

# **An Assessment of Purported Russian Artificial Intelligence Applications in Combat Operations**

## **Introduction An Unreliable Narrator's Tale of AI Warfare**

This analysis delves into claims regarding the Russian Federation's application of artificial intelligence technologies within contemporary combat operations, specifically drawing from a narrative attributed to "Joker DNR, the kremlin fsb proxy". The very source designation immediately necessitates profound skepticism. Research identifies entities like Joker DNR or Joker DPR as pro-Russian hacktivist groups, notorious for disseminating propaganda, engaging in information operations, and potentially operating under the aegis of Russian state intelligence services such as the GRU or FSB. These groups have a documented history of employing tactics like forged documents and spreading disinformation aimed at undermining Ukraine and its partners. Receiving supposedly technical military assessments from such quarters is akin to soliciting financial advice from a casino shill; the intent is persuasion, not objective truth. The explicit labeling within the initial request underscores the perception of this source as a direct conduit for state-sponsored narratives, framing the subsequent claims not as factual reporting but as elements of an information campaign designed to influence perception.

Compounding the challenge of veracity is a critical limitation the video evidence cited in the source material, hosted on the Rutube platform, proved inaccessible for this assessment. Consequently, this analysis must proceed based on the provided textual description and extensive supplementary research concerning Russian military AI development, specific weapon systems, and the operational context. The absence of the video prevents any verification of visual claims, be they genuine combat footage, staged tests, or pure animation. It also precludes confirmation of the specific systems purportedly showcased, such as the Lancet or Orlan drones, S-400 air defense systems, or Krasukha electronic warfare platforms mentioned in preliminary queries. This analytical gap is significant, removing a layer of potential (though likely carefully curated) evidence from consideration. The choice of Rutube itself warrants comment, being a platform controlled by state-affiliated Gazprom-Media and known for hosting pro-Kremlin content. Placing potentially unverifiable claims on such a platform aligns with a strategy of disseminating narratives within a controlled information ecosystem, shielded from external scrutiny.

This report will dissect the claims presented in the text, evaluate the likely intent and motivation behind their dissemination, and assess the potential maliciousness inherent in such information operations. It will further analyze the purported function, capabilities, lethality, targets, and overall maturity of the mentioned Russian military systems allegedly employing artificial intelligence, contrasting the propaganda narrative with available evidence and expert analysis. The structure will move from textual deconstruction and platform context to a reality check on Russian AI capabilities in drones, air defense, and electronic warfare, before concluding with an assessment of the propaganda's objectives and the actual state of Russian military AI maturity.

## **Dissecting the Kremlin Proxy's Communiqué Textual**

## Analysis

The provided text, attributed to the aforementioned Joker DNR entity, presents a confident assertion regarding Russia's use of artificial intelligence in warfare. It claims that Russia is *already* employing AI technologies in *real combat operations* today. The narrative specifically highlights combat drones, air defense systems (PVO), and electronic warfare complexes (REB) as domains where AI elements are purportedly integrated. The text emphasizes the *capabilities* these technologies confer and promises *concrete examples* presumably contained within the inaccessible video. Furthermore, it posits that artificial intelligence is fundamentally *changing the tactics* of modern warfare and boldly asserts that Russian developments in this field *successfully compete* with Western counterparts.

Several key themes and buzzwords permeate this brief description. The repeated use of "искусственный интеллект" (artificial intelligence) coupled with "реальные боевые действия" (real combat operations) aims to project an image of advanced, operationalized technology actively contributing to the current conflict. The phrase "успешно конкурируют" (successfully compete) directly addresses narratives of Western technological superiority, seeking to establish parity or even an advantage for Russian systems. This language aligns perfectly with broader Russian strategic communication objectives, which often emphasize technological prowess and military strength.

Considering the source's established profile as a pro-Russian hacktivist and propaganda outlet, the text's intent becomes transparent. It functions primarily as propaganda and perception management. The claims serve to bolster domestic morale, justify the significant investment in military technology often highlighted by Russian leadership, project an image of a modern, capable military force to international audiences, and potentially sow doubt or apprehension among adversaries. The narrative structure itself is revealing; it makes strong assertions of capability but defers the provision of evidence to the associated video content. This technique, presenting bold claims while rendering verification difficult or impossible, is a hallmark of propaganda designed to shape perceptions through assertion rather than demonstrable fact. The text aims to impress and persuade, not to facilitate critical, evidence-based analysis.

