Commercialized Combat: Analyzing wartime applications of non-military technologies in the war in Ukraine

Completed April 2023

Emily Beaudoin
Muhammad Najjar
Liberty Potter
Jack Shanley
Shawn Singh
David Sweeterman
Advisor: David Bonfili

COLUMBIA | SIPA
School of International and Public Affairs

Table of Contents

Executive Summary

Combatants have always sought to apply innovative technological solutions to problems on the battlefield. While great powers struggle to deploy 6th generation aircraft, hypersonic munitions, and advanced information and communications systems, fighters in Ukraine are engaged in a different kind of arms race. Since Russia's 2022 invasion of Ukraine, both forces have employed commercial technologies in novel combat roles. This report analyzes three categories of commercial technology that have featured heavily in Ukraine: software, space, and uncrewed systems. Across categories, it identifies noteworthy products and their military applications, weighs the tradeoffs between these systems and their military counterparts, and presents generalized implications for the broader conduct of future war and actionable recommendations for the U.S. Department of Defense. An analysis of technologies suggests that:

- The software applications used in the current conflict in Ukraine encourage civilian participation in the collection of military intelligence by prioritizing the agile use of and access to real-time intelligence over secrecy;

- Commercial companies choose to involve themselves in conflict primarily in response to a favorable cost-benefit assessment. This is particularly salient for space providers, both because individual platforms simultaneously serve commercial and military interests, and because most nations rely on commercial solutions in space; and

- Highly attritable, low-cost commercial uncrewed vehicles threaten the status of exquisite military systems.

Completed for participation in student Capstone project at Columbia University, presented to the National Security Innovation Network (NSIN).

Key Insights

⇒ The Ukrainian government's acceptance of the help of private partners and non-military experts has facilitated the country's ability to construct C4ISR networks on the fly, enabling a truly network-centric approach to warfare in which warfighters, civilians, intelligence officials, and weapons are digitally networked to work in tandem.

⇒ The ad-hoc modification of existing technologies in Ukraine has expanded system capabilities across the commercial-military technology continuum. Purely commercial, hybrid, and proprietary military technologies are mixed to develop on-demand solutions to emerging problems.

⇒ The proliferation of accessible commercial technologies in Ukraine encourages civilian participation in the war effort, drawing on previously untapped capabilities while also creating new questions around the definition of a legitimate target in modern war.

⇒ Sensors, analytics tools and processing algorithms that collect, intake, sort, and analyze a massive amount of data across domains and from military and civilian contributors enable sense-making of the modern battlespace and allow the constant observation of enemy forces.

⇒ The need to make it more favorable for companies to provide products and services to support state-sanctioned military operations.

⇒ The software applications in use in Ukraine encourage civilian participation in the collection of military intelligence by prioritizing the agile use of and access to real-time intelligence over secrecy.

⇒ The software applications in use in Ukraine prioritize end-user experience, simplify training, and emphasize interoperable infrastructure that is flexible to adaptations against adversarial relearning.

⇒ Commercial companies choose to involve themselves in conflict primarily in response to a favorable cost-benefit assessment. This is particularly salient for space providers, both because individual platforms simultaneously serve commercial and military interests, and because most nations rely on commercial solutions in space.

⇒ Space debris from kinetic strikes against commercial space assets will generate uncontrollable collateral damage. All orbital assets may be held at risk by a single provider's decision to contribute, or by a combatant's decision to strike.

⇒ Highly attritable, low-cost commercial UVs threaten the status of exquisite military systems.

⇒ Widely accessible commercial UVs empower organic capabilities at lower levels of the force structure.

⇒ The procurement of commercial UVs faces few barriers to entry, enabling NGOs, fighters, and individuals to support the war effort.

⇒ Modular upgrades and add-ons can introduce military-grade capabilities to commercially available systems.

Recommendations for the U.S. Department of Defense

⇒ Empower existing innovation, development, and procurement structures to react flexibly to the immediate needs of small units and individual warfighters.

⇒ Prioritize modularity and cross-compatibility among commercial and purpose-built assets. Develop universal standards for software and capability-enhancing hardware to lower barriers of entry for commercial partners.

⇒ Design contracts to allow for the rapid modification and enhancement of capabilities. Prioritize procuring capabilities over objects.

⇒ Encourage primary defense contractors to create gateways into the national security ecosystem for commercial partners.

⇒ Develop a comprehensive strategic framework to address the risks that face commercial partners interested in defense collaboration. Take advantage of non-monetary incentives to encourage involvement and retention.

1. Software Applications

Russia's invasion of Ukraine demonstrates how competitive advantages in modern warfare are partially defined by data and its processing, software applications, and the new tactics they enable. Analytic tools and processing algorithms are fundamental to sorting, analyzing, and exploiting massive inflows of data across the battlespace. U.S. operational concepts frequently depend on the ability to flexibly combine mission systems to produce more flexible kill-chain options, which is done by splicing software systems together.[1] In the bespoke world a warfighter exists in, however, it becomes difficult to apply the one-size fits all approach of commercial software developers. The software applications to be discussed demonstrate the ways in which the Ukrainian government and civilians have been able to quickly modify existing software and develop new software in the face of adversarial relearning, while remaining interoperable.

While software is incorporated across the entirety of the modern battlespace, in Ukraine, commercial technology has been brought to bear to address two often interrelated use-cases: cueing and crowdsourcing. Software applications – including **Delta**, **GIS Arta**, and **Air Alert** – are being used to inform individuals about the battlespace, known as "cueing." **E-AirDefense** (*ePPO*) and the Ukrainian e-governance app **Diia**, and its integration with the **e-Enemy** (*eVorog*) chatbot, are being used for the crowdsourcing of military intelligence, or essentially crowdsourcing for the purpose of cueing.

The selected technologies demonstrate the foremost ability of the Ukrainian government to draw on talent from the country's robust information technology (IT) sector. Delta and GIS Arta are purely military applications. But, when Russia invaded, the Ukrainian government leveraged the expertise of the commercial IT sector to rapidly develop and deploy systems and tools critical to the nation's defense. Diia's integration with e-Enemy again illustrates collaboration between government and private sector professionals to enable the swift adaptation and modification of existing government technology in wartime. Finally, eAirDefense and Air Alert exemplify the striking initiative and ingenuity present in Ukraine's IT sector and, again, the government's ability to recognize, accept, and leverage the sector.

1.2 Software for Cueing

1.2.1 Delta

Delta is "Google maps for the military," providing real-time views of the battlefield by integrating data including aerial reconnaissance, satellite images, and drone footage from sources like NATO partners and informants behind Russian lines.[2][3] The situational awareness system can be used by military troops, civilian officials, and vetted bystanders to collect, process, display, and share information about Russian forces and coordinate defense forces.[4] All of this data is subsequently embedded in layers on the Delta battlefield interface, which is kept live and accessible to its military users through Starlink satellite communications. Delta works on various devices, including laptops, tablets, and smartphones. Taken together, in a war where information and its dissemination in instantly usable form to individual

[1] Clark, Bryan, and Dan Patt. "The Post-Pandemic Military Will Need to Improvise." *Defense One*. Defense One, April 14, 2021. https://www.defenseone.com/ideas/2020/05/post-pandemic-military-will-need-improvise/165244/.

[2] Mykhailo Fedorov, "Tech innovation helps Ukraine even the odds against Russia's military might," Atlantic Council, last modified February 28, 2023, https://www.atlanticcouncil.org/blogs/ukrainealert/tech-innovation-helps-ukraine-even-the-odds-against-russias-military-might/.

[3] Lara Jakes, "For Western Weapons, the Ukraine War Is a Beta Test," *New York Times*, November 15, 2022, https://www.nytimes.com/2022/11/15/world/europe/ukraine-weapons.html.

[4] Julian Borger, 'Our weapons are computers: 'Ukrainian coders aim to gain battlefield edge," *The Guardian*, December 18, 2022 https://www.theguardian.com/world/2022/dec/18/our-weapons-are-computers-ukrainian-coders-aim-to-gain-battlefield-edge

In the early days of the invasion, Ukrainian drones tracked the advance of a Russian convoy toward Kyiv. At the same time, residents texted real-time reports to the government using the *eVorog* chatbot, integrated with the mobile application, Diia. It was Delta that then collected, analyzed, and disseminated all of this information to enable Ukraine's military to force a Russian retreat. In Kherson, Delta enabled Ukrainian troops to rapidly identify Russian supply lines to attack, leaving Russian troops increasingly isolated.

soldiers is critical to victory or defeat, Delta has given Ukrainian forces an edge over Russia.[5]

The result of a successful public-private partnership (PPP) between the Ukrainian government and a private Ukrainian organization, Delta is indigenous to Ukraine. Within the Center for Innovation and Development of Defense Technologies in Ukraine's Ministry of Defense, the system is run by staff drawn from a largely volunteer organization of drone operators and programmers called *Aerorozvidka* (aerial reconnaissance).[6] Programmers from *Aerorozvidka* built Delta in accordance with NATO standards, with some NATO assistance, meaning the system is compatible with similar solutions used by armies of NATO member states.[7] Delta has played no small role in Ukraine's success against a military superpower.[8] Since Russia's invasion, according to the Ministry of Defense, Delta helped identify 1,500 confirmed Russian targets across the country on any given day – with hundreds of them being eliminated within 48 hours.[9]

1.2.2 GIS Arta

GIS Arta is a military software that is used by the Armed Forces of Ukraine to coordinate artillery strikes. First integrated into the Ukrainian Army in May 2014 following Russia's invasion of Crimea, the advanced situational awareness system has cut the military's targeting time from 20 minutes to one.[10] Though Ukrainian programmers collaborated briefly with British digital mapping companies prior to developing the product, GIS Arta is indigenous to Ukraine.

