

MARCH 2025

Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare

AUTHOR
Kateryna Bondar

A Report of the CSIS Wadhvani AI Center

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES | WADHWANI AI CENTER

Table of Contents

Executive Summary	1
Introduction	5
The Ukrainian Military's Strategic Vision and Technological Road Map	6
AI in Intelligence, Surveillance, and Reconnaissance	12
AI in Automatic Target Recognition	22
AI in Autonomous Navigation	28
Conclusion	36

“On the battlefield I did not see a single Ukrainian soldier. Only drones. I saw them [Ukrainian soldiers] only when I surrendered. Only drones, and there are lots and lots of them. Guys, don’t come. It’s a drone war.”

- Surrendered Russian soldier

Executive Summary

This paper examines how Ukraine is advancing AI-driven unmanned systems to reduce direct warfighter involvement while enhancing combat effectiveness. Although fully autonomous warfare remains an aspiration, significant progress has already been made in partial autonomy—particularly for aerial systems—while human oversight remains critical in engagement decisions.

KEY FINDINGS

- 1. The Ukrainian military’s objective is to remove warfighters from direct combat and replace them with autonomous unmanned systems.** This goal reflects the need to conserve a limited human force and overcome vulnerabilities such as fatigue, stress, and the limited capacity to process and fuse large amounts of data from various sources and sensors. Although not yet formalized into a written strategy, this vision unifies Ukraine’s military and defense industry around the adoption, acquisition, and rapid deployment of advanced technologies—including AI-enabled capabilities—and the expansion of unmanned systems.
- 2. Autonomy—defined by the U.S. military as a system’s ability to accomplish goals independently or with minimal supervision in complex and unpredictable environments—is not yet present on the battlefield in the war in Ukraine.** The primary reason for this is that the necessary technology—AI in particular—has not reached the required level of development. Additionally, Ukraine has no formal legislative or policy definition for “autonomy” or “autonomous weapons systems.” As a result, the Ukrainian military uses the term “autonomous systems” interchangeably with “unmanned systems,” or platforms equipped with basic autonomous functions such as navigation or targeting.
- 3. The current deployment of AI is partial in scope, enhancing certain functions and addressing some operational challenges rather than enabling full system autonomy.** AI is a foundational technology for transitioning from automated to autonomous systems, or systems that can decide how to achieve a goal rather than merely execute human-programmed algorithms. AI significantly enhances specific functions, such as drone footage analysis and target recognition, target tracking, and autonomous navigation, including last-mile navigation and sound and text analysis for intelligence extraction, where AI replaces 99 percent of human labor. While such systems may operate without direct human control, they typically do not perform the entire process of finding, selecting, and engaging targets independently.
- 4. Ukrainian forces have widely adopted small and medium first-person-view (FPV) drones as platforms that may be quickly adapted for diverse missions through modular design and interchangeable equipment.** Unlike the United States, Ukraine categorizes drones based on structural configuration, payload capacity, and propeller diameter. Initially, 7 inch FPV drones were common due to their ease of assembly, but growing operational demands have shifted preferences toward 9-10 inch quadcopters capable of carrying heavier payloads

and achieving longer ranges. Adding an improvised explosive device (IED), an IED release mechanism, various sensors, or signal relaying equipment to the same FPV platform can transform it into a kamikaze drone; a bomber; an intelligence, surveillance, and reconnaissance (ISR) system; or a relay node. This modular approach, which allows for quick adaptation to diverse missions by swapping components, makes FPV drones a flexible and scalable asset on the front line.

5. **Ukraine's defense industry is developing standalone AI-driven software that can be integrated across various platforms to expand battlefield autonomy.** This software enables key autonomous functions such as environmental perception, target recognition, and navigation, including last-mile approach to the target. It comes in standalone modules, consisting of compact chips with embedded software and sometimes cameras. These modules can be integrated into a range of platforms, from small FPV drones and long-range-strike drones to turrets mounted on unmanned ground vehicles. As a result, companies are focusing on developing separate autonomous functions while ensuring their compatibility across multiple platforms and unmanned systems.
6. **The Ukrainian defense industry is pursuing an approach of training small AI models on small datasets rather than developing large, all-encompassing models.** This approach enables fast and efficient onboard processing on the limited computing power of small and inexpensive chips, which can be quickly updated, retrained, and upgraded to adapt to changing battlefield conditions. These datasets can be collected through a company's battlefield operations or open-source data from social media. Military authorities can filter out highly relevant datasets from the Ministry of Defence's broader military dataset and allow companies to train their models in a protected military environment.
7. **Delegating target recognition to AI-enabled automatic target recognition (ATR) systems onboard unmanned platforms reduces human limitations and allows locking on to targets up to 2 km away.** By automating equipment identification and object detection, drones ease the burden on frontline personnel affected by fatigue, stress, or skill variability. Advancements have extended target recognition ranges from 300 meters to an average of 1 km in combat and to up to 2 km in optimal conditions. AI-powered software also counters decoys and camouflage, which can deceive the human eye. As adversaries refine their evasion tactics, AI-enabled ATR models require continuous, real-world data updates to maintain accuracy and adapt to evolving battlefield conditions.
8. **Autonomous navigation makes drones strikes three to four times more likely to succeed.** By removing the need for constant manual control and stable communications—both of which are vulnerable to electronic warfare and lack of operator skills—drones enabled with autonomous navigation raise the target engagement success rate from around 10 to 20 percent to around 70 to 80 percent. Although the striking precision is not very high, when Ukrainian forces expect it to be in “reasonable radius” rather than a specific point on a target, autonomous navigation reduces demand on the skill level of the operator and makes weapons systems with AI-enabled navigation accessible to a larger number of warfighters.
9. **The adoption of drones equipped with AI-enabled autonomous navigation capabilities is driving a marked decrease in overall strike costs by minimizing both drone losses**

and repeated mission attempts. As a result of more efficient mission execution, these systems can often achieve objectives using just one or two drones per target rather than eight or nine. Furthermore, the integration of fully autonomous flight—from takeoff through mission execution to landing—makes systems reusable and reduces the need for frequent equipment replenishment.

- 10. Ukrainian engineers are increasingly leveraging open-source technologies and existing computer vision models to accelerate research and development while keeping costs low.** By integrating readily available software solutions—including open-source computer vision frameworks—developers can rapidly create and deploy autonomous functions. This approach is particularly advantageous for “attritable,” or expendable, platforms, where the benefits of minimizing both per-unit and development costs often outweigh those of highly customized solutions. Additionally, open-source components facilitate faster prototyping, ongoing updates, and a collaborative development environment that draws on global research—all of which help maintain an agile edge in modern conflict scenarios.
- 11. Encrypting onboard AI software enables Ukraine to preserve its technological edge by making autonomous systems difficult to reverse engineer.** Although adversaries can replicate hardware designs in a matter of weeks, sophisticated encryption in AI-enabled software significantly slows down their efforts to develop equivalent systems. This secure software advantage allows Ukrainian forces to maintain a lead in drone autonomy. By investing in robust encryption protocols, Ukraine not only shields its critical algorithms and data but also establishes a strategic deterrent against immediate duplication, reinforcing the enduring value of high-tech innovation in modern warfare.
- 12. Training to operate unmanned systems equipped with autonomous features can now be completed in as little as 30 minutes to one day, substantially broadening access to these weapons systems.** What once required extensive flight hours now requires only a few hours, enabling a wider pool of soldiers to develop the necessary skills with minimal specialized expertise. As self-guided systems become more prevalent, drone training programs increasingly integrate autonomous targeting and navigation into their curricula. Recognizing this shift, institutions that educate drone operators equip learners to handle both manual and AI-assisted functionalities, often mastering autonomous modes in under a day. This accelerated learning curve expands the pool of qualified operators and bolsters overall operational readiness.
- 13. Ukrainian authorities are expediting the formal adoption and procurement of software and modules equipped with autonomous capabilities.** Key initiatives include codifying these autonomous modules in alignment with NATO standards and integrating them into official military service, which helps to scale acquisition. By classifying these modules as distinct components and establishing clear guidelines for their integration and use, the Ukrainian military is speeding up procurement and deployment timelines. In 2024, Ukrainian forces began purchasing 10,000 AI-enhanced drones—a preliminary yet significant step toward broader adoption of advanced autonomous systems. Although this figure represents only a fraction of the nearly 2 million drones built by Ukraine in 2024, it shows Ukraine’s growing commitment to increasingly autonomous and capable platforms.

- 14. Ukrainian military authorities increasingly require all unmanned and reconnaissance systems to integrate with situational awareness and fire-correction platforms, aiming to establish a common operating picture in real time.** To meet this demand, manufacturers must ensure their systems can feed data seamlessly into shared situational awareness and command and control environments. Even foreign suppliers recognize this imperative. For instance, Skydio's drones are linked with the Ministry of Defence's Delta system. The same may be said of the Ukrainian acoustic reconnaissance system Zvook and the text analysis tool Griselda, which provides intelligence from group chats and intercepted Russian communications. By unifying these capabilities, Ukrainian forces create a comprehensive, real-time operational picture that spans domestic and international technology providers.
- 15. Two major challenges lie ahead for AI-enabled autonomy: extending these capabilities to ground, sea, and undersea platforms and enabling swarming for aerial systems.** Although aerial drones have led the way in autonomous operations, adapting similar functionalities for multidomain use requires overcoming more complex technical and environmental hurdles. While the potential for integrating autonomous navigation into ground systems is significant, practical implementation remains largely unexplored by Ukrainian defense companies. In the aerial domain, swarming is currently in a stage of small-scale experiments; however, fully realized swarms—where drones communicate, make decisions, and adapt in concert—have yet to be developed. Achieving such sophisticated coordination will demand substantial advancements in AI algorithms, communication protocols, and real-time decisionmaking capabilities.
- 16. Human oversight remains pivotal—particularly for engagement decisions—reflecting a human-in-the-loop approach that could shift toward higher-level supervision in the future while still maintaining human control of the system.** Although Ukrainian forces aim to expand autonomy wherever it can enhance operational effectiveness, engagement decisions remain squarely in the human domain. Current human-in-the-loop practices allow operators to override autonomous functions, ensuring critical ethical and strategic judgments remain under human control. This approach lays a foundation for broader autonomy in the future—but with sustained human involvement at pivotal junctures where the stakes are highest.

Introduction

To what extent are modern unmanned systems truly autonomous, and how significantly does AI enhance their autonomy in the war in Ukraine? What are the paths for transforming military unmanned systems from ambitious theoretical concepts into practical, AI-enabled battlefield tools? What technological, operational, and strategic barriers still prevent the realization of fully autonomous warfare?

This paper explores these questions by analyzing Ukraine's innovative deployment of unmanned systems and assessing the role of AI in enhancing their effectiveness in contested environments. Drawing on dozens of interviews with Ukrainian military officials and Ukrainian and U.S. defense technology manufacturers, this analysis begins by reviewing the Ukrainian military's broader vision of military strategy and technology development. It clarifies the main definitions related to autonomy and autonomous weapons systems (AWSs) and then outlines the Ukrainian military's long- and short-term perspectives on the future battlefield, though these views have not yet been formalized into an official strategy.

Building on insights from these interviews and acknowledging that current technology cannot yet support fully autonomous missions, this paper describes advancements in three essential functions—intelligence, surveillance, and reconnaissance (ISR); automatic target recognition (ATR); and autonomous navigation—showing how these developments steer the battlefield toward greater AI-enabled autonomy.

