Institute of Management
Faculty of Security, Logistics and Management
Military University of Technology in Warsaw

Instytut Zarządzania
Wydział Bezpieczeństwa, Logistyki i Zarządzania
Wojskowa Akademia Techniczna w Warszawie

ISSN 1896-9380 | eISSN 2719-860X

Modern Management Systems
Volume 22 (2026)
No. 3 (July-September)
pp. 109-122

Nowoczesne Systemy Zarządzania
Zeszyt 22 (2026)
nr 3 (lipiec-wrzesień)
s. 109-122

Civilian technologies as improvised military tools in asymmetric conflict

Technologie cywilne jako improwizowane narzędzia wojskowe w konflikcie asymetrycznym

Paweł Mateusz Kocoń[A-D,F]
General Tadeusz Kościuszko Military University of Land Forces, Poland
pawel.kocon@awl.edu.pl; ORCID: 0000-0002-2792-2406

Tomasz Michał Stefańczyk[D-E]
General Tadeusz Kościuszko Military University of Land Forces, Poland
tomasz.stefanczyk@awl.edu.pl; ORCID: 0009-0002-6335-5274

DOI: 10.37055/nsz/226440

A – Research concept/Koncepcja badania
B – Data collection/Gromadzenie danych
C – Data analysis/Analiza danych
D – Writing the article/Napisanie artykułu
E – Critical revision/Krytyczne zrecenzowanie
F – Final approval/Zatwierdzenie artykułu

Submission/Nadesłano: 06.04.2026
First review/Pierwsza recenzja: 07.04.2026
Second review/Druga recenzja: 10.04.2026
Acceptance/Zaakceptowano: 27.05.2026
Online publication/Opublikowano online: 31.07.2026
Publication/Opublikowano: 31.07.2026

Abstract:

Research objectives and hypothesis/research questions

The study aims to identify the mechanisms through which civilian digital technologies were transformed into improvised military tools and to determine the organizational conditions, operational advantages, and limitations of this adaptation process within the Ukrainian defense system. Hypothesis: The research hypothesizes that the effectiveness of adapting civilian COTS technologies in asymmetric warfare depends on three measurable dimensions: (1) shortening the decision-making/OODA loop, (2) shortening logistical cycles, and (3) reducing unit costs and barriers to entry compared to dedicated military systems, while simultaneously increasing vulnerability to information security risks.

Research methods

The study applies a qualitative research framework combining desk research and case study analysis. The desk research component is based on a systematic review of institutional defense reports (e.g., NATO, Ministry of Defense of Ukraine), academic literature, and industry publications related to military innovation, organizational resilience, dynamic capabilities, and bricolage. The case study method focuses on the operational implementation of selected civilian technologies in wartime conditions, including

communication platforms (Discord, Google Meet, WhatsApp), logistics and HR systems (DOT-Chain, SAP, Lobby X), and digital battlefield coordination tools. The analysis is theoretically grounded in the concepts of Dynamic Capabilities, organizational bricolage, and organizational resilience.

Main results

The findings indicate that widely available civilian technologies significantly accelerated operational responsiveness and decentralized decision-making processes. Communication platforms enabled rapid coordination and reduced command latency, while digital logistics systems shortened supply cycles and reduced bureaucratic inefficiencies. Low-cost and easily accessible technologies lowered training requirements and expanded operational scalability. At the same time, dependence on commercial digital infrastructure increased exposure to cyber threats, electronic surveillance, and information security vulnerabilities.

Implications for theory and practice

Civilian COTS technologies can serve as resilient, scalable, and cost-effective substitutes for conventional military systems in asymmetric conflicts. Their effectiveness is strongly linked to organizational flexibility, improvisation capacity, and the ability to rapidly reconfigure available resources. However, the long-term integration of civilian technologies into military structures requires addressing cybersecurity vulnerabilities and strategic risks associated with dual-use commercial platforms.

Keywords:

crisis management, situational awareness, system resilience, civilian technologies, commercial off-the-shelf (COTS)

Abstrakt:

Cel badań i hipotezy/pytania badawcze

Celem badania jest identyfikacja mechanizmów, dzięki którym cywilne technologie cyfrowe zostały przekształcone w improwizowane narzędzia wojskowe, oraz określenie warunków organizacyjnych, przewag operacyjnych i ograniczeń tego procesu adaptacji w ukraińskim systemie obronnym. Hipoteza: badania zakładają, że skuteczność adaptacji cywilnych technologii COTS w wojnie asymetrycznej zależy od trzech mierzalnych wymiarów: (1) skrócenia pętli decyzyjnej/OODA, (2) skrócenia cykli logistycznych oraz (3) zmniejszenia kosztów jednostkowych i barier wejścia w porównaniu z przeznaczonymi do tego celu systemami wojskowymi, jednocześnie zwiększając podatność na zagrożenia związane z bezpieczeństwem informacji.