To successfully pinpoint Russian positions, real-time data from reconnaissance drones, rangefinders, smartphones, GPS, and NATO-donated radars is fed into the system. Oftentimes referred to as "Uber for artillery," the system identifies a Russian target and quickly selects artillery, mortar, missile, or combat drones within range, similar to ride-share services locating a passenger and assigning the nearest available driver.[11] "Shooting calculator" software subsequently processes the information and determines which weapons should carry out the strike. GIS Arta operates contrary to the Russian method of firing, which traditionally involves positioning artillery batteries in a singular location. Ukrainian units can be scattered across the battlespace, threatening strikes against enemy positions from any direction. Further, the system can confuse Russian counter battery efforts by allowing for simultaneous strikes hailing from different positions.[12]

While the technology has experienced significant success, it is imperfect. In an interview, Lieutenant Colonel (U.S. Army Retired) Erik Kramer described GIS Arta as "well-known, well-liked, and well-received" and "everyone uses it" because it is "extremely effective."[13] On the other hand, Kramer noted that the system has experienced problems with Russian spoofing. GIS Arta uses passwords that change daily but are still occasionally compromised by Russian forces. Furthermore, due to the urgency to rapidly deploy the app, there are

[5] Borger, 'Our weapons."
[6] Ibid.
[7] "Ukraine unveiled its own Delta situational awareness system," Ukrainian Military Center, published October 27, 2022, https://mil.in.ua/en/news/ukraine-unveiled-its-own-delta-situational-awareness-system/
[8] Jakes, "For Western Weapons."
[9] Ibid.
[10] Charlie Parker, "Uber-style technology helped Ukraine to destroy Russian battalion," *The Times,* May 14, 2022, https://www.thetimes.co.uk/article/uk-assisted-uber-style-technology-helped-ukraine-to-destroy-russian-battalion-5pxnh6m9p
[11] Parker, "Uber-style technology."
[12] Ibid.
[13] Interview with Lieutenant colonel (ret) Erik Kramer, March 16, 2023.

limited formal methods to verify requests and minimize civilian casualties.[14] Rather, it is reportedly at the discretion of the individual commander to cross-reference requests and targets alongside available intelligence. While this effort is not formally required, it appears common, as commanders prioritize civilian safety whenever possible. Lastly, there is no system to prioritize fire requests. The lag time of a drone operator or other forward observer identifying a target, calling it in, and receiving that firing request makes a prioritization system valuable to ameliorate delays.

In a single attack in May 2022, GIS Arta helped destroy nearly an entire Russian battalion attempting to cross the Siverskyi Donets River in eastern Ukraine. In a major blow to Russian ambitions in the Donbas, Ukraine destroyed upwards of 70 tanks, armored fighting vehicles, and personnel carriers attempting to cross a pontoon bridge. The Ukrainian military employed GIS Arta alongside a number of tools to orchestrate the attack. While figures such as the total number of identified targets are classified, system programmers confirmed to *The Times* that "information related to Siverskyi Donets events were present in the GIS Arta system and appropriate targets were distributed to means of defeat for demolition."

1.2.3 Air Alert

Air Alert is a mobile application for civilian use that notifies users of the beginning and end of a missile strike, as well as radiation emergencies and outbreaks of street fighting.[15] A quickly-assembled team of programmers from Ajax Systems – experts in home security – and Stfalcon.com built Air Alert in a single day and developers continue to produce continuous updates. In this way, the application is indigenous to Ukraine and a product of Ukraine's existing technology sector. Within a month of the invasion, Air Alert was the most common app in Ukraine and was downloaded from Google Play over 5.72 million times in 2022.[16] In an interview, Roman Osadchuk, a Research Associate with the Digital Forensic Research Lab at the Atlantic Council, confirmed that the application remains in wide use by the Ukrainian populace.

The application filled a critical flaw in Ukrainian air-raid alarms, as the Cold War-era systems could not be heard outside of major cities or below ground in bomb shelters or subway stations. Now, when incoming air raids are detected, a government official pushes two "buttons:" one triggers the traditional sirens and the other sends a notification and siren to millions of phones across the country. In fact, the app works more quickly than traditional sirens, updating app-users before sirens sound on the streets.[17] Air Alert, which sounded 19,000 times in the first year of the invasion, bypasses phones' do not disturb functions to alert users of threats 24/7.[18,19]

1.3 Software for Crowdsourcing

1.3.1 Diia and the integration of e-Enemy (*eVorog*)

In February 2020, the Ukrainian government released a new governance mobile app, Diia, for citizens to access their national identity cards, pay taxes, and receive public services. The app gained additional traction during the COVID-19 pandemic, allowing Ukrainians to receive test results and access their vaccination records with ease. Though less common in rural areas of the country, Diia is used by more than 17 million Ukrainian citizens – approximately 40% of

[14] Interview with Lieutenant colonel (ret) Erik Kramer, March 16, 2023.
[15] Den Prystai, "From Ukrainians to Ukrainians. 5 digital tools and products created to help in wartime," October 5, 2022, https://war.ukraine.ua/articles/digital-tools-created-to-help-in-wartime.
[16] "Most downloaded Android apps in Ukraine 2022, by downloads," Statista, published Feb 1, 2023, https://www.statista.com/statistics/1029262/most-used-android-apps-ukraine/
[17] Cohen, Rebecca. "A Ukrainian Tech Company Created an App to Alert Citizens about Incoming Air Raids before the Traditional Sirens Sound." Business Insider. Business Insider, March 24, 2022. https://www.businessinsider.com/ukrainian-tech-company-alarm-app-alerts-citizens-air-raids-2022-3.
[18] Drew Harwell, "Instead of consumer software, Ukraine's tech workers build apps of war," *The Washington Post*, March 24, 2022, https://www.washingtonpost.com/technology/2022/03/24/ukraine-war-apps-russian-invasion/
[19] John Leicester, "Mark Hamill lends 'Star Wars' voice to Ukrainian air-raid app," March 28, 2023, https://apnews.com/article/russia-ukraine-star-wars-luke-hamill-app-08ec03bf1a2c9c0378857090079f00f9

the population.[20,21] Diia represents an example of the adaptation and modification of existing technology at the outbreak of the war. Following Russia's invasion in March 2022, the Ministry of Digital Transformation, with the support of private-sector teams, launched a new chat-bot feature over Diia: e-Enemy (eVorog). The interface itself is hosted on Telegram, a popular encrypted messaging platform. The feature allows Ukrainian citizens to crowdsource information on Russian troop movements and corroborate evidence of alleged war crimes.[22,23] The chatbot guides users through a list of questions to ascertain what they saw, where, and when, while the satellite navigation system of the user's smartphone confirms the location. [24] The information supplied through eEnemy is then matched with other military sources. In unoccupied Ukraine, civilians use eEnemy to report the location of unexploded bombs and other munitions.[25] Because eEnemy requires users to log in to Diia and authenticate themselves via the e-passport system, the Ukrainian government knows it is a real person sending the information and not a Russian bot. Notably, the aforementioned Delta system also integrates with eEnemy. As of December 2022, the app had received more than 450,000 reports, though the exact figure of strikes that have been enabled by the function has not been made public for security reasons. [26]

While the crowdsourcing of military intelligence is not new, eEnemy appears to be the first government-developed technology of its kind. Furthermore, the Ministry of Digital Transformation enabled its rapid development and deployment by collaborating with the commercial technology sector. The strategy is ubiquitous across the Ministry's work, as many teams cooperate with the Ministry, so many that sometimes you don't know exactly who or what entity was the initial initiator of this idea.[27]

1.3.2 E-AirDefense (ePPO)

The E-AirDefense (*ePPO*) mobile application allows every citizen of Ukraine to participate in the defense of the country's air space by informing the Air Defense Forces of Ukraine about Russian cruise missile trajectories, kamikaze drones, or enemy aircraft.[28] The application is indigenous to Ukraine, developed and tested over the course of five months by civilian Ukrainian developers in collaboration with military and government officials.[29]

To use E-AirDefense, Ukrainians simply install the app on their smartphone and authorize their identity through Diia. When an air target is spotted, the user opens the E-AirDefense app, selects the type of air target, points their smartphone in the direction of the target, and presses the button shown on the screen. Defense specialists then receive a location report, which supplements information from military radars.[30] Like eEnemy, the app only works in conjunction with the Diia app, meaning, in theory, it cannot be used by non-citizens.[31]

While experts attest that E-AirDefense has played a valuable role in Ukraine's layers of defense, it is considered a complement to other, more advanced, targeting technology. To this end, E-AirDefense is particularly valuable in

[20] Vera Bergengruen, "How Ukraine Is Crowdsourcing Digital Evidence of War Crimes," *TIME Magazine*, April 18, 2022, https://time.com/6166781/ukraine-crowdsourcing-war-crimes/
[21] Sabbagh, "Ukrainians use phone app."
[22] Yaroslav Druziuk, "A Citizen-like chatbot allows Ukrainians to report to the government when they spot Russian troops — here's how it works," *Business Insider*, April 18, 2022, https://www.businessinsider.com/ukraine-military-e-enemy-telegram-app-2022-4
[23] Bergengruen, "How Ukraine Is Crowdsourcing."
[24] "How a chatbot has turned Ukrainian civilians into digital resistance fighters."
[25] Ibid.
[26] Ibid.
[27] Interview with Iryna Supruniuk, April 18, 2023
[28] Oleg Danylov, "ePPO – a mobile application for informing about cruise missiles and kamikaze drones," Mezda Media, October 14, 2022, https://mezha.media/en/2022/10/14/eppo-a-mobile-application-for-informing-about-cruise-missiles-and-kamikaze-drones/
[29] Dan Sabbagh, "Ukrainians use phone app to spot deadly Russian drone attacks," *The Guardian,* October 29, 2022, https://www.theguardian.com/world/2022/oct/29/ukraine-phone-app-russia-drone-attacks-eppo
[30] Danylov, "ePPO."
[31] Sabbagh, "Ukrainians use phone app."

crowdsourcing data on the origin and trajectory of an attack, which allows Ukraine to monitor its low-level airspace continuously, something it otherwise does not have the equipment to do.[32] To date, the app has been credited with helping to shoot down previously undetected drones and Kalibr cruise missiles. The Shahed-136, an armed drone made by Iran and used by Russia to attack Ukrainian infrastructure, cruises slowly at low altitudes and is often spotted by civilians.[33] The exact figure, however, has not been made public for security reasons.

