CNA

September 2023

Tomorrow's Technology in Today's War: The Use of AI and Autonomous Technologies in the War in Ukraine and Implications for Strategic Stability

Margarita Konaev

IOP-2023-U-036583-Final

Abstract

Since Russia's full-scale invasion of Ukraine, artificial intelligence has reportedly been used to analyze different types of data to enhance decision-making and inform targeting, to process enemy communications, in facial recognition technology, and in cyber defense, to name a few. Drawing on open-source information and scholarly research, this report, authored by Margarita Konaev of Georgetown's Center for Security and Emerging Technology, surveys the use of AI in the war in Ukraine and assesses the potential implications of these systems and capabilities for conflict escalation and strategic stability. Although AI has played an important role in enhancing battlefield information processing, it is difficult to estimate whether these technologies are being used at scale and to what effect. Although in its current form, the use of AI has had a limited effect on the risk of escalation, this may change with more extensive deployment, especially of untested systems, which highlights the value of confidence building measures to minimize the risk of inadvertent escalation.

This report is part of a series generously funded by a grant from the Carnegie Corporation of New York.

CNA's Occasional Paper series is published by CNA, but the opinions expressed are those of the author(s) and do not necessarily reflect the views of CNA or the Department of the Navy.

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

Administrative or Operational Use 9/12/2023

This work was performed under Specific Authority Contract No. G-19-56503

Cover image: "Lancet kamikaze drone," https://mil.in.ua/, 16 July 2022.

Approved by: **September 2023**

Anya Fink

Anya Fink, Research Program Director (Acting)
Russia Studies Program
Strategy, Policy, Plans and Programs Division

Contents

This page intentionally left blank.

Introduction

The role of artificial intelligence (AI) and autonomous systems in the war in Ukraine has attracted a great deal of attention in the media and from analysts tracking the use of tomorrow's technology in today's wars. Ukraine, with help from the United States, other North Atlantic Treaty Organization (NATO) partners, and a wide range of technology companies, is leveraging AI to continuously update their understanding of the battlefield, support decision-making and gain an advantage in intelligence and operations.[1] Less reliable information is available about Russia's use of AI and autonomous technologies. However, some evidence exists claiming that Russian operators have tried using AI to enhance disinformation campaigns, while the Russian armed forces are extensively using loitering munitions to attack Ukrainian cities and block the Ukrainian military's counteroffensive.

Since Russia's full-scale invasion of Ukraine in February 2022, AI has also reportedly been deployed aboard drones to collect intelligence, carry out strikes and process enemy battlefield communications in facial recognition technology, cyber defense, etc. In recent months, reports about AI on the battlefield have converged with the widespread news coverage of the breakthroughs in generative AI systems to create an impression that the technology is ubiquitous. A careful assessment of the topic, however, must acknowledge that AI is a relatively new technology that has seen few battlefield deployments before the war in Ukraine. The scale and nature of AI deployment in this conflict is therefore unprecedented by default. Still, it is difficult to assess whether these applications and capabilities have been used only on a few occasions or widely deployed. It is also impossible to know, based on open-source materials, whether and what type of AI and autonomous technologies are being used in classified tasks and missions, and to what effect.

As such, it would be incorrect or at least premature to conclude that either the Ukrainians or the Russian forces are employing AI at scale. Rather, it is more likely that the use of AI and autonomous technologies in the war in Ukraine has been limited to certain use cases, tasks, and conditions. Ukraine has mobilized its impressive community of IT workers and software engineers to support the war effort and many if not most of the country's drone companies and other AI startups are working closely with military units on the front lines.[2] However, the more advanced capabilities—such as leveraging AI to collect, fuse, analyze, and exploit different

[1] Samuel Bendett, "Roles and Implications of AI in the Russian-Ukrainian Conflict," *Russia Matters*, July 20, 2023, https://www.russiamatters.org/analysis/roles-and-implications-ai-russian-ukrainian-conflict.

[2] John Hudson and Kostiantyn Khudov, "The War in Ukraine Is Spurring a Revolution in Drone Warfare Using AI," *Washington Post*, July 26, 2023, https://www.washingtonpost.com/world/2023/07/26/drones-ai-ukraine-war-innovation/.

types of commercial and classified data to enhance decision-making and guide targeting—have primarily been developed and deployed by US and allied forces positioned outside of Ukraine. These advanced capabilities are being enabled by private sector companies that are providing Ukraine and its allies with the data, equipment, and technological know-how to fight the Russian forces while gaining operational experience and battlefield data to test and refine their products.

Although the war in Ukraine is showing how new technologies are shaping the battlefield in real time, it also highlights a longer-term trend of militaries around the world accelerating investment into research and development of AI and autonomous technologies. Progress in these fields promises to reduce risk to deployed forces, minimize the cognitive and physical burden on warfighters, and significantly increase the speed of information processing, decision-making, and operations, among other advantages. Yet such technological breakthroughs and the use of these applications and systems in contested environments may also come with risks and costs—from ethical concerns about responsibility for the use of lethal force to unexpected behavior of brittle and opaque systems.[3]

Alongside the technological progress in AI and autonomous technologies, there is also a fast growing body of research dedicated to studying the potential implications of these systems and capabilities for international security, strategic stability, and conflict dynamics. Reports about the use of AI and autonomous technologies in the war in Ukraine, although far from comprehensive, allow us to assess some of the hypotheses put forth by this literature. With that, the remainder of this chapter proceeds in four parts. The first section reviews some of the existing arguments about the potential effect of AI and autonomous technologies on strategic stability and conflict dynamics. Then, drawing on open-source information, the second section offers a brief overview of AI and autonomous technology use in the war in Ukraine. The following section considers how the use of AI and autonomous technologies in the war may have affected the risk of escalation from conventional war to the use of nuclear weapons and conflict spreading to include other parties. The last section assesses how AI and autonomous technologies may affect strategic stability between the United States and Russia beyond the current Russo-Ukrainian war, focusing specifically on the potential role of confidence building measures in minimizing the risk of inadvertent escalation.

[3] Tate Nurkin and Margarita Konaev, "Eye to Eye in AI: Developing Artificial Intelligence for National Security and Defense," Atlantic Council, May 20, 2022, https://www.atlanticcouncil.org/in-depth-research-reports/report/eye-to-eye-in-ai/#introduction.

The Role of AI and Autonomous Technologies on Strategic Stability and Conflict Dynamics

Research on technology and international security has outlined various ways that the integration of AI and autonomous technologies into military systems and missions could affect strategic stability, nuclear risk, and conflict initiation and escalation. The following discussion highlights some of this work but does not offer an exhaustive review of this rapidly expanding field of research.

Building on the literature about how the proliferation of drones could affect international security, some scholars have argued that the ability to use uncrewed systems with increasingly autonomous capabilities may lead to adventurism or aggression in foreign policy decisions.[4] Deploying military forces inevitably bears the risk of human and material losses, economic downturn, and societal unrest, any of which can shift public opinion against incumbent leaders and possibly lead to their removal from office. The use and even the loss of autonomous systems, on the other hand, is less politically costly than the loss of human lives. Scholars have therefore warned that with this perception that deploying autonomous systems for military purposes comes at a lower political cost, leaders may be more inclined to initiate conflict.[5] Others have suggested that this perception of lower political costs may not only make conflicts easier to start but also more difficult to end, especially in the context of urban warfare.[6] The proliferation of these technologies to more countries and nonstate actors will likely increase the risk of conflict and spread instability across the international system.

Another set of arguments centers on how the use of AI and autonomous technologies could increase the risk of intentional, inadvertent, or accidental escalation—whether from a crisis to a conflict, or conventional to nuclear confrontation—due to misperceptions, miscalculations, or accidents.[7] Some arguments have focused more specifically on the connection between AI and nuclear weapons, examining how advances in AI could be exploited across the nuclear deterrence architecture—from early warning and intelligence, surveillance, and

[4] Michael Zenko, "Reforming US Drone Strike Policies," Council on Foreign Relations, 2013, https://www.cfr.org/report/reforming-us-drone-strike-policies.

[5] Michael Horowitz, Sarah E. Kreps, and Matthew Fuhrmann, "Separating Fact from Fiction in the Debate Over Drone Proliferation," *International Security* 41, no. 2 (2016), pp. 7–42, https://www.belfercenter.org/sites/default/files/files/publication/isec_a_00257.pdf.

[6] Margarita Konaev, "With AI, We'll See Faster Fights, But Longer Wars," War on the Rocks, Oct. 29, 2019, https://warontherocks.com/2019/10/with-ai-well-see-faster-fights-but-longer-wars/.

[7] Herbert Lin, "Escalation Risks in an Artificial Intelligence—Infused World," *Artificial Intelligence, China, Russia, and the Global Order*, edited by Nicholas D. Wright, Air University Press, 2019, pp. 143–52, http://www.jstor.org/stable/resrep19585.25.

reconnaissance via command and control to nuclear weapons delivery systems.[8] Today, AI technology remains too brittle and vulnerable to attacks for nuclear-armed states to delegate nuclear command and control functions, and specifically missile-launch decisions to AI. Yet, some scholars have suggested that with improvements in technology, concerns about retaining first strike advantage or ensuring retaliation could prompt countries, perhaps particularly Russia, to activate fully automated nuclear command and control systems (as the USSR has done during the Cold War).[9] Aside from command and control, researchers have posited that improvements in autonomous systems, specifically in undersea vehicles that can locate and shadow adversary submarines, increase the vulnerability of nuclear delivery systems, which could in turn undermine strategic stability and deterrence.[10]

An additional area of research investigates destabilizing effects of AI-enabled information operations. Propaganda and disinformation campaigns have existed throughout history. But until very recently, such efforts have typically involved humans at every stage—to develop and generate engaging content, identify and cultivate target audiences, and create the social media profiles and channels that will disseminate and amplify manufactured messages. Advances in AI and large language models in particular, however, could drive down the costs of generating propaganda by automating the process of content creation and the execution of disinformation campaigns.[11] This opens the aperture for more and different types of actors to initiate disinformation campaigns and also creates the potential for highly scalable campaigns that reach a massive audience.[12] Recent advances in large language models like ChatGPT are also making it possible to generate sophisticated and context-specific messages that may resonate

[8] Vincent Boulanin, ed. "*The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk*," SIPRI, May 2019, https://www.sipri.org/sites/default/files/2019-05/sipri1905-ai-strategic-stability-nuclear-risk.pdf; James Johnson, "AI, Autonomy, and the Risk of Nuclear War," War on the Rocks, July 29, 2022, https://warontherocks.com/2022/07/ai-autonomy-and-the-risk-of-nuclear-war/.