Metody badawcze

Badanie wykorzystuje jakościowe ramy badawcze łączące badania *desk research* z analizą studiów przypadków. Komponent badań *desk research* opiera się na systematycznym przeglądzie raportów obronnych instytucji (np. NATO, Ministerstwo Obrony Ukrainy), literatury naukowej oraz publikacji branżowych związanych z innowacjami wojskowymi, odpornością organizacyjną, dynamicznymi zdolnościami i brikolażem. Metoda studium przypadku koncentruje się na operacyjnym wdrażaniu wybranych technologii cywilnych w warunkach wojennych, w tym platform komunikacyjnych (Discord, Google Meet, WhatsApp), systemów logistyki i HR (DOT-Chain, SAP, Lobby X) oraz narzędzi koordynacji cyfrowych na polu bitwy. Analiza teoretyczna opiera się na koncepcjach dynamicznych zdolności, organizacyjnej współpracy i odporności organizacyjnej.

Główne wyniki

Wyniki wskazują, że powszechnie dostępne technologie cywilne znacząco przyspieszyły operacyjną responsywność i zdecentralizowanie procesów decyzyjnych. Platformy komunikacyjne umożliwiły szybką koordynację i zmniejszyły opóźnienia w dowodzeniu, podczas gdy cyfrowe systemy logistyczne skróciły cykle dostaw i ograniczyły nieefektywność biurokratyczną. Tanie i łatwo dostępne technologie obniżyły wymagania szkoleniowe i zwiększyły skalowalność operacyjną. Jednocześnie zależność od komercyjnej infrastruktury cyfrowej zwiększyła narażenie na zagrożenia cybernetyczne, elektroniczny nadzór oraz luki w bezpieczeństwie informacji.

Implikacje dla teorii i praktyki

Cywilne technologie COTS mogą służyć jako odporne, skalowalne i opłacalne substytuty konwencjonalnych systemów wojskowych w konfliktach asymetrycznych. Ich skuteczność jest silnie powiązana z elastycznością organizacyjną, zdolnością do improwizacji oraz zdolnością do szybkiej rekonfiguracji

dostępnych zasobów. Jednak długoterminowa integracja technologii cywilnych ze strukturami wojskowymi wymaga rozwiązania luk w cyberbezpieczeństwie oraz strategicznych zagrożeń związanych z komercyjnymi platformami podwójnego zastosowania.

Słowa kluczowe:
zarządzanie kryzysowe, świadomość sytuacyjna, odporność systemu, technologie cywilne, komercyjne gotowe rozwiązania (COTS)

Introduction

As a result of Russia's full-scale invasion of Ukraine between 2022 and 2025, the Ukrainian Defense Forces were forced to abandon classic, hierarchical command and management models in favor of more network-centric solutions.

Hammes (2023) argues that the fundamental difference between the two forces was the Ukrainian Armed Forces' ability to adapt in the face of tactical surprise, compared to the rigor of the Russian forces. This evolution fits into the theoretical framework of 'Situation Control' (Llinas, Malhotra, 2022), where the command system must operate as a dynamic, learning control loop. Distributed civilian tools increase its resilience.

Contemporary crises in various types of organizations have forced a certain adjustment in management paradigms, shifting priorities from classic profit maximization to financial liquidity and building multidimensional organizational resilience (Moczydłowska, 2022). For this reason, the integration of transactive memory systems and active stimulation of employees' ability to share information are advocated, which prevents the loss of intellectual capital and allows for transforming the crisis into innovative renewal.

The enemy's superiority in weapons forced improvisation and the use of dual-use technologies.

As Hammes wrote: "Forced improvisation translated into innovative forms of action at the tactical level. Ukrainian commanders demonstrated extraordinary ingenuity and flexibility across the entire battlefield, for example, combining special forces soldiers with local reserves using civilian vehicles" (Hammes, 2023).