## The Phantom Menace Rutube, Propaganda, and the Missing Video

The inaccessibility of the Rutube video creates a significant void in this analysis. Without access to the visual content, it is impossible to evaluate the "concrete examples" promised in the accompanying text. We cannot determine whether the video depicted actual combat use, controlled testing environments, computer-generated animations, or perhaps repurposed footage entirely unrelated to AI applications. The specific systems allegedly featuring AI enhancements – whether Lancet drones striking targets, S-400 batteries engaging threats, or Krasukha systems jamming signals – remain unverified visual claims. This absence fundamentally undermines the ability to assess the veracity of the specific technological assertions tied to the video, forcing reliance on the broader context of Russian AI development and the source's inherent lack of credibility.

The choice of Rutube as the hosting platform is, however, informative in itself. Rutube is not a neutral video-sharing site; it is owned by Gazprom-Media, a subsidiary of the state-controlled energy giant Gazprom. Following Russia's full-scale invasion of Ukraine and the subsequent blocking or restriction of Western platforms like YouTube, Facebook, and Instagram within Russia, the Kremlin has actively promoted domestic alternatives like Rutube and VK Video. Rutube hosts numerous Russian state-controlled media channels that have been deplatformed

elsewhere and demonstrably promotes pro-Kremlin narratives, often interweaving political messaging with entertainment content. This push towards "sovereign" internet platforms serves a dual purpose it restricts citizens' access to independent or critical information while creating dedicated, state-influenced channels for disseminating approved narratives. Hosting a video making bold, potentially exaggerated claims about military AI on a platform like Rutube fits this pattern perfectly. It allows for the controlled release of information, potentially targeting a domestic audience susceptible to state messaging, while limiting exposure to international scrutiny or fact-checking that might occur on more open platforms. The irony of a platform intended as part of a "sovereign Runet" being inaccessible perhaps speaks volumes about the selective nature of the information sovereignty being constructed.

## Reality Check Gauging Russia's Military AI Prowess

The narrative presented by the Kremlin proxy paints a picture of advanced, operational, and competitive Russian AI seamlessly integrated into key military systems. However, a survey of available research and analysis suggests a more complex and often less flattering reality, marked by incremental progress, significant constraints, and a persistent gap between rhetoric and deployment.

### A. Unmanned Ambitions AI in Russian Drones

The claim of widespread and effective AI integration in Russian combat drones requires careful scrutiny. While Russia has undeniably invested in unmanned systems and deployed various types in Ukraine, the role and maturity of artificial intelligence within these platforms appear more limited than often portrayed.

Research indicates that AI applications in Russian drones primarily focus on enhancing specific functions rather than enabling full autonomy. These functions include automatic target recognition (ATR) assistance, terminal guidance for loitering munitions, and navigation capabilities, particularly in environments where GPS signals are jammed or denied by electronic warfare. For instance, the widely used Lancet loitering munition, often touted for its effectiveness and sometimes associated with AI capabilities, likely employs machine vision for terminal homing, allowing it to lock onto a pre-designated or recognized target type in the final phase of its attack. This represents a degree of automation and target recognition but falls short of fully autonomous target selection and engagement without human oversight. Similarly, claims surrounding AI enhancements in Iranian-designed Shahed drones (used extensively by Russia as Geran-2) enabling autonomous targeting and EW resistance are more plausibly explained by the integration of advanced navigation systems like DSMAC (Digital Scene Matching Area Correlator) combined with specific object recognition models trained to identify targets like infrastructure, rather than true, adaptable AI autonomy. The development of drone swarming capabilities, mentioned as a potential application, appears to be in nascent stages, possibly involving basic data sharing between drones rather than sophisticated collective AI behavior. Reconnaissance drones like the Orlan-10 remain crucial for Russian ISR (Intelligence, Surveillance, and Reconnaissance) and artillery spotting, but their AI integration likely centers on supporting data analysis and processing on the ground rather than onboard autonomy. Furthermore, Russia has faced challenges maintaining its inventory of military-grade drones, leading to increased reliance on less sophisticated commercial drones and imports. The maturity level of AI in Russian drones can thus be assessed as ranging from experimental to early operational for specific, bounded tasks like terminal guidance or assisted navigation. Widespread deployment of highly autonomous combat drones capable of complex decision-making in dynamic environments appears aspirational rather than current reality. This

assessment is reinforced by analyses indicating Russia lags behind the US and China in overall AI development and faces significant constraints due to sanctions impacting access to critical Western microelectronics. The rapid adaptation cycle observed in drone warfare, where both sides quickly emulate successful tactics, often using readily available technology like FPV drones, suggests that tactical innovation and the agile application of existing technologies may currently be more decisive than breakthroughs in uniquely advanced military AI, particularly given Russia's documented limitations. The focus seems to be on making existing platforms more resilient and effective in specific phases of engagement, rather than fielding truly autonomous systems at scale.