[9] Boulanin, ed. "The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk."

[10] Jonathan Gates, "Is the SSBN Deterrent Vulnerable to Autonomous Drones?," *RUSI Journal* 161, no. 6 (2016), pp. 28–35, https://www.tandfonline.com/doi/abs/10.1080/03071847.2016.1265834; Sylvia Mishra, "Could Unmanned Underwater Vehicles Undermine Nuclear Deterrence?," *Strategist*, May 8, 2019, https://www.aspistrategist.org.au/could-unmanned-underwater-vehicles-undermine-nuclear-deterrence/; Keir Lieber and Daryl Press, "The New Era of Counterforce: Technological Change and the Future of Nuclear Deterrence," *International Security* 41, no. 4 (2017), pp. 9–49.

[11] Katerina Sedova, Christine McNeill, Aurora Johnson, Aditi Joshi, and Ido Wulkan, *AI and the Future of Disinformation Campaigns*, Center for Security and Emerging Technology, Dec. 2021, p. 6, https://cset.georgetown.edu/publication/ai-and-the-future-of-disinformation-campaigns/.

[12] Josh Goldstein, Renee DiResta, Girish Sastry, Micah Musser, Matthew Gentzel, and Katerina Sedova, *Generative Language Models and Automated Influence Operations: Emerging Threats and Potential Mitigations*, Stanford Internet Observatory, OpenAI, and Georgetown University's Center for Security and Emerging Technology, Jan. 11, 2023, p. 8, https://cdn.openai.com/papers/forecasting-misuse.pdf.

more strongly with the intended audience and make influence operations harder to discover and take down.[13]

AI-enabled deepfake technology is another area of concern, not only for disinformation and propaganda, but also in military and intelligence operations. Countless potential scenarios exist where convincing deepfakes, deployed in opportune moments, could undermine unity and cohesion between soldiers on the battlefield, dampen public support for military missions, deepen societal divisions, divide allies, lead to loss of trust in democratic institutions, and shape the information environment in favor of the aggressor.[14] Efforts to mitigate the spread of misleading and false content are already falling behind; even when disinformation is debunked, research shows that false news spread "farther, faster, deeper, and more broadly" than accurate reports or corrections issued to repudiate false reports.[15]

Finally, there is a burgeoning literature on how progress in AI and autonomous technologies could affect cyber operations, which at times considers the potential for escalation. Some researchers, for instance, have posited that the integration of AI, or more accurately, machine learning-based automation, into cyber operations could potentially "increase the stealthiness of cyber operations and enable malicious code to function more independently of human operations."[16] These developments could shield the perpetrators' identity and make it harder to defend against incursions and cyberattacks. The increased difficulty of attributing responsibility for attacks could, in turn, embolden both countries and nonstate actors in the cyber realm, potentially leading to intensified cyber conflicts, diplomatic crises, and even destabilizing effects in the real world.

At the same time, scholars have also suggested that AI and autonomous technologies have features and potential uses that could decrease the risk of conflict initiation or escalation and enhance strategic stability. With regards to conflict initiation, countries rarely start wars unless

[13] Ben Buchanan, Andrew Lohn, Micah Musser, and Katerina Sedova, *Truth, Lies, and Automation: How Language Models Could Change Disinformation*, Center for Security and Emerging Technology, May 2021, https://cset.georgetown.edu/publication/truth-lies-and-automation/.

[14] Alina Polyakova, "Weapons of the Weak: Russia and AI-Driven Asymmetric Warfare," Brookings, Nov. 15, 2018, https://www.brookings.edu/research/weapons-of-the-weak-russia-and-ai-driven-asymmetric-warfare/; Margarita Konaev and Samuel Bendett, "Russian AI-Enabled Combat: Coming to a City Near You?," War on the Rocks, July 31, 2019, https://warontherocks.com/2019/07/russian-ai-enabled-combat-coming-to-a-city-near-you/; Daniel L. Byman, Chongyang Gao, Chris Meserole, and V.S. Subrahmanian, *Deepfakes and International Conflict*, Brookings, Jan. 2023, https://www.brookings.edu/wp-content/uploads/2023/01/FP_20230105_deepfakes_international_conflict.pdf.

[15] Soroush Vosoughi, Deb Roy, and Sinan Aral, "The Spread of True and False News Online," *Science,* Mar. 9, 2018, https://www.science.org/doi/10.1126/science.aap9559.

[16] Ben Buchanan, John Bansemer, Dakota Cary, Jack Lucas, and Micah Musser, *Automating Cyber Attacks*, Center for Security and Emerging Technology, Nov. 2020, https://cset.georgetown.edu/publication/automating-cyber-attacks.

they believe they can win and that the adversary has inferior military capabilities. The adoption of AI technologies that increase the speed of decision-making and operations, coupled with autonomous functions in weapons systems that augment lethality, can signal military strength and effectiveness; such capabilities, in turn, can discourage potential aggressors, especially if they do not possess the same capabilities, and bolster deterrence.[17]

Deterrence rests on the credible threat of lethal force. With that in mind, some scholars have argued that removing humans partially or entirely from the decision to engage targets can strengthen deterrence by signaling that reprisal is certain.[18] Moreover, greater autonomy and AI in uncrewed systems vastly expand access and reach in denied, hostile, and austere environments, including for operations into anti-access or area denial environments near potential adversaries and contested airspace. This could also reinforce deterrence by improving situational awareness and strengthening early warning mechanisms.[19]

Focusing on escalation dynamics, others have pointed out that countries are less likely to retaliate or escalate in response to a damaged or destroyed autonomous vehicle as opposed to an incident where soldiers are injured or killed.[20] Notably, this particular argument stands in contrast to the aforementioned proposition that the lower political costs associated with deploying and losing autonomous systems can push leaders to take aggressive foreign policy decisions and increase the risk of conflict. The debate about the potential influence of AI and autonomous technology on security, stability, and conflict is therefore still ongoing, offering a broad range of perspectives that sometimes contradict one another.

Some experts have argued that because AI is not afflicted by human sentiments such as anger, hatred, or fatigue, it is less likely to make emotional or irrational decisions that may lead to dangerous or even catastrophic outcomes.[21] AI applications that expedite intelligence processing, improve planning, and enhance situational awareness on the battlefield could also

[17] Margarita Konaev, Husanjot Chahal, Ryan Fedasiuk, Tina Huang, and Ilya Rahkovksy, *US Military Investments in Autonomy and AI: Costs, Benefits, and Strategic Effects*, Center for Security and Emerging Technology, Oct. 2020, p. 17, https://cset.georgetown.edu/publication/u-s-military-investments-in-autonomy-and-ai-a-strategic-assessment/.

[18] Michael C. Horowitz, "When Speed Kills: Lethal Autonomous Weapon Systems, Deterrence, and Stability," *Journal of Strategic Studies* 42, no. 6 (2019), pp. 764–788.

[19] Konaev, Chahal, Fedasiuk, Huang, and Rahkovksy, "US Military Investments in Autonomy and AI: Costs, Benefits, and Strategic Effects."

[20] Michael Horowitz, Sarah E. Kreps, and Matthew Fuhrmann, "Separating Fact from Fiction in the Debate Over Drone Proliferation*," International Security* 41, no. 2 (2016), pp. 7-42.

[21] Forrest E. Morgan, Benjamin Boudreaux, Andrew J. Lohn, Mary Ashby, Christian Curriden, Kelly Klima, and Derek Grossman, *Military Applications of Artificial Intelligence: Ethical Concerns in an Uncertain World*, RAND, 2020, p. 34, https://www.rand.org/content/dam/rand/pubs/research_reports/RR3100/RR3139-1/RAND_RR3139-1.pdf.

allow for more precise and judicious use of force and help reduce the risk of civilian harm and collateral damage, thereby avoiding escalation.[22] Such arguments about the potential of AI-enabled precision warfare for increasing compliance with the laws of war are of course predicated on the assumption that belligerents have the political will to do so to begin with.

Ultimately, the influence of AI and autonomous technologies on international security, strategic stability, and conflict dynamics is deeply intertwined with other factors—other advanced weapons, the nature of political systems where such innovations take place, organizational cultures of the militaries that plan to use these technologies, how these technologies interact with one another, and many others. Because AI has yet to see extensive battlefield deployment, or large-scale adoption across military organizations, its potential effects are still debated. The use of AI and autonomous technologies in the war in Ukraine provides an opportunity to assess some of the aforementioned hypotheses and glean initial insights into the role of these technologies in modern warfare.

Use of AI and Autonomous Technologies in the War in Ukraine

Although the use of AI and autonomous technologies in the war in Ukraine—insofar as can be discerned from open-source information—has been limited to certain tasks and use cases, it has nonetheless been unprecedented in its extent. Both Ukrainian and (to a lesser extent) Russian forces have reportedly made use of drones and loitering munitions with autonomous functions. Commercial companies have provided Ukraine with AI-enabled technology to analyze and fuse different types of classified, commercial, and open-source data to enhance battlefield situational awareness and identify targets, as well as software to process enemy battlefield communications and information. Meanwhile, Russian actors have employed AI to enhance information operations and scale disinformation campaigns, albeit to a limited effect.