The use of commercial products (COTS) and consumer applications for tactical, operational, and logistical tasks was also noted. The adaptation of civilian tools enabled the construction of flexible command systems, the digitization of the supply chain, and the improvement of human resources management and medical care. The asymmetry of the conflict and the blurring of lines between the front and civilian support also forced an evolution in the areas of medical support and protection. In response to new threats, structures responsible for protecting civilians had to adapt their work to utilize new, emerging technologies (Fitz-Gerald, Hennebry, 2025). Adapting civilian applications to military purposes required close collaboration with the private sector. Bojor, Petrache, and Cristescu (2024) emphasize that the integration of civilian innovations, such as the Starlink system, required understanding between

the defense and private sectors. A key factor in this success – as Hammes (2023) points out – was the involvement of talented IT specialists who quickly connected the Diya e-government system with the military network.

On the other hand, the integration of these technologies also creates new threats – especially in the area of information security and the vulnerability of artificial intelligence models to disinformation (Militarnyi, 2024).

The main goal of this work is to analyze how civilian technologies and commercial products (COTS – Commercial Off-The-Shelf) were adapted as tools to support kinetic and non-kinetic military operations during the Ukrainian-Russian war of 2022-2025.

1. Literature review and theoretical framework

The use of commercial off-the-shelf (COTS) solutions in the military context is a subject of growing interest in the literature, although this has remained fragmented to date. Bojor, Petrache, and Cristescu (2024) analyze the role of Starlink in the Russian-Ukrainian war, while broader perspectives on the COTS portfolio remain rare. Hammes (2023) argues that Russia was unprepared for the Ukrainian convergence of new capabilities in command and control, continuous surveillance, and precise, mass fire strikes. Jones, Egan, and Rosenbach (2023) emphasize the role of low-cost drones: "Low-cost drones [...] played a key role in limiting Russian advances." Being inexpensive, they could be deployed en masse, unlike post-Soviet weapons, which lacked ammunition and spare parts.

The use of commercial drones was all the more purposeful given their widespread availability as de facto toys. On the other hand, such a drone is not protected from destruction in any way. This necessitates constant replenishment of resources, especially since some drones are "kamikaze" – they are disposable. The costly (when used in large numbers) use of drones is financially amortized by, among others, the "Army of Drones" initiative, which aims to strengthen Ukrainian forces with drone capabilities through donations from the private sector and individuals (Jones, Egan, Rosenbach, 2023).

In turn, the GIS system has been harnessed to control artillery fire. Gis Arta is the artillery fire control software connected to this system (Ford, 2024). In civil defense, humanitarian organizations responsible for protecting civilians have also adapted their operations to utilize new, emerging technologies (Fitz-Gerald, Hennebry, 2025).

The Russian-Ukrainian war demonstrated that the improvised adaptation of civilian technologies and COTS products can partially compensate for the asymmetry of military capabilities by increasing operational flexibility, situational awareness, and command system resilience (Hammes, 2023; Jones, Egan, Rosenbach, 2023).

These are just a few examples and a brief outline of the thesis. In the management literature, the way these technologies anchor organizations is important. Two key answers to this question are Dynamic Capabilities and Bricolage. Organizational.

Teece, Pisano, and Shuen (1997, p. 516) define dynamic capabilities as the ability to integrate, build, and reconfigure internal and external competencies in response to a rapidly changing environment.

These dynamic capabilities are divided into three processes (Teece, 2007):

1. Sensing (detecting opportunities and threats) – involves continuously scanning, monitoring, and interpreting the external and internal environments to identify opportunities and potential threats early. It includes detecting "weak signals", analyzing trends, and actively shaping the market.
2. Seizing (exploiting opportunities) – is the ability to quickly and effectively exploit opportunities identified in the sensing process. It involves making decisions about resource allocation, building new operating models, and initiating specific actions under conditions of uncertainty.
3. Transforming (also called reconfiguring) involves the continuous adaptation, renewal, and reconfiguration of resources, competencies, tangible and intangible assets, and organizational structures to maintain or rebuild competitive advantage in a dynamic environment.

Based on the operationalization of dynamic capabilities proposed by Bratnicka-Myśliwiec, Dyduch, and Bratnicki (2019), opportunity seizing in the research model is linked to three constructs: a) efficiency, b) bricolage, and c) stakeholder synergy (Dominiczewska, 2025).

Among the various definitions of bricolage, the one frequently cited is the one that refers to the use of combinations of readily available resources when new problems or opportunities arise. Entrepreneurial bricolage in innovation management in an intelligent and socially responsible company (Chodyński, 2020). Importantly, the existence of bricolage is closely linked to social capital. Highly resilient systems or organizations must possess a certain degree of redundancy and slack, or even a modicum of negligence, because excessive planning and strict adherence to procedures render the organization vulnerable in the face of sudden crises (Van de Walle, 2014).

