JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

WIZARD WARFARE: UKRAINIAN TECHNOLOGICAL DEVELOPMENTS OVERVIEW

Stephen DeCoste | Jeff Miers

WIZARD WARFARE

Ukrainian Technological Developments Overview

Stephen DeCoste

Jeff Miers

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

Copyright © 2024 The Johns Hopkins University Applied Physics Laboratory LLC.
All Rights Reserved.

The images used in this document were pulled from BigStock.com. Each image number is included with the figure.

NSAD-R-24-033
December 2024
X11GA

Contents

Figures

Abstract

This document provides an overview of the technological innovations in Ukraine developed as a consequence of the Russian invasion in February 2022. The team focused on the first year of the war to examine what new technologies and technological strategies Ukraine used to fight the Russian invasion. What insights can the United States gain in its efforts to innovate from Ukraine?

Preface

On February 24, 2022, Russia invaded Ukraine. Since then, the world has been watching for what can be learned from this conflict. XVIII Airborne Corps, the Johns Hopkins University Applied Physics Laboratory, and Georgetown University's Center for Security and Emerging Technology teamed up to examine what the Russia-Ukraine conflict can tell us about technology innovation. Our results are summarized in three papers:

(1) Technology and Ukraine: Implications for the United States (classified)

(2) Building the Tech Coalition: A Case Study in Applying Software and AI for the U.S. Department of Defense

(3) Wizard Warfare: Ukrainian Technological Developments Overview (this paper)

Importance of Ukrainian Technology Innovations

The Western world is watching closely the rapid technological innovations that Ukraine has developed as a consequence of the Russian invasion. What can the United States learn to drive future U.S. technology innovation? With Ukraine's smaller, less-funded army thwarting one of the largest armies in the world, the question remains: How have they done it? It would appear that rapid advancements in their information technology (IT) infrastructure, the intelligence cycle, artificial intelligence, stronger public-private partnerships, and the use of unmanned drones may be providing Ukraine an advantage in information war and operational tempo. Ukraine has begun to roll-out federally funded initiatives and push private companies to create emerging software programs and front-line hardware innovations to survive the Russian invasion. Decreasing bureaucratic obstacles during wartime has allowed Ukraine to accelerate their technology development and distribution to warfighters. The success, or failure, of these innovations provides key insights to the United States and its allies for creating a more agile, more innovative, and more effective fighting force.

Image from BigStock.com. Image number 450017407.

Figure S-1. Map of Ukraine

Broad Trends

Since the beginning of the Russian invasion in February 2022, Ukrainian leadership emphasized the importance of *evolution*, turning their Soviet-era army into a NATO-style one [1]. This effort was, in part, supported by over $55 billion in military assistance provided by the U.S. since the invasion began. The broader technological transition appears to be increasing interconnectivity among the Ukrainian army. The approach is led by improving their use of emerging technologies. Early on in the invasion, Ukraine acknowledged disparities with Russia in funding, manpower, and weaponry, which has seemed to motivate the concepts of "agility" and innovation on the battlefield [2]. Since February 2022, Ukraine's technology developments show the following broad trends:

(1) A continued investment in robust technology infrastructure
(2) Increasing access to reliable intelligence from all available sources
(3) Use of artificial intelligence (AI) across all aspects of the conflict
(4) Deployment of both single and multi-use drones on the frontlines

Supporting Innovation – Building a Technology Infrastructure

Even prior to the Russian invasion, Ukraine was known for its thriving information and communication technology sector [3]. With more than 4,000 information and communication technology (ICT) companies, approximately 80 percent of the population having internet access, and the fourth-highest number of certified tech professionals globally, Ukraine was a digital hub. Ukraine focused heavily on leading European tech innovation, becoming the first Country to utilize digital IDs, digital signatures on official documents, and other commercially focused services [4]. Ukraine's ICT infrastructure became a target early in the invasion, with Russian cyber and kinetic attacks on critical parts of its technological backbone. To counter, Ukraine quickly pivoted to offer tax incentives, draft certified technical professionals into the war effort, and fund continuing development of emerging technologies. Ukraine thus positioned itself to build more robust ICT links between front-line troops and, as a result, accelerated decision-making. Ukraine was rapidly able to refocus ICT professionals and existing technologies from the commercial sector to support the war effort [5].

Diia.City

Ukraine has continued to invest financial and manpower resources into both the hardware and software needs of its technological innovations. Ukraine initiated efforts to channel foreign investment into the war and increase innovation from internal privately owned companies. Described as having a "vibrant tech ecosystem" by the Atlantic Council, Ukraine had launched Diia.City just two weeks before the Russian invasion [5]. The Ukrainian Ministry of Digital Transformation started Diia.City to create a tax-friendly environment to attract foreign corporations like Samsung, Nokia, Visa, and Ajax Systems. Diia.City is not a physical location and economic zone, but a collection of legal and tax benefits provided to companies that meet certain criteria. These various benefits create a stable set of conditions for IT companies to develop innovative technologies, which are gained by registering with the Diia.City database. The Diia.City initiative has also launched more than 350 Ukrainian startups as of December 2022 via the Ukrainian Startup Fund [6].

