



Survival of the Smartest?

Defense AI in Ukraine

Vitaliy Goncharuk

DAIO Study 24|22

Ein Projekt im Rahmen von

 **dtec.bw**
Zentrum für Digitalisierungs- und
Technologieforschung der Bundeswehr



About the Defense AI Observatory

The Defense AI Observatory (DAIO) at the Helmut Schmidt University in Hamburg monitors and analyzes the use of artificial intelligence by armed forces. DAIO comprises three interrelated work streams:

- Culture, concept development, and organizational transformation in the context of military innovation
- Current and future conflict pictures, conflict dynamics, and operational experience, especially related to the use of emerging technologies
- Defense industrial dynamics with a particular focus on the impact of emerging technologies on the nature and character of techno-industrial ecosystems

DAIO is an integral element of GhostPlay, a capability and technology development project for concept-driven and AI-enhanced defense decision-making in support of fast-paced defense operations. GhostPlay is funded by the Center for Digital and Technology Research of the German Bundeswehr (dtec.bw). dtec.bw is funded by the European Union – NextGenerationEU.

Ein Projekt im Rahmen von



Survival of the Smartest?

Defense AI in Ukraine

Vitaliy Goncharuk

DAIO Study 24|22

Ein Projekt im Rahmen von

 **dtec.bw**
Zentrum für Digitalisierungs- und
Technologieforschung der Bundeswehr



About the Author

Vitaliy Goncharuk is an entrepreneur. He holds his first company, Augmented Pixels, a company focusing on AI-based autonomous navigation and 3D mapping, to Qualcomm in 2022. Currently he runs two new startups dealing with AI. In addition, he was a member of the external innovation advisory board of Ukroboronprom and the first chairman of Ukraine's AI Committee from 2020-2022. Right now, he is head of the "AI for Defense" working group a Ukraine's AI Advisory Committee and founder of WiseRegulation.org, a think and do tank focusing on AI regulation. His X/Twitter account is @vactivity.

Design

Almasy Information Design Thinking

Imprint

Vitaliy Goncharuk, *Survival of the Smartest? Defense AI in Ukraine*. DAIO Study 24/22 (Hamburg: Defense AI Observatory, 2024).

An adapted version of this paper will appear in: Heiko Borchert, Torben Schütz, and Joseph Verbovsky (eds.) *The Very Long Game. 25 Case Studies on the Global State of Defense AI* (Cham: Springer, forthcoming).

Defense AI Observatory | Chair of Political Theory | Helmut Schmidt University
Holstenhofweg 85 | 22043 Hamburg | T +49 40 6541 2776
www.defenseai.eu | contact@defenseai.eu | @Defense_AIO

ISSN (online): 2749-5337

ISSN (print): 2749-5345

Content

- 1 Summary **6**

- 2 Thinking About Defense AI **8**
 - 2.1 Regulating Defense AI 9
 - 2.2 Re-Evaluating “Human in the Loop” in Modern Warfare 11

- 3 Developing Defense AI **13**
 - 3.1 AI’s War Stimulus 14
 - 3.2 Ukraine’s New Defense AI Priorities 15
 - 3.3 Ukraine’s New Defense AI Ecosystem 17

- 4 Organizing Defense AI **23**

- 5 Funding Defense AI **26**

- 6 Fielding and Operating Defense AI **29**

- 7 Training for Defense AI **32**

- 8 Conclusion **35**

- Literature **38**

1 Summary

Before Russia's full-scale invasion in February 2022, Ukraine had an advanced ecosystem to produce artificial intelligence (AI) solutions for commercial use. The country also ranked first in the number of AI companies in Eastern Europe¹ with more than 7,000 AI engineers and hosting research and development (R&D) offices of multinational companies like Amazon, Lyft, Google, Samsung, Grammarly and many others. In addition, the country approved its first national AI strategy² in 2020, which, among other priorities, also identified the importance of implementing AI in the field of security and defense. However, Ukraine's defense sector only used AI sporadically, as the defense industry was primarily state-owned, focused on traditional hardware, and was not known as a "hotbed" for innovative, especially software-driven solutions.

The current war between Russia and Ukraine has changed almost all these parameters. Unlike other conflicts over the last 30 years, this is a war among technologically advanced countries. Therefore, both sides began developing and fielding AI solutions for tasks like geospatial intelligence, operations with unmanned systems, military training, and cyber warfare. Consequently, the war in Ukraine became the first conflict where both parties compete in and with AI, which has become a critical component of success.

In 2022, Ukraine's resilience originated from a more active use of awareness systems, volunteer and private AI initiatives as well as the crowdsourcing of data, the use of open-source platforms, and advances in the decentralized use of the respective assets. As of 2023, the Cabinet of Ministers began to launch policy initiatives to more systematically advance defense AI and the respective indigenous industrial base by creating a new ecosystem and advancing public and private funding solutions. The ecosystem of information

¹ The Government AI Readiness Index 2020.

² Cabinet of Ministers, "On the approval of the Concept for the development of artificial intelligence in Ukraine."

technology (IT) companies also began to shift its focus from developing civil products to dual-use products and actively recruit the best talents in the AI field. Foreign AI solution developers are using the war as a testbed to evaluate the performance of their solutions on the battlefield. Some defense observers even contend that AI solutions that have not been tested for use in Ukraine's combat environment won't be fit for purpose.

This war poses challenges not only to AI solutions providers but also to AI regulation as battlefield experience prompts the need to reconsider the appropriateness of the "human in the loop" principles and other core assumptions. It seems that many of the existing regulatory principles will be hard to sustain as they have not been designed for war and thus hamper countries in their need to defend against aggressors. Consequently, Ukraine is turning into a most valuable test case for the development and regulation of war-proof defense AI solutions.

2 Thinking About Defense AI

At the time of writing this study, Ukraine is at war. Almost all investments, intellectual and material resources are directed toward survival and enhancing defense capabilities to ensure success on today's battlefield, not in two or three years.

This focus also drives defense AI in Ukraine. According to the national AI strategy, AI is understood as

an organized set of information technologies, with the use of which it is possible to perform difficult complex tasks by using a system of scientific research methods and algorithms for processing information obtained or independently created during work, as well as to create and use own knowledge bases, decision-making models, algorithms for working with information and determine ways to achieve the tasks.³

Ukraine's current efforts are geared towards using AI to establish a competitive edge vis-à-vis Russia and build an ecosystem that will sustain this technological advantage to withstand aggression and rapidly develop much-required defense solutions. While both sides benefit from using defense AI to advance the processing of information, support decision-making, and enhancing existing equipment with defense AI, the question is how to get the upper hand in this technology-driven "tit for tat" game. In this regard, the accumulation of knowledge and experience could become a future strategic currency for Ukraine to advance national force development and share insights with allies and partners. The battle use of defense AI also yields valuable lessons for the future regulation of defense AI. Considering the situation, Ukraine has started to explore how warfighting insights on defense AI could be transitioned from the current state of war into a future state of peace as it is particularly important that data, which has been collected during wartime, would henceforth not be used in ways detrimental to human rights and democratic values.

2.1 Regulating Defense AI

The Ministry of Digital Transformation of Ukraine⁴ is the main body responsible for policies in the field of AI and robotics development. Within the Ministry, a separate department has been established, and since 2020, there is an operating expert committee on developing and deploying AI.

³ Cabinet of Ministers, "On the approval of the Concept for the development of artificial intelligence in Ukraine."

⁴ Cabinet of Ministers, "On making amendments to the Regulation on the Ministry of Digital Transformation of Ukraine."

So far, the national AI strategy⁵ is the country's capstone document, which also foresaw the use of AI for national security and defense as a key area of application. According to the strategy, AI solutions must ensure the protection of human rights and adhere to ethical standards. To this purpose, the strategy also includes developing an ethical code on AI but work in this direction has not yet started.

National security and defense are key use cases for AI in Ukraine. According to the strategy,⁶ the government wants to develop solutions for the use of AI for

- Command and control (C2);
- Weapons and military equipment including unmanned systems and unmanned demining solutions;
- Collection and analysis of information during combat operations;
- Analysis in support of intelligence activities including the processing of cartographic information;
- Defense against cyber threats including applications that allow for the quick detection of cyberattacks, preliminary scanning, and subsequent avoidance of malicious codes;
- Simulation and cognitive modeling of the combat situation.

These use cases suggest that Ukraine sees AI as integral to its attempt to develop unmanned systems and advance cyber defense solutions as envisioned by the country's 2021 Military Security Strategy.⁷ To this end, the Cabinet of Ministers has also adopted an implementation plan.⁸ The plan outlines a series of initiatives such as adopting legal regulation on issues of forming state policy in the field of AI, providing state support to use AI in priority sectors of the economy; implementing AI to enhance national cybersecurity systems, and defining priority tasks and directions for the current and future use of AI for defense.

