Victor KORENDOVYCH
National Defense University of Ukraine
Defense Management Department
v.korendovych@edu.nuou.org.ua
https://orcid.org/0000-0003-2949-1870

Sergiy YASENKO
National Defense University of Ukraine
Defense Management Department
e-mail: s.yasenko@edu.nuou.org.ua
https://orcid.org/0000-0003-1918-9459

https://doi.org/10.34739/dsd.2025.02.12

AN APPROACH TO IMPROVING THE DIGITAL TRANSFORMATION MANAGEMENT SYSTEM (DTMS)

ABSTRACT: Objective: To develop a conceptual model of the Digital Transformation Management Sys-tem (DTMS) integrating digitization processes with capability-based defense planning. The study analyzes Ukraine's defense digital transformation (2014–2025), documenting achievements and proposing requirements for a future integrated management system. The research addresses the problem of 'patchwork automation' that arises from bottom-up vol-unteer initiatives and analyzes the shift of modern conflict toward cognitive warfare, where strategic goals include establishing situational awareness and manipulating adversary deci-sion-making. Hypothesis: Effective defense digital transformation requires systematic integration of management with the Joint Capabilities Integration and Development System (JCIDS). This integration, supported by enterprise architecture, creates an asymmetric ad-vantage through shortened decision cycles and data fusion for cognitive advantage. Meth-ods: A systems approach was applied to analyze the digital ecosystems deployed during the Russo-Ukrainian war, including DELTA, Kropyva platforms, and the 'Army of Drones' ini-tiative, assessed against NATO (NAF) and DoDAF standards. The DOTMLPFI-P model was used to identify functional gaps. Results: The DTMS architecture based on three pillars (People, Technology, Processes) and five functional blocks was substantiated. A federated governance model with an architectural repository was proposed. Conclusions: Success in modern multi-domain warfare depends on strategic alignment of digital innovations with operational needs. DTMS facilitates the transition to flexible network-centric architectures that support operational advantage in cognitive warfare.

KEYWORDS: digital transformation, defense planning, cognitive warfare, management system, multi-domain operations

PODEJŚCIE DO USPRAWNIENIA SYSTEMU ZARZĄDZANIA TRANSFORMACJĄ CYFROWĄ

ABSTRAKT: Cel: Opracowanie modelu koncepcyjnego Systemu Zarządzania Transformacją Cyfrową (DTMS) integrującego procesy cyfryzacji z planowaniem obronnym opartym na zdolnościach. Badanie analizuje transformację cyfrową obrony Ukrainy (2014–2025), dokumentując osiągnięcia i proponując wymagania dla przyszłego zintegrowanego systemu zarządzania. Praca odnosi się do problemu „mozaikowej automatyzacji" wynikającej z oddolnych inicjatyw wolontariackich oraz analizuje przesunięcie współczesnego konfliktu w stronę wojny kognitywnej, gdzie cele strategiczne obejmują kształtowanie własnej świado-mości sytuacyjnej i manipulowanie procesem decyzyjnym przeciwnika. Hipoteza: Skuteczna transformacja cyfrowa obrony wymaga systematycznej integracji zarządzania z Joint Capa-bilities Integration and Development System (JCIDS). Integracja ta, wsparta architekturą korporacyjną, tworzy asymetryczną przewagę poprzez skrócenie cyklu decyzyjnego i wykorzystanie fuzji danych dla przewagi kognitywnej. Metody: Zastosowano podejście sys-temowe do analizy ekosystemów cyfrowych wdrożonych podczas wojny rosyjskoukraińskiej, w tym platform DELTA, Kropyva I inicjatywy „Armia Dronów", oceniając je według standardów NATO (NAF) i DoDAF. Model DOTMLPFI-P wykorzystano do identyfikacji luk funkcjonalnych. Wyniki: Uzasadniono architekturę DTMS opartą na trzech filarach (Ludzie, Technologie, Procesy) i pięciu blokach funkcjonalnych. Zaproponowano federacyjny model zarządzania z repozytorium architektury. Wnioski: Sukces w nowoczesnej wojnie wielodomenowej zależy od strategicznego dostosowania innowacji cyfrowych do potrzeb operacyjnych. DTMS ułatwia przejście do elastycznych architektur sieciocentrycznych wspierających przewagę operacyjną w wojnie kognitywnej.

