Emerging and Disruptive Technologies Transform, but Do Not Lift, the Fog of War – Evidence from Russia's War on Ukraine

Author(s):
Kunertova, Dominika; Herzog, Stephen

Publication date:
2024

Permanent link:
https://doi.org/10.3929/ethz-b-000696795

Originally published in:
Publication series 2: Research reports 2024/33

14

EMERGING AND DISRUPTIVE TECHNOLOGIES TRANSFORM, BUT DO NOT LIFT, THE FOG OF WAR - EVIDENCE FROM RUSSIA'S WAR ON UKRAINE

Dominika Kunertova and Stephen Herzog

Abstract

In this working paper, we ask how have new technologies affected the Clausewitzian fog of war? We leverage examples from Russia's ongoing full-scale invasion of Ukraine to address this research question. The evidence includes both "high-tech" systems like nuclear-capable hypersonic weapons and "low-tech" systems like cheap commercially available drones and affordable open-source intelligence (OSINT) technology. In the case of the former, we find that Russian threats and propaganda created myths surrounding weapons with unclear military applications. Regarding the latter, media and pundit claims were sensational as these systems changed combat dynamics without delivering revolutionary effects. Both cases point to pronounced gaps between expectations about performance and battlefield realities. Emerging weapon technologies have therefore failed to provide clarity about the balance of forces and conditions on the ground—two pathways to reducing the fog of war. In land warfare, history has long shown that new technologies are rarely determinative of victory or defeat. Making claims to the contrary only contributes to the fog of war and necessitates new strategies to counter the hype surrounding exaggerated expectations about weapons.

Introduction

When we read the call for proposals for the Finnish National Defence University's 2024 Russia Seminar, we were immediately struck with a question. During Russia's war on Ukraine, have new emerging technologies helped the fog of war dissipate, or have they made it thicker? Focusing on Russia and emerging and disruptive technologies (EDTs) is essential for understanding today's strategic context.[1] Russian President Vladimir Putin did, after all, indicate in 2017 his country's ambition to rule the world through leading developments in artificial intelligence (AI).[2] Likewise, in 2018, Putin announced "new exotic weapons" that suggest advances in military applications

[1] Stephen Herzog and Dominika Kunertova: "NATO and Emerging Technologies– The Alliance's Shifting Approach to Military Innovation," *Naval War College Review* (2024). Forthcoming.
[2] Russia Today, "'Whoever Leads in AI Will Rule the World': Putin to Russian Children on Knowledge Day," Russia Today, September 1, 2017, https://www.rt.com/news/401731-ai-rule-world-putin.

of AI and the use of autonomous platforms.[3] Furthermore, the Kremlin's investments in nuclear-capable hypersonic missiles were meant to provide capabilities to strike at extreme speeds and overcome existing missile defenses.[4] Russia has indeed used several of these EDTs since the beginning of its full-scale invasion of Ukraine in February 2022. But despite Moscow's interest and investment in disruptive technologies, Russia has not won the war. It continues on, and even Kremlin battlefield successes come with mass casualties among Russian soldiers.

Ideas about new technologies that should theoretically make battlefield outcomes clearer do not just apply to the Russian side. Ukraine has spent considerable resources on whole-of-society efforts to produce small drones that have become ubiquitous in the conflict. This has triggered scores of media and analyst claims about new drone technologies and ways of warfare that revolutionize battlefields, have game-changing effects, and even fundamentally alter the nature of war.[5] However, Kyiv is also remarkably far away from achieving anything resembling meaningful victory in the conflict.

In this working paper, we adopt the Russia Seminar's Clausewitzian framework to explore the relationship between new emerging technologies and warfare. We are therefore inspired by Clausewitz's "fog of war" concept. After sorting through a bevy of evidence on the role of EDTs in the war, we argue that overestimating the role of new technologies widens the expectation gap between their performance and battlefield realities. While there is a hypothetical world in which EDTs could provide clarity of combat outcomes, we find that this is emphatically not the case in Ukraine. Instead, such gaps between performance expectations and battlefield realities contribute considerably to the thickening of the fog of war. Exaggerated claims about the revolutionary nature of certain weapon systems only serve to exacerbate the problem.

Curiously, today's debates about new weapon technologies resemble some of the narratives from the first Gulf War (1990–1991) that implied a lifting of the fog of war. Then, the emphasis was on the advent of advanced networked technology and precision-guided weapons used by the U.S. military. These so-called "game-changing" weapons were emblematic of a revolution in military affairs (RMA) and were thought to remove friction and uncertainty—core elements of Clausewitz's conception of war. The predominant scholarly response was agreement that no new technology alone can provide a decisive advantage in war.[6] Other voices did, however, make claims to

---

[3] Neil MacFarquhar and David E. Sanger: "Putin's 'Invincible' Missile Is Aimed at U.S. Vulnerabilities," *New York Times*, March 1, 2018, https://www.nytimes.com/2018/03/01/world/europe/russia-putin-speech.html.
[4] Justin Williamson and James J. Wirtz: "Hypersonic Or Just Hype? Assessing the Russian Hypersonic Weapons Program," *Comparative Strategy* 40, no. 5 (2021): 468–481.
[5] Yaroslav Trofimov: "Drones Everywhere: How the Technological Revolution on Ukraine Battlefields Is Reshaping Modern Warfare," *Wall Street Journal*, September 28, 2023, https://www.wsj.com/world/drones-everywhere-how-the-technological-revolution-on-ukraine-battlefields-is-reshaping-modern-warfare-bf5d531b; Kristen D. Thompson: "How the Drone War in Ukraine Is Transforming Conflict," Council on Foreign Relations, January 16, 2024, https://www.cfr.org/article/how-drone-war-ukraine-transforming-conflict; and Max Hunder: "Insight: Inside Ukraine's Scramble for 'Game-Changer' Drone Fleet," Reuters, March 24, 2023, https://www.reuters.com/world/europe/inside-ukraines-scramble-game-changer-drone-fleet-2023-03-24.

