Issue Brief
June 17, 2026

Innovation Under Fire: Ukraine's Wartime Adaptation and the Future of European Security

Melita Phachulia

Photo credit: Dancing Man / Shutterstock.com

Russia's illegal, unprovoked, and unjustified full-scale war against Ukraine has accelerated the emergence of one of the most dynamic wartime innovation ecosystems in Europe. Ukraine's adaptation extends beyond battlefield technologies to cybersecurity, artificial intelligence (AI), digital governance, quantum-relevant research domains, and volunteer-driven defense production networks. This issue brief argues that Ukraine represents an emerging model of adaptive statehood, in which innovation is continuous, decentralized, and institutionalized through platforms such as BRAVE1 and the Ministry of Digital Transformation of Ukraine. Under sustained military and hybrid pressure, governance, technology, industry, and society adapt in parallel, blurring traditional civilian-military boundaries. Ukraine's experience demonstrates that modern warfare is defined not only by kinetic capabilities but also by the resilience of interconnected digital, industrial, and institutional systems. For Europe, this model offers critical insights into the future of security, where adaptability, cyber resilience, industrial scalability, and cross-sectoral innovation are becoming crucial to strategic stability and collective defense.

Introduction

War compresses time. Decisions are made faster, systems are stress-tested, and failure has immediate consequences. In Ukraine, Russia's full-scale invasion has acted as a systemic catalyst, reshaping how the state operates across military, technological, and institutional domains. Development cycles that would typically take years have been compressed into weeks or even days, forcing rapid iteration across defense, governance, and industry.

Over more than four years of large-scale war, Ukraine has accumulated extensive operational experience with emerging technologies, particularly unmanned systems. What distinguishes this

adaptation is its multidimensional nature. Innovation has evolved beyond the development of individual technologies to form a broader resilience architecture in which industrial capacity, technological development, and societal mobilization reinforce one another.

The result is a state operating as a continuously adapting system under hybrid and kinetic pressure. Ukraine's wartime experience demonstrates that resilience in modern war increasingly depends on the interaction between digital governance, industrial flexibility, cybersecurity, AI integration, and societal participation.

For European states and NATO, Ukraine provides a practical model of how modern defense structures adapt under sustained threat conditions. The war has become not only a military confrontation, but also a large-scale laboratory for technological and institutional adaptation.

"One of the most significant structural transformations in Ukraine during the war has been the rapid evolution of its digital governance system. The Ministry of Digital Transformation has ensured continuity of state functions under conditions of disruption, displacement, and cyberattack. At the center of this transformation is the Diia platform, which has evolved into a digital backbone connecting citizens, institutions, and security functions.

Adaptive Governance and Digital Resilience

Digital State Transformation and the Emergence of the Agentic Model of Governance

One of the most significant structural transformations in Ukraine during the war has been the rapid evolution of its digital governance system. The Ministry of Digital Transformation has ensured continuity of state functions under conditions of disruption, displacement, and cyberattack.[1]

At the center of this transformation is the Diia platform, which has evolved into a digital backbone connecting citizens, institutions, and security functions.[2] Rather than serving only as an e-governance platform, Diia maintains the continuity of public services during wartime and strengthens overall state resilience.

This aligns with the concept of the "agentic state," in which governance becomes proactive rather than reactive.[3] Through automation, data integration, and real-time processing, state institutions can anticipate needs and respond dynamically. In practice, this has allowed Ukraine to sustain administrative functions under wartime conditions, effectively transforming governance into an integral component of the national security architecture.

Digital systems in Ukraine are therefore increasingly dual-use by design. They support civilian resilience while simultaneously facilitating defense coordination, illustrating how governance itself becomes embedded within broader security frameworks. For Europe, this suggests that digital governance systems must be treated as crit-

ical infrastructure and integrated into national security planning.

Cybersecurity as a Continuous Domain of National Survival

Ukraine's cybersecurity environment has become one of the most intense and sustained cyber conflict zones globally. Since 2014, when Russia first attacked Ukraine,[4] and especially after the full-scale invasion, the country has faced persistent cyber operations targeting government institutions, critical infrastructure, and communications networks.