The following analysis contains several limitations. For one, the discussion includes several examples where it is unclear whether particular systems, platforms, or operations indeed relied on AI. This reflects the limitations of publicly available information; the lack of consensus over what AI is and is not; the fact that remotely operated systems are often discussed interchangeably with autonomous systems; and the impossibility to determine the presence or absence of AI capabilities without access to the software within a given system. The analysis

[22] Larry Lewis and Andrew Ilachinski, *Leveraging AI to Mitigate Civilian Harm*, Center for Naval Analyses, Feb. 2022, https://apps.dtic.mil/sti/trecms/pdf/AD1181578.pdf; Peter Margulies, "The Other Side of Autonomous Weapons: Using Artificial Intelligence to Enhance IHL Compliance," *Impact of Emerging Technologies on the Law of Armed Conflict*, ed. Ronald T.P. Alcala and Eric Talbot Jensen (New York: Oxford Academic, 2019), https://doi.org/10.1093/oso/9780190915322.003.0006.

also refrains from making inferences about the scale and AI's overall effect on the conduct of military operations and other missions. This is because it is difficult to assess whether these applications and capabilities have been used on a few occasions or widely deployed, or whether and what type of AI and autonomous technologies are being used in classified settings, and to what effect. Overall, the account below is not meant to be an exhaustive review of the AI-enabled and autonomous weapons and systems deployed by Russia and Ukraine throughout the war. Rather, it samples relevant capabilities used to illustrate the evolving role of new and emerging technologies on the battlefield.

Drones and loitering munitions

Uninhabited aerial systems have been used extensively by both Ukraine and Russia since the onset of the war for a broad range of tasks, including intelligence, surveillance, reconnaissance, and strikes. They have been deployed on independent missions and integrated into more advanced combined arms operations. Uncrewed aerial vehicles' (UAV) videos have also been used for information operations, showcasing the weapons' precision and devastating effect on various social media platforms. UAVs, including armed UAVs, have been deployed on battlefields around the world for decades. But in recent years, commercial drone technology has evolved significantly while the armed drone market has also expanded to countries like Turkey and Iran joining the top ranks of more established drone manufacturers like the United States, China, and Israel. These developments, in turn, led to the proliferation of this technology to smaller and less advanced militaries and nonstate actors. Although most UAVs today are remotely operated, including those used in the war in Ukraine, tracking the evolution in UAV operations can provide insights into how more advanced autonomous systems may affect the conduct and trajectory of future conflicts.

Ukraine has used a range of civilian and commercially available drones alongside military drones to provide intelligence, surveillance, and reconnaissance (ISR) capabilities at the unit level, receive information about the locations and movements of Russian troops to inform targeting, and enhance military planning at all levels. According to reports, the Ukrainian military drone arsenal includes systems such as Fury, Spectator, Leleka, Punisher, and PD-1 drones which have been used for surveillance and reconnaissance.[23]

During the first months of the war, much attention was paid to Ukraine's use of the Turkish Bayraktar TB2 drones—a medium altitude long endurance UAVs that have a range of up to 300 kilometers, can fly up to 27 hours, and carry up to four laser-guided munitions. The TB2 is remotely operated, but it is advertised as being able to take off, cruise, and land autonomously;

[23] Samuel Bendett and Jeffrey Edmonds, *Russian Military Autonomy in Ukraine: Four Months In*, Center for Naval Analyses, July 2022, https://www.cna.org/reports/2022/07/Russian-Military-Autonomy-in-Ukraine-Four-Months-In.pdf.

although such capabilities may be more akin to an autopilot or preprogrammed automation, rather than autonomy and real-time machine decision-making without human control. Some experts were initially skeptical about the drone's potential effect considering that the Bayraktar TB2s are large, low-flying and radio-controlled which makes them relatively easy targets for layered air defense systems and electronic warfare capabilities.[24] Yet, TB2s have reportedly played an outsized role in destroying Russia's surface-to-air missiles, hitting ammunition depos, targeting supply routes and armed convoys, and even helping sink the *Moskva*, the flagship in Russia's Black Sea Fleet.[25]

The Ukrainian armed forces are also using loitering munitions or kamikaze drones such as the Switchblade Tactical, which were some of the first uncrewed aerial systems that the United States supplied to Ukraine. The benefit of these smaller, exploding drones is that they are portable and can be launched from effectively anywhere, fly above the battlefield, and once zeroed in on a target, dive in to hit vehicles or groups of soldiers with high levels of precision and relatively limited collateral damage.[26] The Ukrainian military has also reportedly made use of the Polish-made Warmate loitering munitions. Both the US-made Switchblades and Polish loitering munitions require humans to decide on a target over a live video feed, although according to the Switchblades' manufacturer, the technology to deploy the weapon autonomously already exists today.[27] In addition to the Switchblades, the United States has also provided Ukraine with Phoenix Ghost Drones, a new type of loitering munitions whose specific capabilities have not been disclosed.[28]

[24] Lauren Kahn, "How Ukraine Is Using Drones Against Russia," Council on Foreign Relations, Mar. 2, 2022, https://www.cfr.org/in-brief/how-ukraine-using-drones-against-russia.

[25] Zachary Kallenborn, *Seven (Initial) Drone Warfare Lessons from Ukraine*, Modern War Institute, May 12, 2022, https://mwi.usma.edu/seven-initial-drone-warfare-lessons-from-ukraine/; Samuel Bendett, "Drones Over Ukraine," *In Depth*, Apr. 25, 2022, https://www.cna.org/our-media/indepth/2022/04/drones-over-ukraine.

[26] Gerrit De Vynck, Pranshu Verma, and Jonathan Baran, "Exploding 'Kamikaze' Drones Are Ushering in a New Era of Warfare in Ukraine," *Washington Post*, Mar. 24, 2022, https://www.washingtonpost.com/technology/2022/03/24/loitering-drone-ukraine/; Giulia Carbonaro, "How Switchblade Drones Could Turn the Tide of Ukraine War," *Newsweek*, Mar. 17, 2022, https://www.newsweek.com/switchblade-drones-ukraine-war-russia-1688906; Kris Osborn, "Ukraine's Switchblade Drones Will Be Game Changers for Urban Combat," *National Interest*, Mar. 4, 2022, https://nationalinterest.org/blog/buzz/ukraine%E2%80%99s-switchblade-drones-will-be-game-changers-urban-combat-202220.

[27] Frank Bajak and Hanna Arhirova, "Drone Advances in Ukraine Could Bring Dawn of Killer Robots," *Los Angeles Times*, Jan. 3, 2023, https://www.latimes.com/world-nation/story/2023-01-03/drone-advances-in-ukraine-dawn-of-killer-robots.

[28] De Vynck, Verma, and Baran, "Exploding 'Kamikaze' Drones Are Ushering in a New Era of Warfare in Ukraine;" Elias Tousif, "Drone Warfare in Ukraine: Understanding the Landscape," Stimson, June 30, 2022, https://www.stimson.org/2022/drone-warfare-in-ukraine-understanding-the-landscape/.

The fact that Ukraine has been able to use UAVs effectively against higher-value Russian targets highlights the failure of Russian air defense systems, especially during the early stages of the war, and raises important questions for US military development of counter-UAV concepts, technologies, and operations. Despite their importance, the attrition rates of UAVs are extremely high. A report from RUSI estimated that around 90 percent of all UAVs used between February and July 2022 were destroyed, and "only around a third of UAV missions can be said to have been successful."[29] More recent calculations suggest that Ukrainian UAV losses stand at about 10,000 per month, as Russian electronic warfare capabilities have notably improved from the early months of the war.[30]

As previously noted, most UAVs used in the war in Ukraine are remotely operated. That said, in July 2022, a Polish news outlet reported that Ukrainian software developers working with the Ukrainian military have developed an AI image classifier capable of identifying military vehicles hidden in camouflage to be used aboard armed drones. Although the decision to strike the identified target still remains in the hands of human operators, the technological components aboard these UAVs, including AI-based military object detection and tracking, could presumably allow for the use of autonomous weapons, especially in communications-denied environments.[31] In October 2022, a Ukrainian military officer told a Ukrainian news agency that his team already conducts fully robotic UAV operations, without human involvement, but did not confirm such autonomous operations included strikes and indicated that these were a "point phenomena" rather than common practice.[32] A growing number of Ukrainian drone companies are working on AI-powered software that can help drones stay on

[29] Mykhaylo Zabrodskyi, Jack Watling, Oleksandr V. Danylyuk, and Nick Reynolds, *Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February-July 2022*, RUSI, Nov. 30, 2022, p. 37, https://static.rusi.org/359-SR-Ukraine-Preliminary-Lessons-Feb-July-2022-web-final.pdf.

[30] Jack Watling and Nick Reynolds, *Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine*, RUSI, May 19, 2023, https://static.rusi.org/403-SR-Russian-Tactics-web-final.pdf.

[31] Marcin Wyrwal, "War in Ukraine: How Artificial Intelligence Is Killing Russians," Onet, July 13, 2022, https://www.onet.pl/informacje/onetwiadomosci/rozwiazali-problem-armii-ukrainy-ich-pomysl-okazal-sie-dla-rosjan-zabojczy/pkzrk0z,79cfc278; Saker UAV, https://saker.airforce/.