In addition to increased income from an influx of private companies entering Ukraine to capitalize on the tax and intellectual property benefits of Diia.City, Ukraine is offering additional benefits to companies with expertise relevant to the war effort. Since the war began, the Diia.City concept has moved on from being a set of policies, to become a mobile application that improves civilian connectivity, promotes tech innovations, and protects proprietary technologies emerging as a result of the war. Similarly, the 21.7 million users of Diia.Portal mobile application rely on it as a central hub to communicate, share intelligence, and find and identify family members separated during the war. [1] The Diia.Portal application hosts more than 70 government-sponsored online services for military personnel, civilians, and companies.

Since the beginning of the war, Diia.City has allowed foreign companies to more easily aid Ukraine in developing critical tools for the war effort. This includes the German drone company Quantum Systems, which has started drone production facilities and research centers in Ukraine. Foreign companies are now better able to protect their intellectual property, securely e-sign documents, and negotiate state contracts, as

[1] The Diia Portal application is one of many apps within the Diia City digital ecosystem. Diia.Portal is used more often by civilians, as opposed to Diaa.City which requires businesses to apply and provide extensive business records to gain access to the platform.

well as receive significant tax breaks for those companies supplying the war effort [7].

The primary platform within Diia.City is BRAVE1, which is a conglomerate of more than 400 new technologies, 200 of which have begun or completed testing. These projects focus on cybersecurity, robotic systems, electronic warfare, and IT management systems. Overall, Diia.City was a pre-war innovation that has been leveraged to support the war and continues to generate additional funding and innovation for the country.

Commercial Satellite Services

A notable success of the conflict for Ukraine has been its acquisition and effective use of commercial satellite services for communications and geospatial intelligence (GEOINT). In the early months of the conflict, some U.S. military experts characterized the war as the "first commercial imagery conflict" [8]. In a continuing trend of leveraging public-private partnerships, Ukraine has worked closely with U.S. companies to access their satellites to gain an advantage in information warfare.

Perhaps most notable among these partnerships is the one with SpaceX for use of its Starlink satellites (Figure 1). Just a few days after the war began, SpaceX opened the use of their low earth orbit Starlink constellation to Ukraine for communications; by May 2022, 150,000 Ukrainians were using Starlink for daily communications [9]. The cost of providing this service seems to be funded by external sources, including partner nations, the U.S. Agency for International Development, and the U.S. Department of Defense. Ukraine subsequently extended its use of Starlink to communications supporting offensive targeting, including coordination of drone strikes against Russian forces. SpaceX then limited the capabilities Ukraine has access to, although those limits are unclear from open-source reporting [10].

Image from BigStock.com. Image number 452765263.

Figure 1. Starlink Equipment Lviv, Ukraine March 2022

Ukrainian forces also use commercial imaging satellites to support GEOINT, locate military equipment, verify battle damage, and monitor both friendly and enemy infrastructure. Companies supporting Ukraine with imagery include BlackSky, Planet, and Maxar Technologies. While these private companies have shared images with Ukraine, who else they sell to is unclear [11]. There is a possibility these companies also share images with Russia or China — potentially lessening the advantage held by the Ukrainian army. Planet's spokesperson to the media has declined to share "specific names of companies or governments we are providing our data to" despite strong public ties with Ukraine.

The continued use of commercial imaging satellites works in tandem with efforts on the ground to verify information from civilians and then upload to various applications on smartphones. Ukraine appears to have created a multidirectional pipeline between information from space and information on the ground, using AI technologies as a means to verify, combine, and transmit information to military personnel. Dr. Robert Clark, a former intelligence officer with the CIA and now a professor at Johns Hopkins University, cited this combination of information as a "breakdown" of the traditional intelligence cycle. He notes that — as opposed to

moving sequentially through the stages of collection, processing, analysis, and dissemination to customers — in the Ukraine conflict these stages all occur in parallel [12]. Just moments after raw footage are collected by a civilian on their mobile device and sent via a private Telegram channel, GEOINT is able to verify with satellite imagery the accuracy of the information, and transmit it to the intelligence community and troops on the frontlines. All of this happens almost simultaneously, increasing the speed of information sharing across the war effort.

A more collaborative intelligence process is similar to other aspects of Ukraine's technology development, emphasizing speed and adaptability to overcome material disadvantages. Dr. Clark noted that GEOINT served as a catalyst for breaking down the traditional intelligence cycle in Ukraine, as a result of near-real-time monitoring of the conflict. Given Ukraine's use of civilian reports to confirm, in real time, what can be observed by satellites in space, Ukraine is able to maintain a near-constant flow of information. Because this information is often captured in video or photo form, there is less concern about "bad" information reaching decision makers. These adaptations are increasing operational tempo across the frontlines.

