical resource for refining drone employment tactics. As these tactics evolve, they feed directly into updates of the system's design and the outputs it can generate. In parallel, the ministry **is testing** a software platform that allows field operators to transmit UAS data automatically into a different database from which a drone management system synthesizes and analyzes the information in an automated mode. The broader objective is to create a continuous feedback loop that links drone operators, command elements, and system developers, ensuring that tactical insights translate rapidly into technical improvements.

OUT-OF-GOVERNMENT EFFORTS TO DEVELOP BATTLEFIELD MANAGEMENT SOFTWARE

Beyond the formal military initiatives, a parallel ecosystem of software solutions has emerged from the commercial sector, volunteer civil engineers, and often anonymous developers. The dynamic resembles a trend observed in Ukraine: Commercial technologies are rapidly weaponized and adapted for military needs by civilian innovators and volunteer groups, who operate with greater speed, agility, and creativity than traditional military institutions shaped by older R&D cultures and methods.

Russian forces have leaned heavily on commercial off-the-shelf software, most notably **AlpineQuest**, a civilian navigation app repurposed by Russia as a battlefield mapping tool. Originally designed for hikers and off-road users, AlpineQuest enabled Russian **troops to work** with offline topographic maps, mark targets and artillery positions, plan routes, and share coordinates across units. Its accessibility and support for multiple coordinate systems had made AlpineQuest a de facto navigation aid **discussed** openly in military Telegram channels. This reliance, however, created a major security vulnerability. In early 2025, a **compromised version** of the app circulated through unofficial channels, **embedding** spyware that quietly exfiltrated geolocation data, contacts, files, and GPS logs. The episode demonstrated how dependence on unsecured commercial software exposed Russian units to surveillance and intelligence collection through their own digital tools.

A similar pattern emerged with **Discord**, a commercial communication platform originally built for gaming. Russian units **adopted** it for ad hoc C2, using voice channels, text chat, and live video to stream drone feeds, exchange targeting data, and coordinate attacks in real time. Discord's ease of use and ability to run on personal devices made it especially attractive to frontline drone teams. Yet this convenience also became a liability. In 2024, Russian authorities **banned** Discord, designating it a foreign platform accused of **hosting** extremist or illicit content. This move abruptly **disrupted** improvised coordination networks and forced Russian units to rely on VPNs to retain access to Discord. Despite the ban, many have **continued to use** the platform due to the lack of comparable alternatives.

5 А. Тихонов [A. Tikhonov], "На повестке дня – совершенствование управления беспилотными средствами" [Improving the Management of Unmanned Systems on the Agenda], Красная Звезда [*Red Star*], no. 180, September 25, 2025.

> *While Russia's rapid repurposing of civilian technologies addressed urgent battlefield needs, it also introduced systemic vulnerabilities.*

These cases demonstrate that while Russia's rapid repurposing of civilian technologies addressed urgent battlefield needs, it also introduced systemic vulnerabilities. In response, volunteer networks and civilian developers supporting the war effort began building domestic alternatives that were later taken up, formalized, and scaled by the Russian Armed Forces.

Beginning in early 2024, the first references to new domestically developed battlefield management systems started to **appear** in Russian media and official communications. These initiatives signaled a wider effort to replace the many improvised and often compromised commercial tools that had dominated the first years of the war in Ukraine. What emerged was the outline of a deliberate push to build secure, purpose-designed systems that could withstand both external threats and the structural vulnerabilities exposed by earlier ad hoc solutions.

The "Glaz/Groza" software system represents one of Russia's efforts to digitize military operations. Though its developer remains unknown, that is typical for many of the civilian-military initiatives which have become fielded Russian battlefield technologies. Originally designed for artillery and mortar fire adjustment, Glaz/Groza developed into a much broader solution. Available **evidence suggests** that the system was developed in 2023 and that pilot versions had entered operational units in early 2024, likely for troop-level trials under combat conditions. However, **reporting from August 2025** suggests that Glaz/Groza has since become relatively widespread, with drone units, artillery batteries, fire control crews, and supporting reconnaissance elements all making routine use of its hardware and software.