[6] See, e.g., Lawrence Freedman: *The Revolution in Strategic Affairs*, *Adelphi Papers*, no. 318 (Oxford: Oxford University Press for the International Institute for Strategic Studies, 1998): 70.

the contrary.[7] This latter camp's arguments may actually contribute to the fog of war. In land warfare, the key determinants of victory are the combination of skills and training, the quantity of armaments, and the enemy's permissive defenses.[8] Stated differently, technology alone will not allow Ukraine to make a breakthrough.[9]

Our working paper counters this strand of dangerous technological optimism that periodically returns in military history when new weapon systems gain popularity. Novel technology has rarely proven to be a solution to the uncertainties of war, and the ongoing war in Ukraine is no exception. We show this with evidence from the conflict, particularly regarding the role of four technology areas—drones, open-source intelligence (OSINT), AI, and hypersonics—in transforming the battlefields of Ukraine. In particular, EDTs have provided clarity about neither the balance of forces nor likely combat outcomes. Ultimately, we conclude with cautionary remarks on the continuing role of humans in war and lay out some of the risks entailed in the current fixations of techno-optimist thinking.

Clausewitz, War, and Technology

> *"War is the realm of uncertainty; three quarters of the factors on which action in war is based are wrapped in a fog of greater or lesser uncertainty. A sensitive and discriminating judgment is called for; a skilled intelligence to scent out the truth."*[10]

To Clausewitz, the nature of war is chaotic. War only abides by rules dictated by fog, friction, chance, and complexity. The well-known Clausewitzian metaphor of the "fog of war" describes the great amount of uncertainty experienced in military operations. Many different elements can contribute to such uncertainty. These include a lack of situational awareness on the battlefield, uncertainty about one's own capabilities, limited information about the adversary's capabilities, and minimal transparency about the enemy's intent. The resultant sorts of misunderstandings between adversaries have inspired seminal works by scholars theorizing about the causes of war and the sometimes surprising inability of states to cooperate.[11]

The role of technology is to reduce this friction and uncertainty by enhancing a state's military power. This can occur through improved weapon systems, logistics, and intelligence. According to Clausewitz, technology is a tool for warfare, not a panacea for the many issues that arise in military campaigns. Technology is employed in Clausewitzian warfare to attack enemies physically and psychologically, as well as to

---

[7] Bill Owens: *Lifting the Fog of War*, Baltimore, Johns Hopkins University Press, 2001.
[8] Stephen Biddle: *Military Power: Explaining Victory and Defeat in Modern Battle* (Princeton NJ: Princeton University Press, 2004).
[9] Stephen Biddle: "How Russia Stopped Ukraine's Momentum: A Deep Defense is Hard to Beat," *Foreign Affairs*, January 29, 2024, https://www.foreignaffairs.com/ukraine/how-russia-stopped-ukraines-momentum.
[10] Carl von Clausewitz: *On War*, ed. and trans. Michael Howard and Peter Paret, (Princeton NJ: Princeton University Press, 1976 [1832]): 101.
[11] Robert Jervis: "Cooperation Under the Security Dilemma," World Politics 30, no. 2 (1978): 167–214; and James D. Fearon: "Rationalist Explanations for War," *International Organization* 49, no. 3 (1995): 379–414.

exploit an adversary's vulnerability and bend the will of its people.[12] It exists within the confines of war rather than defining war.

We postulate that there are two ways that novel EDTs can reduce battlefield uncertainties and contribute to lifting the fog of war. First, in terms of military effects, new technology can improve mission effectiveness and the ability of forces to achieve their objectives. The aggregation of one state's military power with new weapons should therefore change the balance of forces, in turn improving predictions of victory or defeat. New advanced weapon systems could do this by enabling combatants to apply force with greater lethality, accuracy, speed, and/or range. Second, in terms of transparency of/on the battlefield, new technologies can enhance situational awareness. This means that technology can improve access to information both qualitatively and quantitatively. Technology not only accelerates data collection, but it also quickens its processing and dissemination. Today's battlefield commanders can base their decisions off of real-time intelligence, a situation that was rarely possible in Clausewitz's time.

We seek to understand if EDTs can help to lift the fog of war along these two dimensions. To do so, it is important to deploy "a skilled intelligence to scent out the truth" about the capabilities of new weapon technologies and the risks and benefits associated with their integration onto the battlefield. The subsequent sections of this working paper shift to assessing four technology areas frequently claimed to be revolutionizing warfare in Ukraine. They include both "high-tech" systems like nuclear-capable hypersonic weapons and "low-tech" systems like cheap commercially available drones and private sector NewSpace satellites. Furthermore, the case of military AI covers both targeting and decision-making processes. The variation in systems covered by our analysis enables us to reach some preliminary conclusions about emerging technologies and their implications for the fog of war in Ukraine.

Drones

Drones, or uncrewed aerial vehicles, are hardly a new technology. Over the past two decades, drones were primarily seen in the context of the Global War on Terror. That is, military drones were usually advanced large airborne platforms that ensured persistent surveillance and enabled states to carry out precision strikes. Medium-altitude, long endurance drones were a key component of remote warfare, allowing risk-averse political leaders to combat terrorism but avoid sending "boots on the ground."

There is a stark contrast, however, between drone war in Ukraine and drone war in past decades: In Ukraine, drones have boots.[13] What we mean by this is that small drones in Ukraine are not taking troops away from the battlefield. Rather, they are changing the dynamics on the battlefield from lower airspace. There has been an unprecedented proliferation of small-sized drones by both sides in the war, leading to

---

[12] Colin S. Gray: *Weapons Don't Make War: Policy, Strategy, and Military Technology* (Lawrence, Kans.: University Press of Kansas, 1993): 7. See also: Kier A. Lieber: *War and the Engineers: The Primacy of Politics over Technology* (Ithaca, NY: Cornell University Press, 2005).