**Table 1 Claimed versus Assessed Capabilities of Key Russian AI-Enabled Drones**

Drone System	Claimed AI Function (Propaganda/Producer)	Assessed AI Function/Capability (Research-Based)	Assessed Maturity Level	Key Supporting References
Lancet-3	AI target selection/engagement, high autonomy, "intellectual complex"	Terminal guidance/homing, Automatic Target Recognition (ATR) assistance, likely requires human oversight for launch/mission	Early Operational	
Shahed-136/Geran-2	AI for EW resistance, autonomous targeting of critical infrastructure	Advanced navigation (DSMAC-like), specific object recognition models, limited autonomy, not true AI	Operational (as system)	
Orlan-10	(Implicitly part of AI-enhanced forces)	Primarily ISR/artillery spotting; AI likely supports ground-based data analysis, limited onboard AI	Operational (as system)	
KUB-LA	AI target selection/engagement	Loitering munition, likely similar ATR/terminal guidance elements as Lancet; full autonomy claims unverified	Experimental/Limited Op	
Italmas	Special long-range self-guidance system (details unspecified)	Under development, capabilities unclear, likely builds on Lancet-type	Developmental	

Drone System	Claimed AI Function (Propaganda/Producer)	Assessed AI Function/Capability (Research-Based)	Assessed Maturity Level	Key Supporting References
Bylina (EW Control)	AI-based analysis, target identification, prioritization, jamming allocation	Automated EW management system, uses machine learning for prioritization	Operational (Limited?)	

**B. Shields Up AI in Russian Air Defense**

The narrative extends to Russian air defense (AD) systems, suggesting AI integration enhances their capabilities. Systems like the Tor-M2U are explicitly claimed to use AI algorithms for target recognition, classification, and prioritization, enabling engagement of multiple threats simultaneously. Broader claims encompass AI elements in established systems like the S-400 and newer ones like the S-350 Vityaz, purportedly proving effective even against advanced Western missiles like ATACMS and Storm Shadow/SCALP-EG. Development of AI control capabilities for the next-generation S-500 system is also underway.

While Russian AD systems, particularly layered deployments incorporating platforms like Tor, Buk, S-300, and S-400, have demonstrated considerable capacity, achieving high overall intercept rates against many types of threats, the specific contribution and maturity of AI remain subjects of debate. The functions attributed to AI – faster target processing, threat assessment, prioritization, potentially optimizing missile guidance parameters – largely represent advancements in automation and data processing speed rather than a fundamental shift to AI-driven perception or decision-making. These enhancements fall under the umbrella of Russia's push towards "intellectualized" warfare systems, evolving from earlier digitalization efforts.

However, the operational record in Ukraine presents a more nuanced picture. Despite possessing these advanced AD systems, the Russian Aerospace Forces (VKS) signally failed to achieve air superiority, primarily due to their inability to effectively suppress or destroy Ukraine's resilient ground-based air defenses (GBAD). This persistent failure points towards deficiencies not necessarily in individual system performance, but in broader operational concepts, particularly the lack of robust SEAD/DEAD (Suppression/Destruction of Enemy Air Defenses) doctrine and capability. Russian military thought has historically prioritized defensive operations, leading to underdevelopment in offensive counter-air capabilities needed to dismantle a sophisticated, mobile IADS like Ukraine's. Furthermore, even advanced systems face limitations. Faster, more maneuverable threats like ballistic missiles remain challenging to intercept, and systems like the Tor face constraints such as crew endurance under sustained operational tempo. Therefore, while AI may be incrementally improving the automation and reaction time of Russian AD systems, it does not appear to be a panacea overcoming fundamental doctrinal shortcomings or the challenges posed by a diverse and adaptive threat environment. The maturity level seems operational for specific automated functions within existing frameworks, but not yet transformative at the strategic level.