The Glaz/Groza complex functions as a layered digital ecosystem designed to link UAS reconnaissance, geospatial mapping, and artillery fire control into a single integrated workflow. At its core, the system consists of three major components: the **Glaz** family of applications used by drone operators, the **Groza** fire control and mission management environment, and the auxiliary **ZOV Maps** platform that extends the overall system's cartographic and geospatial capabilities.

Glaz represents the drone operator–facing segment of the complex. Installed on DJI and Autel remote controllers as well as on Android tablets, it provides UAS pilots with real-time tools for geolocation, target marking, and rapid extraction of coordinates directly from drone footage. Despite the variety of versions—ranging from lightweight builds for commercial drones to more advanced types optimized for professional platforms—the Glaz suite performs one function: transforming UAS footage into precise digital target data and passing this information seamlessly into the broader system.

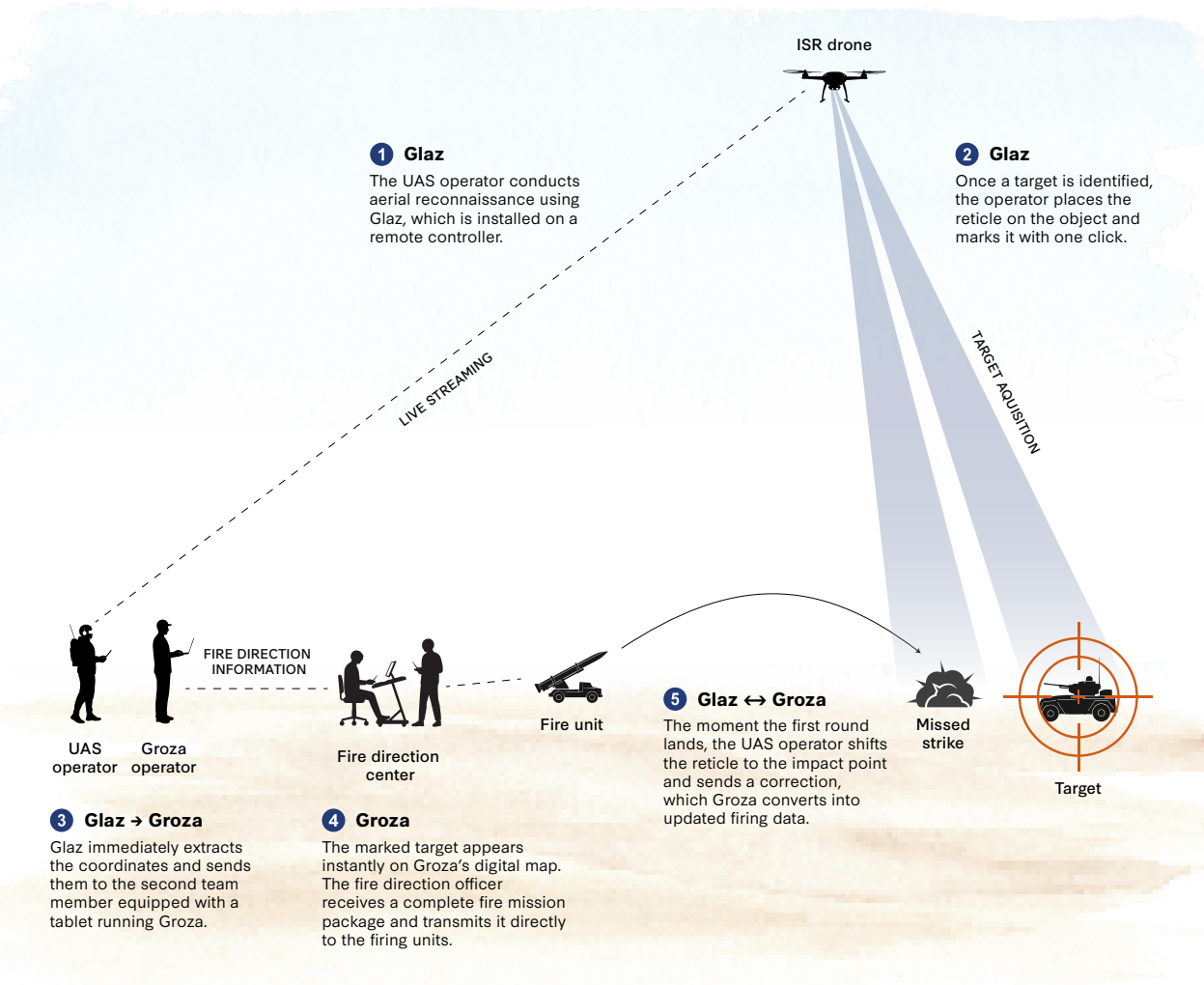
If Glaz is the reconnaissance interface, Groza serves as the decisionmaking and fire support hub. Running on Windows laptops or Android tablets, Groza offers a full-featured digital map environment, automated artillery adjustment tools, and channels for rapidly transmitting coordinates, corrections, and impact assessments to artillery, mortar, and tank crews.