[32] Tatiana Urbanska, "Lt. Col. Yuroslav Gonchar: Our Everyday Life Is Like This: A Respected General Graduated, Took a High Position, but Did Not Even Master Word on the Computer," Unian, Oct. 13, 2022, https://www.unian.ua/war/aerorozvidka-v-ukrajini-yak-pracyuyut-operatori-droniv-na-viyni-interv-yu-z-yaroslavom-goncharom-12010002.html; David Hambling, "Will Ukraine Deploy Lethal Autonomous Drones Against Russia?," *New Scientist*, Nov. 1, 2022, https://www.newscientist.com/article/2344966-will-ukraine-deploy-lethal-autonomous-drones-against-russia/.

target even if they lose contact with the human operator because of electronic interference deployed by Russia.[33]

The Russians have also made extensive use of drones, including systems such as Orlan-10, Orlan-30, Eleron-3, Takhion, Zastava, and Zala ISR drones, along with helicopter-type models, as well as Forpost-R and Orion combat UAVs used for longer-range ISR and combat missions and the Shahed-136 drones supplied by Iran.[34] Since October 2022, the Russian armed forces have increasingly targeted civilian infrastructure with missile and drone strikes, damaging the supply of electricity, heating, and water across the country.[35] In May 2023, for example, Russia launched nearly 60 drones in a single large-scale attack on Kyiv, most being the Iranian Shahed-136 drones.[36]

Russia has also publicized the use of loitering munitions, particularly the KUB-BLA and the Lancet. The use of the KUB-BLA raised concerns about deployment of an "AI-based autonomous weapon" because the system was reportedly capable of "real-time recognition and classification of detected objects" using AI, or as some have put it, identify targets using AI.[37] Still, as some reports have noted, "It is unclear if the drone may have operated in this [an AI-enabled autonomous] way in Ukraine."[38] Russian media reported that in June 2022 the Russian military also used the Lancet-3 loitering munition to strike Ukrainian positions in the Zaporozhnye Region, while Ukrainian channels reported that the Ukrainian armed forces shot

[33] John Hudson and Kostiantyn Khudov, "The War in Ukraine Is Spurring a Revolution in Drone Warfare Using AI," *Washington Post*, July 26, 2023, https://www.washingtonpost.com/world/2023/07/26/drones-ai-ukraine-war-innovation/.

[34] Jeffrey Edmonds and Samuel Bendett*, Russian Military Autonomy in a Ukraine Conflict*, Center for Naval Analyses, Feb. 2022, https://www.cna.org/archive/CNA_Files/pdf/russian-military-autonomy-in-a-ukraine-conflict.pdf.

[35] David L. Stern, "Russia Attacks Kyiv Overnight with Swarm of Self-Denotating Drones," *Washington Post*, Dec. 19, 2022, https://www.washingtonpost.com/world/2022/12/19/kyiv-drones-attack-belarus-putin/.

[36] Susie Blainn and Elise Morton, "Russia Launched 'Largest Drone Attack' on Ukrainian Capital Before Kyiv Day; 1 Killed," Associated Press, May 28, 2023, https://apnews.com/article/ukraine-kyiv-drone-attack-shahed-russia-war-57a856f99e8ec9760b78a2b0669b7383.

[37] Zachary Kallenborn, "Russia May Have Used a Killer Robot in Ukraine. Now What?," *Bulletin of the Atomic Scientists*, Mar. 15, 2022, https://thebulletin.org/2022/03/russia-may-have-used-a-killer-robot-in-ukraine-now-what/; Gregory C. Allen, *Russia Probably Has Not Used AI-Enabled Weapons in Ukraine, but That Could Change*, Center for Strategic and International Studies, May 26, 2022, https://www.csis.org/analysis/russia-probably-has-not-used-ai-enabled-weapons-ukraine-could-change.

[38] Will Knight, "Russia's Killer Drone in Ukraine Raises Fears About AI in Warfare," *Wired*, Mar. 17, 2022, https://www.wired.com/story/ai-drones-russia-ukraine/.

down a Lancet system in the Mykolaiv region.[39] More recently, the Lancet drones were also reportedly being used extensively to counter Ukraine's counteroffensive throughout the summer of 2023.[40] Previously, the Lancet was used in Syria in 2021 by Russian special operations forces, and according to the system's manufacturer, Zala-Aero Group, the system is able to autonomously locate and strike targets in designated areas—although, once again, it is not possible to determine whether it has been employed in such a mode in Ukraine.

AI for battlefield information processing

Advances in AI technology, such as high-fidelity sensing, machine learning, computer vision, and natural learning processing, allow systems to collect, collate, and analyze complex data at unprecedented speed and volume. AI-enabled speed and greater accuracy in information processing can enhance situational awareness and help leaders at all command levels make better decisions. Moreover, that AI applications for information processing can free up personnel for other tasks is of immediate value for both Ukrainian and Russian forces, as both have struggled with manpower shortages throughout the conflict.

In December 2022, the *Washington Post* reported that Ukrainian forces and NATO advisors outside of the country are using a Palantir tool called MetaConstellation that aggregates data from commercial satellites to create a digital model of the battlefield that can help commanders see through the "fog of war."[41] The larger, more sophisticated system located outside of Ukraine uses AI to analyze sensor data to identify enemy positions, estimate which weapons will be most effective against them, and after each strike, conduct battle damage assessments that are then fed back into the digital network to improve the reliability and accuracy of predictive models. NATO advisors can provide this intelligence to Ukrainian commanders on the ground to guide military missions. In February 2023, Palantir's CEO said that the company was "responsible for most of the targeting in Ukraine."[42] Although such statements are difficult

[39] "Russia's Lancet Loitering Munition Downed by Ukraine's Small Arms Fire," Defense Express, July 27, 2022, https://en.defence-ua.com/weapon_and_tech/russias_lancet_loitering_munition_downed_by_ukraines_small_arms_fire-3691.html; "Russia Hammers Ukrainian Military with Game-Changing Kamikaze Drones in Zaporozhnye Region," Tass, July 18, 2022, https://tass.com/politics/1481379.

[40] Reuters, "Lancet: The Russian Kamikaze Drone Blunting Ukraine's Counteroffensive," RFE/RL, July 8, 2023, https://www.rferl.org/a/lancet-drones-russia-invasion-counteroffensive-kamikaze/32493513.html.

[41] David Ignatius, "How the Algorithm Tipped the Balance in Ukraine," *Washington Post*, Dec. 19, 2022, https://www.washingtonpost.com/opinions/2022/12/19/palantir-algorithm-data-ukraine-war/.

[42] Jeffrey Dastin, "Ukraine Is Using Palantir's Software for 'Targeting,' CEO Says," Reuters, Feb. 1, 2023, https://www.reuters.com/technology/ukraine-is-using-palantirs-software-targeting-ceo-says-2023-02-02/.

to verify, it does illustrate that using AI to analyze and fuse data from different types of sources directly enhances precision, speed, and lethality.

The Ukrainian forces have also proved particularly resourceful in gaining access to commercial, off-the-shelf technologies and adapting them for military use. According to news reports, Primer, a US-based company, has supplied Ukraine with machine learning solutions for parsing out and exploiting intelligence information. Though reluctant to disclose details, the company's representative explained that AI algorithms were being used to capture, transcribe, translate, and analyze intercepted Russian military communications transmitted on unsecured or nonencrypted channels.[43] The use of natural language processing technology to analyze military communications exemplifies not only the dual use nature of AI but also the relative ease within which some commercial applications can be used for military purposes—in this case, taking off-the-shelf code and application programming interfaces that can transcribe and translate speech, remove background noise, and other tasks and retraining the machine learning models to better recognize military vocabularies, including colloquial terms for military vehicles and weapons.[44]

Additionally, at least three Ukrainian government agencies said they have used facial recognition technology provided by Clearview AI to identify dead Russian soldiers and prisoners of war, or to verify the identity of travelers across the country amid fears of spies and saboteurs.[45] Since the early days of the Russian invasion, the Ukrainian government has sought to identify dead Russian soldiers and notify their families as part of a broader effort to influence Russian public opinion about the realities and costs of this war. That said, it is hard to say if Clearview's tool can be effective for such a task—facial recognition technology in general has problems with accuracy, and battlefield casualties are particularly difficult to characterize using such technology given the extent and severity of wartime injuries.

AI, cyber, and information warfare

Russian cyber threat activity in the context of the war in Ukraine has focused predominantly on Ukrainian targets—seeking to degrade, disrupt, and destroy Ukraine's military, government, and economic functions; attack critical civilian infrastructure, supply chains, and

[43] Will Knight, "As Russia Plots Its Next Move, an AI Listens to the Chatter," *Wired*, Apr. 4, 2022, https://www.wired.com/story/russia-ukraine-war-ai-surveillance/; Jonathan Guyer, "The West Is Testing Out a Lot of Shiny New Military Tech in Ukraine," Vox, Sept. 21, 2022, https://www.vox.com/2022/9/21/23356800/us-testing-tech-ukraine-russia-war.

[44] Knight, "As Russia Plots Its Next Move, an AI Listens to the Chatter."

[45] Kashmir Hill, "Facial Recognition Goes to War," *New York Times*, Apr. 7, 2022, https://www.nytimes.com/2022/04/07/technology/facial-recognition-ukraine-clearview.html.

logistics hubs; and limit the Ukrainian public's access to information.[46] In a June 2022 report, Microsoft disclosed that it detected "Russian network intrusion efforts on 128 organizations in 42 countries outside Ukraine," including the United States, Poland, the Baltic countries, Denmark, Norway, Finland, Sweden, and Turkey.[47] The extent to which Russia's cyber agencies and affiliated nonstate actors are integrating AI into their operations is not well known. It is however notable that, according to Microsoft, recent advances in cyber threat intelligence, "including the use of artificial intelligence, have made it possible to detect these attacks more effectively," thereby helping Ukraine withstand a high percentage of destructive Russian cyberattacks.[48]

Russian propaganda and influence operations have targeted several audiences: promulgating messages in support of the "special operation" to Russian citizens; attempting to discredit the Ukrainian leadership and undermine morale among the Ukrainian public; and spreading manipulated or false anti-NATO and anti-Ukrainian messages to foreign audiences in the United States, Europe, and around the world. Russian information operations have made use of AI in several reported incidents. During the first days of the war, Facebook took down a small network run by people in Russia and Ukraine (likely the Donbas region) for violating the company's policy against coordinated inauthentic behavior. This network operated fake websites posing as independent news entities, publishing claims that amplified Russian propaganda and misinformation about the West betraying Ukraine and Ukraine being a failed state. They also created fictitious personas, purportedly Kyiv residents, that were active across different social media platforms, including Facebook, Instagram, Twitter, YouTube, Telegram, and the Russian platforms Odnoklassniki and VK. The accounts linked to these fictitious personas used profile pictures that were likely generated using AI techniques such as generative adversarial networks (GAN). The Facebook investigation found links between this network and another operation they removed in April 2020 which traced back to individuals in Russia and the Donbas region, as well as two media organizations in Crimea, NewsFront and SouthFront, that have since been sanctioned by the US government.[49] In another March 2022 incident, an AI-generated deepfake video of President Zelensky stating that Ukraine would

[46] "Cyber Threat Bulletin: Cyber Threat Activity Related to the Russian Invasion of Ukraine," Canadian Centre for Cyber Security, July 14, 2022, https://cyber.gc.ca/sites/default/files/cyber-threat-activity-associated-russian-invasion-ukraine-e.pdf.