[13] Dominika Kunertova:"Drones Have Boots: Learning from Russia's War in Ukraine," *Contemporary Security Policy* 44, no. 4 (2023): 576–591.

innovative developments in the technology and tactics of drone warfare.[14] Drone scouts, bomblets, loitering munitions, and even suicide drones are present throughout the theater in Ukraine. These inexpensive commercial technologies have changed warfighting dynamics on the battlefield with improved cost-per-effect in combat and increased emphasis on verticality in land operations. Drones empower individual soldiers as far as real-time intelligence and the precision of artillery fire.[15]

Small drones are now serving land forces in high-intensity warfare. This includes systems assembled by technology guerillas, as well as directly repurposed hobbyist drones ordered from Amazon or AliExpress on the internet. In the past, drones were thought to be mostly useful in conflicts when one side maintains air superiority, so this marks a significant change. Soldiers have been able to deploy *tens of thousands* of user-friendly, low-cost small drones in Ukraine for spying and dropping hand grenades on targets. These drones play a role in psychological warfare operations and can have non-kinetic effects. Among such notable effects are propaganda, like recording videos of ambushes that can then be posted to social media websites.

Importantly, since the early months of its full-scale invasion, Moscow has been using drones to cause as much damage as possible to Ukraine's critical infrastructure. The so-called one-way attack/suicide/kamikaze drones behave like disposable ammunition for targeting the Ukrainian power grid, transportation network, and even shelters for the civilian population. They offer an unambiguously offensive capability that can loiter in the target zone prior to its impact. Aside from the damage they inflict, these drones are clearly weapons of fear.

Innovation on the battlefield led to the proliferation of First Person View (FPV) drones, the latest milestone among many impressive drone developments. FPV drones are essentially a commercial version of a military loitering munition produced on the cheap. These systems are thus built from off-the-shelf components and operated by a pilot on the ground who navigates the drone to crash into its target thanks to the video feed running through the operator's goggles.[16] This human-guided munition can cost as little as $400 USD, in contrast to a GPS-guided shell that may cost hundreds of thousand dollars. FPV drones are consequently thought to help close the firepower gap caused by artillery shortages because their precision and navigability can facilitate destructive effects comparable to artillery shells.[17]

The focus on small drones is not simply a product of crowdsourced funding. Ukraine has promised to create an "Army of Drones," with Kyiv's Minister for Digital Transformation, Mykhailo Fedorov, announcing the government's intention to build 1–2 million drones. And in February 2024, President Volodomyr Zelenskiy created the

---

[14] Kerry Chávez and Ori Swed: "Emulating Underdogs: Tactical Drones in the Russia–Ukraine War," *Contemporary Security Policy* 44, no. 4 (2023): 592–605.
[15] Dominika Kunertova: "The War in Ukraine Shows the Game-Changing Effect of Drones Depends on the Game," *Bulletin of the Atomic Scientists* 79, no. 2 (2024): 95–102.
[16] Mykola Tkach, Dmytro Drynyov, Igor Kulinich, and Nataliia Mykytiuk: "Trends in the Global Arms Market, Development of the Combat Drone Market: Impact and Consequences for Ukraine," *Political Science and Security Studies Journal* 4, no. 3 (2023): 48.
[17] David Hambling: "Could Small Drones Really Replace Artillery?," *Forbes*, August 23, 2023, https://www.forbes.com/sites/davidhambling/2023/08/16/could-small-drones-really-replace-artillery.

Unmanned Systems Force—dedicated to drone warfare.[18] While Russia had previously prioritized manufacturing military-grade drones, it has almost caught up with Ukraine as far as its frequency of conducting FPV drone strikes.[19]

Drones have now gotten cheap, small, and commercial, easy to spread and operate, and produced on a scale akin to consumer electronics. This has led many observers to say that drones have game-changing effects. Is this technology able to help lift the Clausewitzian fog of war on the battlefield by providing better predictions of victory and defeat, and by offering improved intelligence? The answer appears to be neither when viewed holistically. In fact, sensational claims about drones pale when contrasted to the problems that accompany using these platforms in warfare. There are *at least* five reasons for this.

First, drones have no self-defenses and are vulnerable to weather and countermeasures. Drones act like consumer electronics in conditions with high-speed winds or heavy rains, and also in the cold, which can sap a drone's battery and therefore its range. These problems are particularly acute during the winter months. And even though some FPV drones have been fitted with counter-jamming devices, this add-on substantially increases the cost-per-drone and negatively affects their affordability and scalability.[20]

Second, the success of the drone mission is highly dependent on the skills of its human operator. Among newly formed units whose commanders have been appointed due to their political connections, a hit rate of 10% to 15% is common. In expertly trained units, such as special forces or those from Ukraine's intelligence services, the hit rate can be as high as 70% or 80%. This is a massive difference.

Third, assembling and producing myriads of drone models naturally presents difficulties. These can include heterogeneous safety standards, adoption issues, interoperability hurdles, and problems encountered during repairs and the replacement of components. All of these obstacles can contribute to further scaling problems.[21]

Fourth, drones depend almost entirely on other technologies to operate successfully. Their effective navigation and communication may require access to the internet provided by small commercial satellites, interference-resistant radios, or infrared sensors for night missions. These resources may not always be available, and commercial actors may not always be willing to provide them to militaries.

And fifth, drones cannot take territory or destroy strongholds. They lack the firepower, and the staying power, of traditional boots on the ground. Stated differently,

---

[18] Reuters, "Ukraine's Zelenskiy Orders Creation of Separate Military Force for Drones", February 6, 2024, https://www.reuters.com/world/europe/ukraines-zelenskiy-orders-creation-separate-military-force-drones-2024-02-06.

[19] Roman Vysochanskyy: "Redefining the Battlefield: Drone Warfare Tactics in Ukraine," Project Ploughshares, February 27, 2024, https://www.ploughshares.ca/publications/redefining-the-battlefield-drone-warfare-tactics-in-ukraine.

[20] Stacie Pettyjohn:"Evolution Not Revolution: Drone Warfare in Russia's 2022 Invasion of Ukraine," Center for a New American Security, February 2024, https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/CNAS-Report-Defense-Ukraine-Drones-Final.pdf.