In response, Ukraine has developed a distributed cybersecurity framework that combines state institutions, private sector actors, international partners, and volunteer cyber communities. The Computer Emergency Response Team (CERT-UA),[5] operating under the State Service for Special Communications and Information Protection of Ukraine (SSSCIP),[6] coordinates national cyber defense and incident response. This structure enables rapid detection, response, and recovery.

Recent developments reflect Ukraine's shift toward integrated digital defense. In 2025, Ukrainian President Volodymyr Zelenskyy signed Law No. 4336-IX, strengthening cybersecurity protections for state information systems and critical infrastructure through coordinated incident response mechanisms, enhanced information-sharing protocols, risk-based security management, and designated cybersecurity roles across public institutions. This approach enables rapid detection and recovery while ensuring continuity of critical services even during large-scale cyberattacks.[7]

Cybersecurity has thus become a foundational layer of national resilience, extending far beyond technical protection into the core functioning of the state. For Europe, Ukraine demonstrates that cybersecurity must be understood as a structural component of defense policy rather than merely a supporting capability. European cybersecurity frameworks, including those developed under the EU Cybersecurity Strategy,[8] reflect this shift, but Ukraine provides an operational demonstration of these principles under wartime conditions.

> ***"AI has become a key enabler of Ukraine's wartime innovation landscape. Notably, AI development in Ukraine is highly decentralized. Startups, volunteer programmers, military units, and private technology companies contribute directly to iterative innovation processes, creating a flexible but complex technological environment.***

Artificial Intelligence and Distributed Decision-Making

AI has become a key enabler of Ukraine's wartime innovation landscape, supporting battlefield intelligence, drone targeting, logistics coordination, cybersecurity monitoring, and governance systems. By processing large volumes of drone imagery and sensor data, AI improves situational awareness, shortens decision-making cycles, and reduces the cognitive burden on operators, enabling faster responses in high-pressure combat environments.

In this context, the Ministry of Defense of Ukraine established the Defense AI Center "A1,"[9]

with the support of the Government of the United Kingdom (UK). The initiative reflects a broader shift toward operational integration of AI in warfare, focusing on tools capable of predicting adversary behavior, strengthening resilience against electronic warfare (EW), and accelerating battlefield decision-making speed across domains. It is designed as a coordination hub linking the military, the tech sector, and international partners to accelerate the deployment of AI-enabled defense solutions.[10]

Notably, AI development in Ukraine is highly decentralized. Startups, volunteer programmers, military units, and private technology companies contribute directly to iterative innovation processes, creating a flexible but complex technological environment. This distributed model enables rapid experimentation and deployment, while also introducing challenges related to interoperability, standardization, and coordination across actors.

> ***Ukraine is also integrating its innovation ecosystem with European defense structures. In April 2026, Ukraine and the EU launched BraveTech EU, a joint initiative focused on defense innovation, weapons development, and the scaling of emerging technologies. The initiative reflects Ukraine's growing role not only as a recipient of security assistance, but also as an active contributor to European defense innovation and industrial adaptation.***

At the same time, decentralization is supported by active state coordination. Institutions such as the Ministry of Digital Transformation, the Ministry of Defense, BRAVE1,[11] and the Defense AI Center "A1" provide funding mechanisms, testing environments, procurement support, and direct links between frontline units and developers. Rather than controlling innovation through rigid centralized structures, the Ukrainian state functions as an enabling platform connecting military demand with private-sector and volunteer innovation.

This hybrid model combines the flexibility of decentralized experimentation with the scaling capacity of state institutions. Ukraine's experience demonstrates that AI in modern war functions not only as a tool of automation, but also as a broader infrastructure for adaptive decision-making under crisis conditions.

Wartime Innovation and Industrial Adaptation

Defense Innovation and Industrial Scaling Under Pressure

Since 2022, Ukraine's defense innovation base has expanded rapidly, transforming from fragmented initiatives into a scalable industrial system. The number of defense technology companies has grown to approximately 1,500, with some firms reaching annual revenues of up to USD 150 million.[12]

This reflects the emergence of a scalable wartime innovation economy. While drone systems remain the most visible component of this transformation, the capability spectrum also includes EW tools, AI-enabled targeting

technologies, autonomous logistics platforms, and advanced communications infrastructure.

Innovation is driven by constant interaction between frontline units and developers, ensuring close alignment between operational needs and technological production. This significantly compresses the time between concept development, testing, adaptation, and battlefield deployment.