1.4 Observations

The software applications in use in Ukraine encourage civilian participation in the collection of military intelligence by prioritizing the agile use of and access to real-time intelligence over secrecy.

The integration of war-time tools with widely used, existing smartphone applications encourages the civilian collection of military intelligence. Understanding the importance of real-time intelligence in a theater of war in which belligerents remain under constant observation, the Ukrainian government prioritizes a high-quantity of crowdsourced intelligence over perhaps higher-quality intelligence collected via more traditional methods. This sort of active civilian participation in conflict creates new questions about the definitions of a combatant.

The software applications in use in Ukraine prioritize end-user experience, simplify training, and emphasize interoperable infrastructure that is flexible to adaptations against adversarial relearning.

The gamification of the user interface of applications like E-AirDefense and eEnemy in Ukraine has made evidence and intelligence gathering intuitive for civilians.[34] eEnemy, for example, greets users with options illustrated by icons of helmets and targets. After the user reports Russian troop movements, a reward of a fixed-arm emoji displays with the message: "Remember, each of your shots in this bot means one less enemy."[35] This style of user interface encourages and enables civilian participation in intelligence collection, but is in direct opposition to the way in which the U.S. government has traditionally pursued software development for its warfighters.

> *"One of the things I love about commercial tech [in Ukraine] – and I think the Department of Defense falls short here – is that the human machine interface for commercial technology is built for consumers. We build it for some…spartan warrior who doesn't care about buttons and colors. And I think that is a terrible mistake."*
>
> Emelia Probasco, Senior Fellow, Georgetown University

[32] Sabbagh, "Ukrainians use phone app."
[33] "How a chatbot has turned Ukrainian civilians into digital resistance fighters," *The Economist*, February 22, 2023, https://www.economist.com/the-economist-explains/2023/02/22/how-a-chatbot-has-turned-ukrainian-civilians-into-digital-resistance-fighters
[34] "Ukraine crowdsourcing digital evidence of war crimes with game-like apps," TVPWorld, April 19, 2022, https://tvpworld.com/59703062/ukraine-crowdsourcing-digital-evidence-of-war-crimes-with-gamelike-apps
[35] Ibid.

2. Commercial Space Technology

In Ukraine, satellites are being used predominantly to enable communications and sensing, two critical components of any military operation. Communications allow for the exchange of information between units, commanders, and decision-makers, while sensing supports situational awareness through the use of imagery and geospatial intelligence. Commercial imagery satellites have been instrumental in supporting Ukrainian battlespace awareness through detection, identification, and tracking of targets as well as to support mission planning and battle damage assessments.

In regards to sensing capabilities, we focus on two of the most prominent types of satellite imagery used in Ukraine — Electro-Optical (EO) and Synthetic Aperture Radar (SAR). EO satellite systems image in bands outside of the visible spectrum through the collection of data in wavelengths. These systems are passive sensors, meaning they only operate when there is sufficient light reflected by or emitted from the target, they do not collect imagery at night, and they cannot image through cloud cover. In comparison, SAR produces an image using active sensors to record the energy reflected after interacting with the Earth. In this way, SAR is beneficial for collecting imagery regardless of time of day or weather.

While low earth orbit (LEO) based satellite constellations are not the only space-based communications networks used by the Ukrainians, they have been by far the most impactful due to the wide-spread availability, usability, and reliability of SpaceX's Starlink network. SpaceX demonstrates how battlefield innovation and adaptation can be enabled by commercial technology while also providing insight into the drawbacks of relying on commercial assets rather than dedicated military systems.

2.1 Space Technology for Communications

In the context of Russia's ongoing war in Ukraine, communications technology is being used to counter Russian military aggression and misinformation. Despite facing Russian jamming and hacking attempts, the Ukrainian military has maintained effective communication channels by adopting alternative communication systems, including encrypted messaging applications like Signal, Telegram, Twitter, and Zello, as well as using secure communications via satellite phones provided by the U.S. government.[36]

2.1.1 Starlink

Unlike most satellite internet services that operate in geosynchronous orbit, Starlink consists of thousands of small satellites operating in LEO which improves latency of data transfer. The Starlink satellites communicate with ground-based stations and user terminals to deliver high-speed, stable internet connectivity to Ukrainian government officials, military troops, and civilians.[37] As of October 2022, Ukraine had roughly 20,000 Starlink satellite terminals operating in the country.[38]

Starlink's internet connectivity has revolutionized communications in the theater of war, for both civilian and military actors. The satellite system has boosted Ukrainian efforts to battle Russian propaganda by providing uninterrupted internet access to Ukrainians in occupied territories. Connectivity is invaluable in these regions, where entire communities of Ukrainians are being told by the Russians that their

[36] Jon Bateman, "Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications," *Carnegie Endowment for International Peace*, December 16, 2022, https://carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications-pub-88657

[37] "Technology," Starlink, accessed April 17, 2023, https://www.starlink.com/technology.

[38] Craig Howiet, "The hell With It': Elon Musk Will Fund Ukraine's Starlink After All," *Politico*, October 15, 2022, https://www.politico.com/news/2022/10/15/elon-musk-will-fund-ukraines-starlink-00061982.

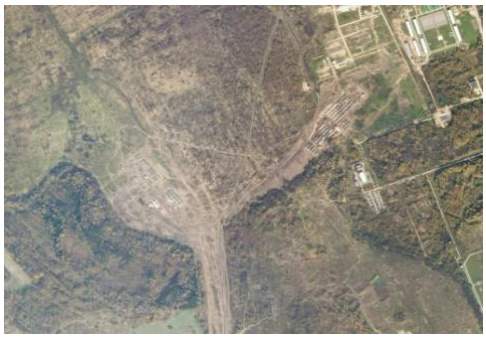
country "does not exist anymore."[39] Additionally, *Aerorozvidka*, the aforementioned Ukrainian unit that promotes creating and implementing netcentric and robotic military capabilities for the Ukrainian security and defense forces, uses Starlink to coordinate unmanned aerial vehicles (UAV) like Bayraktar TB2 drones to fire anti-tank weapons and other military vehicles.[40,41]

Starlink transformed the theater of war for the Ukrainians, but it also illustrates a cautionary tale of the reliance on singular private companies for use in a military conflict whose outcomes are traditionally dictated by governments. Given the public propagation of Starlink and its subsequent use in military operations, Russia quickly adapted threat mitigation measures. Furthermore, the specifications of Starlink's systems – such as its terminals which use a GPS unit to determine satellite priority – are publicly available, making the system particularly vulnerable to GPS jamming. Ukrainian forces have also reported degradation of service and locational targeting after using Starlink terminals, likely because Russian forces can use signals-intelligence to locate the terminals using the transmission frequency of the system.[42]

In February 2023, SpaceX founder Elon Musk grew concerned over the use of the technology in drone strikes and abruptly curtailed the use of Starlink for long-range drone strikes, a widely publicized decision. Starlink leadership subsequently explained their belief that the technology should be intended for humanitarian purposes only, as opposed to warfighting.[43] Ultimately, Musk has expressed concerns that the company could face backlash for its involvement in the conflict.[44]

2.2 Space Technology for Sensing

While the use of satellite imagery to support military operations is not a novel concept, it is an important aspect of the current conflict because, in contrast to countries like the U.S. and U.K., Ukraine does not have state-owned satellites for sensing. To this end, Ukraine relies on a combination of military and commercial imagery support for purposes including ISR, targeting, and battle damage assessment.



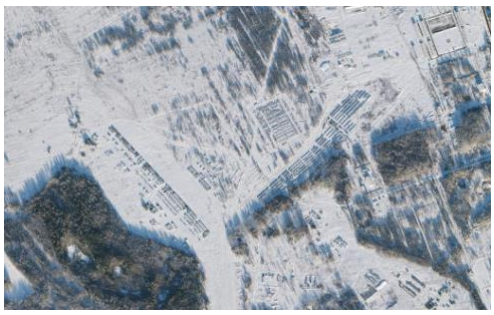


Figure 1 (top) and Figure 2 (bottom)

[39] Tasmin Lockwood, "Zelenskyy praised Elon Musk's Starlink for saving Ukraine from Russian propaganda in Wired interview," *Business Insider*, June 3, 2022, https://www.businessinsider.com/zelenskyy-musks-starlink-saving-them-from-russian-propaganda-2022-6?r=US&IR=T.

[40] Alexander Freund, "Ukraine using Starlink for drone strikes," *DW*, March 27, 2022, https://www.dw.com/en/ukraine-is-using-elon-musks-starlink-for-drone-strikes/a-61270528

[41] "Aerorozvidka," Aerorozvidka: Home, accessed on April, 18, 2023, https://aerorozvidka.ngo/.

[42] Sam Skove, "Using Starlink Paints a Target on Ukrainian Troops," *Defense One*, March 23, 2023, https://www.defenseone.com/threats/2023/03/using-starlink-paints-target-ukrainian-troops/384361/

[43] Adam Satariano, "Elon Musk doesn't want his satellites to run Ukraine's drones." *New York Times*, February 9, 2023, https://www.nytimes.com/2023/02/09/world/europe/elon-musk-spacex-starlink-satellite-ukraine.html

[44] 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/

2.2.1 Maxar Technology and Planet Labs

Figure 3

Maxar Technology and Planet Labs are commercial space companies consisting of EO satellite constellations. Maxar's constellation is capable of imaging 60% of the earth's surface monthly – or 3.8 million square kilometers daily – and can conduct intraday revisits of specific targets.[45] Similarly, Planet Labs' constellation collects over 350 million square kilometers of imagery daily and has a dataset of, on average, 1,300 images of every location on Earth's landmass.[46] Following Russia's invasion, Maxar and Planet made public comments to make imagery available to support global transparency and combat the spread of misinformation.[47,48] For example, Figure 3 represents a Maxar Technologies EO image of the buildup of Russian forces – depicting tanks and other military equipment in the Russian military's Pogorovo training area – in April of 2021.[49] Additionally, Figure 1 and 2 represent a pair of high-resolution SkySat images showing the buildup of infrastructure and vehicles by Russia between October 12 and December 29, 2021.[50] Clearly depicting a military buildup, imagery like this was used by policymakers and the media as evidence to counter Russia's claims that it had no plans to invade.