The three microfoundations of dynamic capabilities map onto the three dimensions of effectiveness formulated in the research hypothesis. Sensing is responsible for recognizing the potential of civilian technologies (e.g., discovering that Discord is suitable for managing militias), seizing for their rapid operational implementation (e.g., launching command channels within hours), and reconfiguring for the institutionalization of solutions (e.g., wd DOT-Chain development in place of paper procedures). Bricolage is the micro-procedure underlying seizing and reconfiguring in conditions of extreme resource scarcity – using what's readily available (consumer drones, communicators, open-source GIS) to accomplish tasks for which they weren't designed.

The aforementioned looseness, carelessness, and over-dimensionality are naturally present in an improvised conscript army like the SZU – unlike more hierarchical armies with a rigid and enduring organizational culture, the SZU are more flexible and open to improvised innovation, so crucial on a volatile battlefield.

2. Research methodology

Research Problem: How did the Ukrainian Defense Forces' adoption of civilian COTS technologies between 2022 and 2025 impact operational capabilities in the areas of command, logistics, and situational awareness?

Objective: To identify the mechanisms by which civilian information technologies were transformed into improvised military tools, and to determine the organizational conditions and constraints of this process.

Hypothesis: The effectiveness of adapting civilian COTS technologies in asymmetric conflict depends on three measurable dimensions: (1) shortening the decision-making cycle/OODA, (2) shortening the logistics cycle, (3) reducing the unit cost and entry barrier compared to dedicated military systems – while simultaneously increasing vulnerability to information security risks.

Common instant messaging (Discord, Google Meet) and e-commerce systems are cheaper, more readily available, and require less training than traditional Battlefield Management Systems (BMS). Instant messaging systems improve military unit capabilities more quickly.

Flexible civilian solutions can match and sometimes exceed the effectiveness of costly dedicated systems, as evidenced by shorter delivery cycles and fire response times.

The authors based their conclusions on a combination of qualitative methods and secondary data analysis. The first method was a literature and source analysis (Desk Research), based on an extensive review of institutional reports (NATO, Ministry of Defense of Ukraine), as well as industry articles (Militarnyi, 2023; Time, 2023), and academic publications (e.g., Journal of Strategic Security, Ankara Medical Journal). The second method is a case study. This study provides a detailed analysis of the implementation of specific civilian tools in combat environments, such as communication platforms: Discord, Google Meet, WhatsApp, and logistics and HR systems: DOT-Chain, SAP, and Lobby X.

3. Communication and command management

Discord and video conferencing

In 2024, the Military website reported that both Russian and Ukrainian soldiers used the Discord platform for conferences, chatting, drone broadcasts, and group management (Militarnyi, 2024). Discord is a widely known platform for computer gamers (Discord, 2026). Ukrainian commands created their own servers with voice channels, allowing for the rapid connection of battle groups deployed in different positions (Militarnyi, 2023). Thanks to the possibilities of topical channels and the ease of creating meetings, command structures became flatter, eliminating information bottlenecks.

In addition to Discord, video conferencing tools such as Google Meet and Zoom were used. It has been confirmed that soldiers also communicate with drone operators via Google Meet during firefights (ChinaTalk, 2024). Thus, virtual command posts created on Discord and videoconferencing have integrated into the OODA (Observation–Orientation–Decision–Action) decision-making loop, shortening reaction times and enabling decentralized decision-making. It's important to note that, on the one hand, we have strictly combat tasks in the mission command methodology, and on the other, a tool dedicated to everyday entertainment – a tool familiar to young people, widely commented on, with instructions accessible to everyone, and at the same time, compatible with other applications.

Whatsapp in the military context

The primary advantage of this tool is encryption. That's why we ensured that all messages are fully encrypted. Each new product reflects our desire to enable people to communicate without barriers anywhere in the world. From the military's perspective, it is an ideal communication and combat coordination tool. In an article by Jones, Grace, Janet Egan, and Eric Rosenbach, a Ukrainian soldier is quoted:

"A small UAV team... would carry a Starlink and a generator or a battery. They would find some hiding places, a place to launch a drone, and release a drone that could be bought at Best Buy. They would communicate with their chain of command by phone using WhatsApp or Signal. And on top of that, they would have a tablet with a map synchronized through Starlink, showing all the targets. This also allows them to mark the locations where the missile landed, because they can see the explosion from the drone. So every element of that chain is commercial equipment. It's not even dual-use. It's a commercial offering that anyone can buy without any restrictions, using only their own funds" (Jones, Egan, Rosenbach, 2023).