In addition, Ukraine participates in international initiatives to regulate the development and use of AI. In particular, the Ukrainian Parliament ratified the agreement with the European Union (EU) on joining the "Digital Europe" program in February 2023⁹ and signed the November 2023 Bletchley Declaration on AI Security at the AI Safety Summit.¹⁰ As an official candidate for EU membership, Ukraine clearly signals its will to synchronize legislative efforts to advance digitalization with the EU's policy initiatives. But while the Ministry of Digital Transformation has outlined

5 Cabinet of Ministers, "On the approval of the Concept for the development of artificial intelligence in Ukraine."

6 Cabinet of Ministers, "On the approval of the Concept for the development of artificial intelligence in Ukraine."

7 President of Ukraine, "On the Strategy of Military Security of Ukraine."

8 Cabinet of Ministers, "On the approval of the action plan for the implementation of the concept for the development of artificial intelligence."

9 "Agreement between Ukraine and the European Union on Ukraine's participation in the European Union program 'Digital Europe.'"

10 Ministry of Digital Transformation, "Ukraine signed an international declaration dedicated to the safety of using AI."

a roadmap for regulating the civilian and commercial use of AI in Ukraine,¹¹ the respective capstone document for the use of AI in support of national security and defense is missing.

2.2 Re-Evaluating “Human in the Loop” in Modern Warfare

In recent years, civil society organizations and AI experts have become increasingly concerned about the emergence of lethal autonomous weapons systems (LAWS), which may use AI to identify targets and thus could harm individuals if used without direct human control.¹² Consequently, there has been a collective initiative at the United Nations to prohibit or impose limitations on using these systems. So far, however, these discussions have not yielded significant results.

Proponents of the “human in the loop” principle, which advocates the ultimate role of humans as decision-makers, have noble intentions. But technical solutions envisaged to ensure ultimate human control are challenging to implement in war without overly limiting a defender’s space for action. First, on the battlefield, the distinction between solutions to find, fix, track, and engage targets with a “human in the loop” or in fully autonomous mode is almost impossible to make as the same technology operates in different modes. In practice, there are only two to five seconds between target identification and engagement, which is hardly enough for a human operator to make a balanced decision. This bears the risk that involving a “human in the loop” becomes a “formality,” that might render the target-engagement cycle more difficult. Second, implementing a “human in the loop” via mechanisms that ensure remote control of assets not only increases the costs of the respective devices. Russia’s frequent use of electronic warfare (EW) also makes connectivity with the platform and the payload unfeasible. Third, there are no effective international mechanisms to verify or ensure that both sides refrain from using weapons without a “human in the loop,” as it is challenging – if not impossible – to assume after a mission has been executed, whether an unmanned asset has been piloted or flown autonomously. Under these conditions, fully autonomous AI solutions would provide the defender with significant advantages in executing its tasks more effectively and more precisely than, for example, with traditional artillery or conventional weapons.¹³

¹¹ Ministry of Digital Transformation, “Roadmap for the regulation of artificial intelligence in Ukraine.”

¹² Kahn, “AI is on the frontlines of the war in Ukraine.”

¹³ Goncharuk, “War in Ukraine.”

In sum, the use of AI in the current war is very likely to shape the future regulatory debate in two different ways. First, war experience will test the binding power of norms and rules when aggressors feel unrestricted by the normative principles that guide a defender's actions. In addition, this will also prompt the need to rethink how the human in the loop logic – which depends on connectivity between operators and unmanned assets – would be ensured under adversarial electromagnetic spectrum dominance.

3 Developing Defense AI

Before the full-scale invasion in 2022, Ukraine's defense sector was considered non-prestigious and corrupt.¹⁴ The defense-industrial complex of Ukraine consisted mainly of state-owned enterprises with only a handful of private defense manufacturers getting state defense orders.¹⁵ The main AI development centers were concentrated in a few state institutes that historically worked with the main customer UkrOboronProm and dozens of private companies.

In 2022, most AI initiatives, including data collection and processing, neural network training for weapon detection, and social media analysis to fight disinformation campaigns, were spearheaded by private companies and volunteers. These private and volunteer-led efforts incorporated advanced technologies such as AI-enhanced detectors and trackers in drones and robots for localization, adapting rapidly to the evolving demands of the conflict, whereas the state continued to focus on conventional weapons production. However, as will be discussed below, systemic changes at the state level, including the development of funding programs and the creation of new structural units with a focus on AI development, began in 2023.

3.1 AI's War Stimulus

Russia pays significant attention to the development of AI technologies in defense. The arsenal of the Russian armed forces already includes a wide range of weapons using AI technologies (CNA 2022). As Katarzyna Zysk¹⁶ shows, Russia's political and military decision-makers understand the importance of AI and are therefore actively investing in its military application, involving state and private development centers.

Given that Russia is ramping up its industrial production of drones and robotic systems, autonomous robots with AI may begin to be used massively from 2025-2026, which could provide a significant advantage on the battlefield. These systems may be EW-proof due to AI's capability to autonomously process and react to electronic threats, dynamically adapt to changing electronic environments, and operate independently without the need for remote signals, which are often targets of electronic jamming. Consequently, Ukraine is forced to compete and develop AI solutions that provide adequate responses to Russia's challenges.

14 Bondar, "Arsenal of Democracy."

15 Kolomychenko, "Army of Drones."

16 Zysk, High Hopes Amid Hard Realities.

From 2023, the Government of Ukraine began actively stimulating the development of innovative defense solutions. The Ministry of Strategic Industries and the Ministry of Digital Transformation are at the forefront of these efforts. Technological defense developments in the field of AI receive organizational and financial support through specialized platforms and projects. In addition, volunteers – who joined to help the Ukrainian armed forces by raising funds for the purchase of weapons, special equipment, transport, communication means, and training – are of pivotal importance in strengthening the country's defense.

This combination also helps explain Ukraine's success in implementing AI on the battlefield, which is driven by the motivation of Ukrainian troops, a high level of technical training of military specialists (who are recruited from the private sector), and the involvement of private companies in spearheading novel defense solutions. Crowdsourcing, involving ordinary citizens collecting important information about military operations shared with Ukrainian authorities, also plays an important role. Together, these aspects highlight the broader trend of democratizing military power, which goes far beyond the current war.¹⁷

Moreover, the unprecedented speed of implementing AI technologies into military systems and their use on the battlefield became possible thanks to the simplification of bureaucratic mechanisms to approve new technologies for use in the defense sector. So far, however, neither Russia nor Ukraine has officially acknowledged deploying fully autonomous weapon systems using AI. This also highlights, that it is "impossible to know, based on open-source materials, whether and what type of AI and autonomous technologies are being used in classified tasks and missions, and to what effect."¹⁸

3.2 Ukraine's New Defense AI Priorities

In September 2023, the Expert Advisory Committee on AI Development at the Ministry of Digital Transformation (Expert Committee Undated) provided recommendations for directing state and private investments to accelerate the development of defense AI solutions between 2023 and 2026. Among other things, the committee identified the following defense AI priorities:

- **AI for Domestic Unmanned Systems (e.g., Drones and Robots)**

The use of AI is meant to support navigation systems (without Global Positioning System, GPS), coordinated task execution management systems, auton-

¹⁷ Kahn, "How Ukraine Is Remaking War."

¹⁸ Konaev, *Tomorrow's Technology in Today's War*, p. 1.

omous task performance systems, enemy weapon and equipment detection (identification) systems, and data collection and storage systems for unmanned systems. These AI applications will be important to augment the “Army of Drones,” that the General Staff of the Armed Forces and the Ministry of Digital Transformation intend to establish to leverage Ukraine’s experience in using unmanned systems to repel Russia’s aggression.¹⁹

- **AI to Combat Disinformation**

AI shall be used for interactive solutions based on generative AI, deep voice and deepfake technologies for special law enforcement agencies, automatic detection systems for sources of disinformation and bots involved in foreign influence operations (FIMI), automation/standardization of information threat description and data exchange, labeling and detecting enemy generative AI to prevent the spread of disinformation, and creating datasets and data collection for generative AI development.

- **AI for Defense and Security-Relevant Logistics Systems**

AI is used to support predictive maintenance of equipment based on operating conditions, simulation analysis of supply logistics operations, systems for predicting supply and logistics needs and risks, management and automation systems for military warehouses, autonomous robots for military cargo delivery and personnel evacuation during active military operations.

- **AI for Mine and Ammunition Detection and Neutralization**

AI should support data collection and accumulation systems from satellites, drones, robots, and other sources (e.g., thermal sensors) for minefield detection, identification of combat sites for demining planning, robotic management systems for demining (urban, field, underwater), and quality control of demining systems.