2.2.2 Capella

Capella is a commercial satellite company operating the first U.S. commercial SAR satellite.[51] On March 3, 2022, Capella Space posted a message from its CEO Payam Banazadeh stating, "Capella Space is working directly with the US and Ukrainian governments…to provide timely data and assistance around the ongoing conflict…[Capella Space] will continue to support Ukraine and its citizens during this incredibly challenging time."[52] While Capella is not sharing any of its Ukraine imagery, Figure 4 represents the capability of SAR imagery of Russia's Engels-2 Air Force Base – a strategic bomber military airbase and is Russia's sole operating location for the Tu-160 strategic bomber. Engels is a strategically significant base for the U.S. and NATO to monitor,

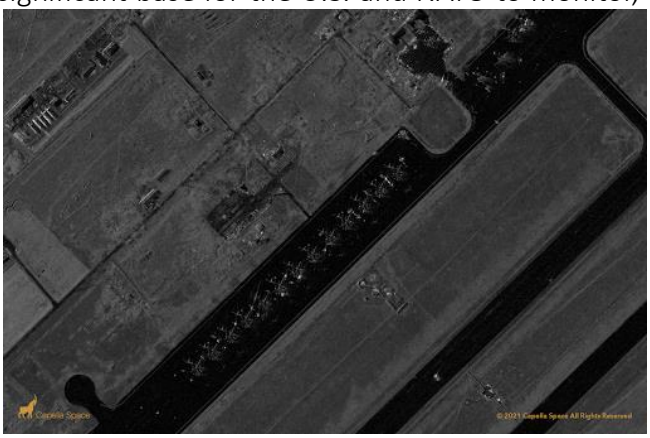


Figure 4

[45] "Constellation," Maxar: Constellation, accessed on April 2, 2023, https://www.maxar.com/constellation.
[46] "Our Constellations," Planet, accessed April 8, 2023, https://www.planet.com/our-constellations/.
[47] Remco Timmermans, "Satellite Imagery Companies in Support of Ukraine," Groundstation, March 03, 2022, https://www.groundstation.space/satellite-imagery-companies-in-support-of-ukraine/.
[48] Planet (@planet), Twitter Post, February 24, 2022, https://twitter.com/planet/status/1496893069873934337.
[49] Reuters, "Satellite Images Show Russian Military Buildup Along Ukraine Border," *Reuters*, April 20, 2021, https://www.reuters.com/news/picture/satellite-images-show-russian-military-b-idUSRTXBN4Y0.
[50] "Gallery: Military Buildup," Planet, accessed April 8, 2023, https://www.planet.com/gallery/#!/post/military-buildup.
[51] "Our Story," Capella Space, accessed April 8, 2023, https://www.capellaspace.com/about-us/our-story/.
[52] Capella Space (@capellaspace), "A Statement from Our CEO," Twitter Post, March 2, 2022, https://twitter.com/capellaspace/status/1499116124486709251.

and this image enables analysts to study the base's 3,500-meter runway and fortifications surrounding the area.[53]

2.3 Advantages of Commercially Generated Data

2.3.1 Increase Dwell Time over Specific Areas

A target is imaged only when a satellite hits a specific point in its orbit and is tasked with collecting on a specific target at a specific time. This means, depending on the system, cloud cover or adverse weather or time of day could prevent collection, or if the adversary is aware of the collection pattern and timing, then the image may be subject to denial and deception. Therefore, methods that increase imagery collection over a specific target increase the likelihood of capturing actionable and adequate imagery of a target. Here, commercial satellite companies offer a crucial advantage: they help to combat these limitations by increasing the dwell time and coverage areas over specific targets. Therefore, there is backup for government-owned systems, which is capable of enabling operations.[54,55,56]

After the Russians withdrew from the part of Kyiv they were occupying, videos began to appear on social media showing Ukrainian people who had been killed. The Russian's claimed it was disinformation and the individuals were staged; however, commercial satellite data was able to verify these posts using the date, time and location of these bodies appearing in the streets and cross referencing with imagery collected at that time.

2.3.2 Transparency and Distribution

Commercial satellite imagery companies are open about their capabilities of collection. Therefore, unlike the exquisite state-owned satellite capabilities, commercial companies are not concerned over protecting sources and methods. The unclassified nature of commercial imagery allows for transparency and ease of distribution. Commercial imagery has been used in conjunction with the reporting from government and media outlets to verify information as truthful. Thus, satellite imagery helps to bring verified information about the conflict to the global stage. Regarding distribution, since there are no concerns over sources and methods, there is no declassification process to share the imagery with partner nations and/or with the public. [57]

2.4 Observations

Commercial companies choose to involve themselves in conflict primarily in response to a favorable cost-benefit assessment. This is particularly salient for space providers, both because individual platforms simultaneously serve commercial and military interests, and because most nations rely on commercial solutions in space.

Military contracts can be a lucrative opportunity or a net loss for commercial space providers. Since the initial invasion, Planet Labs has experienced considerable fiscal growth. For Planet, the war in Ukraine has presented an opportunity to display its capabilities and be seen contributing to a just cause. The provision of Starlink is financially costly to the company, but still

[53] "Gallery: Engels-2 Air Force Base," Capella Space, accessed April 8, 2023, https://www.capellaspace.com/gallery/engels-2-air-force-base/.
[54] Werbeck, "Satellite Images."
[55] Julian Borger, "The Drone Operators Who Halted Russian Convoy Headed for Kyiv," *The Guardian*, March 28, 2022, https://www.theguardian.com/world/2022/mar/28/the-drone-operators-who-halted-the-russian-armoured-vehicles-heading-for-kyiv.
[56] Nicole Werbeck, "Satellite Images Show 40-Mile-Long Russian Military Convoy Nearing Kyiv," *NPR*, February 28, 2022, https://www.npr.org/sections/pictureshow/2022/02/28/1083650286/satellite-images-show-40-mile-long-russian-military-convoy-nearing-kyiv. Image
[57] Marisa Torrieri, "How Satellite Imagery Magnified Ukraine to the World," *Via Satellite*, October 24, 2022, https://interactive.satellitetoday.com/via/november-2022/how-satellite-imagery-magnified-ukraine-to-the-world/.

represents an opportunity for SpaceX to advertise its functionality in high-stress environments. The company threatened to withdraw its services after failing to secure DoD funding, but backed down in response to public backlash.

In future crises, space providers will seek to balance the financial and immaterial benefits of involvement with the costs and risks of contribution. Occasionally they will get the balance wrong, requiring a nimble response from the governmental actors that rely on commercial space systems for combat. In future conflicts against opponents with considerable commercial market power, such as China, it may prove impossible to incentivize meaningful commercial contributions. To date, commercial space systems have not been kinetically engaged in response to their involvement in the conflict in Ukraine. However, these platforms are definitionally legitimate military targets.[58] The degree of military involvement needed to legitimize a strike on a commercial space platform remains up for debate. However, when commercial space providers contribute to a war effort, they inherently risk potentially catastrophic attacks against the platforms that generate their commercial revenue.

The cost-benefit calculation in Ukraine is simplified by the public popularity of Ukraine's defensive effort. By definition, commercial space providers rely chiefly on the civilian market to generate revenue. Investors, shareholders, and non-military customers may shy away from corporations with sizable defense portfolios, especially if future conflicts are not perceived to be as one-sidedly just as the war in Ukraine.

Space debris from kinetic strikes against commercial space assets will generate uncontrollable collateral damage. All orbital assets may be held at risk by a single provider's decision to contribute, or by a combatant's decision to strike.

The majority of satellites in orbit today are commercially owned, and most of these operate in low-earth orbit. If any platform is committed to combat and then damaged or destroyed by anti-satellite weaponry, its debris will jeopardize nearby systems. The risk of uncontrollable collateral damage will fuel new trends regarding the military use of commercial space platforms. Commercial providers could seek to collectively demilitarize commercial space, or establish norms discouraging militarization to preserve their systems. Combatants may respond to their mutual vulnerability in orbit by prioritizing non-kinetic cyber and electromagnetic attacks in space, or they may strive to limit their own reliance on space while seeking indiscriminate orbital damage.

[58] Department of Defense, *Department of Defense the Law of War Manual,* Washington DC: Department of Defense June 2015 (Updated December 2016)

3. Uncrewed Vehicles

The widespread use of UVs has become a defining characteristic of the ongoing war in Ukraine, but the military application of UV technology is not new. Drones such as the American-made AQM-34 Firebee flew over 34,000 operational surveillance missions in support of the Vietnam War between 1964 and 1975, became a symbol of the Global War on Terror, and remain a staple asset in most modern militaries.[59] Across battlefields in Ukraine today, UV-innovation derives from commercially-available systems, not advanced military platforms. For the first time in any interstate conflict, UV systems never intended for battle have been pressed into service at scale.

Throughout the war, both Russia and Ukraine have leveraged commercial UV platforms to pursue basic military objectives. Most commercial UV missions in Ukraine fit into three broad categories: ISR, kinetic strike, and logistics support. The Ukrainian government has prioritized the development of indigenous UV research, development, and manufacturing capabilities. Kyiv plans to spend $450 million on new drones in 2023, and not just only for needs related to aerial reconnaissance.[60] Ukrainian's private and public sectors assemble hobbyist parts, produce rudimentary copies of foreign commercial products, and modify off-the-shelf platforms for combat.[61] To date, efforts to develop more advanced systems domestically remain in the research and development (R&D) phase, and are unlikely to progress without considerable international funding and technical support.[62] Though domestic R&D efforts are lagging, Ukrainian forces have mastered the ad hoc modification of commercial UVs. In conjunction with other commercial technologies like 3D-printers and basic electronics, Ukrainians enable simple quadcopter designs to deliver ordnance, transform DIY kits into improvised loitering munitions, and repurpose legacy munitions for use by UVs.