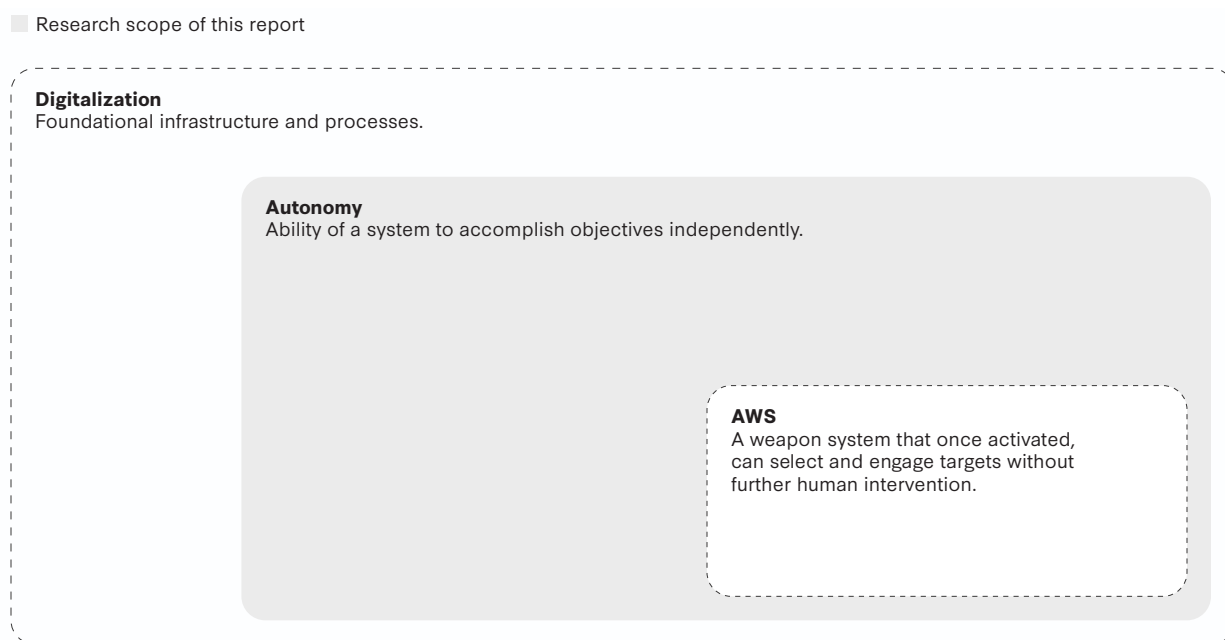
Each section identifies the main challenges AI aims to address, explains AI's role in overcoming these challenges, and provides case studies that illustrate AI's practical application in context. Additionally, the paper provides an overview of key lessons learned and emerging trends within each function.

The Ukrainian Military's Strategic Vision and Technological Road Map

A FRAMEWORK FOR UNDERSTANDING AUTONOMY AND THE SCOPE OF THIS PAPER

It is important to begin by clarifying how digitization, autonomy, and AWSs are defined, particularly given that different actors—including the Ukrainian and U.S. militaries—do not always use the same words to mean the same thing. Figure 1 illustrates how these definitions intersect and relate to one another.

Figure 1: Relationship Between Digitization, Autonomy, and AWSs



Source: CSIS analysis.

Digitization, as used here, denotes strategic adoption of advanced IT solutions, secure networks, and user-friendly interfaces across the whole military ecosystem. This foundational infrastructure enables streamlined operations, improved decisionmaking, and a distinct strategic advantage on the modern battlefield. Although digitization is a **foundation** for all further technical advancements within the military sector, the focus of this paper is more narrow.

Building on digitization, **autonomy** in military contexts refers to the ability of a system to accomplish objectives independently or with minimal oversight in complex and unpredictable environments. AWSs represent a more specialized subset of autonomy. As defined by U.S. Department of Defense **Directive 3000.09**, an AWS is a system that, once activated, can select and engage targets without further human intervention. Thus, while digitization underpins the broader development of autonomy, autonomy ultimately paves the way for advanced applications such as AWSs.

In Ukraine, however, no formal legislative or policy definition of either “autonomy” or “autonomous weapons system” currently exists. Often, Ukrainian sources use these terms interchangeably with unmanned platforms or platforms equipped with basic autonomous functions (e.g., navigation or targeting). While such systems may operate without direct human control, they frequently do not

perform the entire process of finding, selecting, and engaging targets independently. Given this discrepancy, this study employs a broad concept of autonomy to examine AI applications rather than focusing exclusively on AWSs.

THE UKRAINIAN MILITARY'S CENTRAL GOAL: REPLACE HUMANS ON THE BATTLEFIELD WITH AUTONOMOUS SYSTEMS

When it comes to technology, the Ukrainian military identifies removing warfighters from direct combat as its **central objective** in shaping the future battlefield. This goal is not simply an ambition; instead, it is an existential necessity for the Ukrainian armed forces. Given the substantial **numerical superiority** of Russian forces, Ukraine faces significant **constraints** on human capital, training resources, and time spent preparing warfighters.

The Ukrainian military identifies removing warfighters from direct combat as its central objective in shaping the future battlefield. This goal is not simply an ambition; instead, it is an existential necessity for the Ukrainian armed forces.

Furthermore, human personnel face inherent **vulnerabilities**, including fatigue, susceptibility to adverse weather conditions, and **psychological stress**. These human factors substantially impact operational sustainability and combat effectiveness, thereby reinforcing the tactical and strategic imperative for increased battlefield autonomy.

In conversations with CSIS, a diverse group of Ukrainian military and industrial officials repeatedly shared this common vision, even though it has not yet been formalized with a written strategy. Instead, a broad consensus on this vision among commanders already guides the acquisition priorities, deployment of software (e.g., comprehensive situational awareness and fire correction), and integration of unmanned systems into forces and current operations.

ROAD MAP TO BATTLEFIELD TRANSFORMATION: UKRAINE'S PROGRESSIVE APPROACH TO AI-ENABLED AUTONOMY

Strategic Component

The Ukrainian military's long-term strategy integrates AI-enabled autonomous systems with real-time situational awareness as a pivotal step toward achieving its main objective. This approach aims to **unify data from multiple sources**, analyze it quickly with the help of AI, and maintain a real-time operating picture that every autonomous system can access, thereby sharing friendly and adversarial movements instantaneously.

While Ukrainian forces currently envision a human-in-the-loop role, allowing operators to override AWSs when necessary, their long-term objective is to maximize autonomy across the battlefield whenever and wherever it supports improved operational effectiveness. This vision encompasses all functions, from intelligence gathering to progressing through the target life cycle, with human input limited to engagement decisions.

At present, there is a significant gap between aspiration and reality in technology development. AI, in particular, has many issues that have slowed broader deployment. Ongoing technological limitations—from simple **sensor malfunctions** under harsh weather conditions to difficulties tracking **fast-moving** or camouflaged targets—force the Ukrainian defense industry and military to apply a gradual approach and take smaller steps.

As a first step, the Ukrainian military focuses on adapting its command and control and integrating unmanned systems with conventional weapons systems into a single kill chain—for example, artillery. Kateryna Mykhalko, the director of **Tech Force in UA**, a Ukrainian defense manufacturers association, shared with CSIS that the envisioned single kill chain merges reconnaissance and strike unmanned aerial vehicles (UAVs) with artillery in a unified command system. Rather than replace conventional artillery outright, Ukrainian forces employ smaller strike UAVs to execute precise attacks against smaller targets, which reconnaissance drones identify and track. These small attacks exhaust the defenses of bigger and more important targets, leaving them unprotected for a further, decisive artillery blow.

The second step in the transition to fully autonomous military systems involves conducting and testing operations executed exclusively by unmanned platforms. The Ukrainian military has already begun operationally experimenting with this approach. In December 2024, Ukrainian forces took this step by carrying out the **first fully unmanned operation** near Lyptsi, a village north of Kharkiv. The attack involved dozens of uncrewed ground vehicles (UGVs) and first-person-view (FPV) drones, with no infantry participation. UGVs equipped with machine guns and munitions performed tasks such as mine clearance and direct fire. FPV drones supported the operation from the air, creating a coordinated multidomain assault. Following the attack, surviving robotic unmanned systems returned behind Ukrainian positions.

This tactical air-land operation successfully destroyed Russian positions and showcased Ukraine's innovative approach to offset manpower limitations by leveraging attritable technologies. Although described as a “**seminal moment**” in conflict evolution, the robotic systems were still manually (though remotely) operated. Nevertheless, the operation brings Ukraine one step closer to implementing its vision of the future battlefield, which will increasingly utilize AI-enabled autonomous capabilities.

Technological Component

CSIS conversations with Ukrainian warfighters and defense manufacturers reveal the organic approach that Ukraine and its domestic industry are taking toward achieving autonomy on the battlefield. Rather than follow a formal strategy, this process has evolved in response to several influences, including competitive pressures from the adversary, market dynamics, geopolitical considerations, and foreign export controls, especially China's **ban on the sale** of key drone and microelectronic components to Ukraine.

The technological evolution driving this transition may be divided into three key trends progressing in parallel. These trends result in systems that are not only flexible, cost-effective, and highly efficient but also adaptable to diverse mission requirements and equipped with AI-powered software that enables autonomy.

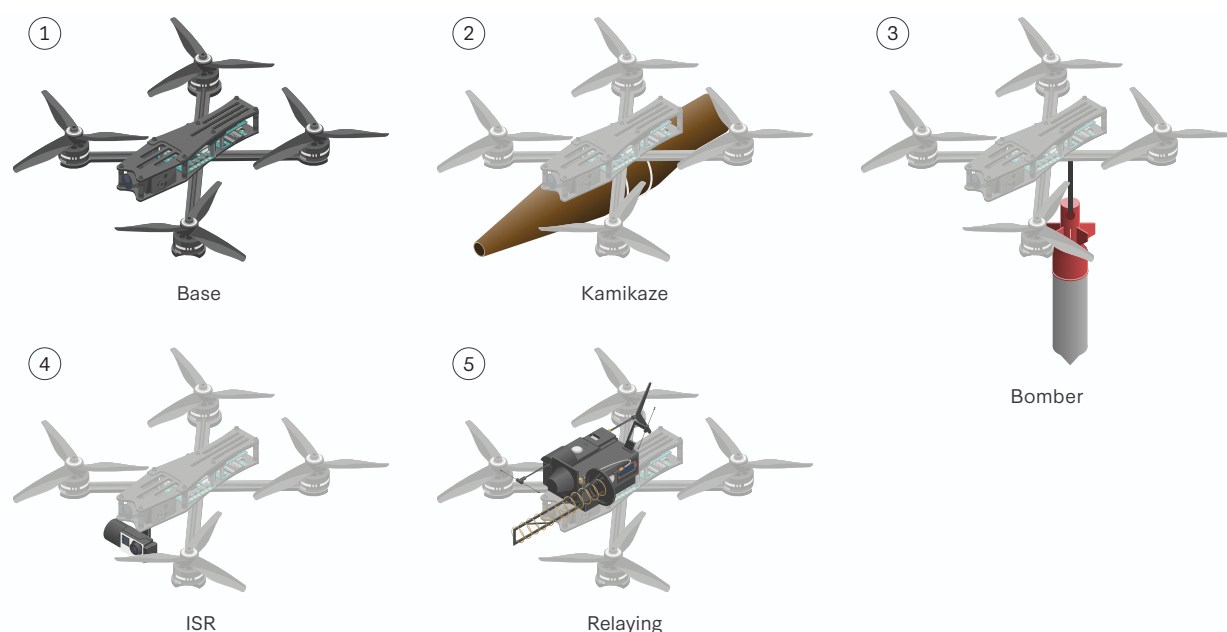
Trend 1: Ukrainian forces have widely adopted small FPV drones as a platform that can be quickly adapted for diverse missions through modular design.