[47] "Defending Ukraine: Early Lessons from the Cyber War," Microsoft, June 22, 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK.

[48] "Defending Ukraine: Early Lessons from the Cyber War."

[49] Nathaniel Gleicher and David Agranovich, "Updates on Our Security Work in Ukraine," Meta, Feb. 27, 2022, https://about.fb.com/news/2022/02/security-updates-ukraine/.

surrender to Russia was uploaded on a hacked Ukrainian news website, but it was quickly debunked.[50]

The Effect of AI and Autonomous Technologies on Strategic Stability and Conflict Dynamics

Assessing the effect of AI and autonomous technologies on the trajectory and dynamics of Russia's war in Ukraine or strategic stability more broadly is not a straightforward task. Nearly all publicly available information about the deployment of AI capabilities and technologies is incomplete. Media reports or statements from public officials rarely provide sufficient technical details to decipher the specific capabilities or functions of a given system. Accounts of how a particular technology has been used are also quite general, missing important details about location, time, conditions, effectiveness, and influence due to concerns about operational security, safety of sources, and sharing classified data. Statements from public officials or company representatives about the capabilities and uses of various AI and autonomous systems are rarely independently verified and may be overstating, minimizing, or neglecting crucial information for a variety of political, commercial, security, or other reasons. Furthermore, at this stage, it is nearly impossible to assess the effect of AI and autonomous technologies on conflict dynamics or strategic stability independently from other factors, including other weapons and military systems or other forms of foreign technological and intelligence assistance provided to Ukraine. With these limitations in mind, this section considers how the use of AI and autonomous technologies in the war in Ukraine may have affected the risks of escalation from conventional war to the use of nuclear weapons and conflict spreading to include other parties.

Risk of escalation from conventional war to nuclear conflict

Since the beginning of Russia's war in Ukraine, Putin has repeatedly threatened to use nuclear weapons. US officials remain concerned that Putin could reach for Russia's arsenal of nonstrategic nuclear weapons if he is losing power, if the Kremlin believes NATO is about to directly enter the war, or if Russia's conventional military collapses, for example, because

[50] Alden Wahlstrom, Alice Revelli, Sam Riddell, David Mainor, and Ryan Serabian, "The IO Offensive: Information Operations Surrounding the Russian Invasion of Ukraine," Mandiant, May 19, 2022, https://www.mandiant.com/resources/blog/information-operations-surrounding-ukraine.

Ukraine's victory grows inevitably.[51] The threat of nuclear escalation is a particularly dangerous element of Russia's war in Ukraine. However, the use of AI and autonomous technologies does not appear to have much of an effect on these dynamics, at least not in any of the ways offered by the literature on the topic, as previously outlined in this paper.

The possibility of nuclear escalation continues to influence decisions about what type of advanced weaponry should be provided to Ukraine.[52] This is particularly true in regard to NATO's or more specifically Washington's reluctance to supply Ukraine with long-range missiles that can hit targets inside Russia. Yet, this strategy of restraint has not constrained the provision of AI-enabled intelligence and battle management software that is helping the Ukrainians target Russian military forces and equipment. Now, if Ukraine defeats Russia on the battlefield and the Russian conventional military disintegrates, there is little doubt that Western military aid would have played a vital role in that outcome. It would, however, be difficult to conclusively claim that it was Western aid specifically in the form of AI that allowed the Ukrainians to defeat the Russian military (or even that this defeat led to the Russian military's collapse). As it stands, only a tenuous connection exists between the wartime use of AI and the risk of escalation from conventional war to the use of nuclear weapons.

Risk of conflict escalation and/or conflict spreading to other countries

As previously discussed, scholars have offered a wide range of arguments about the potential effect of AI and autonomous technologies on conflict dynamics, including analysis on the destabilizing effects of AI-enabled cyber operations and disinformation campaigns. Currently, there is not enough information to assess the validity of these hypotheses primarily because it is not publicly known whether and to what extent Russia's cyber agencies and affiliated nonstate actors are integrating AI into their operations. That said, the evidence surfaced by Microsoft indicates that AI has played a more prominent role in buttressing cyber defenses and making it possible to detect Russia's destructive cyberattacks more effectively. How this AI-enabled defensive advantage may affect cyber conflict and the risk of escalation into a military

[51] Julian E. Barnes and David E. Sanger, "Fears of Russian Nuclear Weapons Use Have Diminished, but Could Reemerge," *New York Times*, Feb. 3, 2023, https://www.nytimes.com/2023/02/03/us/politics/russia-nuclear-weapons.html; Julian E. Barnes and David E. Sanger, "C.I.A. Director Airs Concern That Putin Might Turn to Nuclear Weapons," *New York Times*, Apr. 14, 2022, https://www.nytimes.com/2022/04/14/us/politics/putin-nuclear-weapons.html.

[52] Janice Gross Stein, "Escalation Management in Ukraine: 'Learning by Doing' in Response to the 'Threat That Leaves Something to Chance,'" *Texas National Security Review* 6, no. 3 (2023), https://tnsr.org/2023/06/escalation-management-in-ukraine-learning-by-doing-in-response-to-the-threat-that-leaves-something-to-chance/#_ftnref7.

confrontation or the spread of conflict to other countries is certainly a question that merits further attention.

Although the majority of Russia's cyber activity since the onset of the war has focused on Ukrainian targets, Russian intelligence agencies have also targeted government computer networks and other institutions in other countries, including several NATO members. As such, it is worth considering the risk that cyberattacks (that do not rely on AI or autonomous capabilities) could lead to conflict escalation, for instance, by drawing other parties into the Russo-Ukrainian war. For example, some observers have suggested that Moscow could respond to increased Western sanctions or severe setbacks on the battlefield with intensified cyberattacks that would in turn be met with a direct military response.[53] Alternatively, nonstate affiliated hackers or state-linked cyber proxies could take action not authorized by any proper authority, target, or unintentionally harm highly sensitive systems, such as those related to critical infrastructure, conventional military systems, and even nuclear command and control processes.[54]

Thus far, Russian cyberattacks outside of Ukraine have not led to the use of lethal force which fits the fact that scholars have come to view cyber conflicts as having the characteristics of an intelligence, rather than a military contest.[55] Interestingly, some observers have posited that Moscow seems more concerned about the possibility of unintended escalation or widespread international effects triggered by cyberattacks. And with the stakes being much higher in Ukraine, including the possibility of a direct conflict with NATO, it is possible that "the Kremlin may simply not trust its cyber agencies to achieve carefully calibrated effects within a strategy of deterrence and escalation."[56]

With respect to the destabilizing effects of AI-enabled disinformation campaigns and the risk of escalation, one concern is that Russia's malign information operations will stir domestic unrest in European countries that have sizable Russian populations and have also taken in large numbers of Ukrainian refugees. Generally, it would be difficult to judge the independent effect of AI-enabled disinformation operations from those that rely on human labor to generate

[53] Jason Healey, "Preventing Cyber Escalation in Ukraine and After," War on the Rocks, Mar. 9, 2022, https://warontherocks.com/2022/03/preventing-cyber-escalation-in-ukraine-and-after/.

[54] Andrew A. Szarejko and John Arquilla, "Accidents and Escalation in a Cyber Age," War on the Rocks, Dec. 22, 2021, https://warontherocks.com/2021/12/accidents-and-escalation-in-a-cyber-age/.

[55] Joshua Rovner, "Cyber War as an Intelligence Contest," War on the Rocks, Sept. 16, 2019, https://warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest/.