Over time, Groza has expanded beyond traditional fire control. In its more recent iterations, it integrates newly introduced **drone mission planning capabilities** aimed at solving two chronic,

related operational problems inside Russian UAS units: the uncontrolled competition for frequencies and regular friendly jamming. The new module allows units to reserve frequencies within their area of responsibility, plan routes for drone flights with radio-visibility calculations, and maintain an inventory of drones, effectively centralizing coordination of strike UAS missions within the same digital environment used for reconnaissance and artillery support.

Complementing both systems, ZOV Maps provides an alternative to AlpineQuest. ZOV Maps is a domestic mapping platform, compatible with Groza and other Russian military applications, that **offers** online and offline geospatial layers, improved tools for annotating and editing objects on the map, and more stable handling of live geolocation feeds. ZOV Maps functions as the cartographic backbone of the Glaz/Groza complex, allowing military units to navigate terrain, share positional data, and build a shared operational picture using domestic mapping resources.

Figure 3: The Glaz/Groza Digital Kill Chain



Source: CSIS analysis.

As shown in Figure 3, the Glaz/Groza complex functions as an integrated reconnaissance-strike system that links UAS operators, fire direction centers, and firing units into a single digital kill chain. The **process** of conducting a strike begins with a drone team. The UAS operator conducts aerial reconnaissance using Glaz, which is installed on a remote controller. Once a target is identified, the operator places the crosshair on the object and marks it with one click. Glaz immediately extracts the coordinates from the drone's telemetry and sends them to a second team member equipped with a tablet running Groza.

Groza **operates** as the fire control hub. The marked target appears instantly on its digital map, after which the system automatically performs ballistic calculations using pre-loaded firing tables for Russian artillery and mortar systems. The fire direction officer receives a complete fire mission package—range, deflection, and elevation—and transmits it directly to the firing units. The moment the first round lands, the UAS operator shifts the crosshair to the impact point and sends a correction, if needed, which Groza converts into updated firing data. This digital feedback loop replaces earlier manual orientation and voice reports, reducing the time from detection to impact from hours to just a **few minutes**.

In conversations with CSIS researchers, Ukrainian military sources have mentioned another Russian system, Astra-M, which visually resembles Ukraine's Delta situational awareness platform and is reportedly intended either to provide similar functions to Delta or to serve as a replacement for Discord in Russian units. Its name strongly echoes Astra Linux, the secure operating system developed for the Russian military and government mentioned previously, suggesting that Astra-M may be linked to the same developer or built on a military-approved technological stack. Whether this system will reach full deployment remains to be seen.

> *While the Russian military continues to experiment and often lags behind Ukraine in developing new innovations, it rapidly scales any tools that prove effective.*

The Glaz/Groza complex and the possible existence of the Astra-M system demonstrate that while the Russian military continues to experiment and often lags behind Ukraine in developing new innovations, it rapidly scales any tools that prove effective. New software solutions are rolled out systematically, and they begin with training. Instruction now takes place across formal Russian military academies, dedicated training centers, and volunteer-run drone schools. At the training range of the "Center" force grouping, for instance, mortar crews are **learning** to operate the newly fielded Glaz/Groza software complex—a system also **included** in the curriculum of the Mikhailovskaya Military Artillery Academy and the "Arkhangel" school, where the training program spans **10 days**.