Technological creativity extends beyond high-end systems. Ukraine has used 3D printing for rapid repairs and modernized legacy equipment through digital integration.[13] At the same time, a wide range of solutions, from remote-controlled weapon systems to anti-drone technologies and thermal protection equipment, demonstrates how necessity drives both gradual and disruptive innovation.

As noted by Ukraine's Minister of Defense, Mykhailo Fedorov, Ukraine has withstood massive missile and drone attacks while significantly improving interception rates—approximately 80 percent for cruise missiles and nearly 90 percent for drones—highlighting the role of technological adaptation in strengthening national resilience.[14] Ukraine is also expanding domestic precision-strike capabilities. On May 18, 2026, Fedorov announced that Ukraine's first domestically developed glide bomb was ready for combat deployment,[15] reflecting broader efforts to reduce dependence on foreign systems and strengthen indigenous strike capabilities.

> ***"Electronic warfare functions not only as a tactical domain but also as a structural force shaping the pace and direction of technological innovation. Continuous jamming, signal disruption, and countermeasures have created an environment in which technological advantages are inherently temporary. Every innovation is rapidly countered, generating a cycle of continuous adaptation. This largely invisible contest is fundamental to understanding modern warfare.***

Technology and the Human Dimension of Warfare

Ukraine's wartime adaptation combines automation, robotics, and unmanned systems with a broader effort to reduce battlefield casualties and preserve scarce manpower. During Ukraine's Defense Industry Day in April 2026, President Zelenskyy emphasized the growing role of unmanned systems in modern warfare:

> "The future is already on the front line—and Ukraine is building it. These are our ground robotic systems. For the first time in the history of this war, an enemy position was taken exclusively by unmanned platforms—ground systems and drones. The occupiers surrendered, and the operation was carried out without infantry and without losses on our side…In other words, lives were saved more than 22,000 times when a robot went into the most dangerous areas instead of a warrior. This is about high technology protecting the highest value—human life. Ukraine is not just keeping up with change—Ukraine is among the leaders in the development of security technologies."

In the same address, Zelenskyy showcased more than 50 domestically developed systems, including drones, missiles, robotic platforms, naval drones, and air defense solutions, illustrating Ukraine's rapid transition toward unmanned, multi-domain warfare and its capacity to innovate simultaneously across land, air, and maritime domains.[16]

Institutionalizing Innovation: Coordination and Scale

While decentralized innovation remains a defining feature of Ukraine's wartime adaptation, the country has increasingly institutionalized coordination mechanisms designed to scale successful technologies and accelerate their adoption across the defense sector.

The BRAVE1 platform plays a pivotal role in this process, acting as a bridge between military demand and technological supply. By facilitating collaboration between developers, companies, and defense institutions, BRAVE1 accelerates the transition from prototype to deployment. This reduces bureaucratic delays and enables faster scaling of successful innovations.

> ***A defining characteristic of Ukraine's wartime adaptation is the integration of civil society into defense innovation. Volunteer networks, engineers, and private citizens contribute directly to the development and deployment of technologies, often operating at the intersection of civilian expertise and military necessity.***

Importantly, this institutionalization does not replace decentralization. Instead, it provides a structure through which diverse actors can operate more effectively. The challenge lies in maintaining the flexibility that characterizes Ukraine's innovation ecosystem while ensuring coherence, interoperability and scalability.

Ukraine is also integrating its innovation ecosystem with European defense structures. In April 2026, Ukraine and the EU launched BraveTech EU, a joint initiative focused on defense innovation, weapons development, and the scaling of emerging technologies.[17] The initiative reflects Ukraine's growing role not only as a recipient of security assistance, but also as an active contributor to European defense innovation and industrial adaptation.

At the same time, Ukraine's innovation network is becoming increasingly internationalized. Emerging partnerships, including cooperation with Gulf states in drone technologies, point to the global diffusion of wartime innovation practices.[18] A notable example is a Ukrainian-Japanese initiative to produce low-cost interceptor drones, costing about USD 2,500, designed to counter mass drone attacks. Targeted in part at Gulf markets, these systems illustrate how Ukrainian wartime innovation is redefining the cost-efficiency and accessibility of air defense systems.[19]

Transformation of Warfare: Drones, Iteration, and Electronic Warfare

From Heavy Platforms to Agile Systems

One of the most visible transformations in Ukraine's wartime adaptation is the shift from

platform-centric to system-centric warfare. Traditional heavy platforms, including tanks and naval assets, remain relevant but are becoming more vulnerable to low-cost unmanned systems.