[56] Jon Bateman, Nick Beecroft, and Gavin Wilde, "What the Russian Invasion Reveals About the Future of Cyber Warfare," Carnegie Endowment for International Peace, Dec. 19, 2022, https://carnegieendowment.org/2022/12/19/what-russian-invasion-reveals-about-future-of-cyber-warfare-pub-88667.

and spread manipulated or false narratives. That said, the use of AI-enabled disinformation tools in the war in Ukraine has been limited, at least according to open-source reports. And even in the few publicly reported cases where AI has been deployed, for example in generating fake personas on social media or powering deepfakes, the campaign was countered and quickly debunked. Therefore, it does not appear that Russian actors have effectively used AI to hyperpower their information warfare, which in turn may have caused unrest in other countries and escalated the wider conflict. Still, Russian information operations tactics continue to evolve, with reports suggesting Russian hackers are discussing how to use the newly released AI-enabled ChatGPT to scale malicious activity.[57]

The war in Ukraine also provides early insights into discussions about escalation due to accidents, misuse, and failure of AI-enabled military weapons and systems. For instance, a particularly tense incident unfolded on November 16, 2022 when a deadly blast in Poland killed two people, heightening concerns about escalation and the conflict spreading to include other countries. Shortly after the incident, statements from NATO Secretary General Jens Stoltenberg and Polish sources explained that the explosion was an accident caused by Ukrainian air defenses responding to a Russian missile barrage rather than an intentional attack by Russia on NATO ally territory.[58]

Specific details about the incident where the errant Ukrainian defensive missile hit Poland, including the extent of autonomy embedded in the system or the cause of the misfire, are not publicly available. That said, automated and autonomous features have been integrated into the critical functions of most air defense systems in order to counter and neutralize incoming threats at a speed that humans cannot manage.[59] In the past, there have been several cases where air defense systems with automated and autonomous features brought down civilian aircraft—such as the Malaysian Airlines MH17 flight that was shot down by a Russian Buk system over Eastern Ukraine in July 2014—or hit friendly military aircraft—as was the case with the Patriot air defense system during the 2003 Iraq war. When such systems fail, it raises important questions about meaningful human control of increasingly autonomous systems, the challenge of attributing responsibility for accidental launch, and the risk of inadvertent escalation due to accidents or malfunctions. In this latest incident, the friendly relations

[57] "ChatGPT Helps Hackers Write Malicious Codes to Steal Your Personal Data," *Business Insider*, Jan. 15, 2023, https://www.businessinsider.in/tech/news/chatgpt-helps-hackers-write-malicious-codes-to-steal-your-personal-data/articleshow/97000603.cms.

[58] "Poland and NATO Say Ukrainian Air Defense Likely Caused Deadly Blast," NBC News, Nov. 16, 2022, https://www.nbcnews.com/news/world/live-blog/russia-ukraine-war-live-updates-poland-missile-putin-nato-rcna57416.

[59] Ingvild Bode and Tom Watts, *Meaningless Human Control: Lessons from Air Defence Systems on Meaningful Human Control for the Debate on AWS*, Center for War Studies, University of Southern Denmark, Feb. 2021, https://dronewars.net/wp-content/uploads/2021/02/DW-Control-WEB.pdf.

between Ukraine and Poland and shared understanding that Russia was ultimately at fault for the broader situation helped avert escalation. In future scenarios, however, there is no guarantee diplomacy will prevail, especially between countries hostile to one another or where there are no crisis communications channels in place.

US-Russia Relations and Strategic Stability in the Context of AI and Autonomous Technologies

Beyond the current war in Ukraine, how might the integration of AI and autonomous technologies into military systems and missions affect strategic stability between the United States and Russia? Although trust between the two countries is at a nadir, Washington and Moscow still have a shared interest in preventing accidental war and minimizing the risk of escalation or conflict triggered by AI accidents or unexpected interactions between adversarial autonomous systems.

Currently, there is little appetite for a blanket ban on military uses of AI. Discussions focused on lethal autonomous weapons systems (LAWS) in the Group of Governmental Experts on LAWS at the United Nations have yielded little progress toward a legally binding instrument or any other type of a document to help regulate the development and use of these technologies. In this context, scholars and policymakers have increasingly looked toward confidence building measures (CBMs), a broad set of actions that states can take to increase transparency, enhance clarity about intentions, avoid misunderstandings, and reduce risks linked to military AI.[60]

Several CBMs are applicable to military AI and pertinent to the US-Russia case. Perhaps the most effective approach is to constrain the use of AI in domains of exceptional and possibly catastrophic risk, such as nuclear operations.[61] Some scholars have suggested that the United States, for instance, could propose a multilateral commitment to nuclear command and control systems always including a human in the loop as well as committing to not placing nuclear weapons on uncrewed platforms where a human will not be present to correct errors or

[60] Michael Horowitz and Paul Scharre, *AI and International Stability: Risks and Confidence Building Measures*, Center for a New American Security, Jan. 12, 2021, https://www.cnas.org/publications/reports/ai-and-international-stability-risks-and-confidence-building-measures.

[61] Ioana Puscas, *Confidence Building Measures for Artificial Intelligence: A Framing Paper*, UNIDIR, 2022, https://unidir.org/sites/default/files/2022-12/Confidence-Building_Final.pdf.

override a system in case something went wrong.[62] Nuclear-armed states, including China and Russia, already have nuclear command and control practices that include humans working alongside automated decision aids to launch nuclear weapons, and there is a general consensus that humans should retain control over decisions to use nuclear weapons. It may be possible to raise this issue in future strategic stability dialogues with Russia (when such engagements recommence). Even if Russia refuses to participate in this CBM, the United States can solidify its position as a global leader in AI safety without undermining US nuclear deterrence by advancing such a measure and collaborating with other nuclear-armed states to promote a broader multilateral proposal on AI and nuclear weapons.

As US and Russian militaries incorporate more autonomous functionalities into uncrewed systems deployed in contested regions such as the Black Sea or in NATO countries closest to Russian borders, accidents, malfunctions, and complicated interactions between these systems can further inflame tensions. Information sharing and notification procedures put in place to reduce uncertainty around deployments of autonomous and AI-enabled systems can help minimize or manage the risk of inadvertent escalation. Drawing on the 1972 US-Soviet Incidents at Sea Agreement that created a mechanism for communication and information sharing about the movement of US and Soviet naval vessels, some scholars have suggested creating an international Autonomous Incidents Agreement focused on military applications of autonomous systems. Such an agreement could establish broad rules for acceptable behavior when deploying AI-enabled and autonomous systems, especially in the air and maritime domains, and potentially include a channel for military-to-military communication to respond to incidents in real time.[63]

The success of CBMs such as the Autonomous Incident Agreement would of course depend on states' participation and compliance. Moreover, as the historical record of US-Soviet or US-China relations shows, incidents and skirmishes continue to occur despite the presence of numerous CBMs and other more formal agreements for deconfliction of military forces. Yet, it is precisely in times of heightened tensions that mechanisms for diluting uncertainty and preventing surprise are most needed to help differentiate between normal and unusual behavior. Such mechanisms are particularly necessary at this early stage of military AI development where there is still a great deal that we are unsure about regarding the real-world

[62] Michael C. Horowitz and Lauren Kahn, "Leading in Artificial Intelligence Through Confidence Building Measures," *Washington Quarterly* 44, no. 4 (2021), pp. 91-106, 10.1080/0163660X.2021.2018794; Lauren Khan, "Mending the 'Broken Arrow:' Confidence Building Measures at the AI-Nuclear Nexus," War on the Rocks, Nov. 4, 2022, https://warontherocks.com/2022/11/mending-the-broken-arrow-confidence-building-measures-at-the-ai-nuclear-nexus/.

[63] Michael Horowitz and Paul Scharre, "AI and International Stability: Risks and Confidence Building Measures," Center for a New American Security, Jan. 12, 2021.

capabilities of AI-enabled and autonomous systems and how they may interact with or influence existing military systems, missions, and dynamics.[64]

There are other ways to promote information-sharing and communications, including through Track II academic-to-academic exchanges that can serve as building blocks for formal cooperation between countries in some future point. Discussions and exchanges of ideas between academic communities and technical experts from different countries can shed light on differences in approaches to AI development as well as surface areas of shared interests in AI safety. It may be difficult to imagine such programs gaining much traction amid Russia's brutal war in Ukraine and the intensifying techno-strategic competition between the US and China. Yet, exchanges of this nature also took place during the Cold War when relations between the United States and the Soviet Union were far from amiable; today, US-based scientists and researchers still collaborate extensively with their counterparts in China despite the heightened tensions between the two countries.

The above discussion has focused primarily on the actions that states can take to minimize the risk from military AI amid deep distrust and even open hostilities. The war in Ukraine, however, has highlighted the vital role that commercial technology companies play in modern war, urging us to closely consider their growing effect on conflict dynamics, deterrence, and strategic stability. Companies such as SpaceX, Microsoft, Palantir, Planet, Capella Space, Maxar Technologies, and many others have provided data, equipment, technological capabilities, and other resources to the Ukrainian government, armed forces, and civilians, as well as to US and NATO allies working to help Ukraine win.[65] In this case, it appears that moral imperatives, business calculations, and geopolitical positions of commercial companies, most of them US-based or located in the West, are aligned with US national security priorities and strategic interests in supporting Ukraine. In future conflicts, however, these preferences could diverge or even come to a head. Meanwhile, the working relationships between the government and industry partners in competitor or adversary countries will also have a bearing on how future crises or conflicts may unfold.

With private technology companies at the forefront of AI innovation and commercial off-the-shelf technologies increasingly used on the battlefield, now is the time to ensure these actors are also involved in international efforts to articulate policy on military autonomy and AI or implement confidence building measures to reduce the risk of accidental or unintended escalation. Finally, although certain types of exchanges between the United States and Russia may not be politically feasible at this point, continuing to invest in ways to reduce uncertainty

[64] Horowitz and Kahn, "Leading in Artificial Intelligence Through Confidence Building Measures."

[65] Christine Fox and Emelia S. Probasco, "Big Tech Goes to War: To Help Ukraine, Washington, and Silicon Valley Must Work Together," *Foreign Affairs*, Oct. 19, 2022, https://www.foreignaffairs.com/ukraine/big-tech-goes-war.

and avoid misunderstandings around the use of military autonomy and AI will be critical for solidifying strategic stability and reducing the risk of catastrophic escalation.

References

Allen, Gregory C. *Russia Probably Has Not Used AI-Enabled Weapons in Ukraine, but That Could Change*. Center for Strategic and International Studies. May 26, 2022. https://www.csis.org/analysis/russia-probably-has-not-used-ai-enabled-weapons-ukraine-could-change.

Bajak, Frank, and Hanna Arhirova. "Drone Advances in Ukraine Could Bring Dawn of Killer Robots." *Los Angeles Times*. Jan. 3, 2023. https://www.latimes.com/world-nation/story/2023-01-03/drone-advances-in-ukraine-dawn-of-killer-robots.