Together, these components—Glaz for UAS sensing, Groza for command and fire control functions, and ZOV Maps for geospatial support—form a unified digital architecture intended to accelerate Russia's kill chain at the tactical level. The recent integration of drone mission management indicates a further evolution toward consolidating reconnaissance, strike planning, and artillery coordination within a single software ecosystem.

This larger developmental ecosystem highlights the central role of Russia's volunteer and civilian engineering community in addressing the military's most urgent battlefield gaps. Drawing on a broad civilian talent pool, volunteer groups rapidly adapt commercial technologies and develop bespoke software that supports combat operations using the latest available tools, often faster than formal defense institutions can respond.

Where the Russian military consistently demonstrates strength is not in initial innovation but in scaling what works. Once a software solution proves operationally useful, it is quickly formalized, standardized, and propagated throughout the Russian force, with military training serving as the primary vector of diffusion. From the outset of drone instruction, soldiers are trained not only on platforms and tactics but also on the accompanying digital tools, ensuring that software adoption becomes embedded in routine operations rather than treated as an auxiliary capability.

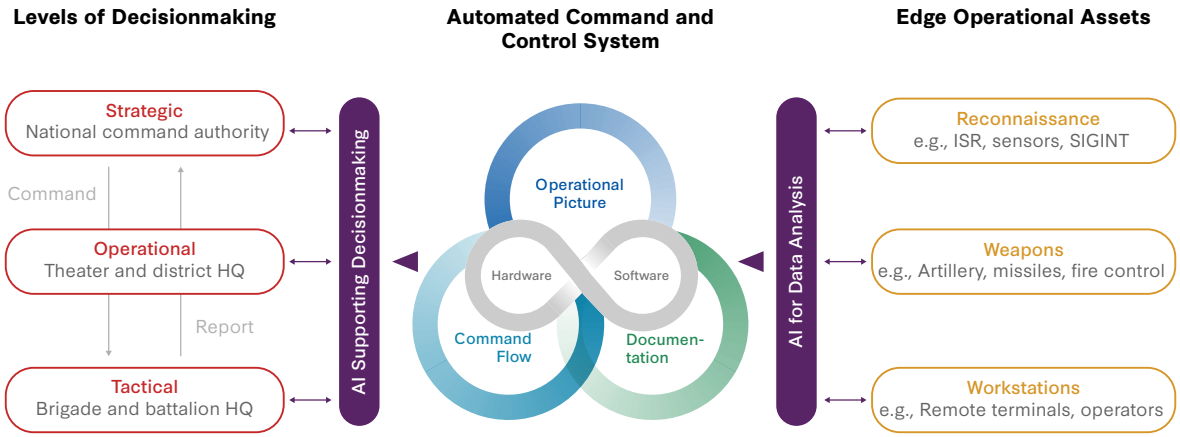
The Role of AI in Russia's C2 Systems

Publicly available information provides only a limited basis for assessing the actual degree to which AI-enabled technologies have been introduced or deployed within Russia's C2 systems. Nevertheless, materials published by the Russian Ministry of Defence and other military institutions outline a coherent vision for how AI is expected to function within the ACCS. According to these sources, the AI-enabled subsystem serves as an "intelligent component" (see Figure 4) that complements existing C2 processes, information flows, and communication channels while drawing on the full spectrum of data circulating within the broader ACCS architecture.

The main task of the AI-enabled subsystem is to generate predictive assessments of the likely trajectory and outcomes of ongoing or future military engagements. Within this framework, AI augments the traditionally creative and analytical work of commanders and staff by producing forecasted metrics—such as the depth and tempo of advance, projected losses, and other aggregate indicators—which are then mapped to develop alternative courses of action for both friendly and opposing forces. Through such prognostic outputs, the "intelligent" subsystem will be able to provide decision support intended to offer more rational operational choices, while the ultimate decisionmaking remains the responsibility of the commander.[6]

6 Ishchekin, Ishchekin, and Evtikhov, "Prospects for the Application of Artificial Intelligence in Command and Control of Troops."