The Ukrainian soldier quoted here points out the reliance on commercially available equipment, such as Starlink and drones, for small UAV teams. This illustrates the significant role of commercial, off-the-shelf technologies in military operations (Jones, Egan, Rosenbach, 2023). Regarding broader usage, it is noted that the majority of Ukrainian soldiers continue to use popular messaging services such as Telegram, Signal, Viber, and WhatsApp. This information stems from cybersecurity agency warnings about increasing espionage attacks on these apps, as reported by The Record from Recorded Future News. This corroborates observations of frontline messaging app use in eastern Ukraine, where while some apps, such as WhatsApp and Telegram, were permitted, Viber was sometimes banned for security reasons, although its use persisted (Horbyk, 2022). Concerns about the security of these apps, including WhatsApp and Telegram, were also discussed in the context of the Russian invasion of Ukraine in 2022, with advice focusing on secure messaging communications (Schmüser, Wöhler, Sri Ramulu et al., 2022).

4. The digital face of logistics

DOT-chain system

Before the invasion, Ukrainian logistics relied heavily on paper documentation, which lengthened delivery processes and hampered quality control. In 2024, the State Operator of the Rear (DOT) launched the DOT-Chain e-procurement system, which initially handled food, fuel, and clothing, and was later expanded to the "DOT-Chain Defense" platform. The Ministry of Defense reported that implementing DOT-Chain shortened the food delivery cycle by four times and reduced bureaucracy by over 30,000 documents per week (MoD, 2025b). Order processing time dropped from 45-60 days to approximately two weeks, with tens of thousands of applications and hundreds of thousands of invoices flowing through the system (MoD, 2025a). A second DOT announcement confirmed that the platform automates ordering and allows soldiers to submit complaints when they report poor product quality (MoD, 2025a).

The platform was also expanded to include a defense version – DOT-Chain Defense. In the first four months of operation, 144,000 pieces of equipment (including FPV drones and electronic warfare systems) worth over UAH 6 billion were delivered through the platform. Ninety manufacturers participated, and the system supported 184 brigades and two National Guard corps (RBC-Ukraine, 2025). Brigades were allowed to independently select equipment from manufacturers, allowing purchases to be better tailored to front-line needs. The Odessa Journal emphasizes that DOT-Chain replaced approximately 30,000 paper documents per week with "a few clicks" and accelerated deliveries fourfold. Shipping documents are instantly uploaded to the system, streamlining payments and quality verification (Odessa Journal, 2024).

SAP and financial integration

Independently of DOT-Chain, the Ministry of Defense initiated a digital transformation of finance and logistics using SAP S/4HANA. The 2025 article describes the launch of a financial accounting module that enables asset recording, expenditure control by budget codes, and integration with the Client Treasurer system. The system utilizes the NATO Stock Number standard (MoD, 2025c). Another implementation – a digital budget system – integrates expenditure planning and execution; over 60% of fund managers used this tool in 2025, significantly shortening decision-making time (MoD, 2025c).

In 2026, an integrated SAP-based Logistics Management System was launched, covering over 1,000 organizational units. It enables real-time tracking of assets (drones, weapons, electronic warfare equipment, fuel, clothing), automates ordering and billing processes, and shares data with commanders at various levels (MoD,

2026). SAP is used by over 90% of NATO armies, making the Ukrainian system interoperable and compliant with Western standards (MoD, 2026). Enabling the recruitment of SAP-savvy logisticians from the civilian sector has shortened training times and increased the professionalization of rear-line services. Furthermore, we have the potential to better handle dual-use materials and link civilian and military supply chains down to the "penultimate mile".

5. Lobby X recruitment platform

The mobilization of hundreds of thousands of people requires a transparent recruitment system that matches civilian skills to the army's needs. The Lobby X platform, created by HR entrepreneurs, allows candidates to search for positions by specialization (e.g., UAV operator, data analyst, medic) and apply directly to specific units (Lobby X, 2024). The system ensures that applications are analyzed solely within the context of the selected posting, minimizing the risk of accidental assignment to an undesirable formation (Lobby X, 2024). According to CEO Vladyslav Greizhev for the "Guardian", by July 2024, the platform had processed over 100,000 applications for 5,000 vacancies in 640 units, with non-combat roles (back-office, IT, cooks, transport, drone operators) attracting the greatest interest (The Guardian, 2024). This approach, known as competency-based recruitment, increases efficiency, morale, and a sense of empowerment among volunteers.