Relatively inexpensive drones are now capable of neutralizing equipment that requires years and substantial resources to produce.[20] This asymmetry has reshaped the economics of warfare and forced a reconsideration of force structures.

Ukraine has responded by scaling production and diversifying its unmanned capabilities. Prior to the full-scale invasion, the country had a limited number of drone manufacturers. Today, it has developed a vast industrial base capable of producing millions of drones annually, from reconnaissance platforms to long-range strike systems.[21]

This expansion reflects a strategic shift toward quantity, adaptability, and rapid deployment. Ukraine's response has been both pragmatic and ambitious. Rather than attempting to compete symmetrically with a larger adversary, it has embraced a model based on scale, diversity, and flexibility.

The country has developed a broad range of unmanned systems, from small first-person-view (FPV) drones to long-range strike platforms and maritime systems capable of challenging Russian naval operations. Ukraine has effectively built an "army of drones," integrating domestic production with international support.[22] Naval innovation further reinforces this trend, with unmanned systems challenging traditional assumptions of maritime dominance in the Black Sea.[23]

The result is a redefinition of military power, where effectiveness comes from interconnected networks of systems rather than from individual platforms alone.

Iteration in Practice: From Improvisation to Serial Production

Ukraine's innovation model is often described as improvisational, but its defining feature is continuous iteration. Early battlefield adaptations have evolved into more standardized and scalable solutions through repeated cycles of testing and refinement.

First-person-view drones exemplify this process. Initially assembled from commercial components, they have been transformed into highly effective strike systems through incremental improvements informed by battlefield experience. This process is now moving toward industrialization. The development of serially produced military drones signals a transition toward standardization, allowing for faster scaling, more efficient training, and greater operational reliability.[24]

At the same time, experimentation continues with coordinated drone operations and early swarm capabilities, reflecting the ongoing evolution of unmanned warfare.[25]

Electronic Warfare as a Driver of Continuous Technological Adaptation

EW constitutes one of the most decisive yet less visible dimensions of the war. Continuous jamming, signal disruption, and countermeasures have created an environment in which technological advantages are inherently temporary.

Every innovation is rapidly countered, generating a cycle of continuous adaptation. This dynamic has driven rapid advances in autonomous navigation systems, resilient communication protocols, and AI-assisted targeting systems.

EW thus functions not only as a tactical domain but also as a structural force shaping the pace and direction of technological innovation across the entire defense ecosystem. This largely invisible

contest is fundamental to understanding the evolution of modern warfare.[26] It also underscores the importance of resilience—not only in physical systems but also in communication and control architectures.

Society, Information, and Distributed Resistance

Innovation from Below: Volunteers as Force Multipliers

A defining characteristic of Ukraine's wartime adaptation is the integration of civil society into defense innovation. Volunteer networks, engineers, and private citizens contribute directly to the development and deployment of technologies, often operating at the intersection of civilian expertise and military necessity.

Organizations such as Aerorozvidka[27] and international initiatives like Defense Tech for Ukraine[28] illustrate how grassroots efforts can evolve into operational capabilities. Crowdfunding platforms, including President Zelenskyy's United24 initiative,[29] channel global support into concrete outputs, from drones to protective equipment.

Volunteer engagement is not limited to technological development. Civilian-led drone-hunting units have emerged, actively targeting enemy UAVs and contributing directly to air defense efforts. These groups operate alongside formal military structures, blurring the line between civilian and combat roles.[30]

The impact of this societal mobilization is not only material but also cultural. Innovation becomes a shared endeavor embedded within a broader narrative of national resistance and resilience. Even modest contributions can have significant battlefield effects.

In August 2025, a Ukrainian long-range drone struck a Russian early-warning radar system approximately 1,800 kilometers from the border. Developed domestically within only a few years, this capability illustrates the speed with which Ukraine's innovation system translates experimentation into strategic reach.[31]

> ***Ukraine's experience challenges traditional European approaches to defense innovation, which have often prioritized stability and long-term planning. In high-intensity conflict environments, however, adaptability and speed of iteration become more important than optimization or long-term predictability.***

Yet decentralization also creates challenges related to coordination, interoperability, accountability, and legal frameworks. The integration of civilian actors into military innovation processes raises broader questions regarding governance and the future relationship between civil society and defense structures in modern warfare.