**C. The Electronic Battlefield AI in Russian EW**

Russia possesses formidable electronic warfare (EW) capabilities, widely acknowledged as among the most advanced globally. Systems like the Krasukha-4 have demonstrated

effectiveness in jamming radar and satellite navigation signals, significantly impacting GPS-reliant Western systems used by Ukraine. The Joker DNR narrative implicitly includes EW complexes among those benefiting from AI integration. Specific systems like the RB-109A Bylina are explicitly reported to use AI based on machine learning to analyze the electromagnetic environment, identify priority targets, and automate jamming tasks within a wide radius. Additionally, claims that AI-enhanced drones possess immunity or resistance to EW suggest AI is being applied defensively in the EW domain as well.

The likely function of AI within Russian EW likely involves automating and optimizing complex tasks such as signal analysis, emitter identification and classification, threat prioritization, and dynamic allocation of jamming resources. This aligns with broader military AI goals focused on improving command and control and decision-making speed in complex environments.

However, discerning the specific impact of AI versus the inherent sophistication of Russia's conventional EW hardware and long-standing doctrinal emphasis on dominating the electromagnetic spectrum is challenging based on open sources. Many core EW functions, while complex, do not necessarily require advanced AI as commonly understood.

The maturity of AI in Russian EW is therefore difficult to ascertain precisely. While systems like Bylina suggest operational deployment of AI for specific control and analysis functions, their prevalence and overall impact remain unclear. Russia's established strength in ground-based EW predates the current focus on AI. A potential tension exists between the narrative of AI rendering Russian drones resistant to EW and the continued Russian emphasis on fielding powerful offensive EW systems designed to counter enemy drones and communications. This suggests that while AI might offer enhanced resilience, particularly for functions like navigation in GPS-denied conditions, it likely does not provide true immunity. The electronic battlefield remains a fiercely contested domain where both offensive EW capabilities and AI-driven countermeasures are deemed necessary, indicating that neither side has achieved decisive dominance through AI alone.

## **Decoding the Deception Intent, Motivation, and Malice**

The narrative disseminated by "Joker DNR" regarding Russia's advanced AI combat capabilities is best understood not as a factual report but as a calculated piece of strategic communication, likely constituting deliberate disinformation. Several factors converge to support this assessment: the highly dubious nature of the source, the use of a controlled, state-affiliated platform (Rutube) for dissemination, the inaccessibility of the purported visual evidence, and the significant gap between the grandiose claims and the more sober reality reflected in independent analyses of Russian military technology.

The primary intent appears multifaceted, serving several propaganda objectives. Firstly, it aims to project an image of Russian military strength and technological prowess, countering narratives of technological lag or decline, particularly in comparison to the West. The claim of successfully competing with Western analogues is central to this theme. Secondly, it targets the domestic Russian audience, seeking to bolster national pride, justify massive defense expenditures, and reinforce confidence in the military leadership and the ongoing war effort, aligning with statements by figures like Putin and Shoigu emphasizing the importance of future technologies like AI. Thirdly, it serves an international influence function, potentially aiming to deter adversaries by exaggerating capabilities, sow doubt about Western technological advantages, or shape threat perceptions within NATO and other nations. Lastly, it functions as psychological warfare directed at Ukraine, attempting to demoralize forces and the population by showcasing seemingly unstoppable, technologically advanced threats.

The maliciousness lies in the deliberate intent to mislead various audiences for strategic gain. By presenting an inflated view of its AI capabilities, Russia seeks to manipulate perceptions and

potentially influence decisions, whether related to military aid for Ukraine, domestic political support, or international alliances. This fits within Russia's broader documented use of information operations and disinformation, sometimes leveraging AI tools themselves for these campaigns.

The target audiences are clearly defined. The domestic population receives reassurance of Russia's power and innovation. The Ukrainian audience is meant to feel technologically overwhelmed and intimidated. Western defense planners and policymakers are presented with a narrative of Russian parity or superiority, potentially complicating threat assessments and strategic planning. Potential international arms buyers may also be targeted, viewing these claims as marketing for Russian military hardware. This entire effort can be viewed as a form of "technological maskirovka," a modern iteration of Russia's traditional doctrine of military deception. By amplifying claims about cutting-edge AI, the narrative attempts to obscure actual battlefield difficulties, technological dependencies, the impact of sanctions, and persistent operational limitations. It constructs a facade of advanced capability to mask underlying vulnerabilities, a classic application of deceptive principles in the information age.