UVs are a common feature of today's technological landscape, commercial or otherwise. Without human operators, Uncrewed Aerial Vehicles (UAVs), Uncrewed Ground Vehicles (UGVs), and Uncrewed Surface Vehicles (USVs) fulfill various military and nonmilitary duties while limiting risk to military personnel. Often controlled by a remote operator, UVs can also travel via a pre-programmed route or with the help of onboard guidance sensors.[63] Truly autonomous AI-powered UVs are still in their infancy, but the technology has matured to the point of becoming a salient policy concern.[64]

Combat-capable UVs broadly fit into three categories: **purpose-built military systems**, **commercial platforms,** and **dual-use technologies**. Purpose-built military UVs common to Ukraine include the **Turkish-made Bayraktar TB2**, the American **AeroVironment Inc. Switchblade** series, **Iranian-made Shahed 131**, and the **Russian Orlan-**

[59] "1960s AQM-34 Ryan Firebee (USA)." PBS. Accessed April 4, 2023. https://www.pbs.org/wgbh/nova/spiesfly/uavs_09.html

[60] Adamowski, Jaroslaw. "Ukraine Plans to Spend $540 Million on Drones This Year." Defense News. February 1, 2023. https://www.defensenews.com/unmanned/2023/02/01/ukraine-plans-to-spend-540-million-on-drones-this-year/.

[61] Interview with Audi Rana, April 1, 2023

[62] Ibid.

[63] Ball, Mike. "This New Drone Guidance System Provides 360-Degree Situational Awareness Inertial Sensor Could Help the Military's Next-Gen Aircraft Navigate Without GPS Satellites." Unmanned System Technology. June 13, 2019. https://www.unmannedsystemstechnology.com/2019/06/new-drone-guidance-system-provides-360-degree-situational-awareness/

[64] Farge, Emma. "U.N. Chief Urges Action on 'killer Robots' as Geneva Talks Open." Reuters. December 13, 2021. https://www.reuters.com/world/un-chief-urges-action-killer-robots-geneva-talks-open-2021-12-13/.

10.[65,66,67] Although military UVs are generally less costly than comparable military platforms, these systems are almost always more expensive than their commercial counterparts. Designed specifically for military use, these platforms feature relatively sophisticated capabilities. Dual-use systems are intended for both military and nonmilitary applications. UV manufacturers may offer truly "dual-use" platforms like the Draganfly Commander2 – which are sold directly to both militaries and corporations – or military-only modifications of commercial products like the Skydio X2D.[68] These systems are commonly smaller than purpose-built military products. Although they offer excellent flight characteristics, advanced sensors, and powerful software, they lack combat features like munitions pylons or advanced electronic warfare countermeasures (ECM). Through government funding or private donations, Skydio and Draganfly products have been delivered to Ukrainian forces since February 2023.[69] Commercial UV platforms were built purely for the industrial, agricultural, and hobbyist markets. These systems range dramatically in their capabilities; some are comparable to dual-use platforms, while others offer considerably lower performance. Chinese-made DJI UVs are ubiquitous on both sides of the war.[70] Commercially available DIY UV kits are also common.

In the early days of the war, drone-provided reconnaissance helped in spotting and ambushing Russian convoys near Kiev. On April 6, 2022, dramatic footage captured a lone Ukrainian tank ambushing an entire column of Russian armored vehicles in Nova Basan – less than 50 miles west of the capital city – destroying several of them and forcing others to retreat.

3.1 Intelligence, Surveillance, and Reconnaissance

UVs equipped with cameras and other sensors regularly collect information about enemy positions and activities. Some platforms gather data in real-time, while others store information on board for later analysis.[71] ISR platforms inform deployments and maneuvers to direct fire. In both contexts, commercial UVs have had an outsize impact in Ukraine.[72] At the unit level, small commercial drones identify targets and correct fires from mortars, artillery, and other indirect-fire weapons.[73] In conjunction with Mk-19 or AGS-series automatic grenade launchers, UVs enable small Ukrainian units to independently produce highly effective indirect fires.[74] At the operational level, UVs identify command and control (C2) infrastructure, supply routes, and logistical hubs for targeting by Ukrainian artillerymen.[75] By correcting shots, commercial UVs dramatically increase the lethality of indirect-fire weapons available to the average artillery unit. In a conflict often characterized by artillery duels, widely available commercial UAVs have proven to be an

[65] Stein, Aaron. "The TB2: The Value of a Cheap and "Good Enough" Drone." The Atlantic Council. August 30, 2022. https://www.atlanticcouncil.org/content-series/airpower-after-ukraine/the-tb2-the-value-of-a-cheap-and-good-enough-drone/

[66] Mehta, Aaron. "AeroVironment Upgrades Switchblade 300 with Extended Endurance." Breaking Defense. March 29, 2023. https://breakingdefense.com/2023/03/aerovironment-upgrades-switchblade-300-with-extended-endurance/

[67] Mitzer, Stijn, and Jakub Janovsky. "Attack On Europe: Documenting Russian Equipment Losses During The 2022 Russian Invasion Of Ukraine." Oryx. February 24, 2022. https://www.oryxspioenkop.com/2022/02/attack-on-europe-documenting-equipment.html.

[68] "Military Drones," n.d. https://www.skydio.com/defense.

[69] "Skydio Soars Into 2023 as It Meets Critical Infrastructure Need." Skydio. February 27, 2023. https://www.skydio.com/blog/skydio-raises-230-million-series-e-funding-round.

[70] Myre, Greg. "A Chinese Drone for Hobbyists Plays a Crucial Role in the Russia-Ukraine War." NPR. March 28, 2023. https://www.npr.org/2023/03/21/1164977056/a-chinese-drone-for-hobbyists-plays-a-crucial-role-in-the-russia-ukraine-war

[71] C4ISRNet. "Drone Advances in Ukraine Could Bring New Age of Warfare," January 5, 2023. https://www.c4isrnet.com/battlefield-tech/2023/01/05/drone-advances-in-ukraine-could-bring-new-age-of-warfare/.

[72] Interview with Eric Kramer, March 10, 2023

[73] Interview with Michael O'Hanlon, April 5, 2023

[74] FUNKER530- Veteran Community & Combat Footage. "Ukrainian Troops Use Automatic Grenade Launcher as A Mortar." YouTube, July 19, 2020. https://www.youtube.com/watch?v=CW68aPsFC_Q.

[75] Lister, Tim, Frederik Pleitgen, and Konstantin Hak. "Drones, Tablets, Cigarettes: How Ukraine's Reconnaissance Warriors Pinpoint the Enemy." CNN. January 30, 2023. https://www.cnn.com/2023/01/30/europe/ukraine-drone-operators-forest-kreminna-intl-cmd/index.html.

effective substitute for precision-guided munitions. Given the persistent scarcity of artillery rounds and precision weapons on both sides (but particularly Ukraine) accuracy facilitated by UAV-assisted targeting improves combat effectiveness and eases logistical constraints.

The collection of data on Russian troop movements and static defenses is another common ISR mission for UVs. At the tactical level, small units use cheap UVs – often equipped with infrared imaging sensors – to find individual enemies in cover or weak points in defensive positions.[76] Tactical aerial reconnaissance and artillery spotting was once an extraordinarily precious resource available only to select units after achieving air superiority.[77] Today, soldiers on both sides of the conflict buy their own Mavic-style platforms or are gifted in online crowdsourcing donations. Ukrainian government websites such as UNITED24 collect donations and transfers funds directly to the account of the Defense Ministry.[78] At the strategic and operational levels, UVs collect data to identify new Russian offensives and locate opportune areas for a counterattack. In February 2023, Ukraine's Defense Minister Oleksiy Reznikov emphasized the importance of ISR for the Ukrainian military. He announced a plan to spend $450 million on building the capability, noting a new contract with the German dual-use UV firm Quantum-Systems for 105 of their Vector reconnaissance drones.[79]

On February 28, 2023, an opposition group in Belarus known as BYPOL claimed responsibility for a UAV attack on a Russian Air Force Beriev A-50 Airborne Early Warning and Control (AWACS) Aircraft at Machuilshchy airfield near Minsk. The improvised loitering munition flew over the airfield without being intercepted, and managed to successful damage a $330 million aircraft. Explosive-laden USVs constructed from commercial components threatened several Russian warships in Sevastopol.

3.2 Kinetic Strike

Both Russian and Ukrainian forces use UVs to attack enemy infantry, vehicles, and defensive positions. Purpose-built military UVs can carry missiles, bombs, electronic warfare (EW) pods, or any payload typical of military aircraft. With simple hardware and surplus ordnance, fighters in Ukraine quickly and cheaply militarize commercial UVs. Commercially available quadcopters are sometimes equipped with simple locally-made weapons pylons to facilitate the delivery of ordnance. Other platforms are mated with explosives and transformed into improvised loitering munitions. Commonly dubbed "suicide drones," these UVs navigate to a target before self-detonating. Originally, UVs featured only basic modifications and were restricted to inaccurately lobbing Molotov cocktails and unmodified hand grenades.[80] Today, Ukrainian forces pair 3D-printed fins and locally-modified impact fuses with Russian-pattern 30mm and Western-pattern 40mm grenades for a considerably more potent payload.[81] These weapons follow a more predictable trajectory after they are dropped, and some variants – like the American-made 40mm High Explosive Dual Purpose (HEDP) grenade – enable even the smallest quadcopters to engage light armor.[82] Larger commercial UVs have since