SŁOWA KLUCZOWE: transformacja cyfrowa, planowanie obronne, wojna kognitywna, system zarządzania, operacje wielodomenowe

INTRODUCTION

Since the beginning of the Russian undeclared war in Ukraine in 2014, there has been a recognition of the need for asymmetric development of capabilities and gaining advantage through a different configuration of relevant components. This awareness extends from small closed expert groups to a wide range of people involved in the war. In the institutionalized environment of the military, state scientific and industrial organizations, and public (civilian-volunteer) circles, understanding, and actions regarding these asymmetric measures have varied. However, starting in 2015, signs of sustained coordination of actions by various participants in this confrontation have appeared[1]. By 2022, digital development in Ukraine demonstrated positive changes, but its overall level remained technologically lower than in leading European countries, although individual service sectors were better developed. In general, the war caused by Russian aggression during 2014-2025 demonstrates a fundamental transformation in the nature of armed conflicts. Modern warfare goes beyond traditional physical domains (land, air, sea, space, cyber) and increasingly encompasses the ‘cognitive domain’ – the realm of perception and understanding, decision-making and narrative formation[2]. In this context, the digital transformation of the defense sector is gaining strategic importance, transforming from a technological process into a tool for creating asymmetric advantage.

The relevance of this study is due to several factors. First, Ukraine has been demonstrating a phenomenon of rapid digitalization under conditions of active high-intensity conflict for a long time. After accelerating automation and digitalization measures since the beginning of the conflict in 2014, over the period 2022-2025, the pace of implementation of digital solutions in the Armed Forces of Ukraine exceeded similar peacetime indicators in NATO countries by several times. At the beginning of Russia's open armed aggression, Ukraine's digital infrastructure was subjected to numerous attacks. In response, Ukraine intensified the development of digital solutions to counteract the aggressor. The war became a catalyst for the rapid development and

[1] Kabinet Ministriv Ukrayiny [Кабінет Міністрів України], "Pro skhvalennya Stratehiyi tsyfrovoho rozvytku innovatsiynoyi diyal'nosti Ukrayiny na period do 2030 roku ta zatverdzhennya operatsiynoho planu zakhodiv z yiyi realizatsiyeyu u 2025-2027 rokakh" [Про схвалення Стратегії цифрового розвитку інноваційної діяльності України на період до 2030 року та затвердження операційного плану заходів з її реалізацією у 2025-2027 роках]. Order No. 1351-r 2024 [Наказ № 1351-р], https://zakon.rada.gov.ua/laws/show/1351-2024-%D1%80#Text (05.02.2025).

[2] Ch. Deppe, G.S. Schaal, *Cognitive Warfare: A Conceptual Analysis of the NATO ACT Cognitive Warfare Exploratory Concept*, “Frontiers in Big Data” 2024, vol. 7, https://doi.org/10.3389/fdata.2024.1452129.

implementation of innovative digital solutions at all levels, from the battlefield itself to strategic management. Everyone participated in this process: the state, IT companies, and volunteers. However, this rapid response created a paradox. The initial phase of digitalization was characterized by a ‘Cambrian explosion’ of disparate software solutions developed by volunteer groups to meet immediate tactical needs. Although this provided critical capabilities in the short term, it resulted in a fragmented digital landscape, often referred to as ‘patchwork automation’. Without a single architectural standard, these heterogeneous systems (communications, logistics, situational awareness) operated in isolation, creating at the same time flexibility, resilience through decentralization, rapid growth through competition, and significant interoperability and waste of public resources. This experience requires systematization and theoretical understanding. Therefore, the lack of a centralized management system meant that data integration required manual intervention, slowing the OODA loop at the operational level. These outline other factors of relevance:

Second, there is a critical need to institutionalize successful volunteer (civic) initiatives to reduce the impact of ‘patchwork automation’ (duplication of efforts, interoperability issues and inefficient use of resources) – a systemic framework is needed to manage digital transformation;

Third, modern conflict, shifting to the ‘cognitive sphere’, aims, along with physical destruction of the enemy, at the destruction of cognitive capabilities. The technological infrastructure becomes the basis for the ‘cognitive infrastructure’, a system that provides cognitive advantage over the enemy;

Fourth, in the context of growing hybrid threats and the concept of multi-domain operations, the Ukrainian model of integrating civilian and military digital ecosystems, rapidly implementing innovations, and creating an asymmetric advantage needs to be studied and adapted for use by Ukraine's partners;

Fifth, the lack of a theoretical framework for managing DTMS in an active conflict creates multiple risks of strategic errors. Traditional approaches to defense planning (including JCIDS, DOTMLPFI-P) do not fully take into account the specifics of the digital era: the speed of change, the greater importance of non-state actors, the changing importance of the cognitive domain. Thus, research into digital transformation management systems is not a purely technical issue, it is a strategic necessity to ensure the competitiveness of defense systems in the 21st century.