Intelligence Exchange and Information Warfare

Ukraine has spent significant resources to improve the exchange of information both vertically between civilians and the government and horizontally among military service members throughout the war effort. Some applications, like Milchat, focus primarily on enabling communications among more than 600,000 service members, including vertically integrating commanding officers with soldiers under their command, and soldiers of the same rank with each other. Others, like eVorog (eEnemy) allow civilians to engage in the conflict, acting as a constant source of intelligence about Russian troop and asset movements [13].

Vertical Information Sharing

Ukraine has created a robust pipeline between civilians and military personnel, providing open-source intelligence to increase fidelity of GEOINT from various commercial satellites. One of the unique platforms used by Ukraine is eVorog, set up in March 2022 by the Ukrainian Ministry of Digital Transformation [14]. The platform is a chatbot that takes users through a series of questions to describe what they saw, and where and when they saw it. Hosted on Telegram and transmitted through encrypted messages, the information is then passed through Diia.Portal. At this point,

the sender's identification is verified by checking their geographic location and cross-referencing the information with other available civilian reports and GEOINT. By December 2022, eVorog had received more than 450,000 reports of Russian troop movements and asset locations.

Another application used by civilians to pass information to service members is ePPO, which focuses on tracking drones, missiles, and enemy aircraft. Similar to eVorog, users are asked what type of weapon they saw and what direction it came from, which is then confirmed with the GPS of the user's cellphone and any existing GEOINT. The first successful use of this platform to shoot down a missile occurred in October 2022 [15].

Beyond these newer platforms developed expressly for the war effort, Ukraine has extensively increased its presence on social media platforms including Instagram, YouTube, and TikTok. Generally speaking, Russia has closed off its civilian access to social media and the internet while Ukraine has leveraged both to generate both pro-Ukrainian and anti-Russian sentiments in the West [16]. Consistent with the notion of evolving from a Soviet-era army, Ukraine has tried to move from a closed society to an open one. The scale of this social media surge began as early as the first week of the war, with #Russia generating more than 40 billion collective views on TikTok.

Horizontal Information Sharing

Beyond increasing the flow of information from civilians to military personnel, Ukraine has continued to develop tools for increasing the quantity, quality, and speed of information and decision-making across its army. Some of the software programs in use include:

- Delta: An advanced digital map that integrates satellite imagery from NATO members and has chatbot implementations to allow for real-time updates across brigades. With more than 30 updates since it was presented to NATO members in October 2022, this software is considered one of the most compelling innovations by Ukraine. It first began development in 2015 by coders called the "Aerorozvidka" (aerial reconnaissance) who make up part of the military units on the front lines [1].
- Milchat: A secure messenger app used by more than 600,000 service members.

- Nettle: Software that performs artillery calculations at rates of 2 to 10 times faster than human personnel, depending on the intended target [17].
- Combat Vision: Geographic information service to capture troop movements, positions, and classifications.

These platforms often span numerous battalions, all of which require different hardware depending on their role. Typically, the information gained on the battlefield is logged into applications residing on tablets. From there, the information is viewed in a command post, sometimes called a "situational awareness center" [1]. These situational awareness centers are deployed across the front lines and are where much of the battlefield software deployment and integration takes place. The centers are also outfitted with 3D printers to reinforce drone hardware, large computers for on-the-go coding, and large screens used to display battlefield maps and drone footage. Most of the Ukrainian battlefield software can be downloaded on a standard tablet and, as such, contributes to better "horizontal communication" according to the Ukrainian Defense Ministry [1].

Programs like Delta and Combat Vision are improving access to real-time intelligence information. Delta receives high-fidelity satellite images supplied by NATO members and subsequently feeds that information into a live battlefield map.[2] Additional photos and information gained from behind enemy lines are uploaded into the program daily, all of which culminate in a multi-layer map of the battlefield space.

Applications like Nettle (also referred to as Kropyva) have spread to nearly every Ukrainian artillery unit to improve strike time against Russian forces. This program automates ballistic calculations that used to take 15-20 minutes, condensing the effort to between 30 seconds and 3 minutes, depending on the target [18]. The Kropyva platform is effective given its "simplicity, autonomy, and prevalence" across the battlefield. Simplicity and speed are Ukraine's advantage in the development and deployment of these new technologies, says Army Survivor Outreach Service, the non-profit that developed the Kropyva platform [19].

[2] This imagery is likely almost all commercial, mostly from the U.S. and NATO countries with commercial-grade imagery systems.

Artificial Intelligence Across the Battlefield

One of the primary levers used by Ukraine to gain advantages in the war has been an increasing reliance on AI. The developments in AI serve multiple purposes, including facial recognition, language detection, and targeting Russian assets. AI is being implemented across multiple fronts in the conflict and is deployed in a variety of scenarios to increase the speed at which decisions are made within the Ukrainian forces.