6. Telemedicine on the front

Difficult battlefield conditions made it difficult for doctors to examine patients face-to-face. A survey of 618 Ukrainian doctors published in the Ankara Medical Journal found that 99.2% of medics continued or increased their use of telemedicine during the war, and 97.6% of consultations were conducted via popular messaging platforms (Viber, Telegram, WhatsApp) (Poberezhets, Demchuk, Mostovoy, 2022). 84.8% of doctors used telephone calls, while only 8% used dedicated telemedicine platforms; experienced doctors used email and SMS more frequently (Poberezhets, Demchuk, Mostovoy, 2022). An analysis published in the Stanford Social Innovation Review highlights that over 98% of teleconsultations were conducted via text message, which minimized bandwidth requirements and allowed for asynchronous communication (Lee, Kumar, Petrea-Imeokhoeva et al., 2023).

Telemedicine has also become a tool for remotely monitoring the health of soldiers on rotation or recovering. On the other hand, doctors reported limitations such as the inability to perform a full physical examination and the need to ensure privacy during video calls. However, the adoption of messaging apps – non-specialist applications – proved crucial for maintaining continuity of medical care.

7. Bureaucracy

Artificial intelligence is also used in bureaucracy. Former minister Tymofiy Mylovanov described in an interview with Cybernews that he sends recordings of meetings to ChatGPT, which creates a transcript within a minute and then generates a summary and a task list with assigned responsibilities. This process shortened planning time and facilitated the enforcement of decisions (Cybernews, 2023).

8. Palantir AI

Since 2022, thanks to Alex Karp's visit to Ukraine, a partnership has been established between Ukraine and Palantir (Bergengruen, 2024). Palantir produces artificial intelligence-based software that automates decision-making processes (Palantir Technologies, n.d.). Through its principal investor, Peter Thiel, Palantir is affiliated with Clearview AI (Clearview AI, 2021; Palantir Technologies, 2026). The system is operationally used by over 1,500 officials in 18 Ukrainian government agencies (Rakhmetov, Murzagulova, 2025, p. 71).

9. Disinformation risks

However, the development of artificial intelligence poses serious threats in the information sphere. A NewsGuard report revealed that the Moscow-based Pravda network published over 3.6 million articles across several hundred fake websites in 2024, attempting to poison the training data of language models; an audit found that leading chatbots repeated Russian propaganda in about a third of cases (NewsGuard, 2025). An analysis by the Alliance for Securing Democracy think tank found that the network consists of approximately 150 websites and generated at least 207 false narratives repeated by chatbots (Alliance for Securing Democracy, 2024). The high risk of disinformation therefore necessitates verifying sources and implementing data-provenance procedures before trusting AI-generated reports. In other words, the Russian side is attempting to disrupt the models' learning processes.

Recommendations

Economy and Accessibility – The use of common civilian technologies allowed Ukraine to quickly build modern command and logistics systems. Discord, Google Meet, and e-commerce systems proved effective and cost-effective compared to dedicated solutions. The example of DOT-Chain, which replaced 30,000 paper documents per week and quadrupled delivery speeds (MoD, 2025a), demonstrates that improvised platforms can achieve business efficiency.

Resilience through Distribution – The lack of a single point of failure has become a strength of the Ukrainian system. Instead of a single "super-system", an ecosystem of multiple applications (Discord, DOT-Chain, SAP) is used, which can be quickly replaced in the event of an attack or failure.

A Culture of Innovation and Competency-Based Recruitment – Success stems not only from technology but also from organizational culture. The Lobby X platform allows volunteers to be matched to positions based on their civilian skills (Lobby X, 2024), which increases efficiency and morale. The improvised use of ChatGPT to manage meetings demonstrates how grassroots innovation can streamline processes (Cybernews, 2023).

Risk management and cybersecurity – the introduction of civilian applications carries the risk of lacking encryption or data control. The Ukrainian command mitigates this by frequently switching channels, distributing systems, and verifying information sources. Monitoring the information environment and countering disinformation campaigns that threaten the credibility of AI tools is also essential (NewsGuard, 2025; Alliance for Securing Democracy, 2024).

Integration with allies – the use of systems compliant with NATO standards, such as SAP, enables better collaboration with international partners and facilitates technology transfer (MoD, 2026). Training civilian logisticians in SAP systems supports the rapid replenishment of personnel resources.