Small and medium Ukrainian-built FPV drones are the most commonly used platforms on the Ukrainian battlefield, aside from consumer off-the-shelf models like the Chinese-made DJI Mavic. While Ukrainian forces use these commercial drones, they cannot directly influence Mavic's technology development. In contrast, local innovators produce and refine many FPV drones, making them the focus of this analysis.

The Ukrainian military classifies drones, including FPV drones, differently than the U.S. military. Instead of using categories like size, weight, or flight altitude, Ukraine groups drones by structural configuration (for example, quadcopter or fixed-wing), payload capacity, and, most importantly, propeller diameter. At the beginning of the full-scale invasion in 2022, FPV drones with a 7 inch propeller diameter were most common due to their ease of assembly, smaller batteries, and greater availability. Over time, though, increased demand for heavier payloads and longer flight range has led to a shift toward larger 9-10 inch quadcopters, which now dominate Ukrainian operations.

FPV drones have not only grown larger but also have become more versatile. As shown in Figure 2, a basic quadcopter platform may be adapted for different missions by adding or changing specific components. This modular approach allows the same platform to carry various payloads and fulfill different roles, making FPV drones a flexible solution across many types of operations.

Figure 2: Types of FPV Drones Used for Various Missions



Source: CSIS analysis.

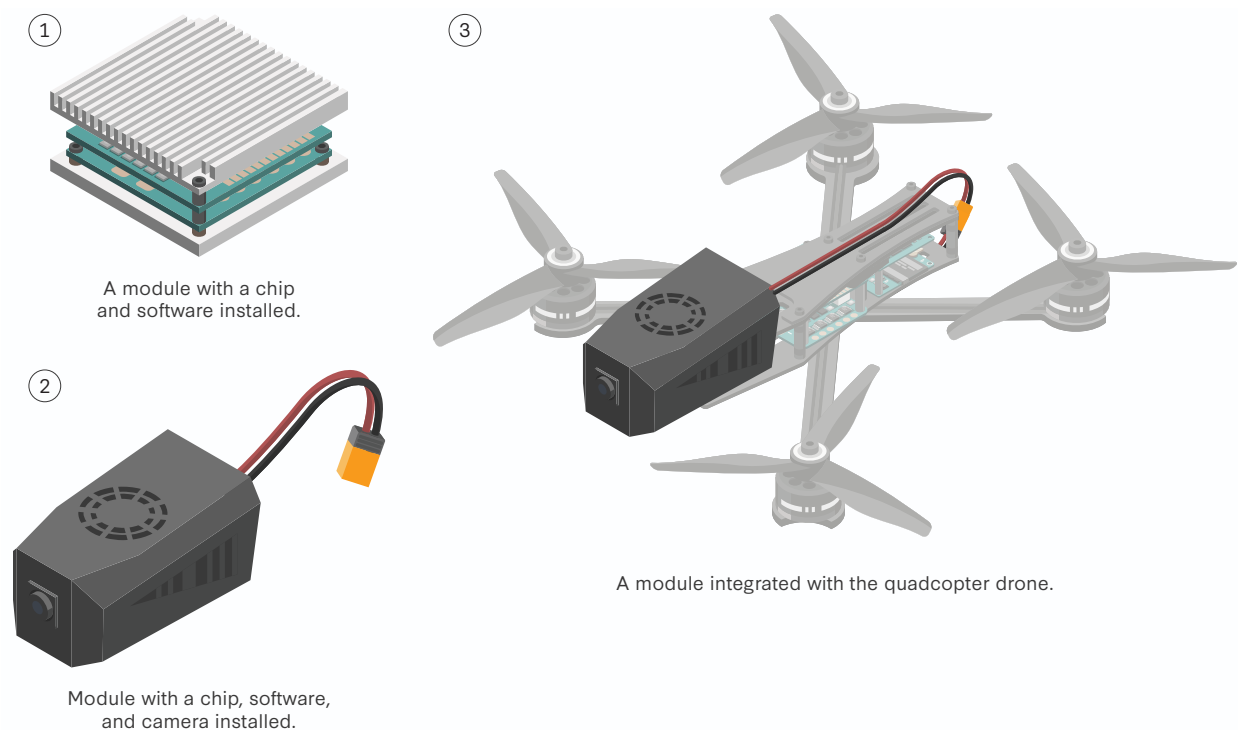
Trend 2: Ukraine's defense industry is developing standalone software that can be integrated across a variety of platforms to incrementally expand battlefield autonomy.

In parallel with the shift toward more advanced drone hardware, Ukraine's defense industry is putting much effort into software engineering. This approach centers on creating modules—electronic and software components developed independently of any specific hardware platform. As shown in Figure

3, these modules often comprise a chip with embedded software (and sometimes a camera) and are usually smaller than a bar of soap. They enable critical autonomous functions, such as perceiving the environment, target recognition, and the capacity to engage targets without direct human flight control (so-called **last-mile** navigation).

By focusing on one specialized function at a time and then offering that function as a standalone product, Ukrainian defense firms and startups can tailor their modules to operate across a broad range of systems. These include FPV drones of various sizes, ground vehicles, and even **turret-mounted weapons**. In doing so, they pave the way for broader autonomy, as each module contributes a distinct capability that can be integrated into larger multifunctional platforms. Examples of such modules and companies are provided in the case studies in the following sections of this paper.

Figure 3: Examples of Modules Enabling Autonomous Capabilities



Source: CSIS analysis.

Trend 3: Ukraine has prioritized scaling and localizing domestic drone production and increasing self-sufficiency.

According to a **statement** by Ukraine Minister of Defence Rustem Umerov, domestic drone production significantly expanded in 2024, reflecting Ukraine's growing focus on scaling and localizing production capacity. In 2024, Ukrainian defense companies manufactured and assembled more than 1.5 million FPV drones. They also produced other advanced platforms, including strike quadcopter bombers, kamikaze drones, winged reconnaissance drones, and long-range deep-strike drones. Overall, Ukraine produced approximately 2 million drones in 2024. Notably, 96.2 percent of all UAVs that the Ukrainian

armed forces used in 2024 were produced domestically, demonstrating the country's increasing reliance on homegrown technology and **localization** of production components.

Overall, Ukraine produced approximately 2 million drones in 2024.

Ukraine has also **introduced** into its **arsenal** more than 200 domestically developed unmanned aerial systems and more than 40 ground robotic platforms since February 2022. Most of these new systems entered service in 2024, showing that local manufacturing is adapting to war conditions and establishing reliable supply chains. Specifically, 140 UAV complexes (designs and unique configurations) and 33 ground robotic systems were approved for operation in the first nine months of 2024 alone. Together, these developments indicate a strategic move to increase self-sufficiency, reduce supply chain risks, and ensure that the Ukrainian military can rapidly adapt to the evolving demands of modern warfare.

In conclusion, Ukraine's strategic emphasis on autonomy reflects its transformative vision for the future battlefield, where advanced AI-enabled unmanned systems will replace humans in direct combat to address manpower limitations and operational vulnerabilities. By integrating modular software development and scaling domestic production, Ukraine is not only adapting to the immediate challenges of war but also laying the groundwork for a future autonomous battlefield environment.

AI in Intelligence, Surveillance, and Reconnaissance

According to CSIS discussions with the Ukrainian military, the battlefield in the war in Ukraine critically differs from prior full-scale conflicts. Key factors of this distinction include the unprecedented **proliferation of sensors** on the front line, the extensive deployment of unmanned systems, and the exponential increase in data sources and volumes. Combined with advanced technological capabilities for data processing and analysis, these elements form part of the autonomous operational paradigm. In this paradigm, real-time situational awareness will provide machines with the contextual understanding required to act effectively within the operational environment.

The Delta system, as outlined in an **earlier paper** in this series, is a good example of how the Ukrainian military's intelligence sources provide video, photo, acoustic, and text data streams in tens of terabytes daily. After being processed, the data go back to the front line, but this time in the form of detailed information on enemy locations, equipment, movements, and activities placed on a digital map and presented in a single operational picture on the phone or tablet of almost every unit commander and even warfighter.

CURRENT CHALLENGES IN ISR

As previously outlined, the envisioned future battlefield differs greatly from practical realities. In ISR, three primary factors hinder the realization of the Ukrainian military's desired future autonomous operational paradigm:

1. **Limitations in Human Processing Capacity:** Modern reconnaissance systems, particularly drones, generate **large volumes of data** at speeds that exceed human processing capabilities. Certain tasks—such as detecting small objects in high-altitude drone footage or interpreting faint acoustic signals—pose significant challenges to human analysts. Fatigue, decreased concentration, and slower work increase the risk of overlooking important information contained in the data.
2. **Delays in Data Processing:** Manual data processing is inherently time-consuming, creating significant lags in intelligence dissemination and operational decisions. Achieving real-time responsiveness becomes nearly impossible under these circumstances, preventing the fast execution of missions.
3. **Complexity of Synthesizing Multisource Data:** Combining and integrating insights from diverse sources, including imagery, signals, and other types of intelligence, presents an intricate puzzle for military analysts. Successful integration demands the **alignment of various data streams** into coherent predictions and actionable recommendations. This task is challenging in real war conditions, given that multiple teams or even different external companies are working to analyze incoming data streams.

HOW AI CAN ADDRESS THE CHALLENGES

The good news is that these limitations may be overcome and data can be quickly processed into high-quality intelligence information. AI allows for handling massive amounts of multisource data in near-real time. Within a broad portfolio of AI-enabled capabilities, there are methods and systems that can help tackle each challenge, from detecting enemy equipment in drone footage to interpreting diverse formats of unstructured textual data.

Table 1 provides a summary of the main data types, the tasks involved in processing them, and the AI-enabled techniques used for these purposes. A more detailed explanation of these techniques is provided in subsequent sections.

Table 1: ISR Sources and the Role of AI

Source	Data	Tasks	Technology
Satellite imagery	Imagery and video	Detect, recognize, and classify objects	Computer vision analysis using deep learning algorithms: 3D convolutional neural networks (CNNs) and recurrent neural networks (RNNs)
High-altitude drones			
Low-altitude drones			
Stationary cameras			
Acoustic systems	Sound	Identifies and classifies distinct sound patterns	CNNs and RNNs; spectrogram analysis enhanced by deep learning
Intercepted communications	Text	Transcribes metadata and extracts key entities and insights	Natural language processing (NLP); transformer models, for both speech recognition and synthesis
Group chat messages			
Chatbot reports submitted by civilians			

Source: CSIS analysis.

Imagery and Video

The imagery and video data the Ukrainian military receives comprises a variety of pictures, video, and objects and comes in different formats and quality. Traditional **overhead intelligence** primarily relies on satellite imagery and has significantly advanced due to the proliferation of commercial sector technologies and services. These include open-source platforms such as **Google Earth** and low Earth orbit satellites offering high-resolution imagery from companies like **Maxar Technologies**, **Planet Labs**, and **Capella Space**.