AI as a Bridge

AI has acted as a bridge between different spheres of the war effort. This includes bridging GEOINT and intelligence provided by Ukrainian citizens, bridging the government and the military, as well as public-private partnerships according to Palantir's CEO [20]. One such public-private partnership is represented by the U.S. company Primer AI, which uses AI to analyze unencrypted Russian radio communications. The platform uses natural language processing to distill complex radio chatter into summaries of information, translated into a language of choice. The platform was first tested in Donbas in the first year of the war, training a "call to action model" that would summarize large bodies of audio into only the commands made by Russian soldiers. Within these summaries, the platform could name the type of assets discussed, their approximate position, and whether the asset is engaging Ukrainian forces [21]. The deployment of Primer AI has contributed to Ukraine's agile warfare approach, with new data ingestion training focusing on the open-source intelligence collected by Ukrainian civilians on the Diia.Portal application.

AI as a Cyber Defense Tool

In addition to increasing the spread of reliable information, Microsoft reported that as early as March 2022, Ukraine began to use AI in the cybersecurity domain [22]. Reported Russian cyberattacks — mostly data theft, phishing attacks, and ransomware attacks on both civilian and military personnel — necessitated a rapid Ukrainian response. While many of Ukraine's specific steps to thwart Russian attacks are unclear, it is estimated that hundreds of cyberattacks were prevented with the use of AI and emerging cyber-defense technologies [23]. While specific tools are also largely unknown, the Ukrainian National Cyber Security Center has partnered with IP3 International to develop the Collective Defense AI Fusion Center (CDAIC) [24]. One known system used to detect and prevent cyberattacks is IronNet, a central platform to detect threats and exchange insights across users in real time — all with

the help of AI technology. The focus of the CDAIC partnership is protection of Ukrainian energy infrastructure from cyberattacks but, much like Diia.City, relies on the use of a central platform with various in-house functions to potentially expand protection to other areas.

AI as an Offensive Tool

Ukraine has invested heavily in drone warfare as a means to strike Russian equipment and troops. Many of these drone systems rely on software powered by AI to identify, locate, and prevent Russian soldiers from infiltrating Ukrainian homes or communities. U.S.-based company Clearview's AI facial recognition technology has been offered exclusively to Ukraine's forces according to one of the company's chief executives [25]. The Clearview AI is trained on more than 2 billion images from Russian social media platform VKontakte. The full scope of the program is unclear, although that same executive indicated that it can be used to identify deceased enemy combatants, identify high-profile targets, and create more certainty in strikes.

Similarly, target-recognition AI is also being tried in tandem with drone pilots on the front line as a way to combat Russian jamming technology. In the case of first-person view (FPV) drones, Russian jammers have consistently caused Ukrainian drone pilots to lose control of their systems, rendering kamikaze style attacks ineffective. Twist Robotics, a Ukrainian-based company, is currently testing a drone-targeting algorithm [26]. The algorithm is trained to identify a target at range based on size, shape, color, or infrared heat signature so the drone can fly on autopilot in the event of the FPV system failing due to Russian jammers. Ukraine has emphasized that one of the core tenants of their drone philosophy is not giving AI control over firing weapons. Meaning, for the time being, that while drones can complete a strike on an operator-chosen target, Ukraine has not expressed a desire to fully automate target detection and engagement with FPV drones.

Drone Warfare

Another highly visible technology embraced by Ukraine is uncrewed air and surface vehicles. Ukrainian innovations in converting commercial drones for combat has been crucial in maintaining a massive volume advantage against the Russian Army. Putin has pledged to domestically produce 18,000 drones a year by 2026 [27]. In December 2023, Ukraine was producing around 50,000 first-person-view [FPV] drones, almost 20,000 more than their end-year goal. As of March 2024, the Ukrainian Minister of

Strategy and Industry claimed production increased to about 100,000 drones a month, with an end of year production capacity expected to reach 1 million units [28]. Ukraine is currently using 10,000 drones a month, and was trying to produce 30,000 a month by the end of 2023. While Russia has seemed to focus on producing more cutting-edge, high-quality drones with China's assistance, Ukraine is seeking to maximize quantity over quality. Although it may not be the primary focus, Ukraine also procured and improved military-grade uncrewed aerial systems (UASs) to use against larger, more high-value Russian assets. Broadly speaking, the Ukrainian strategy has deployed UASs in three capacities:

(1) Single-Use Systems
(2) Multi-Use Systems
(3) Intelligence Systems

Image from BigStock.com. Image number 474918433.

Figure 2. Drone Kamikaze Pilots Exercise in Odessa, Ukraine

Single-Use Systems

By far, the most widely used and most widely modified drones are the single-use "Kamikaze" drones.

In most cases, the single-use systems work like a slower Hellfire missile, at a fraction of the price tag [29]. The base of the system is a commercial or hobbyist drone. These drones are often sourced from Chinese companies, including products like the *Autel EVO MAX 4T*. Commercial drones are ideal for single-strike missions due to their maneuverability, relatively easy assembly, and low cost. These drones are often controlled while pilots wear an FPV system, which also costs around $500. It is common for a $1,000 explosive drone to eliminate a $1-million Russian weapons system [30]. According to the Deputy Prime Minister, in the second week of November 2023, more than 220 Russian units including tanks, armored trucks, artillery systems, and other armored vehicles have been "turned to scrap" [31].