Information, OSINT, and the Transparency of War

The war in Ukraine has also demonstrated the growing importance of open-source intelligence (OSINT), which has become an integral part of both military operations and public understanding of the war.[32]

The widespread use of social media, satellite imagery, and digital platforms has created an unprecedented level of transparency. The ability to collect, verify, and analyze open-source data has become a critical capability.

This development has both advantages and risks. On the one hand, it enhances situational awareness and enables rapid dissemination of information. On the other hand, it creates vulnerabilities related to disinformation and information overload.

Ukraine's experience illustrates how information itself has become both a strategic asset and a contested operational domain within modern warfare.

Policy Implications and Recommendations

Ukraine's wartime adaptation offers several important lessons for Europe and NATO.

First, defense procurement and innovation cycles must become significantly faster and more flexible. Traditional acquisition models are often too slow for high-intensity war environments characterized by rapid technological change.

Second, governments should strengthen civil-military innovation ecosystems by improving cooperation between defense institutions, startups, universities, private industry, and volunteer networks.

Third, digital governance systems and cybersecurity infrastructures should increasingly be treated as core elements of national security architecture rather than as purely administrative functions.

Fourth, Europe and NATO should expand defense-industrial cooperation with Ukraine, particularly in drones, AI-enabled systems, EW, and autonomous technologies.

Finally, NATO interoperability frameworks must adapt to emerging forms of warfare shaped by low-cost systems, decentralized innovation, AI integration, and continuous technological iteration.

Conclusion: Innovation as a Structural Condition of Modern War and Implications for European Security

Ukraine's experience challenges traditional European approaches to defense innovation, which have often prioritized stability and long-term planning. In high-intensity conflict environments, however, adaptability and speed of iteration become more important than optimization or long-term predictability. The Ukrainian model highlights the importance of these qualities, alongside integration across sectors. It demonstrates how decentralized innovation can enhance resilience while also raising questions about coordination and sustainability.

For Europe, this suggests the need to rethink existing defense and security frameworks to better integrate rapid innovation cycles, cross-sectoral collaboration, and dual-use technological systems. This may require rethinking procurement processes, encouraging experimentation, and strengthening links between civilian and military innovation actors.

It also includes embedding cyber resilience, AI capabilities and digital governance systems more deeply within national and European security architectures. At the same time, Europe must adapt these lessons in a way that preserves institutional stability and democratic accountability.

For NATO, Ukraine shows the need to adapt

to faster innovation and more flexible forms of warfare. This means improving interoperability, strengthening civil-military cooperation, and scaling cost-effective technologies such as drones, AI-enabled systems, and EW technologies. Emerging partnerships, such as Ukraine's joint drone production initiative with Norway, illustrate how allied cooperation can accelerate industrial scaling and capability development.[33] It also highlights that resilience, across cyber, industry, and society, must be central to collective defense.

Ukraine's wartime transformation demonstrates that innovation is no longer a discrete phase of defense planning but a continuous condition of survival under pressure. The convergence of digital governance, cybersecurity, AI, quantum-relevant technologies, volunteer mobilization, and industrial-scale defense production illustrates the emergence of a new model of state adaptation.

"Innovation under fire" thus captures this transformation. In modern warfare, resilience depends not on superiority in any single domain but on the ability to adapt continuously across technological, institutional, industrial, and societal domains.

Author –

Melita Phachulia *is an Executive Assistant at the Institute for Security and Development Policy (ISDP), working closely with the Stockholm Center for Research and Innovation Security (SCRIS) and the Asia Program. She holds a master's degree in Disinformation and Societal Resilience from the University of Tartu, a bachelor's degree in Journalism from the University of Georgia, and a modular master's in Adult Education, with a focus on digitalization and democracy from Julius-Maximilians-Universität Würzburg. Her work focuses on hybrid warfare, security, research and innovation, and resilience with regional expertise in the Nordic-Baltic and Black Sea regions, as well as NATO-related security environments.*

About ISDP

The Institute for Security and Development Policy is a Stockholm-based independent and non-profit research and policy institute. The Institute is dedicated to expanding understanding of international affairs, particularly the interrelationship between the issue areas of conflict, security and development. The Institute's primary areas of geographic focus are Asia and Europe's neighborhood.

www.isdp.eu

Endnotes

1 Міністерство цифрової трансформації України [Ministry of Digital Transformation of Ukraine], https://thedigital.gov.ua/.