In addition to this traditional satellite imagery, Ukraine has recently gained access to two novel layers of overhead intelligence. Both layers are obtained through drones conducting ISR missions. The first layer is collected by high-altitude reconnaissance UAVs, which private Ukrainian companies started to **produce** after the 2014 Russian invasion of Donbas. They made high-altitude reconnaissance available to Ukrainian forces quite widely and quickly after the full-scale invasion of 2022. The second layer of imagery comes from short ISR missions conducted at low altitudes by commercial drones such as the DJI Mavic and by Ukrainian domestic ISR drones.

All satellite and drone footage needs processing, analysis, and labeling. **Computer vision** using **machine learning** lies at the core of many AI-driven video and photo analysis systems. It effectively addresses the challenge of detecting and **classifying objects** in visual data using **deep learning algorithms**. By identifying objects such as military equipment or weapons, these algorithms are the basis for additional tasks like **object tracking** and **image captioning**.

To handle the spatial and temporal nature of videos, two main types of neural networks are commonly employed: **3D convolutional neural networks** (CNNs) and **recurrent neural networks** (RNNs). CNNs work by analyzing patterns across space and time, capturing how an object or action evolves from one video frame to the next, whereas RNNs track and interpret sequential data, making them effective for tasks like recognizing specific movements or repetitive activities. These methods train machines to detect objects regardless of changing poses or angles, mirroring how humans recognize items.

Real-time processing complicates the task of object recognition, as it requires analyzing 30 or more frames per second. With each frame containing millions of pixels, the task becomes computationally very demanding, resulting in high costs for such video processing.

Case Study 1: AI-Assisted Drone Footage Analysis Conducted by Ukraine's Ministry of Defence

The first case study **presents an example** of how the Ukrainian military is using AI-enabled systems to extract as much useful information as possible with the limited resources available. A team of volunteers, which later evolved into the Avengers team within the Ministry of Defence's **Delta system project**, began developing a video and imagery analysis platform at the outset of the full-scale Russian invasion in 2022. At that time, Russian military equipment was moving extensively across Ukrainian territory, creating an urgent need for the Ukrainian armed forces to track enemy movements and identify the types and locations of Russian equipment.

To address this need, the Avengers team initially collected and annotated footage from stationary cameras along major roads and highways. Then they used the data to train AI models capable of recognizing various objects, determining geographic locations through metadata, and providing critical insights into Russian troop movements.

However, when Russian forces retreated from northern Ukraine, combat shifted to a more conventional battlefield. The free movement of Russian equipment ceased in most areas, rendering the stationary camera footage (and the models trained on it) less useful. The team began receiving and analyzing drone footage, which presented new challenges, such as varying perspectives, resolutions, and object sizes. Moreover, the amount of footage to be analyzed drastically increased. The Avengers team had to respond by changing its approach to focus on creating infrastructure for AI training, such as employing structured and labeled datasets, developing a secure testing environment for external AI-enabled tools development, and integrating with other products within the Delta ecosystem.

To create a foundation for AI integration into the process of drone footage analysis, the Avengers team took the following steps:

- 1. Standardizing Labeling Practices:** In 2022, no enterprise solution was capable of analyzing drone footage and classifying Russian equipment. This required the team to develop AI models to assist analysts with annotations. However, these models had to be trained on large, relevant datasets. Therefore, creating AI training datasets became the first step in preparing for the transition to AI.

Dataset labeling is a labor-intensive task that requires significant human effort. Because the Ministry of Defence lacked sufficient internal resources, diverse groups, including volunteers and private sector teams, supported its efforts in labeling data. To ensure consistency, the

Avengers team introduced formalized labeling standards and protocols. These guidelines outlined parameters to consider during dataset labeling, such as resolution, seasonal variations, metadata, and other relevant factors.

As a result, the Avengers team created a “universal military data set,” which adhered to these formalized labeling guidelines, making the dataset consistent and standardized. This dataset is large enough to enable high accuracy in AI model performance and may be filtered to produce smaller, more specific datasets for various use cases.

2. **Creating a Validation Dataset:** To benchmark AI model performance, the team created a separate validation dataset containing content that does not overlap with the universal military dataset. For instance, if a model is trained to detect a specific Russian tank, the validation dataset includes color variations and images of the tank camouflaged, hidden in the bush, or with an antidrone net. This approach allows the model to provide accurate assessments of false positives and improves the model’s overall reliability.
3. **Developing Small, Specialized AI Models:** Operational experience has demonstrated that smaller, specialized models can achieve much greater accuracy in analyzing drone footage than a single comprehensive AI model. Therefore, Avengers and external teams started to produce multiple smaller models, each tailored to specific data types (e.g., footage from particular drones and satellite imagery). This approach enhances accuracy and relevance for distinct operational scenarios, focusing primarily on the hardest cases for the human eye and human attention: small objects in low resolution and poor-quality footage.
4. **Facilitating External AI Model Training:** Avengers allow vetted developers to train their models securely, using selected portions of the universal dataset without exposing sensitive data. For instance, a drone manufacturer can request footage from drones that match characteristics of its product, such as a particular flight altitude, camera type, or resolution requirement, and train its algorithm within the platform’s protected environment.
5. **Moving Toward Autonomous Analysis of Real-Time Footage:** The platform integrates with a live-streaming system called VEZHA, which is part of the Delta ecosystem and is designed to analyze real-time drone footage. Although human operators still carry out most of the analytical tasks such as classifying and logging events, improvements in AI model performance and integration with the streaming service have led to a growing role for AI-assisted analysis. This analysis may be divided into two primary use cases:
 - **Real-Time Analysis:** In this scenario, AI algorithms help prioritize videos based on the number and intensity of observable events, such as active combat or significant troop and equipment movement. Drone feeds from reconnaissance missions over relatively empty fields are deprioritized. VEZHA also enables multiple operators to watch the same stream simultaneously and jointly log detected events (e.g., tank positions, destroyed vehicles, and artillery strikes). These events are then connected to a digital map (e.g., via the Delta monitor) and supplemented with screenshots and details for broader situational awareness.
 - **Postanalysis:** The VEZHA team only applies postanalysis to the most challenging cases, such as low-resolution or high-altitude footage. Because AI-assisted analysis consumes

considerable computational resources, the system prioritizes difficult footage over videos that are inherently clearer, such as those captured by low-flying Mavic drones, in which objects are more easily visible to humans. As a result, automated detection resources are conserved for situations where they are most needed.

Case Study 2: Vector, an ISR Drone System

Quantum Systems, a drone technology firm based in Germany, the United States, and Australia—with a newly established **facility in Kyiv**—has been testing and supplying its systems to Ukraine since March 2022. What began as a small donation of a few **Vector drone systems** and a focus on training Ukrainian forces has rapidly evolved into a large-scale partnership, with more than 500 systems now deployed.

Quantum Systems' Vector drones serve ISR functions in Ukrainian strike missions. Acting as agile spotters, they locate targets and transmit precise data to heavier strike drones such as the Ukrainian-made **Nemesis**. This synergy ensures efficient **fire support** and artillery corrections. Quantum Systems has tackled widespread Global Positioning System (GPS) jamming by **employing** optical navigation and advanced data links provided by **Silvus interference avoidance software**. The system enables autonomous scanning and switching to alternative frequencies when one is jammed, maintaining mission-critical communications.

A hallmark of the Vector drone design is its modular architecture. Swappable nose cones and imaging systems allow customization depending on mission needs. Equipped with day-and-night Boson cameras and powered by onboard **Nvidia Jetson Orin AI computers**, these drones collect high-resolution imagery and process it in real time, even under GPS-denied conditions.

Quantum Systems is deploying **Receptor AI**, an advanced software package that enables drones to autonomously perform target recognition. While still under development, these algorithms will be trained to recognize targets based on Ukrainian datasets, ensuring better adaptability to real-world combat settings.

Despite investing heavily in AI to enhance autonomy, Quantum Systems emphasizes keeping human operators in the loop. This human oversight, company representatives told CSIS, should ensure that ethical considerations, strategic objectives, and final decisionmaking remain under direct human control, even as the technology progresses.

Acoustic Reconnaissance

Acoustic reconnaissance is the practice of using sound to gather intelligence and monitor environments. It is not a new concept. It has been employed in **various forms for decades**, from submarine sonar systems during World War II to early warning systems detecting aircraft or artillery fire.

However, the **integration of AI** has revolutionized this field by automating the classification and recognition of sounds with precision and speed. AI technology enables systems to process audio data in real time, making it possible to detect and differentiate sound patterns that are challenging to identify with human hearing alone.

AI-driven acoustic reconnaissance relies on a set of techniques nearly identical to those used for video footage analysis. It uses advanced machine learning techniques and neural networks, such as CNNs and

RNNs, to analyze audio signals. These neural networks are trained to extract features from sound waves and classify them accordingly. Tools like **spectrogram analysis**, enhanced by deep learning, allow systems to visualize and **interpret acoustic signals**, distinguishing between the sounds of drones, vehicles, footsteps, and even specific environmental noises.

Tools like spectrogram analysis, enhanced by deep learning, allow systems to visualize and interpret acoustic signals, distinguishing between the sounds of drones, vehicles, footsteps, and even specific environmental noises.

Case Study 3: Zvook, an Acoustic Reconnaissance System

The following case study of the acoustic reconnaissance system **Zvook** illustrates how such technologies are implemented in practice in Ukraine. Ukraine's use of acoustic detection systems has significantly advanced not only ISR but also air defense capabilities. Zvook **uses sound analysis** to detect and identify aerial threats at lower altitudes, where radar is less effective. It employs high-quality microphones and curved acoustic mirrors to concentrate sound waves, and it uses a computer the size of a shoebox placed behind the dish to process the captured sounds. Currently, Zvook covers approximately 20,000 square km of Ukraine with its grid-like placement of acoustic sensors.

Compared to radar, these systems are cheaper, with each station costing **around \$500**. They are also passive (i.e., they do not emit detectable signals) and are particularly effective against low-flying drones, with detection ranges of up to 4.8 km for drones and 6.9 km for cruise missiles. Zvook processes data quickly, with detections typically appearing in the Delta situational awareness system within **12 seconds**. The rate of false positives is just **1.6 percent**. The information shared includes the type of target and its sound, location, and direction of movement.

AI capabilities for Zvook's acoustic analysis were **introduced** through collaboration with the Ukrainian tech startup **Respeecher**, which before the war was working on AI-generated voices for **collaborations** with Hollywood. Respeecher's AI algorithms, particularly those based on machine learning, analyze acoustic signals captured by sensors.

First, AI-powered analysis filters potential aerial threats from all other sounds, such as cars, birds, and people. Second, the AI system is trained to classify different types of aerial threats based on their unique sound signatures. For instance, it can distinguish between helicopters, cruise missiles, drones with gasoline engines, and turboprop aircraft using sound alone.

The latest generation of these acoustic sensors and AI models brings an innovative feature: the ability to **detect the direction** of the sound source, including the azimuth and elevation angle. This means that multiple sensors can now work in tandem, using the intersecting azimuth information from different locations to precisely determine the coordinates, course, and speed of the target. Essentially, this transforms the system into a passive acoustic radar, providing a new layer of detection that complements existing radar systems. The Zvook system's effectiveness has led to the use of radar

primarily in response to acoustic alerts. Many radar installations are by default turned off to avoid emissions, which might invite Russian attacks. Zvook allows Ukrainian radars to be turned on only in priority situations.