[21] Seth G. Jones, Riley McCabe, and Alexander Palmer: "Ukrainian Innovation in a War of Attrition," Center for Strategic and International Studies, February 2023, https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-02/230227_Jones_Ukranian_Innovation.pdf?VersionId=Vap.5tI65sIt0kH10bxSSgN5q1G0cDhS.

an army of drones cannot replace infantry and cavalry. Drones can, however, delay adversary offensives, destroy infrastructure, frustrate air defenses, and intimidate and demoralize the enemy's troops and civilian population. Their military effects are accordingly limited to tactical realms. Drones lower the costs of combat and thus increase the availability of means to conduct operations. But they do not deliver revolutionary effects because their advantage lasts only until cost-effective countermeasures are operationalized.

Technological adaptations on the battlefields in Ukraine are happening much faster in the case of drones than in the case of other weapon systems.[22] The early headline-grabbing drones were large, sophisticated Turkish Bayraktar TB2 drones on the Ukrainian side, as well as Forpost and Orion military drones deployed by Russia. However, after some initial successes, it quickly became clear that these drones were easy prey for electronic warfare and lower-altitude air defense assets. Furthermore, the ubiquitous DJI Mavic drones turned into a "a hazardous encumbrance" due to Russia's use of the AeroScope drone detection system.[23]

OSINT Technology

Open-source intelligence technologies enable gathering and analyzing information from publicly available sources. These include data/metadata from social media, the internet, and television. Most remarkably, OSINT now includes large constellations of small low earth orbit (LEO) satellites that provide commercial imagery and offer remote sensing capabilities (e.g., synthetic aperture radar, radio frequency). Few Russian military planners considered that they were invading a country with millions of personal data collection devices. Each Ukrainian citizen can use their own phone to produce reconnaissance data in the form of messages, videos, and geotagged photos.

Space has been crucial to the war for the Ukrainian side. Kyiv uses space-based assets––oftentimes of commercial origin—for communications; intelligence, surveillance, and reconnaissance; and space-based positioning, navigation, and timing. These activities are powered in large part by private sector developments that have led to massive increases in the number of satellites, quality of imagery resolution, and availability of imagery. For instance, space launches have increased by a factor of 25 over the past decade due to decreasing costs.[24] As the section after this details, there is also an ongoing major technological revolution in machine learning that helps analysts assess all of the available data. Manual identification of objects is no longer the necessary first step in geospatial intelligence (GEOINT) analysis.

The market for commercial satellite capabilities is rapidly expanding. Most famously, the Starlink satellites of American company SpaceX have provided high-speed internet access to Ukrainian troops. Thousands of Starlink terminals enabled military communication, including guiding drone strikes. Another company, HawkEye 360, has been providing the Ukrainians with access to its radio frequency monitoring satellites

---

[22] Marc R. DeVore: "No End of a Lesson: Observations from the First High-Intensity Drone War, *Defense & Security Analysis* 39, no. 2 (2023): 263–266.
[23] Radio Free Europe, "Drone Wars: Ukraine's Homegrown Response to Deadly Chinese Detection Tech," July 14, 2022, https://www.rferl.org/a/drone-detection-war-ukraine-china-russia/31943191.html.
[24] United Nations Office for Outer Space Affairs, "Online Index of Objects Launched into Outer Space," accessed March 3, 2024, https://www.unoosa.org/oosa/osoindex/index.jspx?lf_id=.

to track Russian ground-based GPS jammers. And commercial satellite imagery from synthetic aperture radars provided by Maxar and ICEYE has been important for strategic communications and countering disinformation. Indeed, military commanders are becoming more receptive to OSINT, sometimes even preferring it to secret intelligence. This has led some media outlets to go so far as to proclaim that OSINT allows for "piercing of the fog of war."[25]

Dependence on commercial assets, however, can give private actors a veto over a military's capabilities and operations. Since the start of the war, Ukraine has been dependent on commercial assets, owned mostly by American companies. While the commercial sector has become a key source of technology innovation, private sector partners can become a security liability. The nature of partnership does not allow for oversight and control by their customers: national governments and military commanders. Companies usually retain control over the use of their assets. For instance, a company's executives can decide to restrict the availability of their product in a certain geographical area (geofencing), or opt to make its service available to the other side of a conflict as well. Recall the case of SpaceX not allowing Kyiv to use its Starlink satellites for military purposes over Crimea—especially for drone strikes.[26]

Furthermore, commercial entities do not usually get involved in wars due to charitable rationales. Following the initial SpaceX donation of satellite internet service, it became clear that if the government of Ukraine could not afford to continue paying the bill, it could not use the service. This is why having allies is important: Some NATO countries have paid Starlink so that Ukraine could continue using its satellites to support military operations.[27]

Space technology issues affect both sides in the war though. Russia has been reportedly having problems with connectivity and integration of space-based assets in its targeting, as well as malfunctioning satellite communication systems. It is plausible, however, that Russian troops may rely less on space for fighting on the ground than their Ukrainian foes.[28]

In addition to the "who is paying" and "who is providing" dilemmas of commercial satellite imagery, who is processing data and making them available across the battlefield is yet another matter. Some of the imagery making its way into social media and news articles features dubious annotations or analysis, and may also be subject to deep fakes or manipulated geotagging. Yet again, these issues point to the significance of (un)skilled human GEOINT analysts. The technology itself is not changing the battlefield.

---

[25] *The Economist*, "Open-Source Intelligence Is Piercing the Fog of War in Ukraine," January 13, 2023, https://www.economist.com/interactive/international/2023/01/13/open-source-intelligence-is-piercing-the-fog-of-war-in-ukraine.

[26] Joey Roulette: "SpaceX Curbed Ukraine's Use of Starlink Internet for Drones -Company President," Reuters, February 9, 2023, https://www.reuters.com/business/aerospace-defense/spacex-curbed-ukraines-use-starlink-internet-drones-company-president-2023-02-09.

[27] Micah Maidenberg and Matthew Luxmoore: "Pentagon Agrees to Pay SpaceX for Satellite Internet in Ukraine," *Wall Street Journal*, June 1, 2023, https://www.wsj.com/articles/pentagon-agrees-to-pay-spacex-for-satellite-internet-in-ukraine-2bdf3bf4.