- **AI for Cybersecurity and Information and Communications Technology (ICT) Protection in the Defense Sector**

AI should support systems for radio reconnaissance and advanced EW, modern data encryption and exchange systems, generative AI (voice) for pentesting (e.g., to verify military authorization procedures), countering sophisticated social engineering using generative AI (e.g., voice, 3D video), research focused on developing necessary innovative cybersecurity systems to protect critical digital infrastructures using advanced AI technologies for automatic threat analysis and classification.

¹⁹ Saballa, “Ukraine’s ‘Army of Drones’ Destroys 200 Russian Targets in One Week: Minister.”

- **General Conditions for Rapid Development of AI Solutions for Security and Defense**
Accelerating the use of AI for national security and defense foresees simplifying import and licensing procedures for components needed for AI solution training and development, deregulating and simplifying data acquisition procedures from the battlefield for drone, robot, and other AI system developers, simplifying testing processes for innovative products “on the battlefield” by domestic and foreign companies, advancing transparency and accessibility of information for defense tech participants, implementing universally accepted data exchange and storage standards, providing legal-regulatory provision for data exchange between different market participants and state bodies.

- **General Infrastructure and Solutions**
Moreover, Ukraine also wants to push for automated combat management systems (automated and AI assistance), simulation modeling solutions for military operations (wargames and military operations research), data analysis and classification systems from surveillance cameras, data collection and accumulation systems from media resources (as part of intelligence data), facial recognition and identification systems, AI-based damage assessment systems with various data types, advanced physical data transmission systems (for drones, robots, between different agents), datasets accessible to market participants for AI training and data collection systems, testing ranges for domestic and foreign developers, data exchange systems between different departments, integration with government business intelligence production of indigenous sensors such as stereo cameras, thermal cameras and others.

3.3 Ukraine’s New Defense AI Ecosystem

Many state agencies, private companies, and volunteer initiatives are involved in developing defense AI. As Ukraine’s defense ecosystem grows it also becomes more complex thus prompting the need for coordination and synchronization. This is an aspect that will need to be strengthened in the future to make sure that ongoing development efforts meet current – and future – warfighting needs.

In addition to the leading Ukrainian ministries, which will be discussed in the next chapter, several para-governmental agencies, a growing number of indigenous defense startups as well as international AI companies flocking to Ukraine constitute the country’s defense AI ecosystem. Adjacent to the public sector is the state-influenced defense industrial complex that harbors many of the traditional defense companies. The following entities are of particular relevance:

- **JSC Ukroboronprom**

JSC Ukroboronprom is a strategic manufacturer of weapons and military equipment in Ukraine, uniting enterprises in the strategic sectors of the state's defense industry.²⁰ Ukroboronprom includes the state enterprise Antonov, which developed more than one hundred types of passenger, transport, and special aircraft, like the Ruslan and Mriya platforms.²¹ Ukroboronprom also includes the enterprise State Kyiv Design Bureau Luch, which is one of Ukraine's leading developers of components for aviation and anti-tank weapon systems.²²

- **Brave1 Platform**

The Brave1 Platform, established by the Ministry of Digital Transformation, acts as an accelerator and an incubator. The main goal of the platform is to assess and promote technological products that can be integrated into various state sectors. In addition, Brave1 offers grants to accelerate the development of technologies considered critically important for Ukraine.²³ Brave1 supports research projects in the field of AI in priority areas like systems and weapons, protection and security, support and logistics, unmanned systems, cybersecurity, intelligence, and navigation. Based on the military cluster of Brave1, the Griselda system was developed using AI to collect intelligence data. This technology is already in use with other systems like Delta (situational awareness), Bronya (artillery fire support), Kropyva (planning support), and GISArta (C2 for artillery fire).²⁴

- **Innovation Development Accelerator.**

Under the auspices of the Ministry of Defense of Ukraine, the Innovation Development Accelerator was created to combine and develop the capabilities of different units inside the Ministry of Defense. This program is designed as a channel for rapid deployment of innovations in the military sphere.²⁵

- **Ukrainian Startup Fund**

The Ukrainian Startup Fund (Ukrainian Startup Fund Undated) was established to promote the development of early-stage technological startups in Ukraine.²⁶ Since the beginning of the full-scale invasion, the fund has focused on supporting defense tech and deep tech projects. The fund allocated USD8.2M in grants, funding 352 startup teams, and conducted over 330 events like

20 For more information, see: <https://ukroboronprom.com.ua/en/> (last accessed 30 January 2024).

21 Skorobogatova/Kalko, "Development of a strategy for forming the export potential of Ukrainian aviation enterprises on the example of the state enterprise 'Antonov'."

22 For more information, see: <https://www.luch.kiev.ua/ukr/> (last accessed 30 January 2024).

23 Pylypiv, "Drones at sea and on land, artificial intelligence, and the Javelin simulator."

24 Denisova, "Griselda."

25 For more information, see: <http://mil-tech.gov.ua/en> (last accessed 30 January 2024).

26 For more information, see: <https://usf.com.ua/#usf-sc-2> (last accessed 30 January 2024).

hackathons, boot camps, educational lectures, or mentoring sessions with 119 startups. The fund has also provided support to attend some of the world's largest technology events and enabled close to 200 pro bono experts to join the fund's work.²⁷

Private funds and non-profit organizations complement the government's efforts to advance Ukraine's defense industrial base. The following organizations play a key role:

- **D3 Military Tech Accelerator**

The D3 military tech accelerator provides investments in early-stage startups and mentorship.²⁸

- **Flyer One Ventures**

Flyer One Ventures, with a presence in Ukraine, invests in Ukrainian startups from Europe and North America.²⁹

- **Aerorozvidka**

Aerorozvidka is a non-profit organization that promotes the creation and implementation of networked and robotic military capabilities for the Ukrainian security and defense forces.³⁰

- **"Come Back Alive" Army Assistance Fund**

The "Come Back Alive" Fund, established in 2014, has already raised over UAH5.2bn (USD138M) for the needs of the Defense Forces of Ukraine. This fund specializes in the procurement of technical means and was the first in Ukraine to obtain permission to import dual-use goods from abroad.³¹

- **Prytula Foundation**

Serhiy Prytula's charity fund provides aid to the Armed Forces of Ukraine and humanitarian aid to civilians since February 2022.³²

- **Ukraine Defense Fund**

The Ukraine Defense Fund provides supplies and supports people fighting on the front lines of Ukraine.³³

27 Tarasovsky, "Grants worth millions of dollars, hundreds of events, and projects."

28 Boshnykov, "D3 military tech accelerator is to launch in Ukraine."

29 For more information, see: <https://www.flyerone.vc/> (last accessed 30 January 2024).

30 For more information, see: <https://aerorozvidka.ngo/> (last accessed 30 January 2024).

31 Melezik, "Ukrainian volunteers and funds that help the country the most during the war."

32 For more information, see: <https://prytulafoundation.org/en> (last accessed 30 January 2024).

33 For more information, see: <https://ukrainedefensefund.org/> (last accessed 30 January 2024).

Ukrainian ministries and national programs are meant to strengthen Ukraine's defense industrial base. Consequently, the number of Ukrainian startups that provide solutions for defense and national emergency management is growing rapidly. Some of these companies also work on defense AI as the following examples illustrate:

- Artelligence, an IT company, has developed neural networks for text analysis, face profile search, and algorithms for cleaning and structuring large data.³⁴
- Athlon Avia, a Ukrainian research and production company, develops unmanned aerial systems for tactical military missions such as intelligence, surveillance, target acquisition, and artillery fire adjustment (A1-CM "Furia").³⁵
- Keep Robotics develops multi-purpose unmanned electric cargo vehicle like Mule for logistics tasks.³⁶
- Kvertus develops and manufactures EW and reconnaissance systems, among other missions, also for counter UAS operations.³⁷
- Logics7 creates the UNITS universal training system for military fire training in Ukraine.³⁸
- MPS Development creates technologies for UAS such as simulators, ground control stations, C2 centers and drone traffic management solutions.³⁹
- Piranha Tech develops and produces EW tools such as radio jammers counter-UAS missions.⁴⁰
- Roboneers develops UGV for surveillance, fire support, logistics, and evacuations tasks, remote-weapon stations for its UGVs as well as a C2 software for tactical-level combat coordination.⁴¹
- Saker develops affordable AI for small businesses, including drone-based vision systems for plant protection. The SAKER SCOUT drone, equipped with AI, is used in Ukraine for autonomous target detection and engagement.⁴²
- Skiftech builds laser-equipped tactical engagement simulators for Ukraine's armed forces.⁴³
- SkyLab manufactures jamming and spoofing resisted UAS like the Shoolika MK-6 strike quadcopter or the Sirko-S1 UGV.⁴⁴

34 For more information, see: <https://artelligence.com/en> (last accessed 30 January 2024).

35 For more information, see: <https://athlonavia.com/en/home/> (last accessed 30 January 2024).

36 Hrudka, "Five Ukrainian war startups taking on Russia's brute force."

37 For more information, see: <https://kvertus.ua/en/> (last accessed 30 January 2024).

38 For more information, see: <https://logics7.com/> (last accessed 30 January 2024).

39 For more information, see: <https://www.mpsdevelopment.com/> and <https://sim.mpsdevelopment.com/> (last accessed 30 January 2024).