When a new type of drone or other weapons system appears, the team needs **about a week** to collect a big enough dataset for AI model training to recognize its sound. After that, the software of acoustic stations is upgraded remotely so that all sensors can recognize the new type of threat.

Text Information Analysis

The Ukrainian military receives text data in large volumes, primarily from three categories of sources: (1) intercepted communications of Russian forces converted to text, (2) chat messages used within the Ukrainian military for information exchange, and (3) reports submitted by civilians through chatbot applications.

Handling text-based intelligence is another core area where AI excels. **Natural language processing** (NLP) and related machine learning approaches can sift through vast collections of messages, chats, and intercepted communications, extracting important insights. Techniques such as named entity recognition and **topic modeling** identify significant information—like names, locations, or critical events—and highlight patterns that might otherwise go unnoticed. By rapidly cross-referencing multiple sources, these AI-driven systems bring geolocated information on a map, indicating the positions and movements of enemy equipment or forces. Consequently, these text-based sources of information serve as an additional layer of data that is equally valuable for enhancing real-time situational awareness.

Case Study 4: ePPO, an Air Defense System

The **ePPO** is a mobile application that uses AI to collect and analyze reports from civilians about air threats, such as missiles and drones. To use the ePPO application, users must first verify their identity through the government's Diia app. Once verified, they can report observed aerial threats by selecting the type of object—drone, missile, aircraft, or helicopter—and pressing a large red button to send the alert.

The AI **processes the data** to estimate the most likely trajectory of the threats, predicting their direction and speed. According to Ukrainian Deputy Minister of Defence Kateryna Chernohorenko, the process ensures that within **two to seven seconds** the data is transmitted to a digital map, which is accessible to all air defense officers. In a social media post, the deputy minister **highlighted** that the system significantly enhances Ukrainian efforts to repel drone and missile attacks.

A unique feature of the app called “It’s coming your way” is a personalized warning to users if a threat is likely to impact their location. The warning is issued based on the AI-enabled data fusion and projection of flight trajectories. Within about 10 minutes of data collection, the AI delivers approximate coordinates of the threat’s movement to users, allowing them to take timely precautions. With more than 600,000 downloads and 200,000 active users contributing to this collective radar system, the ePPO app represents a significant advancement in leveraging crowdsourced data and AI to enhance air defense and protect civilians during the ongoing conflict.

Case Study 5: Griselda, a Data Analysis Platform

Griselda is an AI-driven system for processing unstructured data that may be customized for a wide range of uses. Griselda is sometimes described as Ukraine's Palantir. In an interview with CSIS, the company's founder, Oleksiy Teplukhin, shared two notable applications of this technology that use largely the same underlying methods.

The first use case is analyzing group chats to derive actionable intelligence. At the beginning of Russia's 2022 full-scale invasion of Ukraine, warfighters predominantly shared intelligence information through group chats or messenger platforms such as Signal. Although more advanced communication systems (e.g., Delta) and specialized military channels exist, basic platforms remain widely used even today. Certain channels receive thousands of messages daily, often containing unstructured and unstandardized battlefield reports—such as sightings of Russian equipment. But this high volume of fragmented data can overwhelm frontline warfighters, making it almost impossible to extract essential insights in time without a technical solution.

The second example addresses the management of Russian intercepted audio communications from multiple sources. Traditionally, processing such extensive audio datasets requires considerable human resources, including large-scale call centers staffed by numerous analysts responsible for transcription, comprehension, and extraction of relevant details. This approach is not only labor-intensive but also prone to errors, limiting its efficiency and scalability.

To overcome these challenges, Griselda, which partners with the Ukrainian military on both cases, automates processes with the help of AI. The system replaces human operators in critical functions such as transcription, semantic analysis, and identification of entities and key data points within the intercepted conversations. Moreover, the AI constructs ontological graphs, enabling pattern recognition and semantic connections across vast datasets. These graphs allow analysts to uncover insights and relationships that would be impossible for humans to discern manually. By automating these workflows, AI reduces the need for human labor by an estimated 99 percent, according to Teplukhin. Operationally, this breakthrough translates into markedly enhanced speed, accuracy, and effectiveness in processing intelligence information.

The AI constructs ontological graphs, enabling pattern recognition and semantic connections across vast datasets. These graphs allow analysts to uncover insights and relationships that would be impossible for humans to discern manually.

Importantly, Griselda is integrated with Delta, which ensures that all intelligence insights are instantaneously disseminated throughout the chain of command. These insights are then visualized on a map, enabling seamless distribution to relevant personnel, including drone operators stationed in areas where suspicious activities have been detected. By directing their drones to the designated locations, these operators can validate the intelligence and gather additional details as necessary, thereby enhancing situational awareness and operational efficiency.

LESSONS LEARNED

1. **Employing AI for preliminary data filtering and prioritization optimizes resources for real-time intelligence processing.** By automatically screening large volumes of incoming information—such as multiple video streams from reconnaissance drones—AI systems can highlight critical content that demands immediate attention. This approach helps analyst teams direct their limited bandwidth and processing power toward the most pertinent data.
2. **Standardizing the curation and labeling of military datasets enhances efficiency and flexibility in AI model development.** Adopting consistent protocols for tagging and organizing incoming data—from drone feeds to satellite imagery—makes it easier to separate relevant parameters for different AI applications and filter out smaller datasets. Both military and private sector teams can collaborate in this effort, ensuring that well-structured datasets are readily available for specialized training and more accurate model deployment. Of note, most of this standardization occurs organically instead of, for example, being driven by some standardization committee or organization.
3. **Building specialized smaller-scale AI models addresses specific operational challenges more effectively.** Instead of relying on a single, all-encompassing model, smaller specialized AI models can be trained on targeted subsets of larger datasets for focused tasks. This approach not only enables more precise problem solving but also streamlines the model-training process, making solutions more adaptable to changing mission requirements.

TRENDS

1. **Ukrainian military authorities are increasingly demanding the integration of all unmanned reconnaissance systems into situational awareness and fire-correction platforms.** The Ukrainian military expects manufacturers of unmanned ISR systems of any size and domain, whether designed for tactical or strategic operations, to feed relevant data into shared intelligence systems (e.g., Delta). This demand helps ensure all reconnaissance activities collectively contribute to a comprehensive real-time operational picture.
2. **The Ukrainian military is shifting toward AI-enabled real-time multisensor fusion to enhance situational awareness.** By integrating data from drone imagery, satellite photos, acoustic signals, and textual information, Ukrainian forces create a continuously updated operational picture. This shift increases the need for advanced data-fusion technologies, ensuring that AI tools rapidly extract insights from every source and merge them into a unified common operating picture.
3. **AI systems are evolving beyond basic data analytics to provide commanders with actionable insights and strategic recommendations throughout the target engagement cycle.** Building on real-time intelligence assessments, these tools soon will not only highlight potential threats but also propose prioritized targets, identify gaps in available resources, and determine which assets are best suited to neutralize a given threat.
4. **Military agencies are easing access to vetted datasets for external developers, providing an opportunity to keep their AI models accurate and relevant.** By allowing approved private companies and researchers to securely train or test AI models on government-provided data within secure environments, this approach significantly lowers the burden of data collection

for companies. These efforts seek to develop a pool of advanced AI models better tailored to rapidly evolving operational needs.

5. **AI-enabled real-time situational awareness provides the foundation for joint all-domain operations.** AI-enabled data fusion, integrating intelligence from land, air, sea, space, and cyberspace into one cohesive view, provides a foundation for synchronized actions across domains. It is also a basis for collaboration with allied partners in executing combined operations, allowing decisionmakers to quickly align resources, identify threats, and exploit tactical opportunities.

AI in Automatic Target Recognition

Automatic target recognition (ATR) is a suite of technologies that automate the detection, classification, and tracking of objects or individuals. At its core, ATR relies on **pattern recognition algorithms** that match incoming sensor data against a set of known templates or behavioral models, flagging unusual features as potential targets. It is **not a new concept** to the military, but **AI changes** the way ATR works and the way ATR systems are developed, enabling enhanced performance and reducing costs that previously put such applications out of reach.

In practice, ATR follows a three-step process. First, an AI-enabled ATR system detects targets by scanning a designated area for any signs of interest, drawing on both visual and nonvisual sensor data. Once a target is detected, the system **classifies** it by identifying what it most likely represents—for example, a vehicle, a person, or a structure. Finally, the system tracks each identified target, continuously updating position information and projecting possible movements or changes in status. This continuous monitoring is particularly valuable in fast-evolving tactical scenarios, as it gives warfighters on the ground up-to-the-second insight into **potential threats**.

This section focuses on the role of ATR as a built-in feature of unmanned systems, demonstrating how onboard AI applications help bring these platforms closer to fully autonomous operations. In particular, target recognition plays a pivotal role in enabling future AWSs to independently select targets, though ATR is often incorporated into systems that do not meet the definition of an AWS.

By automating target identification, ATR technology bolsters real-time decisionmaking—whether a human operator or the system itself executes those decisions. Its foundation in AI-based algorithms and **sensor fusion** also makes it highly adaptable to ever-shifting battlefield conditions and marks a significant leap in harnessing AI's ability to process complex data efficiently, accurately, and reliably.

CURRENT CHALLENGES IN ATR

Although ATR technology has become essential on the modern battlefield, it still faces significant limitations. While it performs well in controlled environments, its adaptability and precision diminish under the complex and dynamic conditions of a real war. The following are some key obstacles facing human-operated drones equipped with ATR:

1. **Use of Decoys and Camouflage:** One of the most pressing challenges for ATR lies in distinguishing between genuine threats and elaborate deceptions. Both Ukrainian and Russian forces frequently **deploy decoys**, such as inflatable tanks or false artillery installations, and advanced camouflage techniques, confounding target recognition algorithms and human operators.
2. **Electronic Warfare (EW) Interference:** In addition to physical countermeasures, both sides employ **robust EW systems** designed to disrupt drone communications, sensor data feeds, and the broader chain of command. **EW interference** impairs real-time data transfer, making it far more difficult for drones or their operators to reliably identify and confirm targets. As a result, ATR must operate in environments with degraded or intermittent communication links, handling target recognition and tracking tasks with onboard processing.
3. **Dealing with low visibility and dense urban environments.** **Natural and man-made factors**—such as fog, rain, snow, and nighttime operations—can significantly reduce the effectiveness of standard optical and infrared sensors. In such scenarios, ATR may rely on

alternative methods like radar or acoustic detection, which come with their own performance limitations. **Urban settings** in eastern Ukraine add another layer of complexity given the dense infrastructure. Highly sophisticated sensors and algorithms and well-trained operators often get confused, but Ukrainian developers strive to maintain accurate targeting while minimizing collateral damage.

HOW AI CAN ADDRESS THE CHALLENGES

AI offers significant advantages in the speed, accuracy, and efficiency of identifying and tracking targets in complex operational environments. The good news is that AI-enabled ATR software may be integrated directly onboard an unmanned system. By processing data within a localized, self-contained network, AI algorithms can fuse multiple sensor inputs to give warfighters an understanding of their surroundings and the target, even without live communication with base situational awareness systems.