Figure 4: The Role of AI in ACCS



Note: ISR = intelligence, surveillance, and reconnaissance; SIGINT = signals intelligence.

Source: CSIS analysis.

Russian military writings argue that two foundational technological components must be resolved before a fully functional, AI-enabled ACCS can emerge: advanced visual data analysis and mature natural-language processing. Russian specialists view these domains as progressing at markedly different rates.

VISUAL AND AUDIO ANALYSIS

In the realm of sensory and visual data processing, AI integration has advanced considerably. Automated systems for collecting and analyzing sensor information already employ neural networks for real-time recognition of visual, radar, hydroacoustic, and other signals. Computer vision technologies in particular have reached a relatively high technological readiness level (TRL)—estimated at TRL 6–9—and are usable in practical, field-tested applications. These technologies support automatic target recognition (ATR) and guidance capabilities in unmanned platforms that operate as loitering munitions.

One example of software from this category is Platform-GNS, short for "Unified Software Platform for Developing End-Oriented Complexes for Automatic Object Recognition Using Neural Network Approaches." This is a Russian **software environment** designed to supply a full technological stack for developing applied solutions based on deep neural networks. Platform-GNS was developed by the **Center for Artificial Intelligence Technologies** of the Zhukovsky Research Center, an institution established by leading aviation research bodies, including the State Research Institute of Aviation Systems and the Central Institute of Aviation Motors. Platform-GNS was created for advancing both aviation-related systems and AI-enabled autonomy more broadly. Notably, the platform and its associated tools are distributed **free of charge** to Russian defense enterprises, Ministry of Defence organizations, and educational institutions under a specialized licensing framework, facilitating widespread adoption across the national defense and research ecosystem.

Platform-GNS is a unified environment for developing AI applications based on deep convolutional neural networks. It **supports** the entire AI application development lifecycle, from dataset preparation to model training, testing, and deployment. It includes a graphical no-code interface and advanced tools for engineers, enabling a wide range of machine vision tasks such as detection, classification,

segmentation, tracking, and image enhancement. The system works with multispectral data, includes signal processing modules, and allows integration of custom solutions through an open Application Programming Interface (API). **Planned upgrades** for 2025–2026 will add support for large language models to enable smart assistants and more autonomous AI systems.

Platform-GNS **Avtomat** is a specialized version of the platform designed specifically for high-precision object recognition, particularly the identification of ground targets from airborne sensors. While inheriting the full development workflow of the core platform, Avtomat **adds capabilities** optimized for target recognition missions, automated testing, and deployment on Russian processors such as Elbrus and NeuroMatrix. Avtomat supports a comparable range of machine vision functions, with models exportable in ONNX format for flexible use across different hardware. In short, Platform-GNS provides the general-purpose foundation, while Avtomat serves as its more specialized, mission-tailored extension.

The Platform-GNS family of systems is used, for example, at the ERA military innovation technopolis and provides the underlying infrastructure for training neural networks that support real-time machine vision.[7] These capabilities are being incorporated into prototype AI-enabled control and targeting systems across Russia's defense industrial base.

In combination, these developments indicate that Russia has deliberately concentrated its AI investment where technical feasibility, data availability, and operational payoff align. Visual and sensory data processing have emerged as mature domains because they support concrete military tasks such as target detection, tracking, and guidance that can be validated directly in combat and refined through continuous feedback.

> *A common development environment, broad licensing across defense and education, and compatibility with domestic hardware all lower barriers to adoption and accelerate diffusion.*

Platforms such as Platform-GNS reflect an industrial strategy focused on enabling scale rather than producing singular breakthrough systems. A common development environment, broad licensing across defense and education, and compatibility with domestic hardware all lower barriers to adoption and accelerate diffusion. While these tools do not yet constitute fully autonomous control systems, they do provide a robust backbone for incremental autonomy in unmanned platforms. The result is an AI capability that advances unevenly across domains but progresses steadily where battlefield utility is clear, reinforcing Russia's pattern of prioritizing applied effectiveness over conceptual completeness.