The use of rudimentary tools like tape, zip ties, plastic casings that snap together, handheld batteries, etc., allow these drones to be outfitted on the front lines. Often, a pilot may use multiple drones to increase the likelihood of success against targets, as Russian jammers, anti-UAS weapons, and personnel movements create obstacles these commercial drones struggle to overcome. These systems have a limited range and battery life, which means the pilot must identify the target and move to strike quickly, with little room for error. Ukraine was planning to increase their use by a factor of three to 30,000 drones a month, and invest about $545-million USD in new drone startups in 2023 [32]. In 2024, Kyiv has allocated about $1.14-billion USD to domestic drone production [33]. These easy to maneuver drones offer a cost-effective way to disrupt Russian troop movements and create coordinated attacks with the sniper-like accuracy of a trained pilot.

In addition to inexpensive commercial drones, Ukraine has also leveraged more advanced military grade UAS from U.S. contractors. A primary example includes the AeroVironment *Switchblade 600* drone system. With the *Switchblade* 600, and its lighter counterpart, the *Switchblade* 300, Ukrainian forces are able to use the drones at a range between 40 and 90 km, for a flight time of 40 minutes. The anti-armor warhead and the operable camera on the drone allow it to serve as active reconnaissance, and an effective anti-tank weapon which can be used from further behind the front lines. The two Switchblade drones provide a longer range, military grade single-use system to destroy Russian heavy armored vehicles.

Multi-Use Systems

These systems carry larger explosive payloads, moving from handheld grenade-sized explosives of single-use systems to much larger anti-tank mines. The *R18* octocopter has allegedly struck $130M-USD-worth of Russian targets with RKG-3 anti-tank

grenades and RKG-1600 bombs. The R-18 is capable of carrying two explosives at a time, and is able to hit a target within a radius of 1 meter from a height of 300 meters. The developer, Aerorozvidka, asserts that for every dollar spent on the R18 drones, the Russian army incurs $670 in losses. At a cost of $20,000-$40,000 per unit, Ukraine still has a favorable cost differential using these systems, but cannot afford to burn through them as fast as single-use systems.

The Ukrainian produced *Punisher* drone, produced by UA Dynamics, works in tandem with U.S.-produced Switchblade drones. Unlike most loitering munitions, the *Punisher's* airframe is reused for subsequent attacks, following the release and reload of the payload at the bottom of the airframe. While the *Punisher* is not equipped with the anti-armor warhead as the *Switchblade*, the drone has proven effective at reconnaissance missions, as well as destroying munitions, light armor vehicles, infantry, and mobile control points. As of March, 2022, UA-Dynamics claims that the drones completed 60 successful missions since the invasion began [34].

Multi-use systems are frequently outfitted with thermal sensors and are able to conduct lower altitude, night-time strikes with greater payloads and avoidance of radio frequency signaling and navigation. Multi-use systems are frequently used to destroy vehicles, small fortifications, and ammunition depots [35].

While both single- and multi-use systems have intelligence-gathering capabilities, their primary function is to destroy Russian vehicles and equipment. In tandem, these two approaches to modifying non-military UAS have made drone warfare the leading anti-tank/armored vehicle tactic for the Ukrainian military [36].

Intelligence Systems

Most, if not all, drones in the Ukrainian arsenal can be used for intelligence-gathering. Ukrainian drone pilots note that they learn something new about the enemy on each flight, regardless of whether or not a target is successfully hit [37]. Drone pilots learn more about Russian asset positioning and capabilities with each launched drone, making the conflict an "interactive, two-sided competition" says Stephen Biddle, a senior fellow at the Council on Foreign Relations.

However, certain systems are used *primarily* for intelligence-gathering. This includes the Chinese-designed *Autel EVO Max 4T*, a drone with an imaging sensor that takes excellent high-quality photos. Emerging AI capabilities also allow this system to automatically detect, track, and transmit data on battlefield targets, and their

movement. However, future supply of Autel EVOs to Ukraine is threatened by China's Communist Party, which wants to halt private companies' sales to Ukraine [38].

Conclusion

Since the start of the Russian invasion in February 2022, Ukraine has made rapid advancements in both new and existing technological fronts. Ukraine worked closely with U.S. companies to gain access to satellite imagery, which has significantly reduced the time it takes for Ukrainian soldiers to receive intelligence across the front lines. This reflects a broader trend in Ukraine of increasing warfighting agility by opening channels of both vertical and horizontal communication. Vertical channels leverage widely available social media platforms to allow civilians to contribute to the intelligence cycle, as well as spread anti-Russian sentiment to Western allies. This vertical information sharing, coupled with improved horizontal information sharing within the Ukrainian Army has led to faster decision-making and more precise intelligence on the type, location, and destruction of Russian assets across the front lines. AI is being used for enemy troop and target recognition. AI-enabled autonomy is being used to counter Russian jamming of drones. Building on the previously discussed geospatial intelligence from commercial satellites and human intelligence from civilians, Ukraine is taking the information digital, and streamlining offensive and cyber-defense adaptations that have proven effective in blunting the Russian invasion.