At the core of AI-enabled ATR is the ability to **detect and classify** targets more rapidly and accurately than human operators. Advanced machine learning algorithms, trained on datasets that include real-world combat scenarios, can distinguish among vehicles, human figures, and structures in various terrain and weather conditions. Operating continuously without fatigue, these systems pick up subtle distinctions that **human observers might miss**, enabling identification of decoys and camouflaged targets.

Beyond mere detection, AI excels at rapidly **prioritizing multiple targets** based on real-time variables such as threat level, proximity to friendly forces, and mission objectives. Some Ukrainian AI-enabled ATR systems use the same techniques as described in the ISR section (convolutional neural networks and recurrent neural networks) as well as other techniques such as **reinforcement learning**. However, in this case, the AI models are integrated into the unmanned system's onboard software. With such capabilities, a drone can process massive amounts of sensor data and apply predictive models in real time during the mission. AI systems can determine and advise operators regarding which threats **require immediate engagement**. As a result, AI reduces the cognitive load on human operators while ensuring that vital decisions—such as which target to engage first—are made more rapidly and accurately.

Beyond mere detection, AI excels at rapidly prioritizing multiple targets based on real-time variables such as threat level, proximity to friendly forces, and mission objectives.

AI-driven autonomy also increases resilience against enemy countermeasures, particularly those aimed at disrupting communication links and navigation systems. By shifting from human control to human oversight, AI-enabled platforms can **maintain their targeting focus** even if the operator's signal is jammed or lost. Moreover, technologies like pixel lock can support **high-precision tracking**, allowing drones to maintain a lock on targets despite interruptions in operator communication—a critical benefit in environments subject to heavy EW interference.

Machine learning models fuel this resilience, allowing the system to **learn from each operation** and refine its responses over time. Through **reinforcement learning** and other **adaptive techniques**, AI can identify emerging adversary tactics and continuously improve a platform's targeting accuracy.

This iterative learning cycle helps drones stay effective in fast-changing combat conditions, ultimately minimizing operational downtime and preserving critical military assets.

Although these AI-based technologies are still in their early stages of deployment on Ukrainian battlefields—limited, for now, to basic object recognition and tracking rather than advanced predictive models or onboard recommendation systems—their use by Ukrainian warfighters continues to grow in both scale and sophistication. In parallel, military authorities are actively developing regulatory frameworks and operational procedures to facilitate and standardize (especially for procurement) the adoption of these emerging systems, thereby laying the groundwork for more sophisticated AI capabilities in the near future.

Case Study 6: ZIR, an Autonomy Kit

The company **ZIR System specializes** in developing software that can complement almost any type of strike drone. The key feature of the software and the reason it is called ZIR (which means “eyesight” in Ukrainian) is its ability to **automatically detect targets**. The system includes a hardware component—a compact module with a computer and a digital camera—and a software component, which in this case involves a pretrained AI model capable of identifying targets. This software also adds some autonomous navigation capabilities.

The hardware module, approximately the size of a bar of soap, is designed for seamless integration across a variety of platforms, from quadcopters to aircraft. Presets exist for 7-10 inch standard quadcopter models. For fixed-wing drones, the company provides only essential wiring and components, leaving manufacturers to address weight balancing, camera placement, and other aspects of their product design. Although the hardware integration process may appear straightforward, each new drone still requires manual adjustments. Therefore, the overall process of integrating the ZIR kit can take from several weeks up to a month.

The **AI-powered software**, trained on open-source data, can identify various target types—including infantry, civilian automobiles, minivans, trucks, air defense systems, artillery, armored vehicles, and tanks. It automatically detects targets and locks on them from 1 km away and operates autonomously up to 3 km away, even in tough EW environments. With precision of roughly 90 cm, it can also engage moving targets traveling at speeds up to 64 km/h.

The company is pursuing the goal of full autonomy by developing a system that can independently fly and detect and engage targets. To advance this goal, the company employs **ArduPilot**, an **open-source** autopilot software for unmanned vehicles that supports autonomous navigation, waypoint planning, and real-time telemetry. Through ArduPilot, the system can operate **without communication** by uploading missions to locate and neutralize targets within a specified zone. Additionally, optical navigation replaces GPS in environments lacking satellite coverage, a capability tested and validated by a successful three-mile test range flight that returned to its starting point without GPS.

An additional key consideration for the company is the system’s ease of use and the speed at which operators can train to use it. To achieve this, the company continuously collects feedback from new pilots, identifying issues they encounter and addressing these areas for improvement. The company also provides both video and written instructions for its software and hardware usage and collaborates

with drone schools by integrating the training for its system into their curriculum. Operators can learn the fundamental principles of targeting systems in a single day and enhance their proficiency with further practice.

Case Study 7: Skydio's ATR Evolution from Consumer Tech to Battlefield AI

In an interview with CSIS, the Skydio team shared that their journey in Ukraine began with a critical weakness: Its older drone, the X2, operated on static frequencies, making them **highly vulnerable** to EW. Initially designed based on U.S. military procurement requirements from the early 2010s, these drones lacked frequency agility, as they were intended for environments like Iraq and Afghanistan, where EW challenges were minimal or absent. Consequently, when the war in Ukraine erupted in 2022, the drones struggled against Russian jamming. Just as the Skydio team had warned, EW led to communication failures, reduced operational range, and a damaged reputation among Ukrainian forces.

Determined to address these shortcomings, Skydio teams made over 30 visits to Ukraine between 2022 and 2024, which helped to incorporate insights from the battlefield into the development of the **X10D drone**. While the drone can resist jamming, navigate without GPS, and integrate into various command and control systems, the X10D mainly addresses broader requirements from the commercial sector and for public safety. However, the focus in this case study is a breakthrough in ATR that became central to the drone's effectiveness in ISR missions.

Skydio's ATR capabilities have evolved from simple object tracking—first developed for consumer drones in 2014—to a sophisticated detection system that uses deep learning. Initially used to track athletes in sports applications, the software was later adapted for military use. Today, Skydio's deep learning and computer vision teams continuously refine these models, enhancing detection accuracy for both electro-optical and infrared imagery. The X10D now features the most advanced thermal camera in its class, providing radiometric infrared imaging, which allows operators to assess temperature variations, detect heat signatures, and determine whether, for example, a vehicle was recently active or has been abandoned.

ATR capabilities are enhanced with Skydio's focus **visual-inertial odometry** (VIO). The X10D drone is equipped with six ultra-wide-angle navigation cameras, covering more than 200 degrees each, allowing it to create a 3D map for obstacle avoidance. Initially, VIO was limited to flights below 30 m in altitude, as higher altitudes lacked sufficient visual features for stable navigation. However, by using improved traditional geometric computer vision techniques and leveraging a large amount of internal Skydio data, Skydio extended its GPS-denied navigation to 300 m in altitude, making it far more practical for tactical reconnaissance in both open battlefields and urban environments. This improvement has been crucial for urban warfare and ISR missions in dense cityscapes, where GPS signals are often unreliable due to EW or structural interference.

To maximize its impact, Skydio has worked to integrate X10D drones into Ukraine's command and control networks, including the Delta system, used by the military and other agencies' systems. This integration allows sharing drone ISR feeds across multiple units, enhancing battlefield situational awareness.

Due to these advancements, Skydio has shipped about a 1,000 drones to Ukraine, many of which are now deployed on the **Ukrainian battlefield**. They are primarily used for tactical ISR, helping to detect, track, and target enemy assets, including other drones, ground vehicles, and EW units. Their ability to resist jamming, navigate without GPS, and provide high-fidelity ATR data has significantly improved their effectiveness in combined drone and artillery strike operations, a key tactic in Ukraine's evolving drone warfare strategy.

LESSONS LEARNED

1. **Delegating target recognition tasks to AI-enabled ATR systems onboard unmanned platforms has proved highly effective in reducing human-related limitations and enhancing mission outcomes.** By automating equipment identification and other object-detection processes, drones lessen the burden on frontline personnel, who might be hindered by fatigue, stress, or skill level. This shift allows operators to concentrate on more complex, high-level decisionmaking, ultimately improving operational efficiency and situational awareness.
2. **Ukrainian drone manufacturers prioritize developing specialized autonomy features that can integrate with any unmanned platform.** These companies have developed their core business models around refining standalone autonomous capabilities, such as AI-enabled ATR. They aim to ensure seamless implementation across a variety of unmanned systems, thereby accelerating overall technological advancement in the sector.
3. **Ukrainian engineers leverage open-source technologies and existing computer vision models to accelerate research and development and make it more affordable.** By incorporating readily available software solutions, including open-source computer vision frameworks, developers can expedite the creation and deployment of ATR systems. This cost-effective strategy is particularly appealing for attritable or expendable platforms, where reduced unit and development costs outweigh the benefits of highly customized solutions.

TRENDS

1. **The proven efficiency of ATR-equipped systems drives the Ukrainian military to start procuring more drones with autonomous capabilities.** In 2024, recognizing the operational advantages of ATR, Ukrainian forces initiated the procurement of 10,000 drones featuring AI-enhanced autonomy—an early step toward broader adoption of advanced autonomous systems. Although this number remains a fraction of the nearly 2 million drones contracted in 2024, it signals a significant move toward more autonomous and capable platforms.
2. **Equipping drones with affordable onboard computers enables AI models to perform real-time target recognition.** By installing low-cost processors directly into drone hardware, Ukrainian forces can deploy compact AI modules capable of identifying targets without relying on extensive external processing. This approach reduces latency, conserves bandwidth, and provides greater operational flexibility, particularly in environments where connectivity or remote computing may be limited.
3. **Using AI training techniques that require smaller datasets simplifies target recognition for drone missions.** Training AI algorithms typically demands extensive high-quality data. However, newer models designed for smaller datasets allow for more rapid development and

adaptation. This efficiency leads to quicker deployment of ATR functionalities, even when comprehensive training data for certain target types is limited.

4. To address evolving countermeasures like decoys and camouflage, Ukrainian engineers make continuous model upgrades and frequently retrain on updated operational data.

As adversaries adopt innovative methods to evade detection, ATR models must be repeatedly refined with real-world data. Regular updates not only keep the AI current but also mitigate the risk of misidentification due to emerging tactics, ensuring consistent target recognition performance under varying battlefield conditions.

5. A modular approach to ATR integration extends the technology's applicability across a wide range of unmanned platforms. For instance, when turrets are equipped with ATR systems, their precision in targeting and firing increases significantly. These turrets, in turn, may be mounted on trucks or unmanned ground vehicles, broadening their operational use and enhancing overall mission versatility.

AI in Autonomous Navigation

While impressive footage of drones striking fleeing Russian soldiers and estimates valuing **destroyed equipment** in the millions of dollars may captivate public attention, these visuals do not fully represent the complexities involved. Ukrainian operators on the front lines shared in interviews with CSIS that most small, low-cost FPV drone missions succeed only about 10 to 15 percent of the time, and even highly skilled operators typically reach only a 30 to 50 percent success rate. A last-mile navigation system can offer a significant boost to these numbers.

In the Ukrainian military, last-mile navigation specifically refers to the mechanism that guides the drone through its final approach once it is within visual range and the operator has confirmed the target. Although originally designed as an integrated feature, last-mile solutions are now procured as standalone systems that may be installed on various drone platforms. While their integration requires certain hardware upgrades—such as adding a compact computing chip or replacing **analog cameras** with digital ones—these modifications remain relatively simple, providing a flexible pathway toward more autonomous drone operations.