[76] Forces News. "Dramatic Footage Appears to Show Ukrainian Drones Targeting Russian Navy," November 2, 2022. https://www.youtube.com/watch?v=ELVbTCCuaW8.
[77] Bisht, Inder Singh, and Inder Singh Bisht. "Ukraine Seeks to Crowdsource 'Thousands of Drones' for Battlefield." *The Defense Post*, August 31, 2022. https://www.thedefensepost.com/2022/08/31/ukraine-drone-project-expansion/.
[78] Kossov, Igor. "A Game of Drones: Ukraine Builds up UAV Fleet." *Kyiv Independent*, March 29, 2023. https://kyivindependent.com/a-game-of-drones-ukraine-builds-up-uav-fleet/.
[79] Adamowski, Jaroslaw. "Ukraine Plans to Spend $540 Million on Drones This Year." *Defense News*. February 1, 2023. https://www.defensenews.com/unmanned/2023/02/01/ukraine-plans-to-spend-540-million-on-drones-this-year/.
[80] Kesslen, Ben. "Ukrainians Develop Drone That Drops Molotov Cocktails." *New York Post*, March 10, 2022. https://nypost.com/2022/03/10/ukrainians-develop-drone-that-drops-molotov-cocktails/.
[81] "Ukraine Army 3D Prints Ad hoc Battlefield Weapons « Fabbaloo." *Fabbaloo*, May 2, 2022. https://www.fabbaloo.com/news/ukraine-army-3d-prints-adhoc-battlefield-weapons.
[82] John Pike. "M433 40mm Cartridge High-explosive dual purpose (HEDP)/" Federation of American Scientists. January, 9, 1999. https://man.fas.org/dod-101/sys/land/m433.htm

been modified to deliver significantly larger payloads, including 82mm mortar shells.[83] Improvised loitering munitions are a newer development. These range in size and payload from small, anti-personnel platforms for harassing entrenched infantry to larger systems armed with 85mm PG-7-pattern high-explosive anti-tank (HEAT) warheads for engaging armored vehicles.[84, 85]

For now, there is insufficient data to ascertain the overall combat record of commercial UV strikes during this conflict. Although UVs are far more lethal as artillery spotters, the ubiquity of footage depicting successful attacks on personnel and equipment suggest that commercially-enabled kinetic strikes produce some noteworthy material and psychological effects in battle.[86] Improvised loitering munitions and other uncrewed suicide drones have featured in several high-profile missions since the invasion.

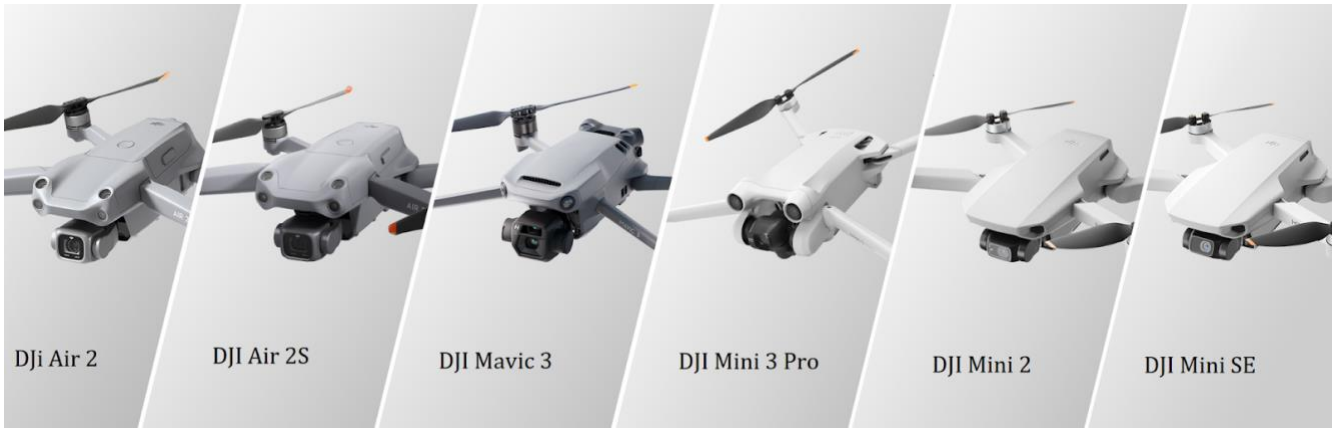
These attacks are not only valuable for killing and terrifying enemy forces – they produce valuable media products that reinforce Ukraine's "resilient resistance" narrative. Since the opening days of the invasion, Ukrainian troops have published footage of drone strikes to demonstrate their unwavering resolve and to appeal for international assistance. The videos are commonly used in online funding campaigns and equipment donation drives.[87]

3.2 Logistics

To keep warm during the winter months, Ukrainian soldiers consume a high quantity of sugar and other sweet snacks. On January 13, 2023 a video showed quadcopter drones successfully delivering a jar of sugar to soldiers in trenches holding the frontline against the Russian adversaries.

Small-scale initiatives indicate that efforts to improve supply chains with UVs are underway in Ukraine. At the unit level, some soldiers use the same systems that drop ordnance to deliver small quantities of food or other goods to the front.[88] Limited-scale initiatives have sought to develop more significant capabilities. SYPAQ, an Australian engineering corporation, has transferred an unknown number of Corvo Precision Payload Delivery Systems (PPDS) to Ukraine.[89] These disposable systems combine extremely low-cost construction materials like waxed cardboard with sophisticated inertial navigation system (INS) and GPS guidance software, and are advertised as a solution to deliver ammunition and medical supplies to frontline fighting positions.[90] Although the systems are specifically intended for government use, nearly all components would be commercially available. Another small-scale initiative mates Draganfly UVs with a climate-controlled cargo payload manufactured by

[83] Kesteloo, Haye. " DJI Matrice 300 RTK Used by Ukrainian Defense Forces to Drop Mortars." Drone XL. June 10, 2022. https://dronexl.co/2022/07/10/dji-matrice-300-ukrainian-forces-mortars/.
[84] Crumley, Bruce. "Ukraine Reportedly Assembles Half of Its 1,000 FPV Drone Fleet for Attacking Russian Targets." DroneDJ. March 1, 2023. https://dronedj.com/2023/03/01/ukraine-reportedly-assembles-half-of-its-1000-fpv-drone-fleet-for-attacking-russian-targets-video/.
[85] Kesteloo, Haye. "Ukraine Uses FPV Drones with Makeshift RPG-7 Explosives to Target Russian Tanks." DroneXL. February 1, 2023. https://dronexl.co/2023/02/01/ukraine-fpv-drones-rpg-7/.
[86] Interview with Eric Kramer, March 10, 2023
[87] Greg, "A Chinese Drone for Hobbyists Plays a Crucial Role in the Russia-Ukraine War."
[88] "A #Ukrainian Drone Delivers a Jar of Sugar to Soldiers at Their Positions." NEXTA. January 11, 2023. https://doi.org/Twitter.
[89] Hambling, David. "Paper Planes? Ukraine Gets Flat-Packed Cardboard Drones from Australia." Forbes. March 6, 2023. https://www.forbes.com/sites/davidhambling/2023/03/06/paper-planes-ukraine-gets-flat-packed-cardboard-drones-from-australia/
[90] McFadden, Christopher. "Ukraine Is Using Cardboard Drones to Do Battle with Russia Now." Interesting Engineering. March 27, 2023. https://interestingengineering.com/innovation/australia-ukraine-cardboard-drones.



Coldchain Delivery Systems.[91] These allow Ukrainian forces to deliver blood and other temperature-sensitive medical supplies to units in need. UVs offer clear potential as tools to deliver supplies to the front, but both sides of the conflict have thus-far been unwilling or unable to institutionalize this mission set. It is practically impossible to move any meaningful fraction of the ammunition and supplies consumed each day in Ukraine with UVs featuring payloads of no more than 30kg.[92] Although UV technology – commercial or otherwise – is not ready to contribute to an army's logistical needs, these systems can have an effect at the margins. In the static trench warfare that defined the conflict during the war's first winter, it was relatively easy to know the location of friendly forces in need of resupply. There, small resupplies were possible with today's technology, and small deliveries could be critical in some situations.

3.3 Commercial Systems Analysis

Commercial systems offer significant advantages and drawbacks as improvised weapons of war. Widely available, relatively inexpensive, and easy to use, commercial platforms are highly accessible for the average soldier. Commercial UVs are radically less expensive than comparable purpose-built military systems. Common commercial quadcopters in Ukraine range in price from several hundred to several thousand dollars. The Black Hornet – a small purpose-built ISR UAV donated to Ukraine – costs approximately $60,000 per unit.[93,94] The hobbyist kits that are assembled in Ukraine to create modified loitering munitions typically cost $1,000 per unit.[95] AeroVironment Inc's Switchblade-series loitering munitions, another purpose-built system found in Ukraine, are estimated to cost $6,000 to $70,000 per unit.[96,97] Additionally, because commercial systems were not intended to be weaponized, they are exempt from International Traffic in Arms Regulations (ITAR) and other trade restrictions.[98] Therefore, individuals and non-state actors can

[91]Singh, Ishveena. "Canadian Draganfly Drones to Deliver Medical Supplies in War-Torn Ukraine." DroneDJ, March 24, 2022. https://dronedj.com/2022/03/22/canada-draganfly-drones-deliver-medical-supplies-ukraine/.

[92]Sylvia Pfeifer and Patricia Nilsson. "Ammunition supply chain crisis: Ukraine war tests Europe in race to rearm" Financial Times, February, 7, 2023. https://www.ft.com/content/ea5b48b1-61e6-4c91-8778-4cc2edaff0ca

[93] "Norwegian-Developed Drone to Ukraine." Government.no, n.d. https://www.regjeringen.no/en/aktuelt/droner/id2924942/?fbclid=IwAR0-lEUzOY5c5gorr6nY0-xBcqyGfgpCzzWQxb55Xgg9OniVOkKThv1Fumw.

[94] Atherton, Kelsey. "The Black Hornet Became Indispensable. Now the UK Is Ordering More." C4ISRNet, August 19, 2022. https://www.c4isrnet.com/unmanned/2019/04/18/black-hornet-drones-return-to-the-uk/.

[95]"Serial Production of FPV Drones." *Hero of Ukraine*, February 24, 2023. https://heroesukraine.org/en/serial-production-fpv-drones/.

[96] Root, Al. "Drone Maker's Stock Jumps on U.S. Assistance to Ukraine," March 16, 2022. https://www.barrons.com/articles/drone-maker-stock-ukraine-military-aid-51647457722.

[97] The Kyiv Independent news desk. "Switchblade Drones Included in $800 Million US Weapons Package." Kyiv Independent, June 23, 2022. https://kyivindependent.com/switchblade-drones-included-in-800-million-us-weapons-package/.