40 For more information, see: <https://piranha-tech.net/> (last accessed 30 January 2024).

41 For more information, see: <https://roboneers.net/en> (last accessed 30 January 2024).

42 For more information, see: <https://saker.airforce/home> (last accessed 30 January 2024).

43 For more information, see: <https://skif-tech.com/> (last accessed 30 January 2024).

44 For more information, see: <https://skylab-ua.com/> (last accessed 30 January 2024).

- Temerland creates UGV like Gnome, which can carry rocket propelled grenades, as well as Scorpio 2 and LASKA 2.0, multifunctional UGVs for fire support and reconnaissance tasks.⁴⁵
- UA Damage developed a platform for analyzing damage and pyrotechnic contamination using AI, satellites, and drones. Its comprehensive analysis allows visual inspection of unexploded rockets and mines, detecting them in grass and underground, and even localizing explosive objects and marking them on maps.⁴⁶
- Ukrspesystems produces SHARK unmanned aerial systems that can be used for ISR and stand-off target identification.⁴⁷
- Zvook company creates neural networks of acoustic sensors for detecting aerial objects. The network helps conventional air defense systems detect and destroy enemy cruise missiles and drone attacks and provides alerts to civilians. Zvook technology is trained on a unique dataset of acoustic imprints for most modern Russian weaponry.⁴⁸

Finally, a unique aspect of military operations in Ukraine lies in the unprecedented support offered by foreign companies. In general, collaboration with the United States has been essential for Ukraine. For example, Ukraine has benefited from SpaceX providing access to real-time data transmission in areas where IT infrastructure had been damaged.⁴⁹ General Atomics and AeroVironment contributed to advancing surveillance, reconnaissance, and precision strikes. CrowdStrike and FireEye helped advance Ukraine's digital defense in cyberspace.⁵⁰ In addition to financial and material support, collaboration is meant to advance Ukraine's indigenous defense industrial base and includes agreements on data-sharing and co-production of defense solutions. In addition, Ukraine and the United Kingdom have signed a far-reaching security agreement in January 2024 to cooperate in defense and military issues, defense industrial affairs, maritime security, and information security.⁵¹ At the time of writing this study in January 2024, a new French support package was reportedly also under preparation.⁵²

45 For more information, see: <https://temerland.com/en/solutions/> (last accessed 30 January 2024).

46 For more information, see: <https://www.uadamage.com/> (last accessed 30 January 2024).

47 For more information, see: <https://ukrspecsystems.com/> (last accessed 30 January 2024).

48 Ministry of Digital Transformation of Ukraine. *Incredible Tech*, p. 43.

49 This services, however, has also been controversial given the ambivalent role of Elon Musk, SpaceX's founder, in taking down satellite connection and preventing SpaceX from being used for offensive military operations. For more, see: Jayanti, "Starlink and the Russia-Ukraine War."

50 Thomas/Arsene/Hendi, "CrowdStrike Falcon protects from new Wiper malware used in Ukraine cyberattacks;" Hultquist et al., "Spear phishing campaign targets Ukrainian government and military;" "Aerovironment stands with the people of Ukraine and all of NATO;" "Statement from GA-ASI CEO Linden Blue on Ukraine conflict."

51 "Agreement on security cooperation between the United Kingdom of Great Britain and Northern Ireland and Ukraine."

52 Caulcutt, "Macron to 'finalize security deal' during Ukraine visit."

Moreover, foreign AI solutions support and enhance Ukraine’s situational awareness and situational understanding regarding Russian threats.⁵³ One notable contributor is Palantir, which played a pivotal role during the conflict by providing extensive data sharing capabilities to the military leadership. Through its Meta-Constellation too, Palantir facilitated large-scale data integration, encompassing sources ranging from commercial satellites to classified information from foreign intelligence services. This empowered Ukraine and its allies to utilize commercial data pertaining to specific battlegrounds, enabling the analysis of combat operations and the strategic planning of military endeavors. Notably, during the liberation of Kherson, the Ukrainian military benefited from accurate intelligence on the movements of Russian forces, allowing precise long-range strikes. The information, processed by NATO outside Ukraine, was then transmitted to the Ukrainian command.⁵⁴

American companies such as Planet Labs, BlackSky Technology and Maxar Technologies also contribute significantly by generating satellite imagery of ongoing combat operations and sharing the data with the government and Armed Forces. Furthermore, Primer, an IT company, adapted its voice-to-text program to efficiently process intercepted messages from the Russian military. This innovative approach spares the Ukrainian military from spending extensive hours manually deciphering intercepted conversations. The Primer Command technology facilitates the creation of AI models that swiftly process substantial volumes of data derived from enemy radio communications.⁵⁵

53 Fontes/Kamminga, “Ukraine A Living Lab for AI Warfare.”

54 Ignatius, “How the algorithm tipped the balance in Ukraine.”

55 Fontes/Kamminga, “Ukraine A Living Lab for AI Warfare.”

4 Organizing Defense AI

Ukraine's war effort leverages decentralized organizational structures and volunteer initiatives to create a vibrant ecosystem of actors that jointly work on complex systems. This approach also nurtures competition for the best ideas and products between different actors. Although beneficial in principle, decentralized efforts create additional layers of complexity related to coordination and synchronization of activities. In this context, several ministries are involved in setting the course for long-term force planning, operational planning to conduct the war, and strengthening the local defense industrial base. Among the public stakeholders, the following are of particular relevance:

- **Ministry of Defense of Ukraine**

In 2021, a Joint Directive of the Minister of Defense of Ukraine and the Commander-in-Chief of the Armed Forces of Ukraine led to the creation of the Center for Innovation and Defense Technologies.⁵⁶ Among other things, the Center has been tasked to develop, test, and provide support for new software that meets the needs of the Armed Forces of Ukraine.⁵⁷

The General Staff of the Ministry of Defense is responsible for military management and develops the country's defense plans. The General Staff is also in charge of strategic planning of the use of the Armed Forces of Ukraine and certain elements and resources of other parts of the Armed Forces. In addition, the Office for the Development of Automation has been set up within the General Staff. This office has been tasked to organize, coordinate, and execute efforts to advance automated defense solutions, create a unified automated control system, and advance the digitalization of Ukraine's Armed Forces.⁵⁸

The Main Intelligence Directorate complements these activities with a focus on conducting intelligence operations relevant for capability development, military construction as well as cybersecurity and military-technical security.⁵⁹

- **Ministry of Digital Transformation**

The Ministry of Digital Transformation implements the state's digitalization policy and is responsible for policies in robotics and AI. In 2020, the Ministry had established an Expert Advisory Committee on AI Development, whose goal is to enhance Ukraine's AI competitiveness. This committee, initially the only governmental body with AI expertise, played a significant role before the war. It focused on educational activities, organizing conferences and training sessions to educate military personnel and other agencies about AI applications relevant to their tasks. With the onset of the war, the Expert Advisory Committee shifted its focus to providing consulting support for various tasks.

56 For more information, see: <https://www.mil.gov.ua/ministry/struktura-generalnogo-shtabu/upravlinnya-rozvitku-avtomatizaczi.html> (last accessed 30 January 2024).

57 Defense Express, "The Ministry of Defense will create an Innovation Center, its own 'light analog' of the American DARPA."

58 Ministry of Defense, "The Ministry of Defense has established the Center for Innovation and Defense Technologies."

59 Verkovna Rada of Ukraine, "On Intelligence."

Additionally, some committee members joined the frontline, contributing directly to the defense efforts.

- **Ministry of Strategic Industries**

The Ministry of Strategic Industries is intended to manage the military-industrial complex with a focus on producing drones and robots and boosting Ukraine's indigenous missile program.⁶⁰

Ukraine's organizational set up to advance defense AI evolves commensurate with the threat landscape that shapes and refines the country's defense AI understanding. As argued above, Ukraine's defense AI focus has become more focused reflecting a maturing understanding of the benefits of AI on the battlefield. Nonetheless, as the war goes on, more emphasis will need to be put on how to synchronize the short cycles of battlefield adaptation, that quickly turn instant lessons identified into product upgrades, with the more medium and long-term cycles that look at the necessary changes of concept and capability development that are indispensable to sustain warfighting. This will also have an impact on defense AI governance and the role of coordinating entities that bring the decentralized group of stakeholders together to make sure that everybody understands, supports, and further develops the long-term defense AI priorities discussed above.