CURRENT CHALLENGES IN AUTONOMOUS NAVIGATION

The low success rate of drone strike missions reveals several critical challenges, which can be divided into four major issues:

1. **The Human Factor:** Operating FPV drones demands a specialized skill set that differs significantly from piloting consumer drones such as the DJI Mavic—often referred to in Ukrainian military circles as the “iPhone of drones” for its self-stabilization and automated flight functions. FPV drones require **precise manual control** of pitch, roll, yaw, and throttle, leaving little room for error.

This complexity is magnified by a range of operational stressors, including signal **latency delays** of two to three seconds, harsh weather conditions, and fast-moving, unpredictable targets. Drone operators must adapt quickly to these variables while facing the added pressure of battlefield threats, such as the risk of detection and counterattack. Combined, these factors considerably increase the likelihood of operator mistakes and the attractiveness of last-mile autonomous navigation. For example, if the target is on a fast-moving vehicle, the signal latency alone may mean that autonomous last-mile navigation (sometimes referred to as “terminal navigation”) is required for a successful strike.

2. **Electronic Warfare:** EW remains a constant threat to drone operations, with both Russian and Ukrainian forces **deploying** advanced jamming and spoofing techniques. Jamming specifically involves **broadcasting** high-power electromagnetic energy over a particular frequency band—commonly used for radio control or GPS—to drown out legitimate signals, severing the communication link between a drone and its operator. Once the drone loses access to navigational or positional data, it becomes nearly impossible to steer or monitor unless it has alternative capabilities onboard.

On the Russian side, EW units **employ** two main strategies. The first consists of localized protection bubbles, a type of portable equipment that jams signals within a radius of roughly 200-300 m around high-value assets, thwarting drones during their final approach. The second strategy, long-range jamming, relies on large power generators and specialized equipment to

project disruption across much larger areas. Although localized jamming affects only a confined zone, both methods pose formidable challenges for UAVs dependent on sustained operator remote control.

Notably, Ukraine's EW efforts sometimes intensify these difficulties. **According** to Colonel Vadym Sukharevskyi, the commander of Ukraine's Unmanned Systems Forces, friendly jamming in shared airspace frequently interferes with Ukrainian drones, creating additional layers of complexity for operators.

3. **Radio Wave Physics:** The physical limitations of **radio wave propagation** present another challenge. The radio horizon, where terrain or obstacles such as hills and buildings interrupt signals, can isolate drones from their operators, leaving them stranded and unable to complete missions. Although **relay systems** can partially address this issue, they are not always available or reliable in the fast-changing and unpredictable conditions of the battlefield, further complicating effective navigation and final approach to the target.
4. **Engaging a Moving Target:** This issue is an especially challenging task and a unique skill for drone operators to master. When a drone chases a target from behind, the relative speed of its approach is reduced due to their simultaneous movement in the same direction, which gives an operator more time to react to changes in movement. In contrast, a head-on approach increases difficulty because both drone and target converge at high speed, limiting the window for flight path adjustments and often requiring some prediction. Lateral or perpendicular movements exacerbate the problem further, as an operator must constantly align with the target's shifting position.

HOW AI CAN ADDRESS CHALLENGES

A major step toward overcoming the challenges of battlefield drone operations is **autonomous navigation**, which leverages machine learning instead of using fixed, rule-based commands. By integrating advanced AI algorithms and sensor suites directly onto the drone, these platforms can make instantaneous decisions about flight paths, localization, and obstacle avoidance independently of a constant operator feed. In essence, the drone constructs an evolving picture of its environment using machine vision and deep learning algorithms, enabling it to **map surroundings**, pinpoint its location without GPS, and dynamically chart a course around unforeseen hazards.

The transition to autonomous flight becomes most critical once a target is identified, whether via ATR or manual operator input. At this stage, a last-mile guidance system assumes direct control over flight, **charting** a final approach and engagement path. By relying on real-time sensor inputs, the drone adjusts for variables like wind gusts, shifting terrain, or unanticipated obstacles.

Techniques such as **visual odometry** allow the drone to continuously assess its position, maintaining stable flight even under degraded communications. Consequently, localized EW efforts—often limited to a specific radius—lose much of their **disruptive power**: the drone locks onto a target from beyond jamming range and proceeds without a human in the loop, significantly lowering the risk of signal loss.

Future iterations of last-mile guidance can achieve an even higher degree of precision against moving targets. With adaptive flight path corrections and predictive modeling informed by large datasets

of vehicle or human movement, AI systems can anticipate potential maneuvers. Simultaneously, continuous optical tracking further refines these forecasts, allowing the drone to rapidly respond to sudden deviations.

Future iterations of last-mile guidance can achieve an even higher degree of precision against moving targets.

Although current systems still operate within what drone operators call a “reasonable impact radius”—meaning a tank or trench is likely to be hit, though not necessarily at its most vulnerable point—ongoing AI advancements and refinements in onboard hardware promise to narrow this margin considerably.

Case Study 8: VGI-9, an Autonomous Navigation System

As drone manufacturers shared with CSIS, **VGI-9** is one of the most widely used targeting systems. It transforms an FPV drone into a semiautonomous weapons system **capable of locking on the target and striking** even moving targets at speeds of up to 80 km/h with precision.

First, the system requires a secure PIN code to activate the targeting function before each mission. Consequently, adversaries capturing the drone without the code cannot use its targeting capabilities. Once the drone is airborne, the pilot guides it to the operational zone while observing a real-time video feed with an enlarged picture in the corner of the screen to facilitate precise target identification.

The system continuously monitors EW threats. The on-screen interface provides real-time feedback on signal interference through **received signal strength** (RSS) and **signal-to-noise ratio** (SNR) indications. If enemy jamming is present, the SNR value drops close to or below zero, indicating that the drone connection is heavily disrupted.

To counteract this, the drone is equipped with a cruise control mode. If the drone encounters a disruption, the operator maintains a steady altitude and activates cruise control. As the name suggests, once engaged, the mode locks the drone’s altitude, speed, and direction, allowing it to continue its flight path even in areas with severe signal jamming. This fail-safe ensures the drone does not crash due to signal loss but instead bypasses jamming zones and remains operational beyond them, where the enemy forces or precious equipment can be located. This feature alone significantly increases the chances of mission success.

As the drone approaches the target area, the pilot searches for the target. Once the target is visually confirmed, the pilot activates the target lock-on function. At this point, control transitions from manual flight to autonomous engagement. The drone’s onboard system locks on to the selected point and begins its final descent toward the target without requiring further input from the pilot. If communication is still available, the pilot retains limited ability to make microadjustments. Using the right control stick, the pilot can slightly adjust the drone’s trajectory to ensure an optimal strike (e.g., the least-armored portion of an enemy tank).

In a fully autonomous strike, the system ensures the drone stays on course, even without pilot intervention. The drone's onboard AI handles the last moments of navigation, ensuring the maximum probability of a successful hit.

The current state of this technology has limitations. The system significantly enhances effectiveness against large, high-value targets like tanks and artillery, but its precision is limited when targeting specific parts of a vehicle. While it ensures the drone reaches the target, it does not guarantee a strike on an exact point, such as a vulnerable section of a tank, to destroy the target completely, though disabling the target remains feasible.

Case Study 9: Autonomous Navigation from The Fourth Law

Yaroslav Azhnyuk, founder of the company **The Fourth Law**, told CSIS that his company's goal is to develop an AI-enabled guidance system for UAVs that allows them to operate in fully autonomous mode. The Fourth Law developed a module for FPV drones—an inexpensive yet powerful electronic component that includes a camera and a small computer board with software that costs **around \$50 to \$100**. This module may be installed on any of the most common configurations of FPV drones, whether 7 or 10 inch, between the two mounting rails where the drone's front camera is usually placed. This technology is already operational and in serial production, integrated with dozens of manufacturers, and these systems are actively in use on the front line.

The demonstration made to CSIS showed an FPV feed with added zoom and an active “target seeker,” illustrating how analog video, despite its poor resolution, remains widely used for its low cost and reliability. Once the pilot identifies a moving truck within the zoomed area, flipping a single switch encases the target in a red square and hands control over to the onboard AI. Two algorithms then work together: one continuously tracks the target's movement, while the other manages the drone's complex flight mechanics. A separate neural network refines the target's boundaries in real time, ensuring precise engagement despite the vehicle's ongoing motion.

Company representatives told CSIS that The Fourth Law will soon introduce last-mile guidance for fixed-wing drones, allowing greater flight range, overcoming radio horizon limitations, and extending the operational distance by 48-96 km. However, the last-mile guidance system is just the first step in the company's five-step road map to full autonomy.

The second stage is the development of autonomous last-mile bombing. The process works like the current system, but instead of crashing into the target, the drone drops a bomb. This autonomous payload release system is already being tested in a lab. A computer can execute a drop with far greater precision than a human, even from complex maneuvers that a human pilot could not perform in time. After bombing is finished, the pilot regains control, bringing the drone back instead of losing it after every mission.

A third crucial technology is also undergoing testing. Automatic targeting uses neural networks to identify and track targets autonomously. The team has successfully optimized object recognition using neural networks to run efficiently on very inexpensive hardware.

By combining all three technologies, the company hopes pilots need only launch the drone and assign a waypoint on the map. The drone would take off, fly to the target, execute the drop, return, and land—all in complete radio silence and full autonomy, without requiring pilot intervention.

As a fourth step, the system will be able to navigate without GPS, using preloaded maps, onboard sensors, and optical navigation, ensuring mission success even in GPS-denied areas.

The fifth stage of development involves automating takeoff and landing processes for both copter and fixed-wing drones, a critical advancement for the autonomous engagement of airborne threats such as enemy FPV drones. For instance, in a scenario in which troops are positioned in a trench under attack by enemy FPV drones, several sentry drones could be deployed in front of the trench and equipped with cameras to scan the sky. Upon detecting an incoming enemy FPV drone, these sentry drones could launch autonomously, either colliding with the threat or detonating nearby, thereby neutralizing the danger and safeguarding allied forces.

In many ways, The Fourth Law's road map to full autonomy reflects the general approach Ukrainian companies take in developing autonomous capabilities.

Case Study 10: Ukrainian Long-Range-Strike Drones

Among the many military systems Ukraine is enhancing with AI capabilities are **one-way attack drones** (OWA-UAVs). While these kamikaze drones are used everywhere along the front line, long-range-strike drones with some elements of autonomy represent a particularly interesting case. These drones are developed exclusively in Ukraine and have seen **widespread use** across various Ukrainian agencies. Their **effectiveness** and **fast evolution** demonstrate their **ability to reach** nearly any strategically significant target inside Russia, carrying enough explosives to destroy critical infrastructure, including factories, buildings, and airfields, along with the aircraft stationed there.

Autonomous navigation has become an indispensable feature of long-range-strike drones, as flying long distances into enemy territory requires overcoming the enemy's air defense and a 60 km-wide strip of EW systems along the border. While official sources in Ukraine refuse to comment on the technology they use, an industry representative revealed in an interview with CSIS that some of these advanced drones leverage basic AI technology for navigation and antijamming capabilities. An onboard computer allows the drones to navigate in EW environments and follow the preplanned flight route, often developed using large amounts of intelligence data collected by Ukraine or shared by allies.

Autonomous navigation has become an indispensable feature of long-range-strike drones, as flying long distances into enemy territory requires overcoming the enemy's air defense and a 60 km-wide strip of electronic warfare systems along the border.