[98] Interview with Audi Rana, Apr 1, 2023

easily acquire unrestricted commercial UVs, which are then easily supplied to the forces that need them, who can quickly militarize them on demand. When DJI announced a secession of sales in Russia and Ukraine, both sides continued to buy systems from third parties in other countries.[99]

Commercial UVs are easy to operate. Ukrainian forces learn to fly quadcopters under combat conditions in just one week. Improvised loitering munitions are somewhat more difficult to operate, but still require only three weeks of training.[100,] [101]While purpose-built loitering munitions like the AeroVironment Switchblade are as fast or faster to learn, most combat UVs like the TB2 require several months of training.[102,103]

Low-cost commercial systems are widely accessible but lack crucial security features and are easily defeated by electronic countermeasures. Unlike systems with military-grade communications components like the TB2, commercial UVs are rarely designed to operate in electronically contested environments.[104] Off-the-shelf commercial systems are regularly rendered inoperable by GPS and radio jamming equipment. Spoofing attacks can relay incorrect navigational information to GNSS-reliant UVs, causing them to crash.[105] Such threats are compounded by Russia's advanced electronic warfare capabilities, but like UVs, jamming and spoofing technologies are widely available on the commercial market.[106,107] UV operators are also vulnerable to detection, from both sophisticated electronic warfare systems, and commercially-available products like the DJI Aeroscope.[108,109] Onboard safety features that prevent commercial UV from operating near airports and other secure locations further inhibit tactical flexibility.[110] None of these hurdles are insurmountable. UV operators and their electronic adversaries are engaged in an ongoing arms race. Ad hoc software modifications can circumvent location-based geofencing and cloak operators from some forms of tracing.[111,112] Aftermarket components like Asio Technologies' NavGuard and infiniDome's GPSdome can allow otherwise vulnerable UVs to overcome jamming and spoofing.[113,114] As relatively light systems not designed for combat operations, UVs are also vulnerable to physical damage by adverse weather conditions and traditional kinetic air defenses. If detected, low-flying quadcopters are easily defeated by anti-aircraft cannon and small arms fire.

All UVs in Ukraine face extraordinary attrition rates, reaching ninety percent in December 2022.[115] In Ukrainian service, quadcopters survive an average of 3 sorties before

---

[99] Crumley, Bruce. "DJI Drones Still Flowing to Russia despite April Suspension of Sales [Report]." DroneDJ, February 20, 2023. https://dronedj.com/2023/02/20/dji-drones-still-flowing-to-russia-despite-april-suspension-of-sales-report/.

[100] Ibid.

[101] Johnson, Kimberly. "Ukrainian Soldiers Trained in U.S. To Use Switchblade Drones." *FLYING Magazine*, April 8, 2022. https://www.flyingmag.com/ukrainian-soldiers-trained-to-use-switchblade-drones-in-u-s/.

[102]Mehta, Aaron, and Aaron Mehta. "AeroVironment Upgrades Switchblade 300 with Extended Endurance." *Breaking Defense*, March 29, 2023. https://breakingdefense.com/2023/03/aerovironment-upgrades-switchblade-300-with-extended-endurance

[103]Ukrinform, and Ukrinform. "Ukrainian Military Learning to Operate Turkish Combat Drones," September 4, 2019. https://www.ukrinform.net/rubric-defense/2773357-ukrainian-military-learning-to-operate-turkish-combat-drones.html.

[104]Sayler, Kelley. "A World of Proliferated Drones: A Technology Primer." Center for a New American Security, 2015. http://www.jstor.org/stable/resrep06394.

[105]*The Economist*. "Ukraine Is Betting on Drones to Strike Deep into Russia," March 23, 2023. https://www.economist.com/europe/2023/03/20/ukraine-is-betting-on-drones-to-strike-deep-into-russia.

[106]"Fundamentals of GPS Threats. White Paper." OSPIRINT. August, 2022.

[107]"What Is GNSS Signal Spoofing- Spirent," n.d. https://www.spirent.com/assets/white-paper-gnss-signal-spoofing.

[108] Skove, Sam. "How Ukraine Learned to Cloak Its Drones from Russian Surveillance." *C4ISRNet*, October 17, 2022. https://www.c4isrnet.com/battlefield-tech/2022/10/17/how-ukraine-learned-to-cloak-its-drones-from-russian-surveillance/.

[109]Northrop Grumman. "Busting Myths about Military Technology and the Electromagnetic Spectrum- Northrop Grumman," April 18, 2022. https://www.northropgrumman.com/what-we-do/busting-myths-about-military-technology-and-the-electromagnetic-spectrum/.

[110]Sayler, "A World of Proliferated Drones."

[111] Ibid.

[112]Skove, Sam. "How Ukraine Learned to Cloak."

[113]Asio Technologies Ltd. "NavGuard- Asio Technologies Ltd.," March 6, 2022. https://asiotech.com/navguard/.

[114]InfiniDome. "GPS DOME 1- InfiniDome," November 7, 2022. https://infinidome.com/gps-dome-1/.

[115]Axe, David. "Russia's Electronic-Warfare Troops Knocked Out 90 Percent of Ukraine's Drones." Forbes. Dec 24, 2022.

they are lost.[116] Although fixed wing systems like the TB2 are estimated to survive twice as long on average, attrition is far less costly for $2,000 quadcopters than $5 million combat TB2s. Indeed, Ukrainian tactics assume a degree of attrition in their commercial UVs that would be unsustainable for dedicated combat platforms.[117]

Other vulnerabilities derive from the nature of commercial industry. Unlike defense contractors, commercial UV manufacturers are not beholden to the national security interests of their prospective clients. In fact, some companies – especially civilian-oriented corporations – seek to minimize their association with conflict. Although ineffective, DJI's aforementioned cessation of sales in Russia and Ukraine highlights a supply-chain vulnerability inherent in commercial UV purchases. Conflict-wide geofencing is another risk so far unrealized in Ukraine. In 2017, DJI responded to ISIS's use of its UVs by geofencing large swathes of Iraq and Syria, thereby preventing any unmodified systems from flying there.[118] The company has refrained from taking this approach in Ukraine, but the risk remains for any armed force which relies on commercial UVs.[119]

Although commercial systems are less costly and more widely available than purpose-built military systems, their use complicates the establishment of reliable supply chains. Ukraine's purchases of hobbyist kits for improvised loitering munitions have strained the global market for these products.[120] A chronic shortage of microchips and other basic electronic components has bottlenecked Ukraine's domestic production of commercial UVs.[121] The global shortage of microelectronic components threatens access to purpose-built military systems too, but the threat is more acute for commercial suppliers. While national industrial policy seeks to secure access to these critical components for defense contractors, manufacturers of commercial products are unlikely to see similar relief.[122] These issues are magnified for the U.S. and its partners by China's dominant roles in the microelectronics and UV industries. DJI and other prominent commercial UV manufacturers are based in China, and are therefore beholden to the PRC. The U.S. Department of Defense (DoD) has placed DJI and similar companies on a list of "Chinese military companies," and has banned their use by DoD personnel in most cases.[123] The subcomponents used by Ukrainian domestically assembled drones are often manufactured in China, which were also banned for DoD use by Congress.[124] Although alternatives to Chinese products do exist, they are significantly more expensive and are produced in fewer numbers.[125]

The severity of these tradeoffs varies between systems. While some American-made dual-use corporations like Draganfly and Skydio are more resilient to countermeasures, they offer greater security, and feature more dependable supply chains than off the shelf quadcopters or hobbyist kits. In return, they are more expensive, less attributable, and more difficult to acquire at scale. Relative to purpose-built military systems,

https://www.forbes.com/sites/davidaxe/2022/12/24/russia-electronic-warfare-troops-knocked-out-90-percent-of-ukraines-drones/?sh=345002e0575c

[116] David, "Russia's Electronic-Warfare"

[117] Interview with Audi Rana, Apr 1, 2023

[118] Grossman, David. "DJI Deactivates Its Drones in Parts of Iraq and Syria." Popular Mechanics, November 14, 2017. https://www.popularmechanics.com/technology/robots/a26258/dji-geofences-large-swaths-of-iraq-and-syria/.

[119] "DJI Refuses to Apply Geofencing in Ukraine," March 23, 2022. https://www.uasvision.com/2022/03/23/dji-refuses-to-apply-geofencing-in-ukraine/.

[120] Juniper, Adam. "Kamikaze Drones in the Ukraine Conflict Are Causing an FPV Component Shortage." Digitalcameraworld, April 2, 2023. https://www.digitalcameraworld.com/news/kamikaze-drones-in-the-ukraine-conflict-are-causing-an-fpv-component-shortage.

[121] Interview with Audi Rana, Apr 1, 2023

[122] Hayashi, Yuka. "Pentagon to Reap Rewards From $53 Billion Chips Act." WSJ, February 28, 2023. https://www.wsj.com/articles/pentagon-to-reap-rewards-from-53-billion-chips-act-c3aaa2ca.

[123] U.S. Department of Defense. "Department Statement on DJI Systems," n.d. https://www.defense.gov/News/Releases/Release/Article/2706082/department-statement-on-dji-systems/.

[124] Ibid

[125] Interview with Eric Kramer, March 10, 2023

almost all commercial platforms present these tradeoffs.

3.4 Observations

Highly attritable, low-cost commercial UVs threaten the status of exquisite military systems.

The Russian Invasion of Ukraine has demonstrated the radical lethality of modern combat. In an environment where even expensive systems are quickly destroyed, fighters are employing systems that they *expect* to be destroyed. Despite their extraordinarily high attrition rates, commercial UVs generate significant combat power. Expensive, high performance military systems continue to offer incredible utility on battlefields across Ukraine. However, the proliferation of lethal and low-cost UVs complicates the future role of exquisite sensors and weapons. Tactical ISR increases the likelihood that high-value targets are identified and neutralized, and improvised loitering munitions now empower small, irregular forces to hold any combat system at risk. Although each individual strike is unlikely to succeed, they introduce an ever-present risk of potentially decisive attrition.