## **Lethality, Targets, and Maturity The Sobering Assessment**

Evaluating the practical implications requires assessing the lethality of the systems discussed, clarifying their targets, and rendering a final verdict on the maturity of Russian military AI. The weapon systems mentioned – combat drones like Lancet, air defense systems like Tor, and EW platforms like Krasukha – are undeniably lethal or disruptive in their own right. Lancet drones have proven effective at destroying valuable Ukrainian assets. Russian AD systems, despite limitations, intercept a significant number of incoming threats. Russian EW poses a serious challenge to communications, navigation, and surveillance. However, the *incremental* lethality or effectiveness specifically added by artificial intelligence, beyond improved automation or guidance algorithms already achievable through conventional means, is difficult to quantify and likely overstated in propaganda narratives. AI might make a Lancet's terminal phase more accurate or a Tor's reaction time faster, but the fundamental destructive potential resides in the warhead or missile itself.

The targets of these systems are twofold. Physically, they aim at Ukrainian military assets (tanks, artillery, AD systems, command posts), critical infrastructure (especially energy facilities targeted by drones like Shahed/Geran), enemy communication and radar systems (targeted by EW), and incoming aerial threats (targeted by AD). Informationally, as discussed previously, the targets are the perceptions and decision-making processes of domestic Russian audiences, Ukrainian citizens and military personnel, and international actors.

Regarding maturity, the synthesized evidence points to a Russian military AI ecosystem that is developing but remains significantly constrained and generally lags behind leading Western nations and China. While specific AI elements are being integrated into operational systems, particularly for enhancing autonomy in drones (navigation, terminal attack phases) and automating processes in AD and EW, these appear to be incremental advancements rather than revolutionary leaps. Claims of widespread, fully autonomous systems successfully competing with the best Western counterparts seem largely aspirational. Development is hampered by international sanctions restricting access to essential high-end microelectronics and software, a reliance on potentially dated imported components, and a reported brain drain of technical experts following the invasion.

Paradoxically, the war in Ukraine appears to be both a catalyst and an impediment to Russian military AI development. The intense demands of the battlefield drive rapid innovation and adaptation in specific niches, particularly drone warfare, where AI elements for targeting and

navigation offer tangible advantages. High-level political directives also push for accelerated AI integration. However, the same conflict triggered the sanctions, resource drain, and human capital flight that hinder broader, foundational AI progress. This results in a complex picture where Russia might achieve localized, tactical successes using specific AI-enhanced tools while struggling to keep pace in the overall strategic AI competition.

## Conclusion Through the Looking Glass of Russian Military AI

The narrative presented by the source "Joker DNR, the kremlin fsb proxy," concerning Russia's advanced and operational use of artificial intelligence in combat, should be assessed as state-aligned propaganda rather than credible technical analysis. Its primary function is information warfare projecting strength, managing domestic perceptions, intimidating adversaries, and masking underlying military-technical limitations. The claims of widespread, effective, and competitive AI integration across Russian drones, air defense, and electronic warfare systems appear significantly exaggerated when compared against available evidence and independent assessments.

While Russia is undoubtedly incorporating elements of AI and automation into its military systems – particularly enhancing drone navigation, terminal guidance, target recognition assistance, air defense automation, and EW management – these applications are generally incremental, often experimental or limited in scope, and face substantial constraints. These constraints include lagging indigenous technological development, dependence on foreign components (particularly Western microelectronics now subject to sanctions), and the broader economic and human capital impacts of the war in Ukraine. The persistent gap between Russia's ambitious rhetoric about military AI and the observable realities on the battlefield, including notable failures like the inability to achieve air superiority despite advanced AD systems, underscores this divergence. This echoes historical patterns where assessments of Russian military capability, sometimes influenced by Moscow's own projections, have proven overly optimistic.

Ultimately, analyzing pronouncements from sources like Joker DNR offers less insight into Russia's actual AI capabilities and more into its information warfare strategies. While Russia publicly declares that artificial intelligence is changing the face of modern warfare through its systems, perhaps the most demonstrably advanced application of AI-related concepts lies in the sophisticated, multi-audience information campaigns designed to convince the world of that very claim. Discerning genuine technological advancement from these elaborate digital Potemkin villages remains a critical challenge for defense intelligence.