2 Diia, Govtech, Digital State UA, https://digitalstate.gov.ua/projects/govtech/diia.

3 Digital State UA, "Why Ukraine's Agentic State Matters Beyond Ukraine," March 17, 2026, https://digitalstate.gov.ua/news/govtech/chomu-kontseptsiia-ukrayiny-agentic-state-vazlyva-ne-lyshe-dlia-ukrayiny.

4 Kateryna Denisova, "When did the war in Ukraine start? A timeline of Russia's aggression," *Kyiv Independent,* February 21, 2024, https://kyivindependent.com/russias-war-against-ukraine-timeline/.

5 CERT-UA, https://cert.gov.ua/.

6 State Service for Special Communications and Information Protection of Ukraine, https://cip.gov.ua/en.

7 State Service for Special Communications and Information Protection of Ukraine, "President Zelenskyy Signs Law Enhancing Cybersecurity of State Information Resources," April 17, 2025, https://www.cip.gov.ua/en/news/prezident-ukrayini-volodimir-zelenskii-pidpisav-zakon-4336-ix-pro-kiberzakhist-derzhavnikh-informaciinikh-resursiv.

8 European Commission, EU Cybersecurity Strategy, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy.

9 Defense AI Center "A1," https://a1.mod.gov.ua/en#start.

10 Міністерство оборони України [Ministry of Defense of Ukraine], "Створюємо центр штучного інтелекту "А1": впроваджуємо AI у війну, щоб бути швидшими та ефективнішими за ворога у небі, на землі та в економічній сфері [We are creating the "A1" Artificial Intelligence Center: introducing AI into warfare to be faster and more effective than the enemy in the sky, on the ground, and in the economic sphere]," Telegram, April 18, 2026, https://t.me/ministry_of_defense_ua/15501.

11 Brave1, https://brave1.gov.ua/.

12 Artur Savchii and Florin Schönborn, "Ukraine's Defense Tech Industry: By The Numbers," Snake Island Institute, February 2026, 4, https://snakeisland-institute.s3.eu-north-1.amazonaws.com/Ukraine%E2%80%99s+Defense+Tech+Industry.pdf.

13 Svitlana Shcherbak, "Not Just "Game of Lego": How Ukraine Turned 3D-Printing into Decentralized Military Conveyor Belt," *Defense Express,* April 7, 2026, https://en.defence-ua.com/events/not_just_a_game_of_lego_how_ukraine_turned_3d_printing_into_a_decentralized_military_conveyor_belt-18078.html.

14 Ministry of Defense of Ukraine, "Losses of Russian forces now exceed Russia's mobilization rates, says Mykhailo Fedorov at the opening of the 34th Ramstein-format meeting," April 15, 2026, https://mod.gov.ua/en/news/losses-of-russian-forces-now-exceed-russia-s-mobilization-rates-says-mykhailo-fedorov-at-the-opening-of-the-34th-ramstein-format-meeting.

15 Mykhailo Fedorov, "Перша українська КАБ готова до бойового застосування [The first Ukrainian KAB is ready for combat use]," Telegram, May 18, 2026, https://t.me/zedigital/6800.

16 Президент України [President of Ukraine], "У зверненні з нагоди Дня зброяра Президент показав понад 50 видів української зброї, що з'явилася в умовах війни та вже довела свою ефективність [In his address on the occasion of the Day of the Gunsmith, the President showed more than 50 types of Ukrainian weapons that appeared in war conditions and have already proven their effectiveness]," April 14, 2026, https://www.president.gov.ua/news/u-zvernenni-z-nagodi-dnya-zbroyara-prezident-pokazav-ponad-5-10382.

17 Владислав Хоменко [Vladyslav Khomenko], "Україна та ЄС запустили BraveTech EU для спільної розробки озброєння [Ukraine and the EU launch BraveTech EU to jointly develop weapons]," *Militarnyi*, https://militarnyi.com/uk/news/ukrayina-ta-yes-zapuskayut-bravetech-eu/.