The success of commercial UVs in an offensive role has also diminished the utility of high-performance defensive systems—when individual munitions cost more than their targets, even successful engagements are a net loss. Ukrainian forces have already supplemented their network of exquisite air-defense missiles with truck-mounted heavy machine guns to engage low-flying UVs. These simple systems often use the same firearm that was fixed to Ukraine's horse drawn *tachankas* of the Russian Civil War. Armed with obsolete guns and chicken-wire barriers, fighters in Ukraine are conducting a low-tech arms race to counter commercial threats.

Widely accessible commercial UVs empower organic capabilities at lower levels of the force structure.

The proliferation of commercial UVs has enabled small units and individual fighters to acquire ISR and strike capabilities that were previously withheld at higher organizational levels. In previous conflicts, upper echelons of command would allocate precision indirect fires, airborne ISR, and tactical aerial resupply to small units as they became available. In Ukraine, fighters procure their own commercial UVs and conduct these missions independently as they see fit.

The procurement of commercial UVs faces few barriers to entry, enabling NGOs, fighters, and individuals to support the war effort.

Commercial UVs are inexpensive, unregulated, and widely available for civilian purchase. This allows non-governmental organizations and individuals to procure, modify, and transport combat-effective systems at scale. Charities, philanthropists, soldiers, and their families now individually contribute to unit-level combat power at an unprecedented scale.

Modular upgrades and addons can introduce military-grade capabilities to commercially available systems.

Some of the combat-specific drawbacks to commercial UVs (like survivability in an electromagnetically contested environment) are easily mitigated by introducing additional military-grade components. EW-resilience, high-performance guidance and navigation, other software features remain as considerable advantages for purpose-built military systems. Products like SYPAQ and infiniDome could capture the strengths of both commercial and military builds. The addon approach offers opportunities for intermediaries to deliver military capabilities

that derive largely from commercial products. Some enablers will simply integrate already-available components, while others produce the components that enable other systems

4. Insights and Implications

The Ukrainian government's acceptance of the help of private partners and non-military experts has facilitated the country's ability to construct C4ISR networks on the fly, enabling a truly network-centric approach to warfare in which warfighters, civilians, intelligence officials, and weapons are digitally networked to work in tandem.

Ukraine's civilian technology sector has been crucial to Kyiv's successful defense. The efforts are due to continue, as exemplified by the upcoming Defense Technology cluster, an initiative by four Ministries to match technology start- ups with the military to expedite innovation. The efforts are relevant to the American national security community, as Ukrainian private-public partnership strives to develop effective, inexpensive solutions to security challenges common to the United States. For example, teaming with the Ministry of Defense, Ministry of Digital Transformation, and commercial software developers focus on solutions to input ISR data to automatically queue available and appropriate weapon systems. Such efforts resemble the American Joint All-Domain Control (JADC2) project that drives for inter-service, meta-networks between legacy platforms and cutting-edge, off-the-shelf technologies.

The ad hoc modification of existing technologies in Ukraine has expanded system capabilities across the commercial-military technology continuum. Purely commercial, hybrid, and proprietary military technologies are mixed to develop on-demand solutions to emerging problems.

In 2019, Ukrainian President Volodymyr Zelensky exclaimed that Diia, which has since been adopted by Estonia, could become the "state in a smartphone." Ukraine's digital transformation, which includes the introduction of digital passports, has been among Europe's most successful. Indeed, the country's digital transformation, specifically the widespread use of Diia before Russia's invasion, has enabled the Ukrainian armed forces to crowdsource verified military intelligence from civilians immediately and with ease. Similar trends exist for commercial space and UV products. Starlink's on-the-fly EW resilience update and Geodome's modular jamming-resistant navigational components similarly enable forces to generate combat-utility from commercial products. The effective combat integration of commercial and dual-use technologies will continue to offer distinct advantages to military forces. It will be increasingly necessary to plan around these dynamics in an era of competition against digital authoritarians.

The proliferation of accessible commercial technologies in Ukraine encourages civilian participation in the war effort, drawing on previously untapped capabilities while also creating new questions around the definition of a legitimate target in modern war.

The Ukrainian government actively sought the help of private partners and non-military sources to facilitate the country's ability to conduct military operations. Despite risks of conducting business in a war-torn country, the demand for the IT, UV, and commercial space industries remains high, and because suppliers face few barriers to entry, NGOs, private firms, and civilians are empowered to support the war effort. However, the newfound reliance on commercial actors means that the personalities, policies, and goals of the private sector hold great influence over the war effort. In future conflicts, the decision of private companies to involve themselves in conflict

will depend upon: the relative popularity of the conflict, the relative business interests in the oppositional nation, and the relative physical risk of involvement (destruction of property, attacks on personnel, etc.). Since private interests may not always align with those of governments, governments must consider the actions and potential hesitations of private companies prior to adopting those services. The US government should work to incentivize commercial participation while defining the amount of risk they should accept and if their assets are legal targets as a party in the conflict.

Sensors, analytics tools and processing algorithms that collect, intake, sort, and analyze a massive amount of data across domains and from military and civilian contributors enable sense-making of the modern battlespace and allows the constant observation of enemy forces.

Ukraine's successful adoption of commercial technology is derived from its willingness to rely on open-source intelligence, prioritizing quantity over quality and enabling non-military actors to contribute. As presented throughout the report, commercial space and UV technology have been central to detecting and receiving data. Specifically, the inclusion of private sector satellite sensing increases both coverage area and dwell time. As a result, Ukraine has bolstered its ISR capabilities, has decreased the potential impacts of cloud cover for EO satellites, and decreased the potential impact of denial and deception by the adversary. Similarly, widely accessible commercial UVs empower organic capabilities at lower levels of the force structure. Though often destroyed, these systems threaten the status of exquisite military systems. Given the vast amount of open-source information, the challenge for governments is now less of who can gather data, but who is able to act on it. Rapid development and deployment of software applications aids in sorting this mass of information. Fundamental to that effort has been, and will remain, the government incentivizing then leveraging commercial technology talent in Ukraine.

In Ukraine, companies have been motivated to support state-sanctioned military operations by non-monetary incentives and favorable business conditions.

Popular opinion and Russia's relative political and economic isolation have made defense contributions palatable to the general public and consistent with commercial business development. Future conflicts may not draw so much global attention and support. Any interstate conflict involving more integrated members of the global economy would also require a more complex cost-benefit analysis. For successful future partnerships with commercial space corporations, governmental bodies must navigate two distinct issues. First, contracts must incentivize initial contributions from commercial providers. These could mitigate the kinetic and market-based risk factors associated with military operations. Second, it is also crucial to acknowledge the freedom commercial providers have to withhold or withdraw support.

5. Recommendations

Empower existing innovation, development, and procurement structures to react flexibly to the immediate needs of small units and individual warfighters.

Servicemembers are often the first to recognize problems on the battlefield, and represent a valuable resource for even the early stages of defense innovation. Ukraine generates combat power from its ability to quickly implement and amplify the good ideas of frontline fighters. Kyiv has embraced an individual-oriented, bottom-up approach to military innovation that is particularly well-suited to capitalize on novel applications of commercial technologies. Although security and standardization requirements prevent the U.S. from adopting a truly bottom-up approach, defense innovators should privilege the perspectives of end-users to identify issues and optimize usability. The widespread availability of commercial technologies has allowed Ukraine to organically identify problems and solutions as identified by warfighters, but American efforts must be more intentional. A human-centered design approach can draw on the strengths of Ukraine's bottom-up efforts while remaining compatible with the organizational structure of the U.S.

Prioritize modularity and cross-compatibility among commercial and purpose-built assets. Develop universal standards for software and capability-enhancing hardware to lower barriers of entry for commercial partners.

Standardized linkages enable a broader range of end-users to benefit from innovative technologies. When modular capability enhancers can be readily added or removed from existing platforms, commercial partners can leverage their unique strengths without facing the barriers to entry that complicate traditional defense innovation. A "plug and play" approach to commercial-military integration allows all services (and units) to cater common platforms to their specific needs. For commercial partners, modularity expands the financial opportunities posed by defense-contributions by expanding customer bases reducing the need for in-house defense expertise. This design approach also enables defense-specialists to cheaply militarize commercial technologies with add-ons.

Design contracts to allow for the rapid modification and enhancement of capabilities. Prioritize procuring capabilities over objects.

In modern combat, adversarial relearning occurs quickly. To stay ahead of the curve, procurement processes must enable rapid adaptation to occur organically. Today's defense contracts commonly grant contractors some degree of authority over deliverables even *after* they reach the end user. This approach limits the U.S. government's ability to modify, hack, and enhance capabilities on the fly. Future contracts might explicitly allow for government-driven modification beyond the initial point of delivery. Another approach reframes procurement as the purchasing of capabilities that a contractor must continue to deliver, even as political and technological landscapes evolve over time.

Encourage primary defense contractors to create gateways into the national security ecosystem for commercial partners.

Partner with defense providers to leverage their established legal and organizational infrastructures to reduce barriers to entry for commercial companies. Commercial providers offer unique advantages and capabilities, translating these into combat capabilities is costly. The establishment of secure, networked facilities that are already integrated into the defense

industrial base could help would-be partners evade the "Valley of Death" that lies between prototypes and defense contracts. Without access to existing infrastructure, defense partnership may not be worth the investment for some commercial providers, regardless of the potential market for their products.

Develop a comprehensive strategic framework to address the risks that face commercial partners interested in defense collaboration. Take advantage of non-monetary incentives to encourage involvement and retention.

Defense-collaboration introduces risks to physical assets, public relations, and international market access. A rigorous ethical framework and a strategic communications effort could mitigate the reputational threat associated with defense contracting. Insurance agreements, protection assurances, and other methods of risk transfer can incentivize commercial actors to risk cyber and kinetic attacks on their personnel, products, and facilities. Defense innovators must realistically assess threats to international market access on a case-by-case basis. Private partners with significant global investment and/or supply chain infrastructure in adversarial nations may limit the scope of potential commercial-defense integration.