TEXTUAL ANALYSIS

Textual analysis presents a far more difficult challenge than that of visual or sensory data. Automated systems for natural language processing (NLP), which underpin analytical functions and many C2

7 А.А. Протасов, А.В. Ширманов, and С.И. Радоманов, "Основные направления использования искусственного интеллекта в автоматизированных системах управления" [Main Directions for the Use of Artificial Intelligence in Automated Command and Control Systems], Вооружение и экономика [*Armament and Economics*], vol. 6, no. 66 (2023): 5–16.

subsystems, lag significantly behind visual processing tools. Russian assessments place current NLP technologies available to the Russian military at roughly TRL 1–3, reflecting an early research and experimental stage. As a result, key tasks—such as constructing semantically structured documents, performing context-aware searches, and generating meaningful automated textual decision support—remain technically immature and far from operational deployment.[8]

Textual analysis capability is particularly important because, for example, analysis of commanders' time distribution indicates that the largest share of time during mission planning and execution is absorbed by the preparation of documents—that is, paperwork. More than half of the allotted time (over 55 percent) is devoted to drafting, presenting, and approving documentation, while less than half is spent on substantive decisionmaking and coordinating essential elements of combat organization, including communication, command, and support. This creates a clear operational demand for an intelligent capability for paper flow management that could enhance the efficiency of command personnel.

The main obstacles in the domain of textual analysis are both technological and organizational. They arise from the difficulty of designing neural network architectures capable of capturing meaning, context, and intent in Russian-language military texts, as well as from the absence of certified, military-grade AI tools suitable for secure deployment within the Russian Armed Forces. At present, no such certified systems are in operational use.

To close the widening gap between relatively advanced visual data processing and the far less mature field of automated text analysis, the Russian military will likely follow the global pattern of adapting commercial large language models (LLMs) for defense needs. Although no public evidence indicates formal partnerships between major Russian tech companies and the Ministry of Defence, the foundational models of private tech companies are well positioned to be repurposed for military applications. Adaptation of commercial LLMs would require controlled collaboration and access to classified datasets to support tasks such as semantic text structuring, contextual searching, and automated information extraction for C2 environments.

More probable than these partnerships would be a dispersed, bottom-up process in which civilian engineers work informally to tailor existing commercial models for military tasks to support the Russian war effort. Over time, this wave of integration of commercial technology is likely to produce a new generation of adapted LLMs capable of processing unstructured textual data at scale, thereby narrowing the gap with visual processing technologies and bringing automated decision support tools closer to operational maturity.

Recent trends in the Russian job market **show** how the country's AI stack is taking shape and what developers actually use to build applications. By mid-2025, companies had already moved from isolated LLM experiments to full-scale deployment. Retrieval-augmented generation (RAG) has become the dominant architecture. More than a third of AI-related vacancies mention it, and developers increasingly build systems that combine LLMs with structured document repositories for search, analysis, and automation. Companies no longer focus on simple chatbots.

8 А.А. Протасов and А.В. Ширманов, "Технологические разработки в области искусственного интеллекта и сдерживание потенциального агрессора" [Technological Developments in Artificial Intelligence and the Deterrence of a Potential Aggressor], Военная Мысль [*Military Thought*], no. 11 (2023).

The technology stack in the Russian innovation ecosystem has also settled. Enterprise teams rely on Russian LLMs such as GigaChat or YandexGPT, while startups and R&D groups choose open-weight models such as Mistral, LLaMA, Qwen, DeepSeek, and Saiga. Most organizations run hybrid deployments: using on-premise infrastructure for government, defense industrial, and financial institutions because of data-sovereignty laws, and cloud/API setups for commercial products and prototypes.

Sector-specific trends mirror this pattern. Industrial firms use LLMs for predictive maintenance and technical documentation automation. Government and infrastructure organizations apply them to route optimization, regulatory analysis, and internal digital workflows.