Conclusions

The experience of the war in Ukraine demonstrates that civilian technologies can be effective improvised tools for supporting command, logistics, and human capital management in asymmetric conflict. Examples of Discord, Google Meet, the DOT-Chain platform, SAP, and Lobby X, as well as WhatsApp and Palanthir products, demonstrate that flexible and accessible solutions can equal or even surpass costly dedicated systems.

However, awareness of threats – particularly those related to information security and data manipulation – and developing a culture of innovation and adaptation are crucial. Lessons from Ukraine can provide valuable guidance for the modernization of armed forces in other countries, including Poland.

REFERENCES

[1] Alliance for Securing Democracy, 2025. *Russia's Pravda network in numbers*, https://dfrlab.org/2025/04/18/introducing-the-pravda-dashboard (accessed: 17.03.2026).

[2] Bergengruen, V., 2024. *How tech giants turned Ukraine into an AI war lab*, https://time.com/6691662/ai-ukraine-war-palantir/ (accessed: 11.03.2026).

[3] Bojor, L., Petrache, T., Cristescu, C., 2024. Emerging technologies in conflict: The impact of Starlink in the Russia–Ukraine war, *Land Forces Academy Review*, No. 29(2), pp. 185-194.

[4] Bratnicka-Myśliwiec, K., Dyduch, W., Bratnicki, M., 2019. Theoretical Foundations of Dynamic Capabilities Measurement: A Multi-logic Approach, *Przegląd Organizacji*, No. 12, pp. 4-13.

[5] ChinaTalk, 2025. *Is the Ukraine war an RMA?*, https://www.chinatalk.media/p/ukraines-drone-war (accessed: 10.02.2026).

[6] Chodyński, A., 2020. *Brikolaż przedsiębiorczy w zarządzaniu innowacjami w firmie inteligentnej i odpowiedzialnej społecznie*, [in:] D. Fatuła (ed.), *Zarządzanie zrównoważonym rozwojem organizacji. Wybrane aspekty*, Kraków: Oficyna Wydawnicza AFM, pp. 11-42.

[7] Clearview AI, 2021. *Clearview AI closes $30 million Series B funding round*, https://www.clearview.ai/press-room/clearview-ai-closes-30-million-dollar-series-b-funding-round (accessed: 10.02.2026).

[8] Cybernews, 2023. *ChatGPT: How OpenAI's bot is used in war-torn Ukraine*, https://cybernews.com/news/chatgpt-openai-bot-use-ukraine (accessed: 25.02.2026).

[9] Discord, 2026. https://discord.com/ (15.01.2026).

[10] Dominiczewska, A., 2025. *Dynamic capabilities and firm performance: Empirical evidence from organisations in Poland*, https://managementpapers.polsl.pl/wp-content/uploads/2025/04/217-DOMINICZEWSKA.pdf (accessed: 10.02.2026).

[11] Fitz-Gerald, A., Hennebry, J., 2025. Protecting civilians in a data-driven and digitalized battlespace: Toward a baseline humanitarian technology infrastructure, *Frontiers in Human Dynamics*, No. 6.

[12] Ford, M., 2024. From innovation to participation: Connectivity and the conduct of contemporary warfare, *International Affairs*, No. 100 (4), pp. 1531-1549.

[13] Hammes, T.X., 2023. *Game-changers: Implications of the Russo-Ukraine War for the future of ground warfare* [Issue Brief], Atlantic Council.

[14] Horbyk, R., 2022. "The war phone": Mobile communication on the frontline in Eastern Ukraine, *Digital War*, No. 3(1), pp. 1-16.

[15] Jones, G., Egan, J., Rosenbach, E., 2023. *Advancing in adversity: Ukraine's battlefield technologies and lessons for the U.S. Belfer Center for Science and International Affairs*, Harvard Kennedy School. https://www.belfercenter.org/publication/advancing-adversity-ukraines-battlefield-technologies-and-lessons-us (accessed: 12.01.2026).

[16] Lee, J., Kumar, W., Petrea-Imenokhoeva, M., Naim, H., He, S., 2023. Telemedicine in Ukraine is showing that high-tech isn't always better, *Stanford Social Innovation Review*, https://ssir.org/articles/entry/telemedicine_in_ukraine_is_showing_that_high_tech_isnt_always_better (accessed: 15.02.2026).

[17] Llinas, J., Malhotra, R., 2022. An expanded framework for situation control, *Frontiers in Systems Neuroscience*, No. 16.

[18] Lobby X, 2024. https://thelobbyx.com/ (accessed: 10.02.2026).