### Works cited

1. Risky Biz News: XakNet "hacktivists" linked to APT28 and Russia's GRU intelligence service, <https://risky.biz/risky-biz-news-xaknet-hacktivists/>
2. Joker DPR and the Information War - Recorded Future, <https://go.recordedfuture.com/hubfs/reports/cta-2023-0406.pdf>
3. Russia-aligned hackers stir up anti-Ukrainian sentiments in Poland - DFRLab, <https://dfrlab.org/2022/09/09/russia-aligned-hackers-stir-up-anti-ukrainian-sentiments-in-poland/>
4. Cyber Vault Ukraine Timeline - OCR of the Document | National Security Archive, <https://nsarchive.gwu.edu/media/29562/ocr>
5. Russia-Ukraine war: Telegram-based hacktivism in 2023 - SecAlliance, <https://www.secalliance.com/blog/russia-ukraine-war-telegram-based-hacktivism-in-2023>
6. Rutube - Wikipedia, <https://en.wikipedia.org/wiki/Rutube>
7. How Russian YouTube copycat RUTUBE promotes pro-Kremlin narratives - DFRLab,

<https://dfrlab.org/2023/01/30/how-russian-youtube-copycat-rutube-promotes-pro-kremlin-narratives/> 8. Russia Capitalizes on Development of Artificial Intelligence in Its Military Strategy, <https://jamestown.org/program/russia-capitalizes-on-development-of-artificial-intelligence-in-its-military-strategy/> 9. "Sovereign" Means Military: How Russia Militarized AI, Drone, and Cryptography Industries - Т-инвариант / T-invariant, <https://t-invariant.org/2025/03/sovereign-means-military-how-russia-militarized-ai-drone-and-cryptography-industries/> 10. The Role of AI in Russia's Confrontation with the West | CNAS, <https://www.cnas.org/publications/reports/the-role-of-ai-in-russias-confrontation-with-the-west> 11. Putin eyes AI and lasers for future warfare - Defence Blog, <https://defence-blog.com/putin-eyes-ai-and-lasers-for-future-warfare/> 12. Путин готовит Россию к затяжному сражению с Западом, <https://ura.news/articles/1036291142> 13. Путин хочет задействовать в войне искусственный интеллект и отправить на фронт лазеры и роботов - Українська правда, <https://www.pravda.com.ua/rus/news/2023/12/19/7433695/> 14. Analysis: Russia's 2024 digital crackdown reshapes social media landscape, <https://monitoring.bbc.co.uk/product/b0003arz> 15. analysis - German Council on Foreign Relations | DGAP, [https://dgap.org/system/files/article\\_pdfs/DGAP\\_Analysis\\_No-5\\_April-2024\\_15pp\\_0.pdf](https://dgap.org/system/files/article_pdfs/DGAP_Analysis_No-5_April-2024_15pp_0.pdf) 16. Russia: Freedom on the Net 2023 Country Report, <https://freedomhouse.org/country/russia/freedom-net/2023> 17. Russia is determined to make RuTube happen - Coda Story, <https://www.codastory.com/newsletters/russia-rutube/> 18. A platform policy implementation audit of actions against Russia's state-controlled media, <https://policyreview.info/articles/analysis/platform-policy-audit-of-actions-against-russias-state-media> 19. Digital Iron Curtain: Russia's Quest for Internet Sovereignty, <https://ridl.io/digital-iron-curtain-russia-s-quest-for-internet-sovereignty/> 20. Evolution Not Revolution - CNAS, <https://www.cnas.org/publications/reports/evolution-not-revolution> 21. Technological Lessons Learned From the Conflict Between Russia and Ukraine - HDIAC, <https://hdiac.dtic.mil/technical-inquiries/notable/technological-lessons-learned-from-the-conflict-between-russia-and-ukraine/> 22. Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare - CSIS, <https://www.csis.org/analysis/ukraines-future-vision-and-current-capabilities-waging-ai-enabled-autonomous-warfare> 23. Battlefield Drones and the Accelerating Autonomous Arms Race in Ukraine, <https://mwi.westpoint.edu/battlefield-drones-and-the-accelerating-autonomous-arms-race-in-ukraine/> 24. The Rush for AI-Enabled Drones on Ukrainian Battlefields - Lawfare, <https://www.lawfaremedia.org/article/the-rush-for-ai-enabled-drones-on-ukrainian-battlefields> 25. Strategic Empathy: Examining Pattern Breaks to Better Understand - Middlebury College, [https://www.middlebury.edu/sites/default/files/2023-09/Strategic%20Empathy%20Report%20Sep23\[45\].pdf?fv=\\_Bk\\_h0jO](https://www.middlebury.edu/sites/default/files/2023-09/Strategic%20Empathy%20Report%20Sep23[45].pdf?fv=_Bk_h0jO) 26. Ukraine War - ResearchGate, [https://www.researchgate.net/profile/Abhay-Singh-44/publication/381772986\\_UKRAINE\\_WAR\\_Military\\_Perspectives\\_and\\_Strategic\\_Reflections/links/667e587d714e0b03152fd258/UKRAINE-WAR-Military-Perspectives-and-Strategic-Reflections.pdf](https://www.researchgate.net/profile/Abhay-Singh-44/publication/381772986_UKRAINE_WAR_Military_Perspectives_and_Strategic_Reflections/links/667e587d714e0b03152fd258/UKRAINE-WAR-Military-Perspectives-and-Strategic-Reflections.pdf) 27. Struggling, Not Crumbling: Russian Defence AI in a Time of War - RUSI, <https://www.rusi.org/explore-our-research/publications/commentary/struggling-not-crumbling-russian-defence-ai-time-war> 28. БПЛА ( беспилотники ) для ВС РФ, новости о БЛА в Российской армии - НачФин.info, <https://nachfin.info/SMF/index.php?topic=10796.375> 29. Russia's war against Ukraine - Doria, [https://doria.fi/bitstream/handle/10024/189938/Forsstr%C3%B6m%20et%20al.\\_Russia%20semi%20nar%2024\\_web.pdf?sequence=5&isAllowed=y](https://doria.fi/bitstream/handle/10024/189938/Forsstr%C3%B6m%20et%20al._Russia%20semi%20nar%2024_web.pdf?sequence=5&isAllowed=y) 30. Запад устроил Украине «снарядный голод» — и ВСУ пытаются компенсировать дефицит боеприпасов «армией дронов». Но заменить артиллерию беспилотники пока не могут Как « - Meduza, <https://meduza.io/feature/2024/03/14/zapad-ustroil-ukraine-snaryadnyy-golod-i-vsu-pytayutsya-k>