Given these trends, the Russian military will likely pull from the same civilian stack. Russian defense organizations already favor on-premise systems, local processors, and strict data control regimes, so they will seek to integrate domestic LLMs, RAG pipelines, and vector databases into their C2 and analytical environments. Civilian engineers and defense industrial enterprises can adapt models like GigaChat, YandexGPT, and open-weight LLMs for tasks such as semantic searches across classified datasets, automated report generation, and faster information extraction for commanders.

Most probably, Russia's next wave of military AI will grow directly out of the tools its civilian developers already use—hybrid LLMs, rapid prototyping with open-weight models, and tightly controlled, on-premise deployments optimized for secure, operational environments.

Conclusion

The findings presented here point to a set of practical lessons for the United States as it modernizes its own C2 systems under increasingly contested conditions. Russia's experience does not offer a model to replicate, but rather highlights where operational pressures, organizational choices, and technology maturity shape real-world outcomes. The recommendations below translate these observations into actionable considerations for U.S. policymakers and defense planners, focusing in particular on how to align C2 and AI development with battlefield realities rather than with purely conceptual or architectural ambitions.

1. **The United States should treat C2 modernization as an operational competition measured by fielded effects, not by conceptual completeness.** Russia's experience suggests that ambitious, end-to-end architectures can stall inside legacy institutions, while task-specific tools that compress the tactical kill chain can deliver disproportionate battlefield value. U.S. C2 efforts should therefore prioritize modular, deployable applications, especially those that integrate unmanned systems with fires and situational awareness, while treating broader integration as an iterative outcome rather than a prerequisite to deployment.
2. **The United States should build and institutionalize a wartime-grade data pipeline as a core C2 capability.** Russia's 2025 push to aggregate UAS video, telemetry, strike effects, and operator performance into structured datasets shows how operational data can be converted into training inputs, unit evaluation, and rapid software refinement. The United States should expand mechanisms that automatically capture, label, and reuse data from training ranges and deployments, thereby enabling continuous improvement of targeting workflows, decision support tools, and autonomous functions without waiting for long acquisition cycles.
3. **U.S. C2 and military AI efforts should align investment and timelines with the areas where AI is already operationally mature in contested environments.** Near-term priorities

should center on perception, sensor fusion, and edge processing that increase survivability and accelerate decision cycles under GPS denial and heavy electronic warfare. At the same time, the U.S. military should harden communications and build robust concepts for operating through intermittent or degraded connectivity.

4. **The United States should expand pathways for nontraditional and commercial developers to access battlefield-relevant data and build C2 software without being trapped in slow, legacy institutional processes.** Russia's wartime adaptation suggests that civilian ecosystems can produce functional tools quickly when they have access to real operational problems and data, after which the military can formalize and scale what works. The United States' advantage should come from doing this deliberately through protected interfaces, curated datasets, and rapid test-and-adopt pipelines that let operational units field prototypes, validate them under realistic conditions, and then scale successful solutions through training, standards, and doctrine.

This paper demonstrates that Russia's evolution in command and control is less about achieving technological elegance and more about adapting under pressure to deliver usable effects in combat. Faced with persistent friction, institutional limits, and battlefield losses, Russia has shifted toward pragmatic, software-driven solutions that shorten decision cycles, integrate unmanned systems with fires, and exploit areas of AI maturity where results can be validated quickly. These adaptations are uneven and often improvised, but they are reinforced by an ability to iterate in combat and scale effective tools rapidly through training and standardization.

For the United States, the central lesson is not to emulate Russia's systems, but to internalize the logic behind its adaptations: Treat C2 modernization as a continuous operational contest, ground AI investment in what works under contested conditions, and build institutional pathways that allow data, software, and operators to coevolve at speed, thereby aligning development with the realities of modern, high-intensity warfare. ■

Kateryna Bondar *is a fellow with the Wadhwani AI Center at the Center for Strategic and International Studies in Washington, D.C.*

The author would like to thank Jorge L. Rivero from the Institute for Defense Analysis and CSIS Wadhwani AI Center intern Nicole Errera for their contributions to this research.

This report is made possible by general support to CSIS. No direct sponsorship contributed to this report.

Cover Photo: MIKHAIL KLIMENTYEV/SPUTNIK/AFP via Getty Images