References

[1] Julian Borger, "'Our weapons are computers': Ukrainian coders aim to gain battlefield edge," The Guardian, 18 December 2022, available at https://www.theguardian.com/world/2022/dec/18/our-weapons-are-computers-ukrainian-coders-aim-to-gain-battlefield-edge. Accessed 14 July 2024.

[2] Grace Jones, Janet Egan, and Eric Rosenbach, "Advancing in Adversity: Ukraine's Battlefield Technologies and Lessons for the U.S.," Harvard Kennedy School Belfer Center for Science and International Affairs, 31 July 2023, available at https://www.belfercenter.org/publication/advancing-adversity-ukraines-battlefield-technologies-and-lessons-us. Accessed 14 July 2024.

[3] Romina Bandura, Janina Staguhn , and Madeleine McLean, "Rebuilding and Modernizing Ukraine's ICT Infrastructure Will Be Essential to Attract Private Investment," Center for Strategic & International Studies, 2 October 2023, available at https://www.csis.org/analysis/rebuilding-and-modernizing-ukraines-ict-infrastructure-will-be-essential-attract-private. Accessed 14 July 2024.

[4] World Economic Forum, "World Economic Forum and Ukraine Agree to Work Towards Country's Digital Transformation," 18 January 2024, available at https://www.weforum.org/press/2024/01/world-economic-forum-and-ukraine-agree-to-work-towards-country-s-digital-transformation/. Accessed December 04 2024.

[5] Mykhailo Fedorov, "Ukraine's vibrant tech ecosystem is a secret weapon in the war with Russia," Atlantic Council, 17 August 2023, available at https://www.atlanticcouncil.org/blogs/ukrainealert/ukraines-vibrant-tech-ecosystem-is-a-secret-weapon-in-the-war-with-russia/#:~:text=While%20Russia%20enjoys%20overwhelming%20advantages,deeply%20rooted%20throughout%20Ukrainian%20society. Accessed 14 July 2024.

[6] Mike Butcher, "Two years since Russia's invasion, Ukraine's startups soldier on," TechCrunch, 23 February 2024, available at https://techcrunch.com/2024/02/23/two-years-since-russias-invasion-ukraines-startups-soldier-on/. Accessed December 4 2024.

[7] Abbey Fenbert and The Kyiv Independent news desk, "German drone manufacturer joins Diia City to produce drones in Ukraine," The Kyiv Independent, 9 December 2023, available at https://kyivindependent.com/german-drone-manufacturer-joins-diia-city-to-produce-drones-in-ukraine/. Accessed 14 July 2024.

[8] Sandra Erwin, "Drawing lessons from the first 'commercial space war,'" Space News, 10 May 2022, Available at https://spacenews.com/on-national-security-drawing-lessons-from-the-first-commercial-space-war/. Accessed on 23 July 2024.

[9] Amritha Jayanti, "Starlink and the Russia-Ukraine War: A Case of Commercial Technology and Public Purpose?" Harvard Kennedy School Belfer Center for Science and International Affairs, 9 March 2023, available at https://www.belfercenter.org/publication/starlink-and-russia-ukraine-war-case-commercial-technology-and-public-purpose. Accessed 14 July 2024.

[10] Dan Sabbagh, "Fury in Ukraine as Elon Musk's SpaceX limits Starlink for drones," The Guardian, 09 February 2023, available at https://www.theguardian.com/world/2023/feb/09/zelenskiy-aide-takes-aim-at-curbs-on-ukraine-use-of-starlink-to-pilot-drones-elon-musk. Accessed 04 December 2024.

[11] Julia Siegel, "Commercial satellite are on the front lines of war today. Here's what this means for the future of warfare," Atlantic Council, 30 August 2022, available at: https://www.atlanticcouncil.org/content-series/airpower-after-ukraine/commercial-satellites-are-on-the-front-lines-of-war-today-heres-what-this-means-for-the-future-of-warfare/. Accessed 04 December 2024.

[12] The Johns Hopkins University Hub, "How Geospatial Intelligence is Providing Vital Insights into Russia's Invasion of Ukraine," Hub staff report, Q&A with Michael Ard and Jack O'Connor, 14 March 2022, available at https://hub.jhu.edu/2022/03/14/michael-ard-john-oconnor-geospatial-intelligence/. Accessed 14 July 2024.

[13] Jason McGee-Abe, "One year on: 10 technologies used in the war in Ukraine," Tech Informed, 24 February 2023, available at https://techinformed.com/one-year-on-10-technologies-used-in-the-war-in-ukraine/. Accessed 14 July 2024.