[28] Amanda Miller: "Boxed Into a Corner," Russia Could Be a Counterspace Wild Card," *Air & Space Forces Magazine*, March 24, 2022, https://www.airandspaceforces.com/boxed-into-a-corner-russia-could-be-a-counterspace-wild-card.

All of the above examples suggest the notion that OSINT may pierce the veil of the fog of war is generally incorrect. By contrast, we observe these technologies resulting in additional uncertainty, thickening rather than lifting the Clausewitzian fog of war in Ukraine.

Artificial Intelligence

Advances in the deployment of AI-enabled systems are present in two major ways in the Russo–Ukraine war. First, such systems are taking part in data analysis on both an operational and tactical decision-making level. Second, they are also operationalizing targeting data for strike operations.

The convergence of data availability and relatively inexpensive microchips and software have created fertile ground for a race to master AI-enabled autonomy at scale. Dramatic increases in data due to open-source personal devices, widespread high-speed internet connectivity, and commercial GEOINT only contributes to this trend. Integrating AI systems into military decision-making processes and weapon systems has led to the rise of algorithmic warfare.[29] This certainly appears to be thickening the fog of war in Ukraine.

The use of AI in decision-making processes has undoubtedly impacted the battle rhythm of the war. AI is most heavily used to analyze large amounts of satellite imagery and geolocate open-source data.[30] Kyiv has relied on various foreign tech companies in these pursuits. For instance, the Ukrainian government is using facial recognition software (Clearview) to identify invading Russian troops and Ukrainian collaborators, natural language processing software (Primer) to analyze unencrypted Russian radio transmissions, and machine learning (Scale AI) to evaluate satellite imagery of Ukraine. Cloud services and cyber protection umbrellas from Microsoft, Amazon, and Google have allowed Ukraine's government to transfer and store critical data.

The Ukrainians notably employ digital battle management software that facilitates and accelerates the integration of various data points and formats. These include photos, videos, and imagery that are used to produce intelligence reports based on pattern identification. They are using ArcGIS Delta on the operational level, and GIS ARTA on the tactical level, to create real-time battlefield maps that are crucial for tracking the war's developments. With these maps, Kyiv can monitor the movement of Russian troops and share target coordinates with its commanders on the ground. Most remarkably, Palantir's data and artificial intelligence software have helped Ukraine assemble data to provide a full battlefield picture, enabling most of its military targeting. This has turned the U.S. firm into "the AI arms dealer of the 21st century."[31]

The ambition of the Ukrainian government, especially of the Ministry for Digital Transformation, is to make the country a major player in global technological innovation markets. With many American and European tech companies opening offices

---

[29] Ingvild Bode, Hendrik Huelss, Anna Nadibaidze, Guangyu Qiao-Franco, and Tom F. A. Watts: "Algorithmic Warfare: Taking Stock of a Research Programme," *Global Society* 38, no. 1 (2024): 1–23.
[30] Robin Fontes and Jorrit Kamminga: "Ukraine A Living Lab for AI Warfare," *National Defense Magazine*, March 24, 2023, https://www.nationaldefensemagazine.org/articles/2023/3/24/ukraine-a-living-lab-for-ai-warfare.
[31] Vera Bergengruen: "How Tech Giants Turned Ukraine Into an AI War Lab," *Time*, February 8, 2024, https://time.com/6691662/ai-ukraine-war-palantir.

in Kyiv, Ukraine's capital is quickly becoming a Mil-Tech Valley.[32] At first glance, all of these developments might suggest that AI can help clear the fog of war on the battlefield. And some techno-optimists have adopted this line of reasoning, arguing that AI is the key to winning the war.[33] But more skeptical voices have warned against the increased power of the private tech companies that are turning the battlefield into a playground for military AI expansion.[34]

Capabilities and services provided by foreign commercial players introduce more complexity into warfare that contributes to—rather than reduces—uncertainty. Corporations enter the battlespace with interests other than national security and the preservation of a state's sovereignty. These can include profit-driven sales incentives, efforts to perfect their product, and opportunities to improve the company's reputation. Quite apart from these Western firms, Russia is investing in AI systems and developing its own internet to avoid foreign interference and ensure its national technological sovereignty. But thanks to sanctions, the brain drain of innumerable Russian tech sector experts, and shrinking resources, major AI breakthroughs are unlikely to emanate from Moscow. This remains the case in spite of an August 2022 decision by the Kremlin to create a department within its Ministry of Defense to develop AI-enabled weapon systems.[35]

Regarding the use of AI in weapons themselves, the available evidence points to ongoing autonomous sensor-based targeting. These functions include autonomous object recognition and terminal guidance. Drones countermeasures based on electronic warfare, which disrupt communications systems, navigation, and data links, led some drone developers to experiment with autonomy. Such capabilities were seen as a potentially effective defense against electronic jamming. Autonomous drones could reach their targets even in case of disruptions since they would be able to make decisions based on integrated onboard data collection and analysis.

Drones could complete the last phase of their attacks even while being subject to jamming because of autonomous object recognition. This object recognition already features in the American-made Switchblade 300. And terminal guidance is present in the Russian FVP drone Ovod and the Ukraine-made Scalpel drone.[36] Ukraine's machine learning-trained Saker Scout drones are even able to identify 64 different types

---

[32] Bergengruen: "How Tech Giants Turned Ukraine Into an AI War Lab."
[33] See, e.g., Olga Tokariuk: "Ukraine's Secret Weapon – Artificial Intelligence," Center for European Policy Analysis, November 20, 2023, https://cepa.org/article/ukraines-secret-weapon-artificial-intelligence.
[34] Jonathan Horowitz: "One Click from Conflict: Some Legal Considerations Related to Technology Companies Providing Digital Services in Situations of Armed Conflict," *Chicago Journal of International Law* 24, no. 2 (2024): 305–337; Ingvild Bode and Tom Watts: "Loitering Munitions and Unpredictability: Autonomy in Weapon Systems and Challenges to Human Control," University of Southern Denmark, AutoNorms Project, June 7, 2023, https://www.autonorms.eu/loitering-munitions-and-unpredictability-autonomy-in-weapon-systems-and-challenges-to-human-control; and Comfort Ero, "Tech Companies Are Fighting for Ukraine. But Will They Help Save Lives in Other Global Conflicts?," International Crisis Group, June 9, 2023, https://www.crisisgroup.org/europe-ukraine-tech-companies-are-fighting-ukraine-will-they-help-save-lives-other-global-conflicts.
[35] Catherine Buchaniec: "Russian Military to Develop Weapons Using Artificial Intelligence," *C4ISRnet*, August 17, 2022, https://www.c4isrnet.com/artificial-intelligence/2022/08/17/russia-military-to-develop-weapons-using-artificial-intelligence.
[36] *The Economist*, "How Cheap Drones Are Transforming Warfare in Ukraine," February 5, 2024. https://www.economist.com/interactive/science-and-technology/2024/02/05/cheap-racing-drones-offer-precision-warfare-at-scale.