Barnes, Julian E., and David E. Sanger. "C.I.A. Director Airs Concern That Putin Might Turn to Nuclear Weapons." *New York Times*. Apr. 14, 2022. https://www.nytimes.com/2022/04/14/us/politics/putin-nuclear-weapons.html.

———. "Fears of Russian Nuclear Weapons Use Have Diminished, but Could Reemerge." *New York Times*. Feb. 3, 2023. https://www.nytimes.com/2023/02/03/us/politics/russia-nuclear-weapons.html.

Bateman, Jon, Nick Beecroft, and Gavin Wilde. "What the Russian Invasion Reveals About the Future of Cyber Warfare." Carnegie Endowment for International Peace. Dec. 19, 2022. https://carnegieendowment.org/2022/12/19/what-russian-invasion-reveals-about-future-of-cyber-warfare-pub-88667.

Bendett, Samuel. "Drones Over Ukraine." *In Depth*. Apr. 25. https://www.cna.org/our-media/indepth/2022/04/drones-over-ukraine.

———. "Roles and Implications of AI in the Russian-Ukrainian Conflict." *Russia Matters*. July 20, 2023. https://www.russiamatters.org/analysis/roles-and-implications-ai-russian-ukrainian-conflict.

Bendett, Samuel, and Jeffrey Edmonds. *Russian Military Autonomy in Ukraine: Four Months In*. Center for Naval Analyses. July 2022. https://www.cna.org/reports/2022/07/Russian-Military-Autonomy-in-Ukraine-Four-Months-In.pdf.

Blainn, Susie, and Elise Morton. "Russia Launched 'Largest Drone Attack' on Ukrainian Capital Before Kyiv Day; 1 Killed." Associated Press. May 28, 2023. https://apnews.com/article/ukraine-kyiv-drone-attack-shahed-russia-war-57a856f99e8ec9760b78a2b0669b7383.

Bode, Ingvild, and Tom Watts. *Meaningless Human Control: Lessons from Air Defence Systems on Meaningful Human Control for the Debate on AWS*. Center for War Studies, University of Southern Denmark. Feb. 2021. https://dronewars.net/wp-content/uploads/2021/02/DW-Control-WEB.pdf.

Buchanan, Ben, John Bansemer, Dakota Cary, Jack Lucas, and Micah Musser. *Automating Cyber Attacks*. Center for Security and Emerging Technology. Nov. 2020. https://cset.georgetown.edu/publication/automating-cyber-attacks.

Buchanan, Ben, Andrew Lohn, Micah Musser, and Katerina Sedova. *Truth, Lies, and Automation: How Language Models Could Change Disinformation*. Center for Security and Emerging Technology. May 2021. https://cset.georgetown.edu/publication/truth-lies-and-automation/.

Byman, Daniel L., Chongyang Gao, Chris Meserole, and V.S. Subrahmanian. *Deepfakes and International Conflict*. Brookings. Jan. 2023. https://www.brookings.edu/wp-content/uploads/2023/01/FP_20230105_deepfakes_international_conflict.pdf.

Carbonaro, Giulia. "How Switchblade Drones Could Turn the Tide of Ukraine War." *Newsweek*. Mar. 17, 2022. https://www.newsweek.com/switchblade-drones-ukraine-war-russia-1688906.

"ChatGPT Helps Hackers Write Malicious Codes to Steal Your Personal Data." *Business Insider*. Jan. 15, 2023. https://www.businessinsider.in/tech/news/chatgpt-helps-hackers-write-malicious-codes-to-steal-your-personal-data/articleshow/97000603.cms.

"Cyber Threat Bulletin: Cyber Threat Activity Related to the Russian Invasion of Ukraine." Canadian Centre for Cyber Security. July 14, 2022. https://cyber.gc.ca/sites/default/files/cyber-threat-activity-associated-russian-invasion-ukraine-e.pdf.

Dastin, Jeffrey. "Ukraine Is Using Palantir's Software for 'Targeting,' CEO Says." Reuters. Feb. 1, 2023. https://www.reuters.com/technology/ukraine-is-using-palantirs-software-targeting-ceo-says-2023-02-02/.

"Defending Ukraine: Early Lessons from the Cyber War." Microsoft. June 22, 2022. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK.

Edmonds, Jeffrey, and Samuel Bendett. *Russian Military Autonomy in a Ukraine Conflict*. Center for Naval Analyses. Feb. 2022. https://www.cna.org/archive/CNA_Files/pdf/russian-military-autonomy-in-a-ukraine-conflict.pdf.

Fox, Christine, and Emelia S. Probasco. "Big Tech Goes to War: To Help Ukraine, Washington, and Silicon Valley Must Work Together." *Foreign Affairs*. Oct. 19, 2022. https://www.foreignaffairs.com/ukraine/big-tech-goes-war.

Gates, Jonathan. "Is the SSBN Deterrent Vulnerable to Autonomous Drones?" *RUSI Journal* 161, no. 6 (2016): 28-35. https://www.tandfonline.com/doi/abs/10.1080/03071847.2016.1265834.

Gleicher, Nathaniel, and David Agranovich. "Updates on Our Security Work in Ukraine." Meta. Feb. 27, 2022. https://about.fb.com/news/2022/02/security-updates-ukraine/.

Goldstein, Josh, Renee DiResta, Girish Sastry, Micah Musser, Matthew Gentzel, and Katerina Sedova. *Generative Language Models and Automated Influence Operations: Emerging Threats and Potential Mitigations*. Stanford Internet Observatory, OpenAI, and Georgetown University's Center for Security and Emerging Technology. Jan. 11, 2023. https://cdn.openai.com/papers/forecasting-misuse.pdf.

Guyer, Jonathan. "The West Is Testing Out a Lot of Shiny New Military Tech in Ukraine." Vox. Sept. 21, 2022. https://www.vox.com/2022/9/21/23356800/us-testing-tech-ukraine-russia-war.

Hambling, David. "Will Ukraine Deploy Lethal Autonomous Drones Against Russia?" *New Scientist.* Nov. 1, 2022. https://www.newscientist.com/article/2344966-will-ukraine-deploy-lethal-autonomous-drones-against-russia/.

Healey, Jason. "Preventing Cyber Escalation in Ukraine and After." War on the Rocks. Mar. 9, 2022. https://warontherocks.com/2022/03/preventing-cyber-escalation-in-ukraine-and-after/.

Hill, Kashmir. "Facial Recognition Goes to War." *New York Times*. Apr. 7, 2022. https://www.nytimes.com/2022/04/07/technology/facial-recognition-ukraine-clearview.html.

Horowitz, Michael, Sarah E. Kreps, and Matthew Fuhrmann. "Separating Fact from Fiction in the Debate Over Drone Proliferation." *International Security* 41, no. 2 (2016): 7-42. https://www.belfercenter.org/sites/default/files/files/publication/isec_a_00257.pdf.

———. "Separating Fact from Fiction in the Debate Over Drone Proliferation." *International Security* 41, no. 2 (2016): 7-42.

Horowitz, Michael, and Paul Scharre. *AI and International Stability: Risks and Confidence Building Measures*. Center for a New American Security. Jan. 12, 2021. https://www.cnas.org/publications/reports/ai-and-international-stability-risks-and-confidence-building-measures.

———. "AI and International Stability: Risks and Confidence Building Measures." Center for a New American Security. Jan. 12, 2021.

Horowitz, Michael C. "When Speed Kills: Lethal Autonomous Weapon Systems, Deterrence, and Stability." *Journal of Strategic Studies* 42, no. 6 (2019): 764-788.

Horowitz, Michael C., and Lauren Kahn. "Leading in Artificial Intelligence Through Confidence Building Measures." *Washington Quarterly* 44, no. 4 (2021): 91-106. https://doi.org/10.1080/0163660X.2021.2018794.

Hudson, John, and Kostiantyn Khudov. “The War in Ukraine Is Spurring a Revolution in Drone Warfare Using AI.” *Washington Post*. July 26, 2023. https://www.washingtonpost.com/world/2023/07/26/drones-ai-ukraine-war-innovation/.

———. “The War in Ukraine Is Spurring a Revolution in Drone Warfare Using AI.” *Washington Post*. July 26, 2023. https://www.washingtonpost.com/world/2023/07/26/drones-ai-ukraine-war-innovation/.

Ignatius, David. “How the Algorithm Tipped the Balance in Ukraine.” *Washington Post*. Dec. 19, 2022. https://www.washingtonpost.com/opinions/2022/12/19/palantir-algorithm-data-ukraine-war/.

Johnson, James. “AI, Autonomy, and the Risk of Nuclear War.” War on the Rocks. July 29, 2022. https://warontherocks.com/2022/07/ai-autonomy-and-the-risk-of-nuclear-war/.

Kahn, Lauren. “How Ukraine Is Using Drones Against Russia.” Council on Foreign Relations. Mar. 2, 2022. https://www.cfr.org/in-brief/how-ukraine-using-drones-against-russia.

Kallenborn, Zachary. “Russia May Have Used a Killer Robot in Ukraine. Now What?” *Bulletin of the Atomic Scientists*. Mar. 15, 2022. https://thebulletin.org/2022/03/russia-may-have-used-a-killer-robot-in-ukraine-now-what/.

———. *Seven (Initial) Drone Warfare Lessons from Ukraine*. May 12, 2022. https://mwi.usma.edu/seven-initial-drone-warfare-lessons-from-ukraine/.

Khan, Lauren. “Mending the ‘Broken Arrow:’ Confidence Building Measures at the AI-Nuclear Nexus.” War on the Rocks. Nov. 4, 2022. https://warontherocks.com/2022/11/mending-the-broken-arrow-confidence-building-measures-at-the-ai-nuclear-nexus/.

Knight, Will. “As Russia Plots Its Next Move, an AI Listens to the Chatter.” *Wired*. Apr. 4, 2022. https://www.wired.com/story/russia-ukraine-war-ai-surveillance/.