[19] Militarnyi, 2023. *Discord is used in the command posts of the Armed Forces of Ukraine*, https://militarnyi.com/en/news/discord-is-used-in-the-command-posts-of-the-armed-forces-of-ukraine (accessed: 4.03.2026).

[20] Militarnyi, 2024. *Russia shuts down Discord, instrument of military communication*, https://militarnyi.com/en/news/russia-shuts-down-discord-instrument-of-military-communication (accessed: 4.03.2026).

[21] Moczydłowska, J.M., 2022. *Zjawiska kryzysowe w organizacji. Diagnoza i zarządzanie*, Warszawa: Difin.

[22] MoD, 2025a. *The DOT-Chain system has introduced automated claims regarding the completeness and timeliness of foodstuff supplies*, https://mod.gov.ua/en/news/

the-dot-chain-system-has-introduced-automated-claims-regarding-the-completeness-and-timeliness-of-foodstuff-supplies (accessed: 4.03.2026).

[23] MoD, 2025b. *DOT-Chain Defense: Enhancing autonomy for brigades and reducing bureaucracy*, https://mod.gov.ua/en/news/dot-chain-defense-enhancing-autonomy-for-brigades-and-reducing-bureaucracy (accessed: 4.03.2026).

[24] MoD, 2025c. *Financial resources of the Ukrainian military under control: The "Budget" digital system is now in operation within the Armed Forces of Ukraine*, https://mod.gov.ua/en/news/financial-resources-of-the-ukrainian-military-under-control-the-budget-digital-system-is-now-in-operation-within-the-armed-forces-of-ukraine (accessed: 4.03.2026).

[25] MoD, 2026. *The military officially launches the digital logistics management system*, https://mod.gov.ua/en/news/the-military-officially-launches-the-digital-logistics-management-system (accessed: 11.03.2026).

[26] NewsGuard, 2025. *A well-funded Moscow-based global 'news' network has infected Western artificial intelligence with Russian propaganda*, https://www.newsguardtech.com/special-reports/moscow-based-global-news-network-infected-western-artificial-intelligence-russian-propaganda (accessed: 10.03.2026).

[27] Odessa Journal, 2024. *DOT-Chain quadruples delivery speed*, https://odessa-journal.com/ (accessed: 7.03.2026).

[28] Palantir Technologies, 2026. *Board of directors*, https://investors.palantir.com/governance/board-of-directors (accessed: 25.01.2026).

[29] Palantir Technologies, n.d. *Palantir AIP*, https://www.palantir.com/ (accessed: 25.01.2026).

[30] Poberezhets, V., Demchuk, A., Mostovoy, Y., 2022. How Russian-Ukrainian War Changed the Usage of Telemedicine: A Questionnaire-Based Study in Ukraine, *Ankara Medical Journal*, No. 22(3), pp. 305-318.

[31] Rakhmetov, B., Murzagulova, K., 2025. Artificial intelligence in warfare: The case of the Russia-Ukraine war, *Journal of Strategic Security*, No. 18(4), pp. 64-77.

[32] RBC-Ukraine, 2025. *DOT-Chain Defense update: Drone deliveries over first 4 months top 6 billion UAH*, https://newsukraine.rbc.ua/news/dot-chain-defence-update-drone-deliveries-1764729207.html (accessed: 26.02.2026).

[33] Schmüser, J., Wöhler, N., Sri Ramulu, H., Stransky, C., Wermke, D., Fahl, S., Acar, Y., 2022. "Please help share!": Security and privacy advice on Twitter during the 2022 Russian invasion of Ukraine [Preprint], *arXiv*, https://arxiv.org/abs/2208.11581 (accessed: 25.01.2026).

[34] Teece, D.J., 2007. Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance, *Strategic Management Journal*, No. 28(13), pp. 1319-1350.

[35] Teece, D.J., Pisano, G., Shuen, A., 1997. Dynamic capabilities and strategic management, *Strategic Management Journal*, No. 18(7), pp. 509-533.

[36] The Guardian, 2024. *'Be yourself': Ukraine launches PR drive to attract recruits to weary army*, https://www.theguardian.com/world/article/2024/jul/15/ukraine-attract-recruits-pr-drive-draft-russia-offensive (accessed: 15.01.2026).

[37] TIME, 2023. *Ukraine's 'secret weapon' against Russia is Clearview AI*, https://time.com/6334176/ukraine-clearview-ai-russia (accessed: 16.01.2026).

[38] Van de Walle, S., 2014. Building resilience in public organizations: The role of waste and bricolage, *The Innovation Journal: The Public Sector Innovation Journal*, No. 19(2), pp. 1-18.