[14] The Economist, "How a chatbot has turned Ukrainian civilians into digital resistance fighters," 22 February 2023, available at

https://www.economist.com/the-economist-explains/2023/02/22/how-a-chatbot-has-turned-ukrainian-civilians-into-digital-resistance-fighters. Accessed 14 July 2024.

[15] Ukraine Today, "The ePPO application has started working in Ukraine: how to notify the Armed Forces of Ukraine about a missile or a drone," Visit Ukraine blog, 27 October 2022, available at https://visitukraine.today/de/blog/1083/the-eppo-application-has-started-working-in-ukraine-how-to-notify-the-armed-forces-of-ukraine-about-a-missile-or-a-drone. Accessed 14 July 2024.

[16] Peter Suciu, "Ukraine Is Winning On The Battlefield And On Social Media," Forbes, 13 October 2022, available at https://www.forbes.com/sites/petersuciu/2022/10/13/ukraine-is-winning-on-the-battlefield-and-on-social-media/?sh=33c7be5d4008. Accessed 14 July 2024.

[17] Таїса Мельник, "Stingling Nettle- How Ukrainian Software for Gunners Affects the Course of the War," Forbes, 25 July 2022, available at https://forbes.ua/innovations/zhalyucha-kropiva-yak-ukrainske-programne-zabezpechennya-dlya-artileristiv-vplivae-na-khid-viyni-22072022-7054 . Accessed 19 July 2024.

[18] Tom Cooper, "Kropyva: Ukrainian Artillery Application," Medium, 10 June 2022, available at https://medium.com/@x_TomCooper_x/kropyva-ukrainian-artillery-application-e5c6161b6c0a. Accessed 14 July 2024.

[19] David Axe, "There's A Good Reason The Russian Air Force Is Faltering. Ukrainian Air-Defense Crews Have Better Apps." Forbes, 18 October 2022, available at https://www.forbes.com/sites/davidaxe/2022/10/18/theres-a-good-reason-the-russian-air-force-is-faltering-ukrainian-air-defense-crews-have-better-apps/?sh=474e7f897960. Accessed 14 July 2024.

[20] Sam Bendett, "Roles and Implications of AI in the Russian-Ukrainian Conflict," Russia Matters, 20 July 2023, available at https://www.russiamatters.org/analysis/roles-and-implications-ai-russian-ukrainian-conflict. Accessed 14 July 2024.

[21] Sean Gourley, "A New Era of Warfare: How AI Unlocks Intelligence from Russian Radio Chatter in Minutes," Primer AI, 4 April 2022, available at

https://primer.ai/public-sector/a-new-era-of-warfare-how-ai-unlocks-intelligence-from-russian-radio-chatter-in-minutes/. Accessed 14 July 2024.

[22] Daniel Pereira, "Ukraine is a Master Class in Cyber Defense and a Real-time AI Accelerator," Oodaloop, 19 April 2023, available at https://www.oodaloop.com/ooda-original/2023/04/19/ukraine-is-a-master-class-in-cyber-defense-and-a-real-time-ai-accelerator/. Accessed 14 July 2024.

[23] Olga Tokariuk, "Ukraine's Secret Weapon – Artificial Intelligence," CEPA, 20 November 2023, available at https://cepa.org/article/ukraines-secret-weapon-artificial-intelligence/. Accessed 14 July 2024.

[24] Dan Kobialka, "Cyber Defense Center Prioritizes Cybersecurity in Ukraine," MSSP Alert, 24 October 2023, available at https://www.msspalert.com/news/cyber-defense-center-prioritizes-cybersecurity-in-ukraine. Accessed 14 July 2024.

[25] Paresh Dave and Jeffrey Dastin, "Exclusive: Ukraine has started using Clearview AI's facial recognition during war," Reuters Technology, 14 March 2022, available at https://www.reuters.com/technology/exclusive-ukraine-has-started-using-clearview-ais-facial-recognition-during-war-2022-03-13/. Accessed 14 July 2024.

[26] David Axe, "Ukraine's AI Drones Are Making War Much Deadlier for Russia," Daily Beast, 15 January 2024, available at https://www.thedailybeast.com/ukraines-ai-drones-are-making-war-much-deadlier-for-russia. Accessed 14 July 2024.

[27] Inder Singh Bisht, "Russia to Ramp Up Kamikaze Drone Production With New Facility," The Defense Post, 29 May 2023, available at https://www.thedefensepost.com/2023/05/29/russia-kamikaze-drone-production/#google_vignette. Accessed 14 July 2024.

[28] Lyuba Balashova, "Ukrainian manufacturers have produces about 200,000 FPV drones since the beginning of this year, Ministry of Strategy and Industry", Forbes Ukraine, February 29, 2024, available at https://forbes.ua/news/ukrainski-virobniki-vipustili-blizko-200-000-fpv-droniv-z-pochatku-roku-zastupnitsya-golovi-minstrategpromu-29022024-19573. Accessed 23 July 2024.