———. “Russia’s Killer Drone in Ukraine Raises Fears About AI in Warfare.” *Wired*. Mar. 17, 2022. https://www.wired.com/story/ai-drones-russia-ukraine/.

Konaev, Margarita. “With AI, We’ll See Faster Fights, But Longer Wars.” War on the Rocks. Oct. 29, 2019. https://warontherocks.com/2019/10/with-ai-well-see-faster-fights-but-longer-wars/.

Konaev, Margarita, and Samuel Bendett. “Russian AI-Enabled Combat: Coming to a City Near You?” War on the Rocks. July 31, 2019. https://warontherocks.com/2019/07/russian-ai-enabled-combat-coming-to-a-city-near-you/.

Konaev, Margarita, Husanjot Chahal, Ryan Fedasiuk, Tina Huang, and Ilya Rahkovksy. *US Military Investments in Autonomy and AI: Costs, Benefits, and Strategic Effects*. Center for Security and Emerging Technology. Oct. 2020. https://cset.georgetown.edu/publication/u-s-military-investments-in-autonomy-and-ai-a-strategic-assessment/.

Lewis, Larry, and Andrew Ilachinski. *Leveraging AI to Mitigate Civilian Harm*. Center for Naval Analyses. Feb. 2022. https://apps.dtic.mil/sti/trecms/pdf/AD1181578.pdf.

Lieber, Keir, and Daryl Press. “The New Era of Counterforce: Technological Change and the Future of Nuclear Deterrence.” *International Security* 41, no. 4 (2017): 9-49.

Lin, Herbert. “Escalation Risks in an Artificial Intelligence—Infused World.” In *Artificial Intelligence, China, Russia, and the Global Order*. Edited by Nicholas D. Wright. Air University Press, 2019, 143-152. http://www.jstor.org/stable/resrep19585.25.

Margulies, Peter. “The Other Side of Autonomous Weapons: Using Artificial Intelligence to Enhance IHL Compliance.” In *Impact of Emerging Technologies on the Law of Armed Conflict*. Edited by Ronald T.P. Alcala and Eric Talbot Jensen. New York: Oxford Academic, 2019. https://doi.org/10.1093/oso/9780190915322.003.0006.

Mishra, Sylvia. “Could Unmanned Underwater Vehicles Undermine Nuclear Deterrence?” *Strategist*. May 8, 2019. https://www.aspistrategist.org.au/could-unmanned-underwater-vehicles-undermine-nuclear-deterrence/.

Morgan, Forrest E., Benjamin Boudreaux, Andrew J. Lohn, Mary Ashby, Christian Curriden, Kelly Klima, and Derek Grossman. *Military Applications of Artificial Intelligence: Ethical Concerns in an Uncertain World*. RAND. 2020.

https://www.rand.org/content/dam/rand/pubs/research_reports/RR3100/RR3139-1/RAND_RR3139-1.pdf.

Nurkin, Tate, and Margarita Konaev. *Eye to Eye in AI: Developing Artificial Intelligence for National Security and Defense*. Atlantic Council. 2022. https://www.atlanticcouncil.org/in-depth-research-reports/report/eye-to-eye-in-ai/#introduction.

Osborn, Kris. "Ukraine's Switchblade Drones Will Be Game Changers for Urban Combat." *National Interest*. Mar. 4, 2022. https://nationalinterest.org/blog/buzz/ukraine%E2%80%99s-switchblade-drones-will-be-game-changers-urban-combat-202220.

"Poland and NATO Say Ukrainian Air Defense Likely Caused Deadly Blast." NBC News. Nov. 16, 2022. https://www.nbcnews.com/news/world/live-blog/russia-ukraine-war-live-updates-poland-missile-putin-nato-rcna57416.

Polyakova, Alina. "Weapons of the Weak: Russia and AI-Driven Asymmetric Warfare." Brookings. Nov. 15, 2018. https://www.brookings.edu/research/weapons-of-the-weak-russia-and-ai-driven-asymmetric-warfare/.

Puscas, Ioana. *Confidence Building Measures for Artificial Intelligence: A Framing Paper*. UNIDIR. 2022. https://unidir.org/sites/default/files/2022-12/Confidence-Building_Final.pdf.

Reuters. "Lancet: The Russian Kamikaze Drone Blunting Ukraine's Counteroffensive." RFE/RL. July 8, 2023. https://www.rferl.org/a/lancet-drones-russia-invasion-counteroffensive-kamikaze/32493513.html.

Rovner, Joshua. "Cyber War as an Intelligence Contest." War on the Rocks. Sept. 16, 2019. https://warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest/.

"Russia Hammers Ukrainian Military with Game-Changing Kamikaze Drones in Zaporozhnye Region." Tass. July 18, 2022. https://tass.com/politics/1481379.

"Russia's Lancet Loitering Munition Downed by Ukraine's Small Arms Fire." Defense Express. July 27, 2022. https://en.defence-ua.com/weapon_and_tech/russias_lancet_loitering_munition_downed_by_ukraines_small_arms_fire-3691.html.

"Saker UAV." https://saker.airforce/.

Sedova, Katerina, Christine McNeill, Aurora Johnson, Aditi Joshi, and Ido Wulkan. *AI and the Future of Disinformation Campaigns*. Center for Security and Emerging Technology. Dec. 2021. https://cset.georgetown.edu/publication/ai-and-the-future-of-disinformation-campaigns/.

Stein, Janice Gross. "Escalation Management in Ukraine: 'Learning by Doing' in Response to the 'Threat That Leaves Something to Chance'." *Texas National Security Review* 6, no. 3 (2023). https://tnsr.org/2023/06/escalation-management-in-ukraine-learning-by-doing-in-response-to-the-threat-that-leaves-something-to-chance/#_ftnref7.

Stern, David L. "Russia Attacks Kyiv Overnight with Swarm of Self-Denotating Drones." *Washington Post*. Dec. 19, 2022. https://www.washingtonpost.com/world/2022/12/19/kyiv-drones-attack-belarus-putin/.

Szarejko, Andrew A., and John Arquilla. "Accidents and Escalation in a Cyber Age." War on the Rocks. Dec. 22, 2021. https://warontherocks.com/2021/12/accidents-and-escalation-in-a-cyber-age/.

Tousif, Elias. "Drone Warfare in Ukraine: Understanding the Landscape." Stimson. June 30, 2022. https://www.stimson.org/2022/drone-warfare-in-ukraine-understanding-the-landscape/.

Urbanska, Tatiana. "Lt. Col. Yuroslav Gonchar: Our Everyday Life Is Like This: A Respected General Graduated, Took a High Position, but Did Not Even Master Word on the Computer." Unian. Oct. 13, 2022. https://www.unian.ua/war/aerorozvidka-v-ukrajini-yak-pracyuyut-operatori-droniv-na-viyni-interv-yu-z-yaroslavom-goncharom-12010002.html.

Vincent Boulanin, ed. *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk*. SIPRI. 2019. https://www.sipri.org/sites/default/files/2019-05/sipri1905-ai-strategic-stability-nuclear-risk.pdf.

Vosoughi, Soroush, Deb Roy, and Sinan Aral. “The Spread of True and False News Online.” *Science*. Mar. 9, 2018. https://www.science.org/doi/10.1126/science.aap9559.

Vynck, Gerrit De, Pranshu Verma, and Jonathan Baran. “Exploding ‘Kamikaze’ Drones Are Ushering in a New Era of Warfare in Ukraine.” *Washington Post*. Mar. 4, 2022. https://www.washingtonpost.com/technology/2022/03/24/loitering-drone-ukraine/.

Wahlstrom, Alden, Alice Revelli, Sam Riddell, David Mainor, and Ryan Serabian. “The IO Offensive: Information Operations Surrounding the Russian Invasion of Ukraine.” Mandiant. May 19, 2022. https://www.mandiant.com/resources/blog/information-operations-surrounding-ukraine.

Watling, Jack, and Nick Reynolds. *Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine*. RUSI. May 19, 2023. https://static.rusi.org/403-SR-Russian-Tactics-web-final.pdf.

Wyrwal, Marcin. “War in Ukraine: How Artificial Intelligence Is Killing Russians.” Onet. July 13, 2022. https://www.onet.pl/informacje/onetwiadomosci/rozwiazali-problem-armii-ukrainy-ich-pomysl-okazal-sie-dla-rosjan-zabojczy/pkzrk0z,79cfc278.

Zabrodskyi, Mykhaylo, Jack Watling, Oleksandr V. Danylyuk, and Nick Reynolds. *Preliminary Lessons in Conventional Warfighting from Russia’s Invasion of Ukraine: February-July 2022*. RUSI. Nov. 30, 2022. https://static.rusi.org/359-SR-Ukraine-Preliminary-Lessons-Feb-July-2022-web-final.pdf.

Zenko, Michael. *Reforming US Drone Strike Policies*. Council on Foreign Relations. 2013. https://www.cfr.org/report/reforming-us-drone-strike-policies.

This page intentionally left blank.

This report was written by CNA's Strategy, Policy, Plans, and Programs Division (SP3).

SP3 provides strategic and political-military analysis informed by regional expertise to support operational and policy-level decision-makers across the Department of the Navy, the Office of the Secretary of Defense, the unified combatant commands, the intelligence community, and domestic agencies. The division leverages social science research methods, field research, regional expertise, primary language skills, Track 1.5 partnerships, and policy and operational experience to support senior decision-makers.

This report may contain hyperlinks to websites and servers maintained by third parties. CNA does not control, evaluate, endorse, or guarantee content found in those sites. We do not assume any responsibility or liability for the actions, products, services, and content of those sites or the parties that operate them.

IOP-2023-U-036583-Final

3003 Washington Boulevard, Arlington, VA 22201
www.cna.org 703-824-2000