JRSR
JOURNAL OF REGIONAL STUDIES REVIEW

Journal of Regional Studies Review (JRSR)
Volume 4, Issue 1 (Winter 2025) | Pages: 516–525
ISSN (Online): 3006-6646
Digital Object Identifier (DOI): 10.62843/jrsr/2025.4a097
Correspondence should be addressed to Aswah Akhtar; aswahakhtar1@gmail.com

RESEARCH ARTICLE

The Role of AI in U.S. and Russian Military Operations and Its Implications on Ukraine's Cyber and National Security

Aswah Akhtar [a]

Abstract: This article explores how the use of artificial intelligence (AI) during military operations by the U.S. and Russia affects Ukraine's security. we study the development and use of AI in intelligence, attacking targets, autonomous systems, cyber warfare and information operations. We see that both the U.S. and Russia are working hard to make use of AI on the battlefield for instance Russia is utilizing AI-driven drones and kamikaze devices while the U.S. is creating large numbers of inexpensive autonomous drones for the same purpose (Bajak, November 25, 2023). As the war in Ukraine continues, AI tools like drones are transforming fighting tactics and strategies for all involved. Now Ukraine must be prepared for greater cyber-sabotage from Russia, as well as for better air defense and stronger security of sensitive information. To conclude we propose that Ukraine happens stand back their AI with help from government agencies, strengthen its resistance to cyber-attacks and grow its anti-drone defense, while working towards global standards for military using AI (Antoniuk, 2025). AI has contributed to a new type of arms race and also resulted in the deepening of the great-power security dilemma that matters to Ukraine.

Keywords: Artificial Intelligence in Military Operations, United States, Russia, Ukraine, Defensive Realism, Autonomous Weapons, Ukraine War, Digital Sovereignty, Cyber Warfare

Introduction

Artificial Intelligence is bringing about another Revolution in Military Affairs (RMA) in the form of modern warfare. With modern technologies improving rapidly AI plays a key role in deciding who has an advantage in the military. Modern militaries are now counting on AI in data processing as well as in the development of weapons that function independently. Key armed forces such as U.S. and Russian have adopted this new military stance as vital to their strength and influence across the globe (Daniels, 2022). AI has been given a prominent role in the United States' plans to bring its military defense into the future. Washington's commitment to using AI in many defense operations is shown through the Defense Innovation Unit and the integrated Joint Artificial Intelligence Center. These technologies consist of accessing current satellite photos, driverless and semi-driverless systems for air and ground, automated decision-making services and planning ahead for maintenance needs. The ultimate goal is to help American forces gain an edge in decision-making and battle tactics in all types of conflicts.

Russia is focusing its military updates largely on the use of AI. With "sovereign AI" in mind Putin has driven Moscow to develop its own AI technology to maintain control over both cyber and military systems. In Russia there is a focus on creating loitering munitions powered by AI groups of swarm drones and robots for combat missions. Russia has greatly improved its abilities in AI-guided electronic warfare, information activities and decision-making systems. As the Russian government indicates AI will improve the speed accuracy and impact on morale in future battles (Reuters, 2024). The rivalry in AI between the US and Russia is developing as the war in Ukraine continues. Since the Russian invasion in Ukraine, Ukraine's conflict has effectively become a trial for the latest developments in military AI. Russian troops are using many low-cost

[a] Student, Department of Political Science and International Relations, University of Management and Technology, Lahore, Punjab, Pakistan.

Cite this Article: Akhtar, A. (2025). The Role of AI in U.S. and Russian Military Operations and Its Implications on Ukraine's Cyber and National Security. *Journal of Regional Studies Review, 4*(1), 516-525. https://doi.org/10.62843/jrsr/2025.4a097

AI-dependent drones such as Lancets and Shaheds made in Iran to strike at Ukrainian military and civilian objectives (Benjamin Jensen, 2025). Ukrainian defense officials, together with local tech startups and troops from the West have adopted AI for use in improving their intelligence, surveillance, reconnaissance, autonomous attacks, decision-making and information activities. What we are seeing now is that AI is a powerful tool with important impacts on both strategy and operations.

This study aims to analyze on how AI is being used in military operations by the U.S., Russia and particularly in the Ukraine conflict. Additionally, the paper looks at how the rivalry in technology shapes Ukraine's national security and control over its digital world in areas such as cyber defense, the flow of information and the way battles are conducted (Sobchuk, 2024). This research analyzes the impact of AI in military technologies using Defensive Realism to show how these new technologies can increase deterrence and also spark competition. The study helps explain the impact of AI on military plans and the strategies of nations in the today's world.

Research Questions

This paper aims to further examine these dynamics through an inquiry building on two primary research questions.

1. How have U.S. and Russian military strategies in the Ukraine war leveraged AI technologies, and in what ways do these uses reflect the defensive realist principles of balancing and security-seeking?
2. What are the implications of AI-driven strategies for Ukraine's defense capabilities and digital sovereignty, and what policy actions should Ukraine undertake to strengthen its security and technological independence?

These questions guide our analysis of AI's role on the battlefield and in cyberspace, through the case of Turkish Bayraktar TB2 drones and Russia's disinformation campaigns.

Theoretical Framework

Since the fighting in Russia–Ukraine has been unpredictable, both large and small nations are using AI in their military and informational campaigns. Defense realism sees states under anarchy focusing on their security and this leads them to strive mainly for survival. According to Stephen Walt and Charles Glaser, states in an uncertain world also take steps to balance against dangers by trying to avoid disputes that could lead to disputes. According to this theory, it is easy to misunderstand good actions taken by AI like self-defense as a threat to others. Ukraine's strategy in fighting is very different from the U.S. and Russia's because of the disparity in their use of AI. Russia is known for aggressively using AI in the military. Experts say that Russian forces are currently relying on AI to help direct drones using optical systems (not affected by jamming) to control groups of drones and to improve how goods and materials are delivered. The military announced it will use AI in its attack drones to improve their accuracy and strength. Russia's intelligence agencies have started using artificial intelligence to help spread fake news. As a specific example in 2022 Moscow published a fake video claiming President Zelensky urged people to give up which satirists laughed off as a juvenile attempt. Later, Ukrainian authorities explained that Russia was increasingly using advanced AI to organize disinformation posts on social media, making them hard for anyone to notice. As a result of Russia's strategy using cyber assaults and AI-aided false news, Ukraine had to increase its efforts to defend itself.

This pattern fits predictions made by defensive realism. Waltz believes that a state like Ukraine will join forces with stronger countries and secure sufficient technology and foreign backing to prevent aggression. The alliance between Ukraine and NATO tech companies along with its efforts in cyber-security, demonstrate the realist "self-help" way of thinking. At the same time such actions create security dilemma challenge. Russia thinks relying on U.S. AI and cloud infrastructure in Ukraine is dangerous, while Ukraine thinks it is not. In essence AI has introduced a new area of managing behavior and Ukraine is responding

by relying on U.S./Western AI support for its defense and seeking digital sovereignty during the war (Bajak, November 25, 2023).

Ukraine's military relies on technology and robots mostly to guard their nation rather than to take aggressive actions. The report indicates that Ukraine's military wants to replace its soldiers in the line of fire with robots and sophisticated automated machines to ensure that soldiers stay safe and are not overworked or exposed to equipment loss. In fact, Ukraine is making strong use of drones and AI to boost its small force. Based on what analysts say AI already helps automate key actions on the battlefield by using computer vision and data fusion to analyze images from drones identify targets and guide travel through unsafe regions. As a result, Ukrainian commanders are quickly warned about most dangers. Experts in defense are creating small AI chips with embedded software that can be added to any machine, helping small drones and armored vehicles become autonomous, all to enhance defense purposes required for survival. As another analyst said, "Now, AI-based technologies are key to Ukraine's safety and freedom from future attacks."

Allies have taken on the same defensive strategy in the cyber realm and with information. Ukrainian tech volunteers used technologies like AI to respond to Russia's activities much before 2022. Grassroots groups have started using AI and technology to identify false videos recognize bot networks and immediately verify suspicious news about Ukraine following the invasion. Decentralized teams immediately supplied fly-by-drone (FPV) footage and AI-equipped map tools to military groups. It mirrors the reasoning of defensive realism in the face of a weak administration social actors assisted in strengthening the country's security by developing new defense measures. They prove that defensive realism is an accurate approach to studying security threats. Ukraine does not intend to overthrow Russia or expand its borders but simply aims to build collective defense. Choosing to use Bayraktar TB2 drones selectively to attack the enemy's supplies and keeping the drones as a strategic reserve, protected from enemy electronic jams, demonstrates how Ukraine plans for its survival. Also, Ukraine realizes that information matters and it has focused on debunking Russian lies and protecting vital information. This gives support to defensive realists who argue that nations seek only enough power and durability not continuous growth, in a system without central authority

Intelligence, Surveillance and Reconnaissance (ISR)

The term for Intelligence, Surveillance and Reconnaissance is ISR. AI speeds up the process of collecting and interpreting data. Machine learning is used by both sides to manage the country's intelligence data. Thanks to help from Silicon Valley's experts the U.S. military has increased its use of AI for ISR. To give an example both projects such as Project Maven (using AI to interpret footage from drones) and efforts launched under the JAIC are part of the Pentagon's AI development work. With the help of Google, Microsoft and Palantir, (James Black, 2024). The U.S. tech sector excels in developing advanced analytics (James Black, 2024). A Pentagon official admits that in 2018 it stepped up its AI spending, launched the Defense AI Strategy and created the Joint AI Center to keep up with Russia and China (James Black, 2024). As a result, U.S. officials can now quickly compile data from several sources to create a real-time image of the situation for commanders.

Russia acknowledges how useful AI is for ISR. The Russian military has been working to use AI to help change its data-processing processes. It appears that Russia is developing AI-driven sensors for its missiles and drones to spy on land, air and sea environments and alleviate the burden of too much data. Russia is using AI to detect targets and assess the destruction caused by fighting in Ukraine (Bendett, 2024). An illustration is that Russian drones now rely on image recognition loaded into the drones to find their own targets, even if lines of communication are blocked. It is also clear that Russia relies on AI to review messages captured during the war as part of information warfare. It has been pointed out that because of its high casualties, Ukraine has made it obvious to Russian leaders that they need closer cooperation between ISR, security and AI researchers. Access to improved ISR equipment has made a big difference for Ukraine's strategy. AI-powered analysts have expanded the sharing of intelligence among Western countries. Ukrainian

soldiers have relied on the data fusion software Palantir to examine UAVs, satellite photos and first-user reports. In the opinion of Ukrainian sources, most of the targeting for missiles is enabled by this AI-driven platform because it analyzes a lot of data (Mazarchuk, 2024). Independent journalists and analysts in Ukraine use AI to find information from social media, photos and events captured on satellites to report about incident locations, war crimes and happenings during the war. These tools have allowed Ukraine to be highly successful, providing the command with information quickly and simply. However, according to CSIS, Ukraine's AI technology for ISR is not widespread since it uses borrowed equipment and human analysts.

Autonomous Weapons and Platforms

AI is mainly used in warfare through autonomous and semi-autonomous weapons. AI technology is being included in unmanned systems in both the U.S. and Russia, even if they use different methods. As written in Pentagon doctrine the U.S. vision involves teaming up humans with drones and using groups of drones. Last year, the U.S. introduced the Replicator plan to deploy thousands of low-cost, fully autonomous drones and vehicles to attack enemy systems (Bajak, November 25, 2023). According to Kathleen Hicks, the goal behind Replicator is to use little, smart, simple and numerous weapons. The U.S. Air Force is creating the Longshot UAV (with support from DARPA) while the Navy continues to develop unmanned drones for operations on and under water. Overall, the goal is to let AI handle certain tasks to go farther protect people from danger and trouble the opposing side. The official policy in the United States aims for significant human control, even though officials realize that lethal drones without humans on the remote control will soon be a reality (Bajak, November 25, 2023). Researchers agree that AI in weapons will create different methods (such as swarming) for conducting warfare, but the end game advantage is still unclear, prompting them to race for superiority. The strategy in Russia is to equip large numbers of unmanned systems by reverse-engineering and importing technology from other countries. Russia is notably making extensive use of small drones called Shahed and Veter which can be programmed to find and attack targets by themselves using their built-in cameras. According to Reuters, Russian troops have dispatched over 3,000 of these explode-and-run drone weapons into Ukraine. Such drones barely require human control, as Russian specialists have tested a system where drones use AI to identify a target and take control if other signals stop (Bajak, November 25, 2023).

The Defense Minister of Russia, Belousov said that Russia is using AI drones on the battlefield in Ukraine and President Putin has directed that production of drones increases ten times for next year (to 1.4 million units). Tests are being carried out in Russia with ground robots and loitering munitions meant for logistics and demining, but they have not been widely used yet. Automation is being adopted in Ukraine to offset any shortages among its workers. (Reuters, 2024). The Ukrainian military aims to have unmanned units to take the place of soldiers in active combat. With AI-driven devices, Ukrainian engineers have managed to create systems that can be used for example by the Avengers drone system. In the war, Ukraine uses Switchblade drones and AI technical trials for systems it has developed. According to CSIS, (Bondar, 2024). full independence is not yet seen in how UAVs and loitering munitions are used in Ukraine, as they still require human intervention or GPS directions. As a result, Ukraine relies on systems using AI assistance for direction when GPS is not available and for controlling groups of drones. In Ukraine, startups collaborating with the military are focusing on developing features for drones that avoid collisions and can act in large groups. All in all, both U.S. and Russian armies want to use autonomous systems to enhance their numbers, and Ukraine responds in the same way by swiftly adopting them mostly via its allies. (Antoniuk, 2025).

Cyber War and Electronic Warfare

AI is bringing significant changes to cyber warfare and electronic operations. Russia and the U.S. believe that AI helps in protecting their cyber networks and conducting cyber-attacks. To defend their bases and command network the U.S. Cyber Command relies on AI for monitoring and detecting possible cyber-attacks. When playing offense on the network AI tools search open-source sites and communication samples in search

of weak points. Russia already plays a major role in cyber warfare and signs show it is using AI to sharpen its cyber-attack skills (therecord.media, 2025). Officials in Ukraine state that Russian hackers depend on machine learning to expedite analysis of their data and prepare individual phishing attacks. As an illustration after getting into the email system, Russian organizations rely on AI to select important content (financial information, war plans) and prepare spear-phishing messages meant for certain Ukrainian soldiers (Antoniuk, 2025). As a consequence, these attacks have become very advanced and are hard to spot. Those in charge of network security in Ukraine notice that cyber attackers will use the name, rank and personal information of victims. Ukraine reported in early 2025 that it is now much harder for anyone to detect Russian hacking (Antoniuk, 2025).

AI also supports the uses of jamming and signals intelligence in electronic warfare. AI technology in the U.S. allows it to manage the use of the airwaves by automatically noticing signals sent by hostile radars or drones. Russia has equipped its aircraft and drones with AI-powered jammers and radio-intelligence devices. Ukrainian authorities suspect that AI provides Russian military with the power to quickly analyze signals picked up by their interception pods. The main idea is that since AI supports the process cyber and EW operations become faster, so people have less time to decide what to do.

Information and Propaganda Operations

AI is now being used to compete in issues related to information. AI is being used by the U.S. and NATO for counter-propaganda and studying how influence works, while Russia forms and amplifies false information with its AI. Russian officials are now openly using AI as a weapon in information warfare. Thanks to recent studies, it is clear that the Kremlin employs AI to produce many false stories, alter images and manage vast numbers of accounts that share pro-Kremlin information online. In a similar case, Western cybersecurity agencies discovered that RT used an AI system named "Meliorator" to develop thousands of fake accounts on different social networks and promote false information about Ukraine and various nations (Sobchuk, 2024). With the help of AI, it is now possible for these campaigns to operate more broadly and rapidly – some chatbots can mistakenly repeat Kremlin narratives just by repeating their contaminated training material.

AI is being used by the U.S. and Ukraine to support their defense against information warfare. To identify fake information, U.S. organizations and nonprofits rely on machine-learning classifiers that prompt social media firms to act (Sobchuk, 2024). In Ukraine, there have been companies created (for example, Osavul and Mantis Analytics) that use information technology to detect and track attempts at coordinated disinformation. Ukraine's journalists and NGOs use AI to help validate and check open-source materials about how war crimes were committed by Russia. Russian disinformation is used to deny support for Ukraine on an international scale, criticize democracies and overstate situations that benefit Russia. Officials on the United States' side are responding by debunking these messages, often with the help of AI. Essentially, AI is supporting both the propagandists and the challengers, making it quicker and easier to fight the war over information.

Lastly, AI is becoming a bigger part of C4ISR (command, control, communications, computers, intelligence, surveillance, reconnaissance) elements. JADC2 by the U.S. military aims to bring together sensors and shooters from all domains and theaters in real time by using AI. Currently, AI is being used to target assets and predict the actions of the enemy during ongoing projects. DARPA is using AI to organize and manage the logistics process and to identify bottlenecks in a supply chain that occur in real time. Unlike the U.S., Russia does not yet have streamlined commands but is also using AI for helpful decision-making. It is said that Russian generals rely on software models powered by AI for their analysis and simulation exercises about future possible events. Still, similar problems exist in using AI ensuring decisions are secure, checking for dishonest behavior and making sure a human reviews decisions involving lethal actions. Despite

all the excitement, most armies such as Russia's, state that humans are still present when significant decisions are made (Bendett, 2024).

Case Studies

Wars in Ukraine have clearly shown AI's role in drone operations. Russia is using large numbers of cheap drones to flood Ukraine's airspace and frighten its people. (Bondar, 2024) The Shahed drones which Iran made, and Russia now produces, are easy to fly and are used by Russia in countless groups. There are drones that have AI built in so they can detect heat and stick to the path they are programmed for. Russia's own Veter drones ("Voxzel") are designed to use onboard target recognition after flying over an area. (Reuters, 2024) At the end of 2024 the Russian Defense Minister Belousov revealed an AI-powered drone that can "detect a target and automatically fly towards it, even if it disconnects from the controller. As of fall 2024 Russia claims to be using two whole squadrons of AI-powered drones in the battles against Ukraine. It has been confirmed by independent analysts that thousands of veteran drones are being flown into Ukraine. As a result, Russia is able to frequently carry out drone attacks on both power plants and cities, leading Ukraine to divide its anti-aircraft units and use them for different needs (Bernacchi, 2025).

The Ukrainians have also turned to drones which even have AI capabilities. For both tactics, Ukrainian soldiers have used off-the-shelf drones with autopilots helping guide their flights. Ukraine is receiving more advanced Western loitering weapons, like the Switchblade drone which waits and attacks at the given command. According to Reuters, Ukrainian drone attacks in 2024 caused a "huge ball of fire" to erupt from a Russian ammunition storage site in Tver, far removed from the fight zones (Reuters, 2024) .Even though Western drones are not independent in targeting and attacking, their arrival certainly enhances the country's ability to strike. In a number of front sectors, Ukrainian commanders humorously refer to it as a drone war since there are only a few soldiers visible in the conflict. A captured Russian soldier revealed that on the battlefield, he never came across Ukrainian forces. This is a type of war where drones are used the most (Bondar, 2024).

In Ukraine, using drones operated by artificial intelligence has taught us that these devices increase the number of forces and challenge defenders. According to Reuters' sources, AI-equipped drones are being utilized by both sides because they help fill areas where other weapons are lacking. Even so, drones make Ukraine's defense less effective, as the sheer number can disrupt response and civilians are now threatened by swarm drones all over the nation (Mazarchuk, 2024). It is proposed by analysts for Ukraine and its allies to use several cheaper and efficient methods (like acoustic sensors, unified air defense, electronic attacks and directed-energy weapons) to stop Russia's attacks by drones. As a result, there has been more interest from Western firms in developing autonomous drones for use in Ukraine, indicating how this war encourages new development.

AI in Intelligence and Targeting (Ukraine's Edge)

Despite the lack of resources, Ukraine has managed to rapidly integrate AI-based intelligence from tools provided by their Western allies. According to Palantir's CEO, Alex Karp, Ukrainian officials use the company's analytics software to put together information from satellites, online sources, images collected by drones and reports from on the ground. It uses AI to speed up the process of spotting troop and artillery movement which is harder for humans to do alone (Daniels, 2022). Most of Ukraine's accurate attacks are possible, thanks to Palantir which helps extend the impact of U.S. missiles (Bond, 2024). At the same time, both tech startups and NGOs in Ukraine have introduced AI tools to check open-source materials, for example, Osavul and Mantis use large language models to detect and warn against Ukrainian misinformation campaigns coordinated on the internet. Independent groups use AI technology to locate and report Russian war crimes as soon as they happen. People have recognized the good work RUSI expresses that analyzing information

using AI has played a key role in supporting Ukraine's narrative against false statements by Russia. (Daniels, 2022).

An additional example is Ukraine carrying out demining operations. Because the front was littered with mines, it took soldiers a long and deadly time to remove them all by hand. Here in Ukraine, AI is helping to create unmanned vehicles that can identify and address mines. The colleagues are working on applying this technology in Ukraine and it covers six main areas identified by experts (autonomy is included, along with mine-clearing). All in all, these case studies reveal that Ukraine employs AI (mainly commercial types quickly adopted) to boost its strength and ability to last in combat. Ukraine will stay ahead by getting continual support and technology, given that their R&D is smaller and the needs are urgent. AI influences the information environment in Ukraine from both the pro-Russian and pro-Ukrainian standpoints. AI is used by Russian state-supported groups in espionage according to Ukrainian cyber safety experts from Munich (2025) after a Russian hacker breaks into Ukrainian networks, they turn to machine-learning technology to examine stolen information and direct highly targeted phishing attacks. An instance of this was when Ukrainian troops got what looked like realized Signal messages containing files, they recognized which was made possible thanks to AI examining the music player's data (Sobchuk, 2024). This means that there are now more significant cyber-attacks aimed at Ukraine. In addition, Ukrainian officials are using AI to protect their own systems by detecting attacks and anticipating hostile measures (even if they have not shared exact systems used).

Using AI, Russian propaganda efforts against Ukraine are matched by Ukrainians using AI as well (Sobchuk, 2024). Russian operatives created AI-assisted deepfakes and viral fake news designed to change how the U.S. and other countries view their affairs (for instance, Russian channels recently spread a fake video of a State Department official created with AI). Because it uses analytics supported by AI, Ukraine responds quickly to any fake news. An analyst points out that using AI in OSINT has allowed Ukraine to create reliable accounts about Russia's actions. All in all, the war in Ukraine is acting as a "laboratory" for AI in informational warfare. Because events in the war are evolving so quickly, Ukraine must ensure its domestic security can recognize AI-fried misinformation and invest in AI-powered filters for content.

Implications for Ukraine's Cyber and National Security

Ukraine's safety is widely influenced by the AI competition between the U.S. and Russia. AI-assisted cyber-spying from Russia brings increasing danger to Ukraine's digital infrastructure and how the military communicates. Advanced phishing techniques and data-mining activities might reveal Ukraine's important information and details about people in the armed forces (Mazarchuk, 2024). Consequently, Ukraine needs to rapidly improve its cyber security. Ukraine should use AI-supported systems for detecting attacks, set up zero-trust networks and frequently work with cyber groups in the US and other Western countries to receive threat information. While Ukraine relies on more AI in its cyber defenses, its networks are still at significant risk compared to Russia.

Kinetic Defense: Given Russia's large-scale use of AI-driven drones and missiles, new defensive systems are needed. Low-cost drones and missiles bombard both civilians and military buildings in Ukraine every night, as part of an attrition strategy. Ukraine has not been able to fully protect itself from the overwhelming attacks in the air. It clearly suggests that Ukraine should concentrate on making new defense tools (like Israeli anti-drone systems, multi-radar networks, jammers and lasers) and moving its manufacturing to several locations. Besides buying missiles, (Bondar, 2024). Ukrainian defense industries should also pump out point-defense weapons and robotic units to protect against attacks. Ukraine faces a threat to its overall strength and allies' support from Russian AI-driven propaganda. Deepfake videos and narratives made by AI may erode people's trust in the government. Ukraine should increase its cyber security by including AI in its monitoring and verifying processes for news and information. To do this, it should maintain and improve homegrown AI start-ups and help analysts quickly use them to refute fake news. (Mazarchuk, 2024).

Awareness-raising initiatives at a global scale and with NATO's help can immunize both Ukrainians and their allies against AI-generated fake news.

An important result is that Ukraine is counting more on its allies' AI and intelligence to support its decisions. Currently there is no big-data analytics industry in Kyiv comparable to Silicon Valley. It is supported by firms from the West such as Palantir and Microsoft, who supply the necessary AI-enabled hardware for free. There are positives and negatives to this relationship. It allows Ukraine to obtain the most advanced certain tools. It also means Ukraine's safety depends on the strategy chosen by both the U.S. and the EU. As an illustration, in late 2023 the U.S. decided to halt some intelligence-sharing for a while which made the data advantage for Ukrainians unavailable. Because of this, diplomatic work and strengthening local tech skills should be included in Ukraine's plans for national security. Autonomous weapons have brought up problems for Ukraine under international laws. Using autonomous weaponry in Ukraine could make it difficult to assign responsibility. Ukraine (along with its allies) will face such dilemmas and at times might suggest new ways to address them. Since countries cannot agree on AI use during wars (for example at recent UN talks) Ukraine should rely on current regulations and aim to establish stricter guidelines (Reuters, 2024).

Strategic and Policy Recommendations

Based on the above analysis, we offer several strategic recommendations for Ukraine its partners and the broader international. Advance Ukraine's AI Strength (Sobchuk, 2024). The country should sustain its "Mil-Tech Valley" by helping tech incubators and startups (for example, BRAVE1 and D3) to develop AI for defense use. The government may make it easier to approve and get AI systems built locally and prompt military groups to partner up with civilian AI companies. Ukraine's partnership with companies such as Osavul and Mantis ought to be expanded to include additional collaborations. The EU, U.S. and NATO can provide funding, support with training and send technology to Ukrainian AI experts. (Sobchuk, 2024) Due to Russia's use of AI in cyber-attacks, Ukraine should work on improving its cyber defense systems. You should use AI to protect from cyber-attacks, continuously enhance security protocols and rehearse cyber defense by organizing red-team exercises (possibly with partners at the Cooperative Cyber Defense Centre of Excellence). Adding AI technology to military command systems would make it easier for Ukraine to respond to quick cyber or electronic attacks. Since Russia often uses drones and missiles, Ukraine is advised to invest in strong counter-autonomy measures and further develop air defense. This might require stocking more short-range air-defense guns, increase C-RAM defenses, as well as bring in acoustic sensors, high-energy lasers and UAV jammers. The countries in the alliance should work together to develop new counter-swarm technology with Ukraine. Ukraine should, at the same time, divide vital facilities and strengthen their infrastructure so that they are less likely to suffer from solo strikes (Mazarchuk, 2024). Ukraine should apply AI tools in how it handles strategic communications. Therefore, it is important to put together teams within the Ministry of Defense and journalistic groups that use AI to detect disinformation (like Osavul does) and provide truthful responses promptly.

AI-powered technology and educational programs can assist in training the public against fake news. Ukraine should team up with NATO and the EU to pressure both platforms and other states about AI-produced propaganda and promote laws (especially those proposed by the EU) that reduce the impact of AI on false information. There should be closer partnership between the U.S., NATO and Ukraine in the field of AI. Shared intelligence and ideas generated from AI should be kept secure. It is also important to go on with U.S. satellite examinations (using AI) and, when required, private services from France's Safran company could be used. Allies can develop AI tools specifically for use by Ukraine. Interoperability can be achieved if joint exercises are supported with AI scenarios, for instance, by letting Ukraine attend NATO "AI hackathons" (Reuters, 2024). Although Ukraine and its allies cannot expect Russia and the United States to agree on AI regulations, they should still work with other countries to agree on rules for AI in war. Ukraine may use the upcoming talks to talk about the use of autonomous drones against civilians and encourage action toward restricting

the use of LAWS that have no accuracy. At the same time Ukraine can take part in efforts to control the export of AI that could be used by Russia, making it more difficult for Moscow to get advanced chips and machine-learning technology. Joining security talks with ethics-based governance, Ukraine and its allies can influence how AI is governed. They should make sure that AI plays a role in Ukraine and NATO's strategies to discourage attacks. This could mean making it clear to Russia that Ukraine's AI defense is gaining strength and making sure Ukraine is used for NATO to test new AI tech. Continued support for Ukraine's military (supported by AI) will add cost to Russia for any future attacks. In short, AI should be seen as part of deterrence apart from only being an option in battle.

Conclusion

Warfare is being changed by AI, and this is clearly evident in the current U.S. Russia conflict over Ukraine. American and Russian armed forces are dedicating significant efforts to AI to improve surveillance, attacks on targets and independent operations, hoping to stay ahead while being concerned about what the other side might realize. For Ukraine, the war has turned into an experiment with drones, cyber-attacks and psychological warfare as major warfare tactics (Reuters, 2024). Ukraine has to adapt to both new challenges like AI-based cyberattacks and propaganda and benefits from the use of automation to reduce its shortage in manpower. According to our study AI is leading to a stronger focus on arms by major powers which will likely impact Ukraine's security for years to come. No state can be certain about how its rivals will apply AI which makes all parties eager to invest the most (like in previous times when doubt about actions led to increased investment). Because Ukraine is in the middle of these rival countries, it must use new AI solutions combined with strong defense capabilities.