of Russian targets on their own.[37] However, Ukrainian AI-enabled drones are not fully autonomous; they point out targets and pass the information to human-operated FPV attack drones that then carry out the strike.

While it is in vogue to suggest that autonomous weapons are, or close to, revolutionizing warfare, the reality might be more complex.[38] Training an AI-enabled weapon system is insufficient. These systems also require many iterations of live testing and evaluation in order to become reliable. Indeed, it seems that Russia prematurely fielded the Lancet-3 loitering munition, which promised autonomous target identification and engagement without human intervention, and had to issue a "product recall."[39] Problems abound in the autonomy domain, which indicate that these AI technologies are far from changing the balance of forces.

Regardless, algorithmic warfare is the next stage of the network-centric warfare of the 1990s. AI is expected to help avoid information overload by enhancing the speed and quality of data analysis. AI-enabled data processing systems are thought to be capable of sifting through the storm of information noise from continuous real-time battlefield data. However, for Clausewitz, "accurate information is both an objective impossibility and a dangerously deceptive fantasy" because "we know more, but this makes us more, not less, uncertain."[40] It is not difficult to imagine how easily AI algorithms can be fooled through decoys and concealment, or misled by rogue data that can lead to classification inaccuracies. Furthermore, generative AI systems can be used to spread disinformation and propaganda, such as Russia's deep fake video of Zelenskiy purportedly calling for Ukraine's surrender in 2022.

However, a more serious problem with AI lies in its algorithms. While the nature of war demands decisions based on abductive logic and adaptation to unexpected situations, machine learning in most AI-enabled military systems relies on inductive logic and pattern recognition. Scholars have recently argued that no amount of data and computing power can correct this limited utility of AI for command.[41] Object recognition and situational awareness are fundamentally different concepts. AI-enabled conflicts will still be full of many types of environmental uncertainty and thus in need of a human take on the situation.[42] AI is therefore a good soldier but a bad general, and it does not appear to be helping reduce the fog of war in Ukraine.

---

[37] David Hambling: "Ukraine's AI Drones Seek and Attack Russian Forces Without Human Oversight, *Forbes*, October 17, 2023, https://www.forbes.com/sites/davidhambling/2023/10/17/ukraines-ai-drones-seek-and-attack-russian-forces-without-human-oversight.

[38] See, e.g., Paul Sharre: "The Perilous Coming Age of AI Warfare," *Foreign Affairs*, February 29, 2024, https://www.foreignaffairs.com/ukraine/perilous-coming-age-ai-warfare.

[39] Sydney J. Freedberg Jr.: "The Revolution That Wasn't: How AI Drones Have Fizzled in Ukraine (So Far)," *Breaking Defense*, February 20, 2024, https://breakingdefense.com/2024/02/the-revolution-that-wasnt-how-ai-drones-have-fizzled-in-ukraine-so-far.

[40] Thomas Waldman: "'Shadows of Uncertainty': Clausewitz's Timeless Analysis of Chance in War," *Defence Studies* 10, no. 3 (2010): 349–350.

[41] Cameron Hunter and Bleddyn E. Bowen: "We'll Never Have a Model of An AI Major-General: Artificial Intelligence, Command Decisions, and Kitsch Visions of War," *Journal of Strategic Studies* (2023), forthcoming, https://doi.org/10.1080/01402390.2023.2241648.

[42] Avi Goldfarb and Jon R. Lindsay: "Prediction and Judgment: Why Artificial Intelligence Increases the Importance of Humans in War," *International Security* 46, no. 3 (2021–2022): 7–50.

Hypersonic Weapons

The new generation of hypersonic weapons—gliders and missiles—combine extreme speed, maneuverability, and a low-altitude flight trajectory. This technology has not matured yet and therefore these emerging weapons are still in the making. Flying within the atmosphere at five times the speed of sound comes with a number of problems due to the laws of physics.[43] Additionally, hypersonic missile delivery vehicles that may one day carry nuclear warheads are not exactly a new EDT capability. Ballistic missiles, a technology first pioneered in the early 1940s, travel at hypersonic speeds.

Difficulties entailed in fielding hypersonics have not prevented their use. The Russian Ministry of Defense confidently announced the first battle use of its hypersonic Kinzhal weapon in Ukraine in March 2022.[44] However, this alleged wonder weapon turned out to be a "mere" ballistic missile—a modified version of the surface-launched Iskander-M tactical ballistic missile. It is true that being air-launched from a supersonic MiG-31 jet gives the missile a boost to reach higher speeds at an altitude that is unusual for a ballistic missile. Regardless, Russia's terrifying missiles failed to hit high-value targets in Ukraine. A few months later, the Ukrainians intercepted seven of these "unstoppable" missiles using an old Patriot missile defense system.[45]

The Russian Kinzhal is therefore a propaganda weapon. Using nuclear-capable, but conventionally-armed, hypersonic weapons may increase fears about the Kremlin's willingness to cross the nuclear threshold.[46] But the added military value of this air-launched ballistic missile remains unclear, aside from thickening the fog of war. By designating and press releasing Kinzhal as a new class of hypersonic weapon, Moscow creates a psychological effect of intimidation. Furthermore, Russia signals to the West that it possesses and is willing to use weapons that are thought to overcome missile defenses on NATO's eastern flank.