Usually such a flight path consists of more than **1,000 waypoints** to evade Russia's air defense systems. The computer uses machine vision algorithms to compare what the drone "sees" using its sensors with the satellite and terrain data preloaded in its computer. AI models, trained to recognize geography and

targets, allow the drone to autonomously identify its location and navigate to its target during the final approach with high precision and without requiring satellite communication.

One prominent example of a successful long-range-strike drone is the Lyutyi, which is reportedly responsible for up to **80 percent** of successful attacks on Russian oil refineries. However, this drone is not yet fully autonomous. It can conduct some parts of the **flight route autonomously**, but its final approach to the target is mainly a manual process. Ukrainian officials declined to comment on how the system maintains communication with operators during the final approach phase. Also, such long-range-strike missions require meticulous preparation by analysts, intelligence officers, special services, and the operators themselves.

One Lyutyi operator **noted** he usually receives a detailed target analysis before the mission. He does not know the people who create the analysis, but the mission plan is a 15-20-page document describing the target and mission plan in minute-by-minute detail. It includes comprehensive information on factors such as air defense systems, satellite imagery, and radar data.

The same operator illustrated the complexity of planning an attack route by describing the challenges associated with a drone's approach to its target. The drone must approach the target against the wind, and can face additional obstacles in its trajectory, such as pipes or other structural elements, necessitating careful navigation to ensure precise strikes. Moreover, the target is situated over 1,250 km away, and the operation often proceeds without an optical channel, thereby intensifying the level of difficulty involved and showing that the drone is operated manually in the last-mile approach.

Case Study 11: Autonomous Long-Range ISR Capability from Shield AI

During 2024, CSIS conducted several discussions with Shield AI, a U.S. defense technology firm focused on AI and drone systems. These conversations provided insights into how the company's technology and collaboration with the Ukrainian military have evolved.

Early in the summer of 2024, Shield AI delivered a small batch of **V-BAT** systems to Ukraine for testing. At the time, to contend with EW, the V-BATs relied on sophisticated frequency hopping, spectrum changes, and higher-powered communication links rather than fully autonomous functionality.

Later in 2024, Shield AI organized a two-part demonstration of the V-BAT's capabilities in Ukraine. The first phase took place at a testing range, where seven powerful jammers operated simultaneously to challenge the aircraft's resilience—an exercise the V-BAT passed successfully. In the second phase, Ukrainian forces launched the V-BAT from roughly 40 km behind the front lines, flew it an additional 95 km into contested territory, and located a battery of SA-11 Buk surface-to-air missiles. During this mission, the V-BAT relayed the target coordinates for a successful High Mobility Artillery Rocket System (HIMARS) strike, with Shield AI engineers providing field support.

In both phases, the aircraft was equipped with Shield AI's **Hivemind** software, which offers **state estimation** capability in GPS-denied environments. The company stated that such capabilities are crucial to mission success. This **state estimation software** employs factor graph optimization, enabling unmanned vehicles to accurately determine their position, orientation, and velocity in real time by integrating sensor data from cameras, GPS, and inertial measurement units, even in

environments with limited communication or GPS access. The system continuously refines this sensor information, recognizing potential hazards and adapting its flight path accordingly.

AI-driven navigation in GPS-denied environments has proved a cornerstone for long-duration reconnaissance efforts.

The demonstrations revealed another advantage of V-BAT for Ukrainian battlefield operations—its flight range and loiter times. When the operation time of a drone increases to 8 to 10 hours instead of 1 to 2, it dramatically enlarges the window for ISR missions to identify and track critical targets. Therefore, AI-driven navigation in GPS-denied environments has proved a cornerstone for long-duration reconnaissance efforts.

Consequently, the Ukrainian military placed an **order** with Shield AI for more than 200 Shield AI drones, though the company's production capacity at the time was only 120 units per year, according to an interview with company representatives.

LESSONS LEARNED

- 1. Autonomous navigation makes drones strikes three to four times more likely to succeed.** By removing the need for constant manual control and stable communications—both vulnerable to EW and human stress—autonomous drones raise the target engagement success rate from around 10 to 20 percent to around 70 to 80 percent. Multiple interviewees from different Ukrainian military organizations and companies agreed that these figures are correct. This high level of reliability reduces demands on the skill level of the operator and makes the weapons system accessible to a greater number of warfighters.
- 2. Drones with autonomous navigation reduce overall strike costs by minimizing both drone losses and mission attempts.** Because these drones can conduct missions effectively and then return to base, fewer replacement units are required. In turn, military budgets may be allocated more strategically, focusing on additional research and development or acquiring specialized assets.
- 3. Faster, more precise strikes decrease the time frame for enemy detection and retaliation, ultimately reducing the risk of counterattack.** When missions are completed in fewer attempts, adversaries have less opportunity to pinpoint the location or timing of an attack. This improved operational tempo decreases the likelihood of immediate enemy responses and increases the odds of mission success.
- 4. Minimal training time for autonomous drone operation broadens access for frontline personnel.** Training that used to require extensive flight hours can now be condensed into a matter of hours or even minutes, according to a CSIS conversation with a Ukrainian military drone pilot instructor. This development empowers a larger pool of soldiers to operate drones effectively with minimal specialized skills.
- 5. Encrypting onboard AI software preserves Ukraine's technological lead by making autonomous systems difficult to reverse engineer.** Although adversaries can replicate hardware designs within weeks, sophisticated encryption measures on AI-enabled software slow

down their ability to produce comparable systems. By maintaining a secure software advantage, Ukrainian forces continue to outpace opposing drone autonomy initiatives.

TRENDS

- 1. Ukrainian authorities proactively introduce standalone autonomous modules into service, paving the way for scalable procurement and frontline deployment.** The Ukrainian military has initiated the process of codifying autonomous modules and introducing them into service in order to scale their procurement. By standardizing these modules as distinct components and developing guidelines on their integration and usage, the military can enable quicker adaptation of its arsenal and tactics to operational demands.
- 2. Drone training programs are incorporating autonomous navigation into their core curriculum to address the growing prevalence of self-guided systems.** Recognizing the shift toward AI-assisted flight, educational institutions for drone operators now equip students with the skills to manage both manual and autonomous functionalities. On average, training to use autonomous functionalities takes less than a day.
- 3. Enabling fully autonomous flights—from takeoff through mission execution to landing—reduces operational costs and the need for constant equipment replenishment.** This holistic approach to autonomy mirrors advances in commercial aerospace, where [reusability](#) significantly lowers costs. By extending the life cycle of unmanned systems, militaries can allocate resources more efficiently while maintaining readiness.
- 4. Implementing AI-enabled navigation in ground, sea, and undersea platforms marks the next major challenge, given the higher complexity and cost of these systems.** While aerial drones have led the way in autonomous operations, adapting similar capabilities for multidomain use requires tackling tougher technical and environmental hurdles. The promise to integrate autonomous navigation for ground systems is big, but practical implementation represents a challenge that Ukrainian defense companies have not yet tackled.
- 5. Autonomous navigation serves as a key building block for drone swarms, though fully autonomous swarm operations remain in the early stages.** While Ukrainian forces have conducted small-scale experiments, they have yet to field true swarms in which drones communicate, make decisions, and adjust actions collaboratively. Developing this level of coordination will require substantial progress in AI algorithms, communication protocols, and real-time decisionmaking capabilities.

Conclusion

Modern unmanned systems in Ukraine are not yet fully autonomous. While AI substantially enhances certain functions—from ISR to ATR and navigation—these enhancements are still partial in scope. The need to remove humans from direct combat remains a driving vision, but the limited scale of true autonomy reveals the extent of current technological limitations.

Rather than rely on comprehensive end-to-end solutions, Ukraine has adopted a step-by-step approach, incrementally introducing AI-driven capabilities to address specific operational challenges. This approach not only reflects the realities of ongoing warfare but also demonstrates the practical ways that military concepts, such as target selection and last-mile navigation, are being converted into battlefield-ready functionalities.

Overall, AI has made a substantial difference in streamlining data analysis, reducing human error, and coping with electronic warfare, but it still requires human oversight—particularly for engagement decisions.

Overall, AI has made a substantial difference in streamlining data analysis, reducing human error, and coping with EW, but it still requires human oversight—particularly for engagement decisions. Although these discrete functions bring Ukrainian unmanned systems closer to a vision of full autonomy, they have not converged into a seamlessly integrated autonomous process. In addition, a number of factors should be considered for future autonomy deployment:

- **AI Model Complexity and Transparency:** Modern AI systems may be smaller and faster to train, but their black-box nature makes outcomes unpredictable in combat. Full autonomy remains high risk unless human operators can understand AI decisionmaking, ensuring reliable performance in life-or-death situations.
- **Operational Readiness and Integration in Military Strategy:** Adopting autonomous systems calls for thorough planning, including clear concepts of operation and inclusion in every part of the doctrine, organization, training, materiel, leadership, personnel, and facilities (DOTMLPF) framework, so that processes and policies match the demands of new technology.
- **Regulatory and Legal Gaps:** Autonomy’s legal boundaries vary by country and remain largely undefined. Ukraine, for example, lacks definitions for “autonomy” and “autonomous weapons systems.” At the same time, it plans to align with international law, which also has critical uncertainties regarding ethical and legal questions related to autonomous systems.
- **Data for AI Training Enabling Autonomy:** The war in Ukraine provides ample datasets to accelerate AI development and training using real-world data on enemy equipment. Nations lacking such direct battlefield information must plan well ahead to build and refine suitable datasets on enemy equipment for training and validating autonomous systems.

Nevertheless, key trends in Ukraine point toward a future in which reliable full autonomy might become a reality. First, the adoption of modular architectures for both hardware and software demonstrates a

flexible approach that reduces development costs and streamlines upgrades. By separating AI software from the physical platforms, Ukrainian defense companies can more quickly update or replace specific functions, such as target recognition, without redesigning entire systems.

Second, a strong emphasis on open-source technologies and separate software sales demonstrates the benefits of leveraging existing innovations rather than reinventing each component from scratch. This helps maintain a rapid research and development cycle while keeping hardware affordable.

Third, the growing miniaturization of AI models, trained on smaller, carefully curated datasets, makes onboard real-time processing increasingly feasible. The resulting ability to execute advanced tasks, such as last-mile autonomous navigation, without depending on stable communications or satellite guidance reduces susceptibility to EW and expands operational reach.

Fourth, broader integration of unmanned systems into military strategy and operations, from common operating pictures to doctrinal reforms, signals that Ukrainian forces are serious about scaling AI beyond the experimental stage.

Although these measures do not yet combine into an entirely autonomous battlefield, they form the essential foundations of a technology road map that one day might yield fully autonomous warfare—but with continued human involvement where critical ethical and strategic judgments are required. ■

***Kateryna Bondar** is a fellow with the Wadhwani AI Center at the Center for Strategic and International Studies in Washington, D.C.*

This report is made possible by general support to CSIS. No direct sponsorship contributed to this report.

The author would like to thank Henry Riche for research support.

This report is produced by the Center for Strategic and International Studies (CSIS), a private, tax-exempt institution focusing on international public policy issues. Its research is nonpartisan and nonproprietary. CSIS does not take specific policy positions. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the author(s).

© 2025 by the Center for Strategic and International Studies. All rights reserved.

Cover Photo: Anton Petrus/GettyImages