ompensirovat-defitsit-boepripasov-armiey-dronov-no-zamenit-artilleriyu-bespiilotniki-poka-ne-mo gut 31. How Russia's AI-Powered Shahed Drones Are Changing Modern Warfare, <https://armyrecognition.com/news/aerospace-news/2025/how-russias-ai-powered-shahed-drone-s-are-changing-modern-warfare> 32. Inside Russia's plan to build autonomous drone swarms - Breaking Defense, <https://breakingdefense.com/2025/01/inside-russias-plan-to-build-autonomous-drone-swarms/> 33. Roles and Implications of AI in the Russian-Ukrainian Conflict - CNAS, <https://www.cnas.org/publications/commentary/roles-and-implications-of-ai-in-the-russian-ukrainian-conflict> 34. From the Frontlines to the Future - Belfer Center, [https://www.belfercenter.org/sites/default/files/pantheon\\_files/files/publication/PDF%20Frontlines%20to%20Future.pdf](https://www.belfercenter.org/sites/default/files/pantheon_files/files/publication/PDF%20Frontlines%20to%20Future.pdf) 35. The Role of AI in Russia's Confrontation with the West - Amazon S3, [https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/Russia-AI\\_2024-final.pdf](https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/Russia-AI_2024-final.pdf) 36. Silicon Lifeline: Western Electronics at the Heart of Russia's War Machine - RUSI, [https://static.rusi.org/RUSI-Silicon-Lifeline-final-updated-web\\_1.pdf](https://static.rusi.org/RUSI-Silicon-Lifeline-final-updated-web_1.pdf) 37. Антисанкционная и санкционная экономическая политика России 2022–2025. Часть 1: Анализ и прогноз управления антироссийскими санкциями | Манушин | Russian Journal of Economics and Law, <https://www.rusjel.ru/jour/article/view/2470> 38. Влияние санкций на электронные компоненты в России, <https://indpages.ru/elektr/vliyanie-sankcij-na-elektronnye-komponenty-v-rossii/> 39. Ukraine Conflict Updates | Institute for the Study of War, <https://www.understandingwar.org/backgrounder/ukraine-conflict-updates> 40. Russian TOR-M2U Air Defense System Using AI Technologies Intercepts US HIMARS and Vilkha Rockets - Army Recognition, <https://armyrecognition.com/focus-analysis-conflicts/army/conflicts-in-the-world/russia-ukraine-war-2022/russian-tor-m2u-air-defense-system-using-ai-technologies-intercepts-us-himars-and-vilkha-rockets> 41. Russian defense plan kicks off separate AI development push, <https://www.defensenews.com/global/europe/2024/08/16/russian-defense-plan-kicks-off-separate-ai-development-push/> 42. Breaking Down Russian Missile Salvos: What Drives Neutralization? - CSIS, <https://www.csis.org/analysis/breaking-down-russian-missile-salvos-what-drives-neutralization> 43. Новое вооружение войск ПВО ,ВКС, <https://pvo.forum24.ru/?1-30-0-00000004-000-10001-0-1657217603> 44. Russian Combat Air Strengths and Limitations: Lessons from Ukraine - CNA.org., <https://www.cna.org/reports/2023/04/Russian-Combat-Air-Strengths-and-Limitations.pdf> 45. Failures of the Russian Aerospace Force in Ukraine - Air University, [https://www.airuniversity.af.edu/Portals/10/ASOR/Journals/Volume-2\\_Number-3/Galamison\\_Petersen.pdf](https://www.airuniversity.af.edu/Portals/10/ASOR/Journals/Volume-2_Number-3/Galamison_Petersen.pdf) 46. Meeting Expectations: Failure in Ukraine Will Not Change the Russian Aerospace Defense Force - Army University Press, <https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/January-February-2025/Meeting-Expectations/> 47. Meeting Expectations: Failure in Ukraine Will Not Change the Russian Aerospace Defense Force, <https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/January-February-2025/Meeting-Expectations/Meeting-Expectations-UA.pdf> 48. Russian TOR-M2U Air Defense System Using AI Technologies Intercepts US HIMARS and Vilkha Rockets - YouTube, <https://www.youtube.com/watch?v=O9HoxaB6rv4> 49. Russian Ground-Based Electronic Warfare: Assessing the Real Threat Versus the Hype, <https://nationalsecurityjournal.org/russian-ground-based-electronic-warfare-assessing-the-real-threat-versus-the-hype/> 50. Russia's Electronic Warfare Dominance: A Comprehensive Overview, <https://idstch.com/geopolitics/russias-electronic-warfare-dominance-a-comprehensive-overview/> 51. Russia's Electronic Warfare Force: Blending Concepts with Capabilities - DTIC,