These exaggerated expectations do not square with the military utility of the Kinzhal. In reality, hypersonic delivery vehicles and other exotic systems hyped by Putin do very little to change the balance of forces and the dynamics of warfare. However, Russia is not a newcomer to the symbolic use of weapons for the intended purposes of deterrence and compellence. Such systems are more likely bargaining chips to trade for missile defenses and other U.S. and NATO systems feared by the Kremlin; they do not really convey any worrisome novel military capabilities.[47] They appear instead to be psychological weapons intended for signaling rather than actual use on the

---

[43] Dominika Kunertova: "Hypersonic Weapons: Fast, Furious…and Futile?," *RUSI Newsbrief* 41, No. 8 (2021), https://www.rusi.org/explore-our-research/publications/rusi-newsbrief/hypersonic-weapons-fast-furiousand-futile.

[44] Paul Kirby: "Russia Claims First Use of Hypersonic Kinzhal Missile in Ukraine," BBC, March 19, 2022, https://www.bbc.com/news/world-europe-60806151.

[45] Luke Harding and Dan Sabbagh: "Russia's Most Potent Hypersonic Weapon Neutralised, Says Ukraine," *The Guardian*, May 16, 2023, https://www.theguardian.com/world/2023/may/16/ukraine-russia-targets-kyiv-with-massive-overnight-airstrike.

[46] Rebecca Davis Gibbons and Stephen Herzog: "Nuclear Disarmament and Russia's War on Ukraine: The Ascendance and Uncertain Future of the Treaty on the Prohibition of Nuclear Weapons," in Rebecca Davis Gibbons, Stephen Herzog, Wilfred Wan, and Doreen Horschig: *The Altered Nuclear Order in the Wake of the Russia–Ukraine War* (Cambridge, Mass.: American Academy of Arts and Sciences, 2023), 1–36.

[47] Alexander K. Bollfrass and Stephen Herzog: "The War in Ukraine and Global Nuclear Order," *Survival* 64, no. 4 (2022): 7–32.

battlefield. Media perceptions of new and seemingly sophisticated Russian weapon systems certainly need some debunking. The Russian propaganda machine may find an audience of journalists—eager for reads and clicks—who are ready to repeat the overblown narrative of such weapons as revolutionary and unstoppable. But a closer look reveals only unremarkable additional strike options at best, and unsafe weapons at worst.

Net Assessment

In this working paper, we discussed two possible paths by which EDTs can reduce uncertainty and therefore lift the fog of war. On the one hand, there are theoretical ways that new weapon technologies could increase the likelihood of military successes and increase transparency on the battlefield. On the other hand, we drew on evidence from Russia's war in Ukraine to show how new technologies can thicken the fog of war by increasing uncertainty. They may do so by introducing more complexity (commercial assets and private actors) and more ambiguity (unclear capabilities of new systems). We have identified four ways in which the integration of new EDTs warfare transform, but do not lift, the fog of war.

1. New technology creates new vulnerabilities the opponent can exploit[48]

Thousands of small drones flying over the battlefield create deconfliction problems for militaries. The digital battlefield can mean not only increased military efficacy thanks to connectivity and real-time information streams, but it also produces an undesirable digital footprint that facilitates enemy targeting. Mobile phones are the new cigarette of the trenches.[49]

In contrast to the previous decades dominated by the traditional military–industrial complex, new commercial entities are becoming more prominent.[50] Private actors now drive the bulk of investment into satellite surveillance, drone development, AI, software, and advanced manufacturing, leading to a rapid decrease in the cost of precision guidance technologies.[51] However, the entry of commercial actors (especially foreign ones) into an ongoing war creates access issues regarding privately owned infrastructure and control over the provision of services. Another related issue is interoperability and military standards of dual-use drone technology. Furthermore, the quality of AI analytics on the battlefield is contingent upon the availability of big data that come from open sources. There is thus a need for a better framework for public–private open-source technological innovation in terms of data collection, integration, analysis, and operational targeting.[52]

---

[48] See, e.g., Colin S. Gray: *War, Peace, and Victory: Strategy and Statecraft for the Next Century* (New York: Simon & Schuster, 1990).
[49] Alex Horton: "Two Years of War in Ukraine: What the Pentagon Has Learned, *Washington Post*, February 22, 2024, https://www.washingtonpost.com/national-security/2024/02/22/ukraine-war-pentagon-lessons-learned.
[50] Herzog and Kunertova: "NATO and Emerging Technologies."
[51] T. X. Hammes: "Game-Changers: Implications of the Russo–Ukraine War for the Future of Ground Warfare, Atlantic Council, *Issue Brief*, April 2023, https://www.atlanticcouncil.org/wp-content/uploads/2023/04/Game-Changers-or-Little-Change-Lessons-for-Land-War-in-Ukraine-.pdf.
[52] Audrey Kurth Cronin: "Open Source Technology and Public-Private Innovation Are the Key to Ukraine's Strategic Resilience," August 23, 2023, https://warontherocks.com/2023/08/open-source-technology-and-public-private-innovation-are-the-key-to-ukraines-strategic-resilience.

2. Surprise effects of novel weapon systems will eventually be negated by countermeasures[53]

Small drones on the battlefield in Ukraine have transformed warfare not in terms of effects like winning wars or contributing to the success of a counteroffensive, but in terms of means. Drones have decreased the cost of precision-guided munitions and alleviated strains on production capacities given their relatively inexpensive costs. This has led to a situation wherein the defending side fires multi-million-dollar missiles to neutralize attacking drones that cost only a few hundred dollars. Protecting one's troops, population, and critical infrastructure may depend on it.

Yet, this measure–countermeasure adaptation cycle is not some sort of techno-miracle. Greater investments in electronic warfare have become a key part of counter-drone systems. Indeed, Russian forces have learned to integrate electronic warfare, missile systems, and connected sensors to frustrate and repel Ukraine's drone offensives. Further developments in directed energy weapons may rebalance asymmetry in conflict by decreasing the cost of countering such low-cost drone threats.[54] And while the proliferation of surveillance drones—and livestreaming of battlefields—has introduced unprecedented transparency, it has already led to adaptive measures in the form of the tactics of deception and dispersal. Clausewitz's fog of war has changed in the new era of EDTs, but it remains intact.