⁶⁰ "Minstrategprom was conceived as a powerful center for coordinating industrial policy and military-industrial complex: Dmytro Kysilevsky."

5 Funding Defense AI

According to the Stockholm International Peace Research Institute (SIPRI), Ukraine significantly increased its military spending in 2022 by 640% to USD44bn.⁶¹ For comparison, Russian military spending grew by 9.2% to USD86.4bn, which is 4.1% of its GDP.⁶² Especially as of 2023, Ukraine accelerated funding for AI development. However, due to the war, some program details cannot be disclosed:

- On 19 October 2023, Ukraine's Parliament approved the first reading of the 2024 state budget, allocating nearly UAH56bn (USD1.5bn) for the Ministry of Strategic Industries (Minstrategprom 2023). The 2024 budget also provides UAH2.55bn (USD60M) for the Ministry of Digital Transformation's digitalization, six times more than in 2023. The approved budget for 2024 includes an increase in funding for defense industry development, specifically for weapon production worth UAH51bn (USD1.3bn) as well as unmanned aerial, surface, and underwater systems worth UAH43.3bn (USD1.1bn).⁶³
- BRAVE1 launched an AI startup funding program in 2023, awarding 84 defense tech grants worth USD1.53M for AI and other technologies. The platform aims to fund Ukrainian startups with over USD2M by the end of 2023. The 2024 budget foresees a significant increase of the budget to more than USD39M. As of late 2023, an average grant is about USD5,000-25,000, and in 2024, grants will reach amounts of USD50,000, USD100,000, and USD250,000.⁶⁴
- The State Innovative Financial Credit Institution systematically invests in innovative developments through competitions among universities, institutes, and other state structures. As of 2022, it started including AI projects in dual-use sectors, but specific data is not available.⁶⁵
- International VC Funds⁶⁶ are actively monitoring the Ukrainian market, as it serves as a testing ground for creating and testing new weapons, with the goal of investing or engaging on mergers and acquisitions (M&A). Among others, Ukrainian AI startup Swarmer secured funding from D3 Accelerator, a fund co-managed by Eric Schmidt. Swarmer's flagship product AI Copilot enables a single operator to fly a swarm of drones thus boosting battlefield capacities.⁶⁷
- In addition, international companies open local branches in Ukraine to speed up technology development initiatives. German drone manufacturer Quantum Systems, for example, attracted substantial funds with its recent Series B funding round and has decided to join the special economic zone in Diia City to shift parts of its production to Ukraine.⁶⁸

61 SIPRI, "World military expenditure reaches new record high as European spending surges."

62 Radio Svoboda, "SIPRI: Ukraine's military spending in 2022 increased by 640% of GDP compared to 2021."

63 Ministry of Finance, "Verkhovna Rada of Ukraine adopted the state budget for 2024."

64 TechUkraine, "Ukraine's Defense Tech Cluster BRAVE1 Plans to Invest \$39M in Startups in 2024."

65 For more information, see: <https://sfii.gov.ua> (last accessed 30 January 2024).

66 Stojkovski, "Can Ukraine Become the Silicon Valley of Defense Tech?"

67 Yarova, "Ukrainian AI startup Swarmer secures funding from D3 Accelerator."

68 Crumley, "Quantum Systems' Ukraine drone, enterprise tech attracts \$63M in Series B funding."

Overall, the funding infrastructure for defense innovations focused on AI in Ukraine is in its early stages, actively engaging in processes to establish international cooperation. Considering the high value of local players' experience, a wave of small and medium-sized M&A of Ukrainian developers by global defense market players is likely to occur within the next years.

6 Fielding and Operating Defense AI

Ukraine's defense AI ecosystem operates within a rapid development-to-deployment cycle, characterized by the integration of government and military efforts to recruit top engineering talent. This strategy offers engineers an alternative to frontline service, allowing them to contribute to defense projects in secure settings. The approach indicates a strategic use of civilian expertise in military applications, balancing defense development needs with the protection of skilled personnel.

There's a notable cultural and operational shift as engineers and managers from the civilian IT sector adapt to the traditional military culture. This transition is significant, blending civilian technological expertise with military operational practices, which is essential for developing relevant and practical AI solutions.

A key feature of the ecosystem is the real-time combat testing of AI technologies. Unlike controlled environments, this rigorous testing allows for immediate feedback and rapid iteration, crucial for practical application and improvement of AI in military contexts. It underscores a focus on developing solutions that can withstand the dynamic and unpredictable nature of modern warfare.

However, the ecosystem faces challenges in system integration due to the diversity of systems and standards, affecting the speed and efficacy of AI implementation. This complexity points to a need for standardized protocols and integration strategies to streamline the process.

Many AI solutions, while showing promise, are still in their early developmental stages. This immaturity can lead to increased long-term operational costs, emphasizing the ongoing development, refinement, and investment required to fully realize the potential of these technologies. The ecosystem's characteristics reflect a strategic blend of civilian and military expertise, rapid adaptation in real-world scenarios, and the ongoing challenge of integrating diverse technologies into a cohesive defense strategy.

Key projects and initiatives include:

- **Situational Awareness Solutions**

The Delta platform is a situational awareness and battlefield management system.⁶⁹ It consolidates information from various sources, including personnel, officials, sensors, and drones. This system is crucial for planning military operations, coordinating unit movements, and securely exchanging enemy location data. Delta was created at the Center for Innovation and Development of Defense Technologies of the Ministry of Defense. The platform is used

⁶⁹ Rosengren, "Network-Centric Warfare in Ukraine: The Delta System."

by intelligence to recognize and identify objects such as enemy soldiers or military equipment. Delta played a pivotal role in destroying the Russian Cruiser “Moskva” in April 2022,⁷⁰ as the system enabled the military command to assess the situation in a short period of time and decide to destroy the military target. The Delta system was created according to NATO standards and is compatible with similar situational awareness systems of NATO members.⁷¹ Kropyva is another situational awareness system developed by the volunteers of “Army SOS.” Based on target localization by drones, Kropyva provides fire supports to gunners by computing ballistic calculations. The system receives daily updates on frontline developments. The Ukrainian Army uses Kropyva in combination with other systems like GISArta and more.⁷²

■ **Data Set Collection Projects**

Students at the Ukrainian Catholic University’s Faculty of Applied Sciences (APPS UCU) prepared a specific dataset for object recognition. Data is collected from open sources and can be used by experts to prototype and validate hypothesis.⁷³ Kaggle, another database of more than 50,000 public datasets such as equipment losses, for example, can be used for AI training.⁷⁴

■ **Disinformation and Bots**

With the help of AI, the Mantis analytics platform monitors and analyzes the information space to detect disinformation.⁷⁵

In sum, Ukraine’s defense AI sector is rapidly evolving, marked by a shift towards accelerated development cycles and a focus on integrating advanced AI technologies into defense strategies. Defense AI and other novel defense solutions benefit in particular from

- easier access to combat data, which manufacturers need to negotiate with the government, to continually refine their products and train AI more effectively.
- the efforts of the Ministry of Defense to support a community-driven response to streamline certification processes that significantly reduce the time from an average year to just one to two months for drone certification.
- international companies that establish service and development centers in Ukraine, enabling quick resolution of issues and reduced maintenance time.
- the fact that key end-users are creating general requirements for defense solutions, providing clear long-term development objectives, and reducing market uncertainty.

70 Krasnomovets, “‘Neptune’ struck ‘Moskva’.”

71 Dobrovolsky, “Ukraine showed NATO a unique battle management and enemy surveillance system.”

72 Melnyk, “Singing ‘Nettle.’ How Ukrainian software for artillery affects the course of the war.”

73 Applied Sciences Faculty of UCU, “Building a dataset for prototyping ideas for object detection.”

74 For more information, see: <https://www.kaggle.com/datasets/piterfm/2022-ukraine-russian-war>. Last accessed 30 January 2024.

75 Sobachynskyi, “Ukrainian-made AI platform Mantis Analytics detects Russian fakes in the news.”

7 Training for Defense AI

Amid the ongoing conflict with Russia, Ukraine's educational landscape has been significantly disrupted. The constant destruction of educational institutions and private residences, coupled with frequent power outages and the tragic loss of family members, have profoundly impacted the quality and accessibility of education. As of June 2023, Russian bombardments have damaged 3,290 Ukrainian educational institutions, destroying 262 of them.⁷⁶ This destruction accounts for about 10% of the country's educational infrastructure.⁷⁷

Despite these challenges, Ukraine trained over 7,000 experienced AI developers as of 2022, with its education system producing about 27,000 science, technology, engineering, and mathematics (STEM) graduates each year. Before the full-scale invasion in 2022, AI education in Ukraine typically distinguished between civilian and defense applications. However, the onset of the war prompted a significant shift, with almost all academic programs incorporating military-related components. This shift led to close collaborations between universities and the military sector on various projects.