<https://apps.dtic.mil/sti/trecms/pdf/AD1137511.pdf> 52. Analysis: Russia's Electronic Warfare Equipment - Kyiv Post, <https://www.kyivpost.com/analysis/32435> 53. Understanding the Military AI Ecosystem of Ukraine - CSIS, <https://www.csis.org/analysis/understanding-military-ai-ecosystem-ukraine> 54. How AI and Autonomy in Russia-Ukraine War Affect Stability - CNA.org., <https://www.cna.org/reports/2023/10/ai-and-autonomous-technologies-in-the-war-in-ukraine> 55. «Заявление Президента России об искусственном интеллекте дает основания верить в создание условий для развития этой сферы»,.. | ВКонтакте, [https://vk.com/wall-4311\\_45268](https://vk.com/wall-4311_45268) 56. Российская армия сделает упор на внедрение искусственного интеллекта - Armiya.az, <http://armiya.az/ru/news/170441> 57. RUSSIAN PERCEPTIONS OF MILITARY AI, AUTOMATION, AND AUTONOMY - Foreign Policy Research Institute, <https://www.fpri.org/wp-content/uploads/2022/01/012622-russia-ai-.pdf> 58. A Net Assessment of Russian and Allied Capabilities in a Modern Strike Campaign - RUSI, <https://static.rusi.org/russian-and-allied-capabilities-modern-strike-campaign-feb-2025-rusi.pdf> 59. Preliminary Lessons from Ukraine's Offensive Operations, 2022–23 - RUSI, <https://static.rusi.org/lessons-learned-ukraine-offensive-2022-23.pdf> 60. The Russia-Ukraine War - AWS, [https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-09/240924\\_Cohen\\_Russia\\_Ukraine.pdf?VersionId=1YNnRnwS.6DkrwNcAkdb5Dbsfjclg0JR](https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-09/240924_Cohen_Russia_Ukraine.pdf?VersionId=1YNnRnwS.6DkrwNcAkdb5Dbsfjclg0JR) 61. Russia's Integrated Air Defense System: A Comprehensive Analysis of its Evolution, Capabilities and Global Impact - Debug, <https://debuglies.com/2024/04/25/russias-integrated-air-defense-system-a-comprehensive-analysis-of-its-evolution-capabilities-and-global-impact/> 62. Full article: Western Estimates of Russian Military Capabilities and the Invasion of Ukraine, <https://www.tandfonline.com/doi/full/10.1080/10758216.2023.2253359>