3. Humans still matter

Most new emerging technology requires people with new skills and roles. The expectation that robotic and autonomous systems would compensate for decreased troop numbers has proven to be false in Ukraine. Technology may remove people from performing dangerous, dull, or dirty tasks, but the operators, technicians, data analysts, communications specialists, software engineers, and force protection units remain present on, or nearby, the battlefield.[55]

Drones are not organic extensions of human combatants. They may represent a capability gain, but they may also come with an attendant loss in force structure efficiency. Armed with grenades or as one-way attack munitions, drones have proven their tactical utility in high-intensity warfare. However, echoing the previous point, it is the relentless human-driven adaptability to an opponent's countermeasures that helps militaries to prevail. In the end, training, military organizational adaptation, and learning are proving crucial in effective adoption of new weapon technologies. It is also instructive to remember that in Ukraine, drones are aiding soldiers and contributing to land warfare, not replacing boots on the ground in a manner analogous to past counterterrorism operations.

---

[53] See, e.g., Brendan Rittenhouse Green and Austin Long: "Conceal or Reveal? Managing Clandestine Military Capabilities in Peacetime Competition," *International Security* 44, no. 3 (2019): 48–83; and David M. Allison, Stephen Herzog, Brendan Rittenhouse Green, and Austin Long: "Correspondence: Clandestine Capabilities and Technological Diffusion Risks," *International Security* 45, no. 2 (2020): 194–198.

[54] Stuart Dee and James Black: "Directed Energy Dilemmas: Industrial Implications of a Military-Technological Revolution," RAND Corporation, *TheRANDBlog*, February 20, 2024, https://www.rand.org/pubs/commentary/2024/02/directed-energy-dilemmas-industrial-implications-of.html.

[55] Jack Watling: "Automation Does Not Lead To Leaner Land Forces," *War On The Rocks*, February 7, 2024, https://warontherocks.com/2024/02/automation-does-not-lead-to-leaner-land-forces/.

4. New technologies and emerging weapon systems add complexity to decision-making

EDTs create numerous opportunities for actors to try and manipulate adversary perceptions of their weapons. The reputation of the system becomes a weapon in itself that is designed to intimidate the opponent. Clausewitz's maxim requiring "skilled intelligence to scent out the truth" therefore seems ever more relevant for developing a strategy to counter the threat from weapons that have not matured, alongside hyperbolic narratives regarding their capabilities. Sensational statements about new weapon technologies can obscure the actual problem. For instance, claims about drones revolutionizing the battlefield detract attention from the shortage of artillery shells at the front. This distractive hyping and the use of drones by both sides in the Russo–Ukraine war means that little is being done to decrease the uncertainty of the fog of war.

A better understanding of the comparative advantages of existing and new weapon technologies depends on accurate and verifiable scientific assessments. Similarly, it is imperative for analysts to pay attention to the human ability to convert technology into political effects. Drones do not perform best alone; they do so in tandem with artillery. When combined with digitized battle command-and-control and civil–military sensor networks, drones are indeed part of forces transforming the battlefield.[56]

Conclusion

New emerging weapon technologies on both the high and low ends of the innovation spectrum have not lifted the fog of war in Ukraine. This working paper further points to two current techno-optimist fallacies that are present in the discussion of Russia's war of aggression against Ukraine.

First, technological superiority feeds overconfidence. Developing exotic weapon systems could have given Kremlin leadership a false sense of superiority in the days ahead of the invasion, and then Russian troops seriously underperformed on the battlefield.[57] This is also why Western expectations about Russia's new EDT-driven weapons have simply not corresponded with the realities on the battlefield.

Second, fixating on new weapons can divert attention away from other critically important factors that may contribute to conflict outcomes. These include: human factors such as courage and determination, and fighting for one's homeland; and domestic and international political factors like security alliances, strategic culture, and public opinion.[58]

However, overestimating the impact of new technologies contributes to an outsized influence of a certain category of humans: tech companies. While these firms' know-how and investments into battlefield-relevant innovation have been remarkable—turning Ukraine into the world's technology research and development lab—apps and

---

[56] Clint Hinote and Mick Ryan: "Empowering the Edge: Uncrewed Systems and the Transformation of U.S. Warfighting Capacity," Special Competitive Studies Project, February 2024, https://www.scsp.ai/wp-content/uploads/2024/02/SCSP-Drone-Paper-Hinote-Ryan.pdf.
[57] Marina Favaro and Heather Williams: "False Sense of Supremacy: Emerging Technologies, the War in Ukraine, and the Risk of Nuclear Escalation," J*ournal for Peace and Nuclear Disarmament* 6, no. 1 (2023): 28–46.
[58] Waldman, "'Shadows of Uncertainty,'" 336–368.

repurposed hobbyist drones simply cannot not help Ukraine retake its territory or repulse the Russian occupiers. In the words of one U.S. defense official, "We're not fighting in Ukraine with Silicon Valley right now, even though they're going to try to take credit for it."[59]

Commercially-driven military technology innovation is moving toward algorithmic warfare on a digital battlefield. The proliferation of semi-autonomous drones, with goggled human operators in decline, and AI software fusing and analyzing data that flows across platforms and domains, both contribute to a gamified version of war. But these moves overshadow the role of humans and human qualities that influence decision-making, like intuition, judgment, and morale. So far, AI-enabled military systems have object recognition, not situational awareness. Just because AI can beat humans in playing chess or Go, with clearly defined rules and a stable environment, does not mean that AI algorithms will fundamentally redefine all the parameters of warfare.

At this point in history, the war in Ukraine shows us that it is not new technology that will lift the fog of war. Rather, if technology is to play a role in this endeavor, it will be due to the supreme skills of humans operating EDT-driven military systems. For Clausewitz, war is a human affair, one that is too important to be left to the machines. We find that said machines are actually helping to thicken the fog of war by producing further uncertainty about the balance of forces and conditions on the battlefield.

[59] Vera Bergengruen, "How Tech Giants Turned Ukraine Into an AI War Lab."