A noteworthy aspect of Ukraine's educational response to the war has been the grassroots development of numerous training programs and courses, such as drone operations. These initiatives were often driven by charitable foundations and volunteers, rather than state funding. This approach reflects a unique, community-driven response to the urgent need for specialized training in a war time.

Ukraine's higher education institutions, including the Ukrainian Catholic University, Taras Shevchenko National University of Kyiv, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute," Kyiv School of Economics, and American University Kyiv, have adapted their programs to meet these new challenges. These adaptations include offering courses and degrees in Data Science, machine learning, and AI that are increasingly tailored to address defense needs.

Given the destruction of the civilian education infrastructure, the military training ecosystem for drone pilots and users of systems like Delta and Kropyva has become even more important. The rapid development of these programs, primarily facilitated by volunteers, underscores the agility of Ukraine's response to the evolving demands of the war. Military units of the Air Defense Forces, for example, use a Virtual Reality (VR) simulator for military training. This synthetic training environment ensures a more effective preparation of pilots to shoot down enemy cruise missiles, drones, and aircraft.⁷⁸

⁷⁶ For more information, see: <https://saveschools.in.ua/en/> (last accessed 30 January 2024).

⁷⁷ Center for Economic Strategy, "10% of Ukraine's educational infrastructure was damaged by Russian shelling."

⁷⁸ Press Service ODA, "Air Defense Forces 'West' received a VR simulator for practicing the skills of destroying enemy aerial targets."

Based on current war experiences, Strata-22 has developed immersive multimedia platforms to train infantrymen, gunners, and tankers. Military operators learn how to handle weapons with the help of largescale models using VR glasses. This simulation environment is built according to NATO standards.⁷⁹ In addition, Ukrainian IT company Logics7 has created a universal training system for the fire training of Ukrainian military units. Right now, the system provides digital replicas of different weapon systems like the Next Generation Light Anti-Tank Weapon (NLAW), Javlin anti-tank systems, as well as Stinger and Ingla anti-aircraft systems.⁸⁰ Finally, the war has also highlighted the effectiveness of AI laboratories established at universities, under the aegis of the Ministry of Digital Transformation and the AI Expert Committee. These labs have become instrumental in developing AI tools for wartime use.

In summary, the war has catalyzed a significant transformation in Ukraine's educational system. Traditional university programs have swiftly pivoted to focus on AI applications in military contexts. Meanwhile, the private sector and non-profit initiatives have stepped in to fill the immediate needs for specialized training and program development, demonstrating remarkable adaptability and resilience in the face of war.

⁷⁹ Ossipova, "We reduced the cost of training a soldier by at least 30 times."

⁸⁰ Pylypiv, "Drones at sea and on land, artificial intelligence, and the Javelin simulator."

8 Conclusion

War needs require Ukraine to focus on what works best on the battlefield while considering future warfighting requirements as well. This has prompted a clear focus on delivering the best solutions to the frontline and making sure to nurture the talent pipeline for technology development. By contrast, ineffective concepts and burdensome procedures and regulation are pushed aside.

After two years of intensive war fighting, it becomes more and more obvious that Ukraine and Russia actively compete in enhancing existing defense solutions with AI and providing new AI-enhanced systems. Against this background, Ukraine is increasingly focusing on:⁸¹

- investing in AI to enhance the autonomy and effectiveness of drones and robotic systems, in particular by enabling these systems to operate without GPS and engage adversarial drone systems;
- expanding the use of sophisticated sensors, including thermal and real-time satellite video feeds, thereby using for data analysis and data fusion to support decision-making for complex combat operations;
- developing fully autonomous systems to engage autonomous adversarial systems, thereby using AI to enhance autonomy;
- establishing new research and development centers to underline the government's commitment to advancing AI and other defense technologies;
- integrating AI into all levels of military operations, and
- making AI solutions more affordable to accelerate a broader and quicker adoption of defense AI by the country's Armed Forces.

It is important to note that in the ongoing war, Ukraine's defense AI solutions will be significantly improved thanks to continuous training based on battlefield experience and data. The Ukrainian AI ecosystem has evolved rapidly due to the war, transitioning from

⁸¹ Expert Committee on AI of Ukraine, "Regarding critical development priorities of artificial intelligence technologies in the field of security and defense of Ukraine."

grassroots volunteer and commercial efforts to more organized government-backed initiatives and funding. This shift reflects the government's strategic commitment to leveraging AI for defense. The ecosystem now robustly incorporates R&D, academia, private sector collaboration, and significant government investment, focusing on dual-use technologies for military and civilian benefits. This approach underlines a comprehensive, multi-faceted advancement in AI capabilities driven by the urgency of war.

These advancements are also very likely to shape the future international discussion on the use of defense AI on the battlefield. In this regard, NATO countries should first monitor AI developments in Ukraine and Russia during the war and reflect upon the likely consequences for their own capability planning as well as R&D priorities. Second, it can be assumed that violent non-state actors will also closely follow this war and consider how to best benefit from defense AI. This prompts the need to reconsider how to prevent and limit the proliferation of AI-relevant technologies to non-state actors, which broadens the regulatory debate. Third, countries will also need to be aware that many of the existing data and privacy protection ideas are unfit for warfighting when the comprehensive collection, assessment, fusion, and sharing of public and private data might produce distinct advantages in fighting an adversary. Fourth, this should also lead to a more realistic understanding and reconceptualization of the "human in the loop" principle that will be essential for future certification standards as well defense AI compliance and verification regimes.

Finally, even advanced countries should not underestimate the benefits of crowdsourcing, open-source technology, decentralization, and volunteer efforts that tend to be overlooked in a more mature institutional environment. As these efforts have been crucial in Ukraine's early and ongoing defense efforts it would be worth analyzing how these efforts can infuse defense innovation elsewhere.

Literature

"Aerovironment stands with the people of Ukraine and all of NATO," Aerovironment, undated, <https://www.avinc.com/lms/ukraine> (last accessed 30 January 2024).

"Agreement on security cooperation between the United Kingdom of Great Britain and Northern Ireland and Ukraine," Prime Minister's Office, 12 January 2024, https://assets.publishing.service.gov.uk/media/65a14a6ae96df50014f845d2/UK-Ukraine_Agreement_on_Security_Co-operation.pdf (last accessed 30 January 2024).

"Minstrategprom was conceived as a powerful center for coordinating industrial policy and the military-industrial complex – Dmytro Kysilevsky," Press Service of the Office of the Verkhovna Rada of Ukraine, 23 March 2023, https://www.rada.gov.ua/news/news_kom/234613.html (last accessed 30 January 2024).

"SIPRI: Ukraine's military spending in 2022 increased by 640% of GDP compared to 2021," Radio Svoboda, 24 April 2023, <https://www.radiosvoboda.org/a/news-viisk-ovi-vydatky-ukraina-sipri/32376625.html> (last accessed 30 January 2024).

"Statement from GA-ASI CEO Linden Blue on Ukraine conflict," General Atomics Aeronautical, 1 February 2023, <https://www.ga-asi.com/statement-from-ga-asi-ceo-linden-blue-on-ukraine-conflict> (last accessed 30 January 2024).

"The Ministry of Defense will create an Innovation Center, its own 'light analog' of the American DARPA," Defense Express, 8 October 2021, https://defence-ua.com/news/minoboroni_stvorit_tsentr_innovatsij_svij_vlasnij_lajt_analog_amerikanskoji_darpa-4975.html (last accessed 30 January 2024).

"Ukraine's Defense Tech Cluster BRAVE1 Plans to Invest \$39M in Startups in 2024," TechUkraine, undated, <https://techukraine.org/2023/11/30/ukraines-defense-tech-cluster-brave1-plans-to-invest-39m-in-startups-in-2024/> (last accessed 30 January 2024).

Applied Sciences Faculty of UCU, "Building a dataset for prototyping ideas for object detection," undated, <https://apps.ucu.edu.ua/projects/stvorenniya-nabo->

[ru-danyh-dlya-prototypuvannya-idey-shhodo-vyavlen-ya-ob-yektiv/](https://apps.ucu.edu.ua/projects/stvorenniya-nabo-ru-danyh-dlya-prototypuvannya-idey-shhodo-vyavlen-ya-ob-yektiv/) (last accessed 30 January 2024).

Artificial intelligence and autonomy in Russia. Special Issue (Arlington: CNA, 2022), <https://www.cna.org/Newsletters/Ai%20and%20Autonomy%20in%20Russia/AI-and-Autonomy-in-Russia-Special-Issue-September-2022.pdf> (last accessed 30 January 2024).

Bondar, Kateryna. "Arsenal of Democracy: Integrating Ukraine Into the West's Defense Industrial," Carnegie, 4 December 2023, <https://carnegieendowment.org/2023/12/04/arsenal-of-democracy-integrating-ukraine-into-west-s-defense-industrial-base-pub-91150> (last accessed 30 January 2024).