[29] Ken Dilanian, "Kamikaze drones: A new weapon brings power and peril to the U.S. military," NBC News, 6 December 2021, available at

https://www.nbcnews.com/news/military/kamikaze-drones-new-weapon-brings-power-peril-u-s-military-n1285415. Accessed 14 July 2024.

[30] Ciaran McGrath, "Putin's nightmare as Ukraine destroys £1.65m Russian tanks with drones costing just £330," Express, 30 October 2023, available at https://www.express.co.uk/news/world/1829487/vladimir-putin-russia-ukraine-tanks-drones. Accessed 14 July 2024.

[31] Ukrinform.net, "Ukraine's Drone Army turns 220 units of Russian military equipment into scrap – minister," newsletter, 13 November 2023, available at https://www.ukrinform.net/rubric-ato/3786480-ukraines-drone-army-turns-220-units-of-russian-military-equipment-into-scrap-minister.html. Accessed 14 July 2024.

[32] Maria Kostenko, "Ukraine plans to spend $545 million on drone purchases, defense minister says," CNN, 30 January 2023, available at https://www.cnn.com/europe/live-news/russia-ukraine-war-news-1-30-23#h_534160f9954eff509fa7f2c54458fb93. Accessed 14 July 2024.

[33] Singh Bisht "Ukraine Producing More Drones Than State Can Buy," The Defense Post, 11 January 2024, available at https://www.thedefensepost.com/2024/01/11/ukraine-producing-drones-state/. Accessed 23 July 2024.

[34] Alia Shoaib, "Ukraine's army is using a nimble 'game-changing' drone called The Punisher that has completed scores of successful missions against the Russians, say reports," Business Insider, 5 March 2022, available at https://www.businessinsider.in/international/news/ukraines-army-is-using-a-nimble-game-changing-drone-called-the-punisher-that-has-completed-scores-of-successful-missions-against-the-russians-say-reports/articleshow/90015103.cms. Accessed 23 July 2024.

[35] Andrew E. Kramer, "Homemade, Cheap and Lethal, Attack Drones Are Vital to Ukraine," The New York Times, 8 May 2023, available at https://www.nytimes.com/2023/05/08/world/europe/ukraine-russia-attack-drones.html. Accessed 14 July 2024.

[36] Natalie Musumeci, "Ukraine is using $100,000 octocopter drones to destroy Russian tanks and artillery worth millions, even in the dead of night, operator says," Business Insider, 6 October 2023, available at

https://www.businessinsider.com/ukraine-using-octocopter-drones-to-destroy-russian-tanks-2023-10. Accessed 14 July 2024.

[37] Samya Kullab, Associated Press, "How Ukraine soldiers use inexpensive commercial drones on the battlefield," PBS News, 26 September 2024, available at https://www.pbs.org/newshour/world/how-ukraine-soldiers-use-inexpensive-commercial-drones-on-the-battlefield. Accessed 14 July 2024.

[38] Vitaly Shevchenko, "Ukraine fears drone shortages due to China restrictions," BBC, 21 October 2023, available at https://www.bbc.com/news/world-europe-67078089. Accessed December 04 2024.

Abbreviations and Acronyms

AI	Artificial Intelligence
CDAIC	Collective Defense AI Fusion Center
FPV	First-Person View
GEOINT	Geospatial Intelligence
IT	Information Technology
ICT	Information and Communication Technology
UAS	Uncrewed Aerial System
USD	U.S. Dollar

About the Authors

Stephen DeCoste

Stephen DeCoste is an operations research analyst in the National Security Analysis Department, at Johns Hopkins University Applied Physics Laboratory. Joining APL in the Summer of 2023, he contributed to efforts in modeling and simulation of SATCOM systems, and spearheaded T&E efforts on a project developing an LLM for use by IC analysts. Prior to his work at APL, he worked in the Center for Defense Concepts and Technology at the Hudson Institute in Washington D.C. In this role, he consulted DARPA and the Japanese Maritime Self Defense Force (JMSDF) on improving operational tempo and force posturing in the Indo-Pacific.

Expertise Areas: Operations analysis, experimentation, statistical modeling and analysis, LLM training, machine learning and NLP.

Jeffrey Miers

Dr. Miers is a senior analyst in the National Security Analysis Department, at Johns Hopkins University Applied Physics Laboratory. He joined JHU/APL in 2016 and has led numerous projects related to the intersection of emerging or future technology, operations and logistics. Prior to joining JHU/APL, Dr. Miers served as an analyst and manager at the Center for Naval Analyses (CNA) for over 23 years, beginning in 1992. At CNA, he focused on operational analyses and test and evaluation of naval weapons systems, electronic warfare capabilities, tactical data links and communications systems.

Expertise areas: Operations analysis, test and evaluation, experimentation, electronic warfare, ISR systems, intelligence analysis.

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY