Connections: The Quarterly Journal
ISSN 1812-1098, e-ISSN 1812-2973

I. Porkoláb, I. Lakatos & F. Dávid
Connections QJ 23, no. 1 (2024): Preview
https://doi.org/10.11610/Connections.23.1.09

Research Article

Innovation and Technology in the Russo-Ukrainian War

Imre Porkoláb,[1] *István Lakatos,*[2] *and Ferenc Dávid*[3]

[1] *Defense Innovation Research Institute, Budapest, Hungary, https://defenseinnovation.hu*

[2] *Széchenyi István University, Győr, Hungary, https://www.uni.sze.hu*

[3] *Technology Transfer Institute, National Laboratory of Cooperative Technologies, Budapest, Hungary, https://www.techtra.hu*

Abstract: Technology and innovation have significantly influenced the Russo-Ukrainian war, impacting not only the armed conflict but also the reconstruction of reclaimed territories and the restoration of services. Few believed in Ukraine's survival when the Russian invasion began in February 2022. This article examines how Ukraine, through its ability to embrace technological advancements and apply innovative solutions, gained a comparatively advantageous position against Russian aggression. We focus on the fundamental differences in the early stages of the war, particularly highlighting Ukraine's adept integration of emerging dual-use and advanced Western products and technologies.

Keywords: Russo-Ukrainian war, defense innovation, dual-use technology

Introduction

Technology and innovation significantly influence the Russo-Ukrainian war, impacting not only the armed conflict but also the reconstruction of reclaimed territories and restoration of services.[1] When the large-scale Russian assault began in February 2022, few believed in Ukraine's survival. With Russia possessing an

[1] Jason McGee-Abe, "One Year on: 10 Technologies Used in the War in Ukraine," *TechInformed*, February 24, 2023, accessed May 4, 2023, https://techinformed.com/one-year-on-10-technologies-used-in-the-war-in-ukraine/.

army more than twice the size and a defense budget nearly ten times greater, the prevailing belief was that Kyiv would fall within a week or two.[2] However, the course of events was significantly shaped by one particular factor: technology and, consequently, the innovative power of a nation.[3] Innovation power encompasses the ability to invent, adapt, and adopt new technologies.[4] Its significance lies in how emerging and disruptive technologies [5] and interconnected discoveries reshape our theories concerning the geopolitical determination of a nation.[6]

Ukraine gained an advantageous position against the Russian invasion through its ability to adopt technological innovations and apply innovative solutions. Not only did Ukraine halt the attack on Kyiv in February 2022, but when military operations shifted in April to the Donbas—where local knowledge, open terrain, and shorter supply routes favored the Russian side—they also stood their ground. In September 2022, Ukraine reclaimed parts of the occupied territories through the Kharkiv counteroffensive. These events contrasted sharply with Russia's effectiveness in the 2014 Crimean and Eastern Ukrainian military campaigns and their 2015 operation in Syria.

A fundamental difference during this initial phase of the war was that Ukraine more ingeniously integrated advanced, mostly dual-use Western products and

---

[2] Faine Greenwood, "The Drone War in Ukraine Is Cheap, Deadly and Made in China," *Foreign Policy*, February 16, 2023, accessed June 10, 2023, https://foreignpolicy.com/2023/02/16/ukraine-russia-war-drone-warfare-china/; Nan Tian et al., "Trends in World Military Expenditure, 2022," SIPRI Fact Sheet, April 2023, 9-11, https://www.sipri.org/sites/default/files/2023-04/2304_fs_milex_2022.pdf.

[3] Alternatively phrased but with similar content, it highlights the synergy between "disruptive" technological solutions and human capabilities. See also Zdzisław Śliwa, "The Synergy Between Technology and Soldiers in Warfare – The Russian Armed Forces Image During the War in Ukraine," *Wiedza Obronna* 281, no. 4. (2022): 53-69, https://doi.org/10.34752/2022-d281.

[4] Eric Schmidt, "Innovation Power: Why Technology Will Define the Future of Geopolitics," *Foreign Affairs* (March-April 2023): 40, https://www.foreignaffairs.com/united-states/eric-schmidt-innovation-power-technology-geopolitics; See also: Śliwa, "The Synergy Between Technology and Soldiers in Warfare," 55.

[5] Emerging, revolutionary, and disruptive technological innovations and research areas encompass advanced computing solutions, data science, artificial intelligence, autonomous vehicles and robotics, hypersonic technologies, space systems, biotechnology, and more. See, for example, Njall Trausti Fridbertsson, "Technological Innovation for Future Warfare," NATO Science and Technology Committee, Sub-Committee on Technology Trends and Security, 5-8, accessed March 20, 2023, https://www.nato-pa.int/document/2022-future-warfare-report-fridbertsson-025-stctts; Kelley M. Sayler, "Emerging Military Technologies: Background and Issues for Congress," Congressional Research Service Report R46458, updated February 22, 2024, 2, https://sgp.fas.org/crs/natsec/R46458.pdf.

[6] Amy Zegart, "Open Secrets: Ukraine and the Next Intelligence Revolution," *Foreign Affairs* 102, no. 1 (January-February, 2023): 54-70, 56-57, www.foreignaffairs.com/world/open-secrets-ukraine-intelligence-revolution-amy-zegart.

technologies into its operations.[7] In contrast, it seemed that Russia either could not or would not widely apply its technological innovations in the Ukrainian theater of war.[8] Naturally, official Ukrainian reports about successful implementation should also be approached with a degree of skepticism.[9] Conventional military equipment continues to dominate the Ukrainian theater of war,[10] but Kyiv is interested in emphasizing the successes of advanced weapon systems to maintain the ongoing support of the United States and European allies. However, it is challenging to determine from open-source information whether the use of specific technological innovations occurred extensively or sporadically.[11]

The Ukrainian military's proficiency in integrating advanced weapon systems and new technological solutions surprised not only their adversaries but also their partners and allies. Nevertheless, despite the sophistication of these technological innovations and weapon systems, it is unlikely they will determine the war's ultimate outcome. According to our assessment, the role of conventional weapon systems will remain pivotal in the Russian-Ukrainian conflict, and it cannot be asserted that a war of this nature could have a conclusive end. The warring parties often struggle to transform technological superiority on the battlefield into a strategic victory. While possessing the right technology is essential for effectiveness, having high-quality equipment alone does not offset the long-term economic costs of warfare, along with the associated political and societal consequences.[12]

---

[7] The term "dual-use" refers to technological solutions that serve both civilian and military purposes. The paradox arises from the fact that many products and technologies inherently have multiple uses, yet their distinction lies in their original development for specific civilian and commercial applications. See also Giulio Perani, *Military Technologies and Commercial Applications: Public Policies in NATO Countries*, NATO Research Fellowship, Rome: CeSPI, Final Report to the NATO Office for Information and Press (Rome, 1997), 5-6, https://www.nato.int/acad/fellow/95-97/perani.pdf.

[8] For relevant statements, please also refer to Donatas Palavenis, "The Use of Emerging Disruptive Technologies by the Russian Armed Forces in the Ukrainian War," *Air Land Sea Application Center*, October 1, 2022, accessed May 26, 2023, www.alsa.mil/Portals/9/Documents/articles/221001_ALSA_Article_Donatas_Palavenis.pdf, 2-3; and Śliwa, "The Synergy Between Technology and Soldiers in Warfare," 57-59. Initial experience from the Ukraine war reveals that the Russian defense industry struggles to produce advanced military equipment without Western technology, and significant improvements seem unlikely even with support from Iran, Belarus, or China.

[9] At this stage of the conflict, we must critically assess the available yet incomplete information, while acknowledging the lack of credible and verifiable performance indicators.

[10] Fridbertsson, "Technological Innovation for Future Warfare," 4; Palavenis, "The Use of Emerging Disruptive Technologies by the Russian Armed Forces in the Ukrainian War."

[11] Margarita Konaev and Owen J. Daniels, "Agile Ukraine, Lumbering Russia: The Promise and Limits of Military Adoption," *Foreign Affairs*, March 28, 2023, www.foreignaffairs.com/ukraine/russia-ukraine-war-lumbering-agile.

[12] Driven by geopolitical considerations, the United States currently provides—and will continue to provide—support to Ukraine, ensuring a level of commitment through the

The Russian-Ukrainian war extends beyond the battlefield into the broader realm of technology and the pursuit of technological supremacy among nations.[13] Alongside military and political events, the technological competition now revolves around state ranking and the methods and means of waging future wars. The reevaluation of Ukrainian experiences provides insight into a near future where armed conflicts will be fought and won through closer collaboration between humans and machines, with revolutionary technological innovation and data as the driving forces behind nations. Based on the initial experiences of the war, this article aims to offer insights into the significance of emerging, mostly dual-use, Western products and technologies that appeared in Ukraine.[14] This analysis seeks to provide a glimpse into how these experiences could potentially reshape the landscape of armed conflicts and technological innovations.

Cyber Space and Critical Infrastructure

Various cyberattacks and the countermeasures taken against them played a fundamental role in the Russian-Ukrainian conflict.[15] In February 2022, the physical invasion by Russia was preceded by hours of sustained cyberattacks launched in the virtual realm, characterized by distributed denial-of-service attacks and disruptions to information systems.[16] The deployment of Russian cyberweapons followed the initial attacks. Malicious programs, identified by Microsoft,[17] were

supply of weapons. However, unlike its two-decade involvement in Iraq and Afghanistan, the Russian-Ukrainian war has highlighted the depleted American and European arsenals and the vulnerability of their supply chains. The United States seems to lack resources to sustain long-term support for Ukraine while simultaneously deterring China over Taiwan. See Jacquelyn Schneider, "Does Technology Win Wars? The U.S. Military Needs Low-Cost Innovation – Not Big-Ticket Boondoggles," *Foreign Affairs*, March 3, 2023, https://www.foreignaffairs.com/ukraine/does-technology-win-wars; Schmidt, "Innovation Power: Why Technology Will Define the Future of Geopolitics," 43-44; Konaev and Daniels, "Agile Ukraine, Lumbering Russia."

13 McGee-Abe, "One Year on: 10 Technologies Used in the War in Ukraine."

14 Śliwa, "The Synergy Between Technology and Soldiers in Warfare," 55; Fridbertsson, "Technological Innovation for Future Warfare," 3, 5; Zegart, "Open Secrets: Ukraine and the Next Intelligence Revolution," 56-57, 63.

15 While the events have often been labeled as the first "cyber world war" (see, for example McGee-Abe, "One Year on: 10 Technologies Used in the War in Ukraine;" Kenneth R. Rosen, "The Man at the Center of the New Cyber World War," *Politico*, July 14, 2022, https://www.politico.com/news/magazine/2022/07/14/russia-cyberattacks-ukraine-cybersecurity-00045486), such exaggerated terminology should be avoided. Nevertheless, the actions unfolding in the virtual realm during the attack had an unprecedented impact in both speed and scope.

16 Consider DDoS (Distributed Denial of Service) attacks, which overwhelm and incapacitate network services and systems by overloading their resources.

17 See, for example, FoxBlade, Lasainraw (also known as IsaacWiper), DesertBlade, FiberLake, SonicVote, CaddyWiper, etc.; Microsoft, "Special Report: Ukraine. An Overview of Russia's Cyberattack Activity in Ukraine," April 27, 2022, 19-21, https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/.

utilized to cripple the Ukrainian internet network and government management systems, with repeated attempts to cause further damage.

In response, Ukraine swiftly transitioned its digital infrastructure to cloud services, with support from European data centers.[18] This strategic move aimed to safeguard against further disruptions and strengthen the resilience of Ukraine's cyber capabilities.[19]

The Russian intrusion and subsequent damage extended beyond Ukraine, affecting at least 42 countries and 128 organizations.[20] Part of this attack involved disrupting the service of the high-performance KA-SAT geostationary telecommunications satellite operated by Viasat.[21] The United States and Western technology companies, particularly Cloudflare and Microsoft, played a crucial role in supporting Ukraine. They aided in restoring its digital infrastructure, strengthening the resilience of its systems, and enhancing encryption capabilities.[22] Even before the invasion, Cloudflare had noticed the escalating Distributed Denial of Service (DDoS) attacks.[23] To ensure the continuous operation of Ukraine's governmental and telecommunications systems, Cloudflare provided free access to its services. This collaboration between the United States, Western technological entities, and Ukraine was pivotal in addressing the challenges posed by the cyberattacks.[24]

---

[18] Microsoft, "Special Report: Ukraine. An Overview of Russia's Cyberattack Activity in Ukraine," 19-12. It remains unclear whether Russia is holding back more effective cyber weapons or if their capabilities in this area have been overestimated. Fridbertsson, "Technological Innovation for Future Warfare," 4.

[19] Microsoft, "Special Report: Ukraine. An Overview of Russia's Cyberattack Activity in Ukraine," 19; McGee-Abe, "One Year on: 10 Technologies Used in the War in Ukraine."

[20] Microsoft, "Defending Ukraine: Early Lessons from the Cyber War," June 22, 2022, 10-11, https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/.

[21] Viasat, "KA-SAT Network Cyber Attack Overview," March 30, 2022, accessed May 12, 2023, https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview. The service interruption on February 22, 2022, disrupted internet access for thousands of Ukrainian customers and tens of thousands of other wired broadband users. The outage was confined to the infrastructure operated by Skylogic, a subsidiary of Eutelsat, for Viasat. It did not affect Viasat's direct commercial, governmental, or other users of the KA-SAT satellite. Damage from the Denial of Service (DoS) attack was mitigated within hours, with full system stabilization achieved within a few days.

[22] Fridbertsson, "Technological Innovation for Future Warfare," 4.

[23] The interconnectedness of systems and technological services is evident in the fact that the service outage, caused by the attack on certain parts of the network, was first detected in the United States. See Microsoft, "Special Report: Ukraine. An Overview of Russia's Cyberattack Activity in Ukraine," 6.

[24] John Graham-Cumming, "Internet Traffic Patterns in Ukraine since February 21, 2022," *The Cloudflare Blog*, March 4, 2022, accessed May 14, 2023, https://blog.cloudflare.com/internet-traffic-patterns-in-ukraine-since-february-21-2022/; Matthew Prince, "Steps We've Taken around Cloudflare's Services in Ukraine, Belarus, and Russia," *The Cloudflare Blog*, March 7, 2022, https://blog.cloudflare.com/steps-taken-around-cloudflares-services-in-ukraine-belarus-and-russia/. Cloudflare's Project Galileo offers

It is important to emphasize that the physical and virtual damage during the conflict occurred concurrently and were closely interconnected.[25] For example, according to the Ukrainian telecommunications provider RETN,[26] as of October 2022, 22 % of the country's fiber-optic network had been damaged, necessitating ongoing repairs.[27] Simultaneously, since August 2022, there has been a marked increase in malicious cyberattacks coinciding with Russian air and missile strikes. These cyberattacks targeted critical services such as search and rescue operations, healthcare systems, and organizations responsible for providing essential supplies like food, water, and medicine. This synchronized and interlinked damage across both physical and virtual realms has added a significant layer of complexity to the overall impact of the conflict, illustrating the multifaceted nature of modern warfare.[28]

Since cyberattacks will likely accompany any future conflict, enhancing defense mechanisms and resilience against such threats is crucial. This effort should include developing advanced technological capabilities and increasing automation to reduce human response times, thereby alleviating the burden on human resources.[29] In view of physical infrastructure vulnerabilities, the telecommunications industry is expected to witness a growing reliance on wireless networks and cloud services. However, this shift may be counterbalanced by the persistent threats posed by malicious software, Distributed Denial of Service (DDoS) attacks, and the high energy demands of IT systems. Therefore, a comprehensive approach is necessary to address these evolving challenges in the

free security services to vulnerable yet socially important groups facing threats from DDoS and other cyberattacks. Since February 2022, 81 Ukrainian organizations, primarily engaged in emergency response, have benefited from this service, https://www.cloudflare.com/galileo/ (accessed April 24, 2023).

25 Microsoft, "Special Report: Ukraine. An Overview of Russia's Cyberattack Activity," 3-4; Microsoft, "Defending Ukraine: Early Lessons from the Cyber War," 7-9.

26 RETN, registered in the United Kingdom, offers capacity, data transmission, and IP-based telecommunications services in Europe and Asia, serving both Ukraine and Russia. See https://www.retn.net (accessed May 10, 2023).

27 McGee-Abe, "One Year on: 10 Technologies Used in the War in Ukraine." See also: International Telecommunication Union (ITU), "Interim Assessment on Damages to Telecommunication Infrastructure and Resilience of the ICT Ecosystem in Ukraine" (ITU, December 2022), https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Interim%20assessment%20on%20damages%20to%20telecommunication%20infrastructure%20and%20resilience%20of%20the%20ICT%20ecosystem%20in%20Ukraine%20-2022-12-22_FINAL.pdf.

28 Jocelyn Woolbright, "Nine Years of Project Galileo and How the Last Year Has Changed It," *The Cloudflare Blog*, June 5, 2023, https://blog.cloudflare.com/nine-years-of-project-galileo-and-how-the-last-year-has-changed-it/.

29 Schmidt, "Innovation Power: Why Technology Will Define the Future of Geopolitics," 49-50.

cyber domain, ensuring that both infrastructure and technology are robust enough to withstand and adapt to the complexities of modern cyber warfare.[30]

Satellites and Communication

According to the State Service of Special Communications and Information Protection of Ukraine,[31] by October 2022, approximately 4,000 relay stations, 60,000 kilometers of optical cable lines, and 18 broadcasting stations had been damaged or destroyed.[32] In these dire circumstances, Ukraine quickly recognized the potential of advanced technological solutions. Following a direct appeal to SpaceX, the American company made its satellite internet network Starlink [33] available for free. Despite the extensive destruction of infrastructure, this initiative allowed Ukraine to maintain continuity in both civilian and military communications.[34]

The services provided by SpaceX,[35] supported by a network of 4,000 satellites and over 42,000 ground stations, ensured that Ukrainian citizens had internet access and that defense coordination could continue.[36] However, this solution also presented challenges due to service restrictions and associated costs. Notably, SpaceX did not support the use of its satellite internet service for offensive military operations, a condition that Ukraine did not fully adhere to.[37] Moreover,

---

30 "The Telecommunications Industry and Its Biggest Challenges for 2023," *ISB Tech*, January 23, 2023, https://www.isbtech.pl/2023/01/branza-telekomunikacyjna-i-jej-najwieksze-wyzwania-na-2023-rok/. – in Polish

31 See https://cip.gov.ua and https://cip.gov.ua/en/news/u-bukharesti-trivaye-povnovazhna-konferenciya-mizhnarodnogo-soyuzu-elektrozv-yazku-mse (accessed May 12, 2023).

32 McGee-Abe, "One Year on: 10 Technologies Used in the War in Ukraine;" Romina Bandura and Janina Staguhn, "Digital Will Drive Ukraine's Modernization," *Center for Strategic & International Studies (CSIS)*, January 10, 2023, accessed March 24, 2023, 2, https://www.csis.org/analysis/digital-will-drive-ukraines-modernization.

33 Konaev and Daniels, "Agile Ukraine, Lumbering Russia."

34 Schmidt, "Innovation Power: Why Technology Will Define the Future of Geopolitics," 40.

35 See https://www.starlink.com (accessed May 10, 2023).

36 There are approximately 7,700 functioning satellites orbiting Earth (as of 2023), with more than 4,000 of them owned by SpaceX as part of the Starlink project. See Stephen Clark, "SpaceX Rockets Past 4,000 Starlink Satellites in Orbit with Another Launch," *Spaceflight Now*, May 04, 2023, https://spaceflightnow.com/2023/05/04/falcon-9-starlink-5-6-coverage/. For additional information refer to https://planet4589.org/space/con/star/stats.html (accessed May 10, 2023).

37 Elon Musk's argument states: "[Starlink] is the communication backbone of Ukraine, especially at the front lines, where almost all other Internet connectivity has been destroyed. But we will not enable escalation of conflict that may lead to WW3," https://x.com/elonmusk/status/1624876021433368578, published February 12, 2023. It is worth noting that alongside emphasizing moral considerations, SpaceX's significant financial losses incurred through Starlink operations in Ukraine were also a factor. For more information, see Amritha Jayanti, "Starlink and the Russia-Ukraine

maintaining the free service became financially burdensome. By October 2022, SpaceX announced plans to discontinue its financial support, and in December 2022, the company increased the fees for its tools and services.[38] As a result, Ukraine now relies on the support of the U.S. government to access this crucial service.[39]

Commercial satellites owned by various companies have unexpectedly become key players in the Russo-Ukrainian conflict, particularly through the extensive use of satellite imagery and the public disclosure of assessments related to Russian operations.[40] What distinguishes this development is not the mere capture of images by Earth observation satellites—which have long been employed for various purposes, including military—but rather the dramatic growth of the private sector over the past decade, which has led to rapid accessibility and coverage.[41] One main advantage of commercial satellite networks is the speed and ease of access to crucial information. Unlike state-owned, often classified systems, private companies' service-based data-sharing practices have significantly facilitated and accelerated the flow of data essential for military decision-making.[42] Although the technology employed by these private companies might not be as advanced as that of state-owned systems, the quality of their services continues to improve. These systems are now well-suited for continuously observing specific areas and monitoring changes under various circumstances, providing a valuable resource in the ongoing conflict.[43]

Ukraine's response to the Russian invasion included an unprecedented level of public monitoring and analysis of Russian military preparations and operations, made possible through the support of eight commercial satellite companies, with significant backing from the United States.[44] From the outset of the

War: A Case of Commercial Technology and Public Purpose?" *Harvard Kennedy School*, *Belfer Center for Science and International Affairs*, March 9, 2023, www.belfercenter.org/publication/starlink-and-russia-ukraine-war-case-commercial-technology-and-public-purpose.

38 McGee-Abe, "One Year on: 10 Technologies Used in the War in Ukraine."

39 Alex Marquardt, "Exclusive: Musk's SpaceX Says It Can No Longer Pay for Critical Satellite Services in Ukraine, Asks Pentagon to Pick up the Tab," *CNN Politics*, October 14, 2022, https://edition.cnn.com/2022/10/13/politics/elon-musk-spacex-starlink-ukraine/index.html.

40 Fridbertsson, "Technological Innovation for Future Warfare," 4.

41 As of 2023, there are 7,700 satellites in orbit, a dramatic increase from just 11 in 2006. After 2015, the number of commercial Earth-observing satellites surged, reaching 596 by the end of 2022. Notably, two-thirds of these satellites are owned by American corporations. For further details refer to the UCS Satellite Database, www.ucsusa.org/resources/satellite-database (updated January 01, 2023).

42 Mariel Borowitz, "War in Ukraine Highlights Importance of Private Satellite Companies," *Astronomy Online*, August 16, 2022, https://www.astronomy.com/science/war-in-ukraine-highlights-importance-of-private-satellite-companies/.

43 Zegart, "Open Secrets: Ukraine and the Next Intelligence Revolution," 58, 60.

44 Borowitz, "War in Ukraine Highlights Importance of Private Satellite Companies." With support from American companies and government assistance, Ukraine received data

conflict, American companies such as Maxar Technologies, Planet,[45] and BlackSky, all experienced in electro-optical imaging, played a crucial role in this cooperative effort.[46] Additionally, Microsoft[47] and Capella Space provided notable support.[48]

Researchers and experts played a critical role in analyzing satellite imagery and real-time events, often sharing their findings on social media platforms. This transparency allowed for a broader understanding of the conflict and helped to hold aggressors accountable. A group of Stanford University students exemplified this by preparing a report for the United Nations, documenting atrocities committed by the Russian military in Ukraine. They utilized a combination of thermal and electro-optical satellite imagery, TikTok videos, geolocation applications, and other tools to compile their findings.[49]

Another significant effort was undertaken by the Institute for the Study of War, which created an interactive map of the Ukrainian theater of war.[50] This map, based on open-source and non-classified primary sources, was developed with the support of military experts, analysts, and researchers.[51] It provided a detailed and accessible overview of the ongoing conflict, further enhancing public understanding and contributing to the global response to the Russian invasion.

covering over 40 million square kilometers during the first two weeks of the conflict. To put this in perspective, this volume of data would have been sufficient to map Ukraine five times a day, or to map the territory occupied by Russian forces in March 2022 and its changes eighteen times a day. While the precise coverage of satellite imagery is not publicly known, it is believed to include both Ukrainian territory and the operational and rear zones of both Ukrainian and Russian forces.

45 See, for example, Planet Labs PBC, "Global Heritage Fund Leveraging Planet SkySat to Protect the Cultural Fabric of Ukraine," *Planet*, August 18, 2022, accessed March 25, 2023, https://www.planet.com/pulse/global-heritage-fund-leveraging-planet-skysat-to-protect-the-cultural-fabric-of-ukraine/.

46 Courtney Albon, "Intelligence Agencies Accelerate Use of Commercial Space Imagery to Support Ukraine," *Defense News Online*, April 6, 2022, www.defensenews.com/battlefield-tech/space/2022/04/06/intelligence-agencies-accelerate-use-of-commercial-space-imagery-to-support-ukraine/.

47 Microsoft, "Special Report: Ukraine. An Overview of Russia's Cyberattack Activity," 16.

48 The first space company in the United States to launch and operate synthetic aperture radar (SAR) satellites is Capella Space, https://www.capellaspace.com (accessed May 12, 2023); Konaev and Daniels, "Agile Ukraine, Lumbering Russia."

49 Zegart, "Open Secrets: Ukraine and the Next Intelligence Revolution," 56.

50 See https://www.understandingwar.org/interactive-map-russias-invasion-ukraine.

51 Zegart, "Open Secrets: Ukraine and the Next Intelligence Revolution," 56. See also Allison Puccioni, "How to Change the World from Space," *Futuring Peace*, UN DPPA, July 9, 2021, accessed May 14, 2023, https://medium.com/futuring-peace/how-to-change-the-world-from-space-d4186e76da43.

Social Media and Information Society

Social media and the proliferation of open-source information have become double-edged swords in the Russo-Ukrainian war, offering both significant advantages and potential pitfalls. These platforms allow for the rapid dissemination of critical information, but they also blur the lines between collective wisdom and misinformation, where public contributions can either aid in defense efforts or create chaos.[52]

Ukraine's strategic move toward digitalization, initiated years before the war, played a crucial role in leveraging open-source information to counter the Russian invasion. This initiative was preceded by the establishment of the Ministry of Digital Transformation of Ukraine [53] in August 2019 and the launch of the e-governance service, Diia,[54] in February 2020.[55] Diia initially served as a platform for public services, but it was quickly adapted in March 2022 to meet the urgent needs of the war. The revamped Diia application allowed for registering and tracking internal refugees,[56] uploading photos and videos of hostile military vehicles and their movements, sharing geolocation data, and reporting suspicious individuals to authorities.[57] This tool effectively turned every Ukrainian citizen with access to a smartphone into a potential contributor to the country's defense.

In parallel, the eVorog mobile application,[58] launched in March 2022, further enabled Ukrainian citizens to report hostile activities. Accessible through the Diia

---

[52] Zegart, "Open Secrets: Ukraine and the Next Intelligence Revolution," 63.

[53] Ministry of Digital Transformation of Ukraine, https://thedigital.gov.ua (accessed June 01, 2023).

[54] The application serves as an interface between the Ukrainian people and the government, currently boasting more than 18 million registered users. This e-government initiative offers a total of 99 services, accessible both through an internet-based platform and mobile applications, and 26 services available via mobile apps. Through this service, citizens can query information related to their properties, vehicles, and businesses, renew licenses, purchase parking permits, report road defects, and more. International Telecommunication Union (ITU), "Interim Assessment on Damages to Telecommunication Infrastructure and Resilience of the ICT Ecosystem in Ukraine," 22.

[55] Schmidt, "Innovation Power: Why Technology Will Define the Future of Geopolitics," 38, 40.

[56] International Telecommunication Union (ITU), "Interim Assessment on Damages to Telecommunication Infrastructure and Resilience," 23.

[57] McGee-Abe, "One Year on: 10 Technologies Used in the War in Ukraine;" Den Prystai, "From Ukrainians to Ukrainians. 5 Digital Tools and Products Created to Help in Wartime," *Official Website of Ukraine*, October 5, 2022, accessed June 10, 2023, https://war.ukraine.ua/articles/digital-tools-created-to-help-in-wartime/.

[58] See eVorog [eEnemy] bot link: https://t.me/evorog_bot (accessed June 5, 2023); StrategEast, "Ukrainian Digital Resistance to Russian Aggression" (Washington, D.C.: StrategEast Center for a New Economy, 2022), 9, https://www.strategeast.org/all_reports/Ukrainian_Digital_Resistance_Report_web.pdf.

interface, eVorog operates as a secure Telegram chatbot, allowing users to confidentially relay information to military decision-makers, Ukrainian intelligence, and counterintelligence.[59] This digital resistance, fueled by widespread public participation, became a crucial element of Ukraine's defense strategy, enabling the rapid collection and utilization of data from occupied territories.[60]

Various applications and social media platforms have become battlegrounds for open-source information gathering, propaganda, disinformation, and psychological operations. All parties involved have sought to shape public opinion, spread false information, and manipulate narratives. Both the Russian and Ukrainian sides have exploited digital and social media tools in their information (propaganda) operations. The Ukrainian military's technical and tactical versatility is evident in their ability to capture key moments and maintain interest in the virtual space and on social media, even when the frontlines remained static for months during the winter of 2022 and the spring of 2023.[61]

Artificial intelligence-supported applications and technological solutions are widely accessible, making it increasingly easy to create and spread false or manipulated content without having significant technical expertise. The Russian side has successfully produced so-called "deepfake" images and audio recordings, creating uncertainty by fabricating news related to Ukrainian events.[62] Notably, a fake video statement of President Volodymyr Zelensky from March 2022 urged Ukrainian soldiers to lay down their weapons and cease hostilities. Similarly, false communication attempts were spread in September 2022 featuring

---

[59] In March 2022, users were allowed to upload photos and videos, share geolocation data, and provide comments about their experiences. This feature was expanded in April 2022 to include the collection and sharing of information related to warcrimes committed by the Russian military. Starting in August, users were also able to report the locations of unexploded ordnance, landmines, explosives, and similar items. Prystai, "From Ukrainians to Ukrainians. 5 Digital Tools and Products Created to Help in Wartime."

[60] McGee-Abe, "One Year on: 10 Technologies Used in the War in Ukraine;" Fridbertsson, "Technological Innovation for Future Warfare," 4.

[61] Greenwood, "The Drone War in Ukraine Is Cheap, Deadly and Made in China;" Konaev and Daniels, "Agile Ukraine, Lumbering Russia." The statement illustrates the interconnectedness among various technological domains, where small-scale, commercially available unmanned aerial vehicles—referred to as drones—have become tools for PR and propaganda during the war. These drones have presented military events from previously unseen perspectives, then disseminated through social media channels such as Telegram, YouTube, Twitter, and others. They have successfully conveyed unconventional situations, exemplified by projects like "I Want to Live," in which a Russian soldier surrendered to a Ukrainian drone in November 2022, and "Saving Private Mavic," where a lost drone behind Russian lines was recovered and transported back to Ukrainian territory with the help of two other drones in January 2023.

[62] Michael C. Horowitz, Lauren Kahn, and Laura Resnick Samotin, "A Force for the Future: A High-Reward, Low-Risk Approach to AI Military Innovation," *Foreign Affairs* (May-June, 2022), 157-158, https://www.foreignaffairs.com/articles/united-states/2022-04-19/force-future.

Michael McFaul, the former U.S. ambassador to Russia (2012-2014), seeking information about Ukraine's wartime efforts.[63] Another example is a conversation—presumably of Russian origin—between a (fake) Vitali Klitschko, the mayor of Kyiv, and Gergely Karácsony, the mayor of Budapest, aimed at spreading uncertainty.[64]

Unmanned Air and Ground Vehicles

Since the outbreak of the Russo-Ukrainian war, both sides have used extensively military-designed[65] and commercially available remotely operated unmanned aerial vehicles (UAVs) and systems.[66] These tools have been employed more than ever, particularly for reconnaissance and observation.[67] This surge in usage has been driven not only by cost-effectiveness but also by the need to compensate for the lack or limited applicability of conventional air forces. Opinions diverge regarding the current role and future significance of unmanned and remotely operated aerial vehicles. Some suggest that they represent revolutionary technological innovations, while others argue that they have merely reshaped our perception of modern warfare. The truth likely lies somewhere between these two perspectives: the Ukrainian experience will help us understand the present and provide guidance for the future.[68] The only noticeable absence is in the use

[63] Zegart, "Open Secrets: Ukraine and the Next Intelligence Revolution," 61.

[64] The original recording can be found on the channel named "Orosz Hírek" (see "Russian News"): "Mayor Gergely Karácsony talks with Ál-Vitalij Klitschko," August 8, 2022, accessed June 10, 2023, www.youtube.com/watch?v=x1GhWEe9o2o. - in Hungarian

[65] In this article, we do not examine military ground and aerial vehicles designed for military purposes. Without going into detail, please consider examples such as the Turkish Baykar Bayraktar TB2 used by the Ukrainian side, the Punisher manufactured by UA Dynamics in Ukraine, the Polish WB Electronics' Warmate, the American Switchblade, or the Soviet-origin Tupolev-produced Tu-141 Strizh. Additionally, there are Russian-made unmanned systems like the Kalashnikov and ZALA AERO group KYB, the Eleron-3SV developed by ENICS, the Orlan-10 developed by Russian UAS, the Israeli-licensed Forpost R used by the Russian side (based on the Israeli IAI Searcher II), and the Orion-E developed by Kronshtadt, among others. Adam Lowther and Mahbube K. Siddiki, "Combat Drones in Ukraine," *Air and Space Operations Review* 1, no. 4 (Winter 2022): 3-13, www.airuniversity.af.edu/Portals/10/ASOR/Journals/Volume-1_Number-4/Lowther.pdf.

[66] Konaev and Daniels, "Agile Ukraine, Lumbering Russia." To avoid inconsistencies arising from different terminological definitions and categorizations (such as those used by the FAA or NATO), this article uses the term "drone" in line with everyday language. Here, "drone" refers to smaller-sized and less complex unmanned aerial vehicles typically designed for civilian and commercial use.

[67] McGee-Abe, "One Year on: 10 Technologies Used in the War in Ukraine;" Greenwood, "The Drone War in Ukraine Is Cheap, Deadly and Made in China."

[68] Lowther and Siddiki, "Combat Drones in Ukraine," 3-4.

of unmanned ground vehicles. Although Russia has access to advanced autonomous and ground vehicle systems at various stages of development, they either do not wish to deploy them or are unable to do so.[69]

Initially, the spotlight was on the Bayraktar TB2 military drone, equipped with laser-guided air-to-ground missiles. However, its success story faded due to the effectiveness of Russian air defense and electronic warfare, pushing the Bayraktar into the background, where it was used more to complement reconnaissance capabilities.[70] Ukraine was the first to deploy commercially available, cost-effective small unmanned aerial vehicles (drones) in large numbers.[71] Unlike military-designed, comparatively expensive drones, Ukraine primarily operated commercial products equipped with high-resolution cameras, controllable via smartphones and used mainly for observation and reconnaissance.[72] For these mass-deployed drones, key factors included device weight, features, and procurement cost.[73] In this technological and cost-efficiency race, inexpensive Chinese products, particularly the DJI Mavic 3 drone, emerged as the winner.[74] Alt-

[69] Palavenis, "The Use of Emerging Disruptive Technologies by the Russian Armed Forces in the Ukrainian War," 2; Konaev and Daniels, "Agile Ukraine, Lumbering Russia." The Russians have deployed various vehicle systems in Syria for mine clearance, underground tunnel exploration, and direct fire support, including the Scarab, Uran-6, and Uran-9. However, each system has encountered significant issues related to communication, control, and fire guidance.

[70] Konaev and Daniels, "Agile Ukraine, Lumbering Russia;" Lowther and Siddiki, "Combat Drones in Ukraine," 5-6, 13.

[71] Palavenis, "The Use of Emerging Disruptive Technologies by the Russian Armed Forces in the Ukrainian War," 3; Greenwood, "The Drone War in Ukraine Is Cheap, Deadly and Made in China;" Konaev and Daniels, "Agile Ukraine, Lumbering Russia."

[72] McGee-Abe, "One Year on: 10 Technologies Used in the War in Ukraine."

[73] Schmidt, "Innovation Power: Why Technology Will Define the Future of Geopolitics," 42-44; Mykhaylo Zabrodskyi et al., *Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February-July 2022* (London: Royal United Services Institute for Defence and Security Studies (RUSI), 2022), 2-3, www.rusi.org/explore-our-research/publications/special-resources/preliminary-lessons-conventional-warfighting-russias-invasion-ukraine-february-july-2022.

[74] The only publicly available statistics come from Faine Greenwood, an unmanned aerial vehicle expert who analyzed drone types used by both Russian and Ukrainian forces based on approximately 900 verified open-source samples. In this analysis, 463 instances, or 59 % of all cases, involved Chinese DJI products, with the manufacturer's small, portable Mavic drones being the most widely used. The remaining 41 % comprised a diverse range of drone types from various origins. For more details, refer to Ukraine's "drone army" initiative, which had procured around 1,400 commercially available drones by July 2022, funded through donations collected by the Ukrainian United24 platform. Greenwood, "The Drone War in Ukraine Is Cheap, Deadly and Made in China."

hough the Chinese supplier did not officially sell its products for military purposes, it also did not take any countermeasures to prevent their use in the conflict.[75]

Afterward, as artillery fire and missile strikes became decisive during the winter of 2022 and the spring of 2023, both sides enhanced the accuracy of their attacks using small drones.[76] These drones provided real-time fire support and gathered target data for future strikes. Although the promise of domestically developed Ukrainian UAVs did not fully materialize, significant knowledge was accumulated within community groups like Ukrainian Aerorozvidka.[77] This expertise was evident on the battlefield through constructing, modifying, and adapting civilian drones.[78] Efforts were made to complement the reconnaissance capabilities of these drones with less effective combat support solutions. Additive manufacturing technology proved valuable, enabling on-site customization of devices and the addition of stabilizer wings to hand and armor-piercing grenades,[79] allowing the latter to be used in free fall.[80]

With the proliferation of various UAVs, particularly small drones, both sides focused on detecting and neutralizing enemy equipment. To disrupt command and control infrastructure, both Russia and Ukraine extensively employed electronic warfare systems to interfere with communication networks, radar signals,

---

[75] It is worth noting that the Chinese supplier, DJI, has the capability to restrict the use of its commercially available drones in war zones through a system known as a "virtual fence," as it did in Iraq and Syria in 2017. In practice, this means DJI could be aware of the military use of its devices. The company's AeroScope system is designed to detect and prevent unauthorized drone use. However, despite these capabilities, DJI continues to supply drones to Russia and Ukraine's neighboring countries, raising concerns about their use in the ongoing conflict. Greenwood, "The Drone War in Ukraine Is Cheap, Deadly and Made in China."

[76] Konaev and Daniels, "Agile Ukraine, Lumbering Russia;" Zabrodskyi et al., *Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine*, 17.

[77] Aerorozvidka is a social and community initiative that has been supporting Ukraine's military efforts with network-centric and technological capabilities since 2014. The organization has garnered significant media attention for its key role in operations, including the gradual destruction of Russian vehicle columns advancing toward Kyiv and ongoing strikes on Russian positions. For more information see https://aerorozvidka.ngo (accessed June 12, 2023).

[78] Greenwood, "The Drone War in Ukraine Is Cheap, Deadly and Made in China."

[79] For example, additive manufacturing (3D printing) was utilized to modify cumulative RKG-3 anti-tank grenades in Ukraine by removing the handle and adding plastic stabilizing fins to the threaded portion of the grenade body, making them suitable for free-fall attacks on targets. Notably, by April 2022, a 3D-printed release mechanism that could be attached to drones became available for DJI products and could be ordered through the Chinese AliExpress shipping service. Greenwood, "The Drone War in Ukraine Is Cheap, Deadly and Made in China."

[80] McGee-Abe, "One Year on: 10 Technologies Used in the War in Ukraine;" Greenwood, "The Drone War in Ukraine Is Cheap, Deadly and Made in China;" Konaev and Daniels, "Agile Ukraine, Lumbering Russia."

and enemy sensor systems. Russia's effectiveness was evident in the near incapacitation of Ukrainian communications in Donbas after 2015 and its ability to hinder the proper use of smaller UAVs. However, this Russian advantage seemed to diminish in 2022.[81] While Russian electronic warfare proved less effective, both sides attempted to mitigate each other's capabilities with countermeasures.[82] In the future, the massively used UAVs are expected to remain small, cost-effective, and easy to modify, requiring opposing forces to continuously adapt to technological advancements and the challenges posed by electronic warfare.[83]

Artificial Intelligence

With the spread and advancement of artificial intelligence (AI), we are witnessing a technological revolution significantly impacting warfare, as seen in the Russian-Ukrainian conflict.[84] Both sides are leveraging algorithms to analyze and visualize vast amounts of information. This technology enables the mapping of real-world battlefields onto the virtual realm, facilitates the creation of more convincing false or manipulated images and audio recordings, and aids in disseminating disinformation. Additionally, AI supports decision-making by analyzing open-source data from social media.[85] When applied in a military context, AI offers substantial advantages. It can provide real-time alerts for hostile activities, automatically process and analyze massive datasets, and identify critical patterns. As human resources become increasingly limited, supervised AI-driven automated systems will play a crucial role in building and maintaining defense and resilience.[86]

Unlike the Russian side, the Ukrainian military effectively used AI to fuse information from diverse intelligence and reconnaissance sources, accelerating the processes of observation, orientation, decision-making, and action. While AI

---

[81] Konaev and Daniels, "Agile Ukraine, Lumbering Russia."

[82] Greenwood, "The Drone War in Ukraine Is Cheap, Deadly and Made in China;" Zabrodskyi et al., *Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine*, 2-3. Between February and July 2022, 90% of drones were lost, making cost-effectiveness and disposability top priorities. According to a November 2022 analysis, a Ukrainian drone could typically complete an average of three missions before being grounded, either due to disrupted communication between the transmitter and receiver or by neutralizing the operator. Electronic warfare efforts had to adapt constantly to the software environments updated by DJI, whose drones were the most widely used on the battlefield.

[83] If we accept the possibility and proliferation of the mass use of small autonomous drones, such as SWARM (Smart Warfighting Array of Reconfigured Modules), countermeasures will necessitate the development of enhanced electronic warfare capabilities, as well as defensive laser, microwave, artillery, and missile systems. See Schmidt, "Innovation Power: Why Technology Will Define the Future of Geopolitics," 43, 49-52.

[84] AI offers a wide range of applications, as referenced at several points throughout the article.

[85] Horowitz, Kahn, and Samotin, "A Force for the Future: A High-Reward, Low-Risk Approach to AI Military Innovation," 157-158.

[86] Schmidt, "Innovation Power: Why Technology Will Define the Future of Geopolitics."

primarily supports human decision-making, technology is evolving beyond this. It is anticipated that, even in wartime, AI systems will eventually make some decisions autonomously. From the start, American technology companies supported Ukrainian intelligence, reconnaissance, and decision-making efforts. Machine learning algorithms automated the interception, transcription, translation, and analysis of communications transmitted via insecure Russian channels.[87] Additionally, the Ukrainian company Primer adapted its AI-compatible speech transcription and translation software to filter and process militarily significant portions of intercepted communications.[88]

AI and dual-use technologies have seen practical application on the battlefield, notably through Clearview AI's facial recognition service, which gained significant media attention. With support from the American company, Ukrainian authorities identified deceased Russian soldiers using photos posted on their social media profiles and notified their families. Since March 2022, following a voluntary offer from Clearview AI, cooperation between the company and Ukraine has expanded further. Clearview AI has provided extensive support not only in identifying deceased soldiers but also in countering disinformation, detecting Russian saboteurs, identifying individuals at checkpoints, reuniting families, and assisting in war crimes investigations.[89]

Additionally, Palantir Technologies Inc.,[90] a company with over two decades of experience supporting U.S. intelligence, has played a key role in Ukraine's defense and reconstruction efforts since the outbreak of the war.[91] Palantir's data processing and visualization services have been instrumental in real-time battlefield mapping.[92] The company gathers and analyzes information on Russian troop movements and positions within its situational awareness system. It also

---

87 Konaev and Daniels, "Agile Ukraine, Lumbering Russia;" Schmidt, "Innovation Power: Why Technology Will Define the Future of Geopolitics."

88 McGee-Abe, "One Year on: 10 Technologies Used in the War in Ukraine."

89 McGee-Abe, "One Year on: 10 Technologies Used in the War in Ukraine." Hoan Ton-That, the founder and CEO of ClearView AI, reached out to the Ukrainian government on March 1, 2022, offering the company's services free of charge. At the onset of the war, ClearView AI's database included around two million photos from users of the Russian social media platform Vkontakte. Between March and July 2022, seven Ukrainian authorities and over 600 soldiers made regular use of the platform, conducting more than 60,000 searches in just four months. "War in Ukraine," *Clearview AI*, accessed May 20, 2023, https://www.clearview.ai/ukraine.

90 Palantir Technologies Inc., https://www.palantir.com.

91 Alex Karp, the CEO of Palantir, was the first among major technology company leaders to meet with the Ukrainian President. Additionally, Palantir opened an office in Ukraine to further support the country's efforts during the conflict. Jeffrey Dastin, "Ukraine Is Using Palantir's Software for 'Targeting,' CEO Says," *Reuters*, February 2, 2023, www.reuters.com/technology/ukraine-is-using-palantirs-software-targeting-ceo-says-2023-02-02/.

92 For example, the technology company's software can utilize images from commercial satellites and social media to create digital maps of enemy units. McGee-Abe, "One Year on: 10 Technologies Used in the War in Ukraine."

assists in assessing and documenting infrastructural damage resulting from conflict, offering data-driven support for efficient reconstruction decisions.[93]

Summary and Conclusion

The sharing of information, implementing new technological applications, and ensuring access to these technologies played a pivotal role in safeguarding Ukraine's digital systems and infrastructure. These efforts helped counter false Russian narratives and supported Ukraine during its attacks on Russia. While disruptive technological solutions, either in addition to or as substitutes for conventional weapons, were not immediately or decisively impactful on their own, Ukraine's successes were largely due to the integration of innovation and Western technological products. Although short-term technological superiority did not guarantee a strategic victory, the combination of new technologies and conventional weapon systems provided valuable insights into the future arsenal and methods of armed conflict. The extensive use of open-source information, communications systems, UAVs, and the emergence of AI-supported innovations in decision-making all played a defining role in Ukraine's defense strategy.

In the early phase of the conflict, we witnessed the simultaneous emergence of conventional, often dual-use products and technologies alongside innovative technological solutions. This created a paradox: private-sector leaders had responsibilities they did not want, while government leaders sought capabilities they did not possess.[94] Drawing lessons from the Ukraine war, it is essential to identify long-term research and development priorities. The defense industry must address upcoming challenges posed by emerging technologies through collaboration with the commercial tech sector, forming a shared innovation network, potentially with government support.[95] Prioritizing cost-effective technologies, reducing administrative burdens, and minimizing sector-related expenditures are critical. Investment in defense industrial capacity is necessary, but resilience and innovation should not be measured solely by product costs.[96]

---

[93] "Media Coverage," *Palantir*, accessed: June 12, 2023, https://www.palantir.com/newsroom/media/.

[94] Zegart, "Open Secrets: Ukraine and the Next Intelligence Revolution," 61.

[95] See also the research summary on the South Korean defense industry, which examines the experiences and lessons learned from the Russo-Ukrainian war: Jaret C. Riddick and Cole McFaul, "Lessons from the Ukraine-Russia War," *Issues in Science and Technology* 39, no. 3 (Spring 2023), https://issues.org/lessons-ukraine-russia-war-joeng-seo-heo/; Josep Borrell, "Lessons from the War in Ukraine for the Future of EU Defence," *European Union External Action*, May 29, 2023, www.eeas.europa.eu/eeas/lessons-war-ukraine-future-eu-defence_en.

[96] Schmidt, "Innovation Power: Why Technology Will Define the Future of Geopolitics." An innovative society or military is characterized by its ability to seamlessly integrate new technologies. The future military unit will gain a strategic advantage by being mobile, networked, and decentralized. It will excel in network-centric decision-making and effectively utilize advanced artificial intelligence tools.

Disclaimer

The views expressed are solely those of the authors and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

Acknowledgment

Project no. 2022-2.1.1-NL-2022-00012 has been implemented with the support provided by the Ministry of Culture and Innovation of Hungary from the National Research, Development and Innovation Fund, financed under the 2022-2.1.1-NL-2022-00012 funding scheme.

About the Authors

Imre Porkoláb, Ph.D., is the Chief Executive Officer of the Defense Innovation Research Institute. *E-mail*: porkolab.imre@hm.gov.hu

István Lakatos, Ph.D., is the Vice Dean at the Széchenyi István University, Audi Hungaria Faculty of Automotive Engineering, and Head of the Department of Road and Rail Vehicles. *E-mail*: lakatos@sze.hu

Ferenc Dávid, Ph.D., is a Senior Advisor and Research Fellow at the Technology Transfer Institute and the National Laboratory of Cooperative Technologies. *E-mail*: david.ferenc@techtra.hu

Bibliography

"Defending Ukraine: Early Lessons from the Cyber War," Microsoft, June 22, 2022, https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/.

"Interim Assessment on Damages to Telecommunication Infrastructure and Resilience of the ICT Ecosystem in Ukraine" (International Telecommunication Union, December 2022), https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Interim%20assessment%20on%20damages%20to%20telecommunication%20infrastructure%20and%20resilience%20of%20the%20ICT%20ecosystem%20in%20Ukraine%20-2022-12-22_FINAL.pdf.

"KA-SAT Network Cyber Attack Overview," Viasat, March 30, 2022, https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview.

"Special Report: Ukraine. An Overview of Russia's Cyberattack Activity in Ukraine," Microsoft, April 27, 2022, https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/.

"The Telecommunications Industry and Its Biggest Challenges for 2023," ISB Tech, January 23, 2023, https://www.isbtech.pl/2023/01/branza-telekomunikacyjna-i-jej-najwieksze-wyzwania-na-2023-rok/. – in Polish

"Ukrainian Digital Resistance to Russian Aggression" (Washington, D.C.: StrategEast Center for a New Economy, 2022), 9, https://www.strategeast.org/all_reports/Ukrainian_Digital_Resistance_Report_web.pdf.

"War in Ukraine," *Clearview AI*, accessed May 20, 2023, https://www.clearview.ai/ukraine.

Albon, Courtney, "Intelligence Agencies Accelerate Use of Commercial Space Imagery to Support Ukraine," *Defense News Online*, April 6, 2022, www.defensenews.com/battlefield-tech/space/2022/04/06/intelligence-agencies-accelerate-use-of-commercial-space-imagery-to-support-ukraine/.

Bandura, Romina, and Janina Staguhn, "Digital Will Drive Ukraine's Modernization," Center for Strategic & International Studies, January 10, 2023, www.csis.org/analysis/digital-will-drive-ukraines-modernization.

Borowitz, Mariel, "War in Ukraine Highlights Importance of Private Satellite Companies," *Astronomy Online*, August 16, 2022, https://www.astronomy.com/science/war-in-ukraine-highlights-importance-of-private-satellite-companies/.

Borrell, Josep, "Lessons from the War in Ukraine for the Future of EU Defence," European Union External Action, May 29, 2023, www.eeas.europa.eu/eeas/lessons-war-ukraine-future-eu-defence_en.

Clark, Stephen, "SpaceX Rockets Past 4,000 Starlink Satellites in Orbit with Another Launch," *Spaceflight Now*, May 04, 2023, https://spaceflightnow.com/2023/05/04/falcon-9-starlink-5-6-coverage/.

Dastin, Jeffrey, "Ukraine Is Using Palantir's Software for 'Targeting,' CEO Says," *Reuters*, February 2, 2023, https://www.reuters.com/technology/ukraine-is-using-palantirs-software-targeting-ceo-says-2023-02-02/.

Fridbertsson, Njall Trausti, "Technological Innovation for Future Warfare," NATO Science and Technology Committee, Sub-Committee on Technology Trends and Security, 5-8 (2023), https://www.nato-pa.int/document/2022-future-warfare-report-fridbertsson-025-stctts.

Graham-Cumming, John, "Internet Traffic Patterns in Ukraine since February 21, 2022," The Cloudflare Blog, March 4, 2022, https://blog.cloudflare.com/internet-traffic-patterns-in-ukraine-since-february-21-2022/.

Greenwood, Faine, "The Drone War in Ukraine Is Cheap, Deadly and Made in China," *Foreign Policy*, February 16, 2023, https://foreignpolicy.com/2023/02/16/ukraine-russia-war-drone-warfare-china/.

Horowitz, Michael C., Lauren Kahn, and Laura Resnick Samotin, "A Force for the Future: A High-Reward, Low-Risk Approach to AI Military Innovation," *Foreign Affairs* (May-June, 2022), https://www.foreignaffairs.com/articles/united-states/2022-04-19/force-future.

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

Konaev, Margarita, and Owen J. Daniels, "Agile Ukraine, Lumbering Russia: The Promise and Limits of Military Adoption," *Foreign Affairs*, March 28, 2023, https://www.foreignaffairs.com/ukraine/russia-ukraine-war-lumbering-agile.

Lowther, Adam, and Mahbube K. Siddiki, "Combat Drones in Ukraine," *Air and Space Operations Review* 1, no. 4 (Winter 2022): 3-13, www.airuniversity.af.edu/Portals/10/ASOR/Journals/Volume-1_Number-4/Lowther.pdf.

Marquardt, Alex, "Exclusive: Musk's SpaceX Says It Can No Longer Pay for Critical Satellite Services in Ukraine, Asks Pentagon to Pick up the Tab," *CNN Politics*, October 14, 2022, https://edition.cnn.com/2022/10/13/politics/elon-musk-spacex-starlink-ukraine/index.html.

McGee-Abe, Jason, "One Year on: 10 Technologies Used in the War in Ukraine," TechInformed, February 24, 2023, https://techinformed.com/one-year-on-10-technologies-used-in-the-war-in-ukraine/.

Palavenis, Donatas, "The Use of Emerging Disruptive Technologies by the Russian Armed Forces in the Ukrainian War," Air Land Sea Application Center, October 1, 2022, https://www.alsa.mil/Portals/9/Documents/articles/221001_ALSA_Article_Donatas_Palavenis.pdf.

Perani, Giulio, "Military Technologies and Commercial Applications: Public Policies in NATO Countries," NATO Research Fellowship (Rome, 1997), 5-6, https://www.nato.int/acad/fellow/95-97/perani.pdf.

Prince, Matthew, "Steps We've Taken around Cloudflare's Services in Ukraine, Belarus, and Russia," The Cloudflare Blog, March 7, 2022, https://blog.cloudflare.com/steps-taken-around-cloudflares-services-in-ukraine-belarus-and-russia/.

Prystai, Den, "From Ukrainians to Ukrainians. 5 Digital Tools and Products Created to Help in Wartime," Official Website of Ukraine, October 5, 2022, https://war.ukraine.ua/articles/digital-tools-created-to-help-in-wartime/.

Puccioni, Allison, "How to Change the World from Space," *Futuring Peace*, UN DPPA, July 9, 2021, https://medium.com/futuring-peace/how-to-change-the-world-from-space-d4186e76da43.

Riddick, Jaret C., and Cole McFaul, "Lessons from the Ukraine-Russia War," Jaret C. *Issues in Science and Technology* 39, no. 3 (Spring 2023), https://issues.org/lessons-ukraine-russia-war-joeng-seo-heo/.

Rosen, Kenneth R., "The Man at the Center of the New Cyber World War," *Politico*, July 14, 2022, https://www.politico.com/news/magazine/2022/07/14/russia-cyberattacks-ukraine-cybersecurity-00045486.

Sayler, Kelley M., "Emerging Military Technologies: Background and Issues for Congress," *Congressional Research Service Report* R46458, (February 2024), https://sgp.fas.org/crs/natsec/R46458.pdf.

Schmidt, Eric, "Innovation Power: Why Technology Will Define the Future of Geopolitics," *Foreign Affairs* (March-April 2023): 40, https://www.foreignaffairs.com/united-states/eric-schmidt-innovation-power-technology-geopolitics.

Schneider, Jacquelyn, "Does Technology Win Wars? The U.S. Military Needs Low-Cost Innovation – Not Big-Ticket Boondoggles," *Foreign Affairs*, March 3, 2023, https://www.foreignaffairs.com/ukraine/does-technology-win-wars.

Śliwa, Zdzisław, "The Synergy Between Technology and Soldiers in Warfare – The Russian Armed Forces Image During the War in Ukraine," *Wiedza Obronna* 281, no. 4. (2022): 53-69, https://doi.org/10.34752/2022-d281.

Tian, Nan et al., "Trends in World Military Expenditure, 2022," SIPRI Fact Sheet, April 2023, 9-11, https://www.sipri.org/sites/default/files/2023-04/2304_fs_milex_2022.pdf.

Woolbright, Jocelyn, "Nine Years of Project Galileo and How the Last Year Has Changed It," The Cloudflare Blog, June 5, 2023, https://blog.cloudflare.com/nine-years-of-project-galileo-and-how-the-last-year-has-changed-it/.

Zabrodskyi, Mykhaylo, et al., *Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February-July 2022* (London: Royal United Services Institute for Defence and Security Studies, 2022), https://www.rusi.org/explore-our-research/publications/special-resources/preliminary-lessons-conventional-warfighting-russias-invasion-ukraine-february-july-2022.

Zegart, Amy, "Open Secrets: Ukraine and the Next Intelligence Revolution," *Foreign Affairs* 102, no. 1 (January-February, 2023): 54-70, 56-57, https://www.foreignaffairs.com/world/open-secrets-ukraine-intelligence-revolution-amy-zegart.