Boshnyakov, Ilya, "D3 military tech accelerator is to launch in Ukraine. Ex-Google CEO Eric Schmidt is among the LPs," AIN, 11 May 2023, <https://ain.capital/2023/05/11/d3-military-tech-accelerator-is-to-launch-in-ukraine-ex-google-ceo-eric-schmidt-is-among-the-lps/> (last accessed 30 January 2024).

Brave1. Undated. <https://brave1.gov.ua> (last accessed 30 January 2024).

Cabinet of Ministers of Ukraine, "On making amendments to the Regulation on the Ministry of Digital Transformation of Ukraine," Order of the Cabinet of Ministers of Ukraine No. 916, 25 August 2023, <https://ips.ligazakon.net/document/MN027216?hide=true> (last accessed 30 January 2024).

Cabinet of Ministers of Ukraine, "On the approval of the action plan for the implementation of the Concept for the development of artificial intelligence in Ukraine for 2021-2024," Order of the Cabinet of Ministers of Ukraine No. 438-p, 12 Mai 2021, <https://zakon.rada.gov.ua/laws/show/438-2021-%D1%80#Text> (last accessed 30 January 2024).

Cabinet of Ministers of Ukraine, "On the approval of the Concept for the development of artificial intelligence in Ukraine. Order of the Cabinet of Ministers of Ukraine No.1556-p," 2 December 2020, <https://zakon.rada.gov.ua/laws/show/1556-2020-p#Text> (last accessed 30 January 2024).

Caulcutt, Clea, "Macron to 'finalize security deal' during Ukraine visit," Politico, 17 January 2024, <https://www.politico.eu/article/emmanuel-macron-security-deal-ukraine-volodymyr-zelenskyy/> (last accessed 30 January 2024).

Crumley, Bruce, "Quantum-Systems' Ukraine drone, enterprise tech attracts \$63M in Series B funding," DroneDJ, 25 October 2023, <https://dronedj.com/2023/10/25/quantum-systems-ukraine-drone-enterprise-tech-attracts-63m-in-series-b-funding/> (last accessed 30 January 2024).

Denisova, Kateryna, "Griselda. A system of intelligence based on artificial intelligence has been developed in Ukraine," New Voice, 20 December 2023, <https://nv.ua/ukr/ukraine/events/v-ukrajini-na-bazi-shtuchno-go-intelektu-rozrobili-sistemu-rozvidki-50362114.html> (last accessed 30 January 2024).

Dobrovolsky, Vadim, "Ukraine showed NATO a unique battle management and enemy surveillance system," Speka, 27 October 2022 <https://speka.media/ukrayina-pokazala-nato-unikalnu-sistemu-stezennya-za-protivnikov-9g1zd9> (last accessed 30 January 2024).

Expert Committee on AI of Ukraine, "Regarding critical development priorities of artificial intelligence technologies in the field of security and defense of Ukraine," August 2023. <https://ai.org.ua/wp-content/uploads/2024/01/criticaldevelopment-prioritiesinAI-1.pdf> (last accessed 30 January 2024).

Fontes, Robin, and Jorrit Kamminga, "Ukraine A Living Lab for AI Warfare," National Defence, 24 March 2024, <https://www.nationaldefensemagazine.org/articles/2023/3/24/ukraine-a-living-lab-for-ai-warfare> (last accessed 30 January 2024).

Gaidai, Yurii, "10% of Ukraine's educational infrastructure was damaged by Russian shelling. How much damage has Russia caused to Ukrainian education?" Centre for Economic Strategy, 20 April 2023, <https://ces.org.ua/en/10-of-ukraines-educational-infrastructure-was-damaged-by-russian-shelling-how-much-damage-has-russia-caused-to-ukrainian-education/> (last accessed 30 January 2024).

Goncharuk, Vitaliy, "War in Ukraine: AI Weapons and the Debate Over 'Human in the Loop'," Medium, 20 September 2023, <https://vactivity.medium.com/war-in-ukraine-ai-weapons-and-the-debate-over-human-in-the-loop-ba2e48a97390> (last accessed 30 January 2024).

Hrudka, Orysia, "Five Ukrainian war startups taking on Russia's brute force," Euromaidan Press, 19 October

2023, <https://euromaidanpress.com/2023/10/19/five-ukrainian-war-startups-taking-on-russias-brute-force/> (last accessed 30 January 2024).

Hultquist, John et al., "Spear phishing campaign targets Ukrainian government and military," Mandiant, 16 April 2019, <https://www.mandiant.com/resources/blog/spear-phishing-campaign-targets-ukraine-government-and-military-infrastructure-reveals-potential-link-so-called-luhansk-peoples-republic> (last accessed 30 January 2024).

Ignatius, David, "How the algorithm tipped the balance in Ukraine," The Washington Post, 20 December 2022, <https://www.washingtonpost.com/opinions/2022/12/19/palantir-algorithm-data-ukraine-war/> (last accessed 30 January 2024).

Jayanti, Amritha, "Starlink and the Russia-Ukraine War: A Case of Commercial Technology and Public Purpose?" Belfer Center for Science and International Affairs, 9 March 2023, <https://www.belfercenter.org/publication/starlink-and-russia-ukraine-war-case-commercial-technology-and-public-purpose>.

Kahn, Jeremy, "A.I. is on the frontlines of the war in Ukraine," Fortune, 1 March 2022, <https://fortune.com/2022/03/01/russia-ukraine-invasion-war-a-i-artificial-intelligence/> (last accessed 30 January 2024).

Kahn, Lauren, "How Ukraine Is Remaking War Technological Advancements Are Helping Kyiv Succeed," Foreign Affairs, 29 August 2022, <https://www.foreignaffairs.com/ukraine/how-ukraine-remaking-war> (last accessed 30 January 2024).

Kolomychenko, Tetiana, "Army of drones:" How private drone manufacturers "master" the defense budget," Biznes Tsenzor, 11 November 2023, <https://biz.censor.net/r3448681> (last accessed 30 January 2024).

Konaev, Margarita, Tomorrow's Technology in Today's War: The Use of AI and Autonomous Technologies in the War in Ukraine and Implications for Strategic Stability (Arlington, CNA: 2023), <https://www.cna.org/reports/2023/10/Use-of-AI-and-Autonomous-Technologies-in-the-War-in-Ukraine.pdf> (last accessed 30 January 2024).

Krasnomovets, Pavlo, "'Neptune' struck 'Moskva.' How the Ukrainian missile system paid itself off tenfold," Forbes Ukraine, 14 April 2022, <https://forbes.ua/inside/neptun-uraziv-moskvu-yak-ukrainskiy-raketniy-kompleks-okupiv-sebe-desyatkratno-14042022-5449> (last accessed 30 January 2024).

Melezhib, Tetiana, "Ukrainian volunteers and funds that help the country the most during the war," TSN, 25 October 2022, <https://tsn.ua/ukrayina/top-volonteriv-ta-fondiv-yaki-zaluchili-naybilshe-groshy-dlya-shvidshoyi-peremogi-ukrayini-2181787.html> (last accessed 30 January 2024).

Melyk, Taisa, "Stinging 'Nettle.' How Ukrainian software for artillery affects the course of the war," Forbes Ukraine, 24 July 2024, <https://forbes.ua/innovations/zhalyucha-kropiva-yak-ukrainske-programne-zabezpechennya-dlya-artileristiv-vplivae-na-khid-viyni-22072022-7054> (last accessed 30 January 2024).

Ministry of Defense, "The Ministry of Defense has established the Center for Innovation and Defense Technologies: the relevant joint Directive was signed by the Minister of Defense of Ukraine and the Commander-in-Chief of the Armed Forces of Ukraine," undated, <https://www.mil.gov.ua/special/news.html?article=64623> (last accessed 30 January 2024).

Ministry of Digital Transformation, "Ukraine signed an international declaration dedicated to the safety of using AI," 2 November 2023, <https://www.kmu.gov.ua/news/ukraina-pidpysala-mizhnarodnu-deklaratsiiu-prysviachenu-bezpetsi-vykorystannia-shi> (last accessed 30 January 2024).

Ministry of Digital Transformation, Incredible Tech: Investors guide to Ukrainian IT (Kyiv: Ministry of Digital Transformation, 2023), <https://itukraine.org.ua/files/ITIGUIT.pdf> (last accessed 30 January 2024).

Ministry of Digital Transformation, Roadmap for the regulation of artificial intelligence in Ukraine (Kyiv: Ministry of Digital Transformation, 2023). https://cms.thedigital.gov.ua/storage/uploads/files/page/community/docs/%D0%94%D0%BE%D1%80%D0%BE%D0%B6%D0%BD%D1%8F_%D0%BA%D0%B0%D1%80%D1%82%D0%B0_%D0%B7_%D1%80%D0%B5%D0%B3%D1%83%D0%BB%D1%8E%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F_%D0%A8%D0%86_%D0%B2_%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D1%96_compressed.pdf (last accessed 30 January 2024).