18 "The Drone Bridge: How Ukraine's Wartime Innovation Forges a New South-South Axis," March 27, 2026, Policy Stability, https://policystability.com/post/2026-03/the-drone-bridge-how-ukraines-wartime-innovation-forges-a-new-south-south-axis/.

19 Vlad Litnarovych, "A Ukrainian-Japanese $2,500 Drone Is About to Change the Gulf War—And Sparks Russian Fury," *United24 Media,* April 9, 2026, https://united24media.com/latest-news/a-ukrainian-japanese-2500-drone-is-about-to-change-the-gulf-war-and-sparks-russian-fury-17769.

20 Олександр Шумілін [Oleksandr Shumilin], "СБС і ГУР показали знищення в Криму літака АН-72 і бази підготовки важких дронів [SBS and GUR showed the destruction of an AN-72 aircraft and a heavy drone training base in Crimea]," Українська Правда *[Ukrainian Pravda],* April 2, 2026, https://www.belfercenter.org/publication/advancing-adversity-ukraines-battlefield-technologies-and-lessons-us.

21 Göran Roos and Johan Roos, "How Ukraine's defense industry innovates at the speed of modern war," Defense One, April 2, 2026, https://www.defenseone.com/ideas/2026/04/ukraine-defense-industry-innovates-modern-war/412594/.

22 Міністерство цифрової трансформації України [Ministry of Digital Transformation of Ukraine], "Армії дронів — рік. Масове виробництво дронів в Україні, ударні роти БПЛА, навчання операторів дронів — головні досягнення проєкту [Drone armies — a year. Mass production of drones in Ukraine, UAV strike companies, training of drone operators — the main achievements of the project]," Прес-офіс Міністерства [Ministry Press Office], July 26, 2023, https://thedigital.gov.ua/news/army/armii-droniv-rik-masove-virobnitstvo-droniv-v-ukraini-udarni-roti-bpla-navchannya-operatoriv-droniv-golovni-dosyagnennya-proektu.

23 H. I. Sutton, "Innovative Submarine Drone Is Ukraine's New Weapon Against Russian Navy," Naval News, May 10, 2023, https://www.navalnews.com/naval-news/2023/05/innovative-submarine-drone-is-ukraines-new-weapon-against-russian-navy/.

24 Roman Pryhodko, "Ukraine Develops Serially Produced 18 Inch Military Drone," *Militarnyi,* December 1, 2025, https://militarnyi.com/en/news/ukraine-develops-serially-produced-18-inch-military-drone/.

25 Міністерство оборони України [Ministry of Defense of Ukraine], "Лінія дронів: як працює нова доктрина війни [Drone Line: How the New War Doctrine Works]," Dronelife, April 9, 2026, https://mod.gov.ua/news/liniya-droniv-yak-praczyuye-nova-doktrina-vijni.

26 IISS, "Chapter Three: The Uninhabited War in Ukraine," March 2026, https://www.iiss.org/publications/strategic-dossiers/2026/uavs-isr-deterrence-and-war/the-uninhabited-war-in-ukraine/.

27 Aerorozvidka, https://aerorozvidka.ngo/en.

28 Defense Tech for Ukraine, https://defensetechforukraine.org/.

29 United24, https://u24.gov.ua/.

30 Veronika Melkozerova, "Inside Kyiv's volunteer drone-hunting squads," *Politico,* February 19, 2026, https://www.politico.eu/article/volunteer-drone-hunting-squad-ukraine/.

31 Illia Kabachynskyi, "Turns Out, Ukrainian "Housewife Drones" Hit Hard," *United24 Media,* April 2, 2026, https://united24media.com/war-in-ukraine/turns-out-ukrainian-housewife-drones-hit-hard-17520.

32 Jack Hewson, "A Private Company Is Using Social Media to Track Down Russian Soldiers," *Foreign Policy,* March 2, 2023, https://foreignpolicy.com/2023/03/02/ukraine-russia-war-military-social-media-osint-open-source-intelligence/.

33 Ministry of Defense of Ukraine, "Ukraine and Norway launch joint production of mid-strike drones," April 27, 2026, https://mod.gov.ua/en/news/ukraine-and-norway-launch-joint-production-of-mid-strike-drones.