For the future Ukraine needs to use AI technology in its security and win assistance from other countries. Investing in both offensive and defensive AI is required nowadays for a nation's security. On the other hand, global management of AI in warfare is still in its early stages. The situation in Ukraine emphasizes the importance of putting norms and safeguards in place for military AI. Only through international agreements will it be possible to curb the unplanned increase in violence or harms caused by autonomous military systems. All in all, the AI fight happening in Ukraine gives us a clear idea of warfare to come. As a consequence of its ideas, both researchers and experts in the field should re-evaluate traditional ways of working strategies such as intelligence, deterrence and defense will have to develop with the rise of AI. If governments take advantage of these principles and models, they will do better in facing the transformation. Hopefully gaining a better understanding will lead nations to enact sensible policies instead of spending heavily on armaments alone

References

Antoniuk, D. (2025). *Ukraine warns of growing AI use in Russian cyber-espionage operations.* Therecord.media. https://therecord.media/russia-ukraine-cyber-espionage-artificial-intelligence

Bajak, F. (2023, November 25). *Pentagon's AI initiatives accelerate hard decisions on lethal autonomous weapons.* AP News. https://apnews.com/article/us-military-ai-projects-0773b4937801e7a0573f44b57a9a5942

Bendett, S. (2024, May 3). *The Role of AI in Russia's Confrontation with the West.* Www.cnas.org. https://www.cnas.org/publications/reports/the-role-of-ai-in-russias-confrontation-with-the-west

Bernacchi, G. (2025, February 24). *Baykar Tests TB2 Drone Equipped With AI Features, Turbo Engine.* The Defense Post. https://thedefensepost.com/2025/02/24/bayraktar-tb2-ai-turbo-engine/

Black, J., Eken, M., Parakilas, J., Dee, S., Ellis, C., Kiran Suman-Chauhan, Bain, R. J., Fine, H., Aquilino, M. C., Lebret, M., & Palicka, O. (2024, September 6). *Strategic competition in the age of AI: Emerging risks and opportunities from military use of artificial intelligence.* Rand.org; RAND Corporation. https://www.rand.org/pubs/research_reports/RRA3295-1.html

Bond, S. (2024, June 6). *Russian propaganda in 2024 includes deepfakes, sham websites and social media swarms.* NPR. https://www.npr.org/2024/06/06/g-s1-2965/russia-propaganda-deepfakes-sham-websites-social-media-ukraine

Bondar, K. (2024, November 12). *Understanding the Military AI Ecosystem of Ukraine.* Csis.org. https://www.csis.org/analysis/understanding-military-ai-ecosystem-ukraine

Jensen, B., & Yasir Atalan. (2025). *Drone Saturation: Russia's Shahed Campaign.* Csis.org. https://www.csis.org/analysis/drone-saturation-russias-shahed-campaign

Mazarchuk, A. (2024). *VIEWPOINT: AI for War and Peacetime: A Ukrainian Perspective.* Nationaldefensemagazine.org. https://www.nationaldefensemagazine.org/articles/2024/11/1/viewpoint-ai-for-war-and-peacetime-a-ukrainian-perspective

Reuters Staff. (2024, October 11). *Russia says it is ramping up AI-powered drone deployments in Ukraine.* Reuters. https://www.reuters.com/business/aerospace-defense/russia-says-it-is-ramping-up-ai-powered-drone-deployments-ukraine-2024-10-11/

Sobchuk, M. (2024, February 12). *How Ukraine uses AI to fight Russian information operations.* Www.globalgovernance.eu. https://www.globalgovernance.eu/publications/how-ukraine-uses-ai-to-fight-russian-information-operations

Thompson, A. (2022, December 21). *The AI "Revolution in Military Affairs": What Would it Really Look Like? Center for Security and Emerging Technology.* https://cset.georgetown.edu/article/the-ai-revolution-in-military-affairs-what-would-it-really-look-like/