Ministry of Finance, "Verkhovna Rada of Ukraine adopted the state budget for 2024," 9 November 2023, <https://www.kmu.gov.ua/news/verkhovna-rada-ukrainy-pryniala-derzhbiudzheta-na-2024-rik> (last accessed 30 January 2024).

Minstrategprom, "The draft budget-2024 provides for almost 56 billion UAH for the development of the defense industrial complex in Ukraine," 16 September 2023, <https://www.kmu.gov.ua/news/na-rozvytok-opk-v>

[ukraini-proektom-biudzheta-2024-peredbacheno-maizhe-56-mlrd-hrn](https://www.kmu.gov.ua/news/na-rozvytok-opk-v) (last accessed 30 January 2024).

Ossipova, Viktoriia, "We reduced the cost of training a soldier by at least 30 times". The developer of Strata 22 on how the Armed Forces of Ukraine are acquiring combat skills in AR and VR," DOU, 24 October 2022, <https://dou.ua/lenta/interviews/multimedia-systems-for-military-training/> (last accessed 30 January 2024).

President of Ukraine, "On the Strategy of military security of Ukraine." Decree of the President of Ukraine No. 121/2021, 25 March 2021, <https://www.president.gov.ua/documents/1212021-37661> (last accessed 30 January 2024).

Press Service ODA, "Air Defense Forces 'West' received a VR simulator for practicing the skills of destroying enemy aerial targets," LOVA, 8 March 2023, <https://loda.gov.ua/news/57059?fbclid=IwAR1hnl-kdP-GUCkLAB1fsR22kFQcs1SvrJPQTAHGWTwX55jMrr6kPJBrMoew> (last accessed 30 January 2024).

Pylypiv, Ihor, "Drones at sea and on land, artificial intelligence and the Javelin simulator: how military-tech developments bring Ukraine closer to victory. The EP talks about projects that help the Defense Forces beat the enemy. Which of them are already working to win?" Epravda, 5 July 2023, <https://www.epravda.com.ua/rus/publications/2023/07/5/701912/> (last accessed 30 January 2024).

Rosengren, Oscar, "Network-Centric Warfare in Ukraine: The Delta System. Grey Dynamics," 3 February 2023, <https://greydynamics.com/network-centric-warfare-in-ukraine-the-delta-system/> (last accessed 30 January 2024).

Saballa, Joe, "Ukraine's 'Army of Drones' Destroys 200 Russian Targets in One Week: Minister," The Defense Post, 14 September 2023, <https://www.thedefensepost.com/2023/09/14/ukraine-drones-russian-targets/> (last accessed 30 January 2024).

SIPRI, "World military expenditure reaches new record high as European spending surges," SIPRI, 24 April 2023, <https://www.sipri.org/media/press-release/2023/world-military-expenditure-reaches-new-record-high-european-spending-surges> (last accessed 30 January 2024).

Skorobogatova, N.Ye., and Yu.V. Kalko, "Development of a strategy for forming the export potential of Ukrainian aviation enterprises on the example of the state enterprise 'Antonov'," Effective Economy, no 11, 2016,

<http://www.economy.nayka.com.ua/?op=1&z=5247> (last accessed 30 January 2024).

Sobachynskyi, Rostyslav, "Ukrainian-made AI platform Mantis Analytics detects Russian fakes in the news," AIN, 15 September 2023, <https://ain.capital/2023/09/15/ukrainian-mantis-analytics-detects-russian-fakes/> (last accessed 30 January 2024).

Stojkovski, Bojan, "Can Ukraine Become the Silicon Valley of Defense Tech?," The Recursive, 5 October 2023, <https://therecursive.com/can-ukraine-become-the-silicon-valley-of-defense-tech/> (last accessed 30 January 2024).

Tarasovsky, Yuriy, "Grants worth millions of dollars, hundreds of events, and projects. The Ministry of Digital Transformation showed the results of the work of the startup fund," Forbes Ukraine, 11 July 2023, <https://forbes.ua/news/granti-na-milyoni-dolariv-sotni-iven-tiv-ta-proektiv-mintsifri-pokazalo-rezultati-roboti-fondu-startapiv-11072023-14732> (last accessed 30 January 2024).

The Government AI Readiness Index 2020 (Malvern: Oxford Insights 2020), <https://oxfordinsights.com/wp-content/uploads/2023/11/AIReadinessReport.pdf> (last accessed 30 January 2024).

Thomas, William, Adrain Liviu Arsene, and Farid Hendi, "CrowdStrike Falcon protects from new wiper malware used in Ukraine cyberattacks," CrowdStrike, 25 February 2022, <https://www.crowdstrike.com/blog/how-crowdstrike-falcon-protects-against-wiper-malware-used-in-ukraine-attacks/> (last accessed 30 January 2024).

Verkhovna Rada of Ukraine, "Agreement between Ukraine and the European Union on Ukraine's participation in the European Union program 'Digital Europe' (2021 – 2027)," Law of Ukraine No. 2926-IX, 23 February 2023, https://zakon.rada.gov.ua/laws/show/984_005-22#Text (last accessed 30 January 2024).

Verkhovna Rada of Ukraine, "On Intelligence," Law of Ukraine, 12 December 2022, <https://zakon.rada.gov.ua/laws/show/912-20#n73> (last accessed 30 January 2024).

Yarova, Maia, "Ukrainian AI startup Swarmer secures funding from D3 Accelerator," AIN, 16 November 2023, <https://ain.capital/2023/11/16/ukrainian-swarmer-secures-funding-from-d3/> (last accessed 30 January 2024).

Zysk, Katarzyna, High Hopes Amid Hard Realities. Defense AI in Russia. DAIO Study 23/11 (Hamburg: Defense AI Observatory, 2023), https://defenseai.eu/daio_study2311 (last accessed 30 January 2024).

Defense AI Observatory Studies

- 24|22** Vitaliy Goncharuk, Survival of the Smartest? Defense AI in Ukraine
- 24|21** Youngwook Park, Will the One Ring Hold? Defense AI in South Korea
- 23|20** Tomas Jermaliavičius, Caught Between Today and Tomorrow. Defence AI in Estonia
- 23|19** Nikolaos Karampekios, Konstantinos Sakalis, and Iraklis Oikonomou, Harnessing the Potential. Defense AI in Greece
- 23|18** Andreas Graae, Servers Before Tanks? Defence AI in Denmark
- 23|17** Kévin Martin and Lucie Liversain, A Winding Road Before Scaling-Up? Defense AI in France
- 23|16** Sami O. Järvinen, Cautious Data-Driven Evolution. Defence AI in Finland
- 23|15** Inbar Dolinko and Liran Antebi, Embracing the Organized Mess. Defense AI in Israel
- 23|14** Alastair Finlan, A Fertile Soil for AI? Defense AI in Sweden
- 23|13** John Lee, "Overtaking on the Curve?" Defense AI in China
- 23|12** Heiko Borchert, Torben Schütz, and Joseph Verbovzsky, Master and Servant. Defense AI in Germany
- 23|11** Katarzyna Zysk, High Hopes Amid Hard Realities. Defense AI in Russia
- 23|10** Yvonne Hofstetter and Joseph Verbovzsky, How AI Learns the Bundeswehr's "Innere Führung." Value-Based Engineering with IEEE7000™-2021
- 23|09** Robert C Engen, When the Teeth Eat the Tail: A Review of Canada's Defence Artificial Intelligence
- 23|08** Çağlar Kurç, Enabling Technology of Future Warfare. Defense AI in Turkey
- 23|07** Lauren A. Kahn, Risky Incrementalism. Defense AI in the United States
- 22|06** Yvonne Hofstetter, Wie KI Innere Führung lernt. Wertbasierte Technik mit IEEE7000™-2021
- 22|05** Andrea Gilli, Mauro Gilli, and Ivan Zaccagnini, Exploring the Benefits of a New Force Enabler: Defense AI in Italy
- 22|04** Kenneth Payne, Bright Prospects – Big Challenges. Defense AI in the United Kingdom
- 22|03** Heiko Borchert, Christian Brandlhuber, Armin Brandstetter, and Gary S. Schaal, Free Jazz on the Battlefield. How GhostPlay's AI Approach Enhances Air Defense
- 22|02** Peter Layton, Evolution not Revolution. Australia's Defence AI Pathway
- 21|01** Heiko Borchert, Torben Schütz, Joseph Verbovzsky, Beware the Hype. What Military Conflicts in Ukraine, Syria, Libya, and Nagorno-Karabakh (Don't) Tell Us About the Future of War