Therefore, it is necessary (for this purpose of the article) to describe a conceptual approach to the digital transformation management system for integrating digitalization approaches with defense planning processes in the context of a modern conflict. To meet this need, it is necessary to answer the following questions: What key trends have emerged in the defense sector of Ukraine during the armed aggression of Russia; How to align digital transformation processes with defense planning processes and capability models; what architecture of the DTMS system will ensure the integration of technological innovations and current organizational processes?

Hypothesis: Integration of digitalization processes into the existing defense planning framework by implementing the conceptual model will increase the efficiency of the implementation of defense technology.

METHODOLOGY

Type of research: conceptual-analytical research with elements of system analysis. The research is based on a comprehensive system approach to analyze the Ukrainian transformation of the defense sector during active combat operations. The methodology is based on the analysis of the empirical experience of widespread implementation of digital situational awareness and command and control systems (such as DELTA, Kropyva, and others)[3], as well as automated/robotic systems in 2014–2024.

The Ukrainian experience demonstrates a unique model of civil society-led defense innovation. In contrast to traditional top-down procurement, the integration of digital tools followed a bottom-up trajectory. Volunteer initiatives acted as flexible 'research laboratories' that tested hypotheses on the battlefield with minimal bureaucracy. The challenge for the state, and in particular for the Ministry of Defense, was not to stifle these innovations, but to institutionalize them. The transition from chaotic volunteer support to a structured Digital Transformation Management System (DTMS) requires establishing clear architectural boundaries where private flexibility can coexist with national security standards and long-term support requirements.

To formalize these boundaries, the study uses the principles of the NATO Architecture Framework (NAF)[4] and the US Department of Defense Architecture Framework (DoDAF)[5]. These frameworks are used to map the chaotic landscape of 'patchwork automation' into a coherent enterprise architecture. This allows the identification of functional gaps and interoperability issues between different systems developed by different groups.

Furthermore, the study used the Joint Capability Development and Integration System (JCIDS) methodology to link digital solutions to operational requirements. The analysis used the DOTMLPFI-P (Doctrine, Organization, Training, Materials, Leadership, Personnel, Facilities, Compatibility, and Policy) factor model[6] to assess how digital transformation affects not only the technical ('Hardware') aspect, but also requires changes in doctrine and personnel training. This methodological synthesis ensures that the proposed DTMS is not just a technical solution but a holistic management system capable of generating asymmetric cognitive advantages.

[3] Ukrayins'ka Pravda [Українська правда], *DELTA u triytsi naypopulyarnishykh boyovykh system v Ukrayini – Ministerstvo oborony* [*ДЕЛЬТА у трійці найпопулярніших бойових систем в Україні – Міністерство оборони*] 2024, https://www.pravda.com.ua/eng/news/2024/10/09/7478839/ (05.02.2025).

[4] North Atlantic Treaty Organization, *NATO Architecture Framework Version 4.0*, 18.11.2025, https://www.nato.int/cps/en/natohq/topics_157575.htm (05.12.2025); H.D. Jørgensen, et al., *Aligning TOGAF and NAF - Experiences from the Norwegian Armed Forces*, "The Practice of Enterprise Modeling" 2011 92, pp. 131-146.

[5] *DM2 Conceptual Data Model. DoDAF Architectural Framework Version*, 02.02.2021, https://dodcio.defense.gov/Library/DoD-Architecture-Framework/dodaf20_conceptual/ (05.02.2025).

[6] AcqNotes, *Joint Capabilities Integration and Development System (JCIDS) Process Overview*, https://acqnotes.com/acqnote/acquisitions/jcids-overview (05.02.2025).

Research questions:

1. What are the key trends of digitalization observed in the defense sector of Ukraine in 2014-2025?
2. How to align digital transformation processes with the existing defense planning framework (capability development system, capability component configuration model)?
3. What DTMS architecture will ensure the integration of technological innovations and organizational processes?

Thus, the research methods:

1. System analysis: using well-known frameworks JCIDS, NAF/DoDAF, and DOTMLPFI-P to structure digitalization processes;
2. Analysis of secondary sources: systematic review of NATO doctrinal documents, Ukrainian government reports, scientific publications (2014-2025);
3. Case study method: analysis of specific systems (DELTA, Kropyva, Art GIS, Virage Tablet, Action) as empirical examples;
4. Conceptual modeling: development of the DTMS architecture based on the synthesis of theoretical frameworks and empirical data.

Limitations of this study:

- conceptual nature: the model requires empirical validation;
- limited access to classified data in military systems;
- Rapid dynamics of change: Some data may become outdated in 3-6-12 months.

By digital transformation (DT) in defense, we mean:

- integrating digital technologies into all areas of military art and defense management to fundamentally change the way we fight;
- improving the capabilities of the defense forces;
- Implementing cultural changes that require the defense forces to continually improve, experiment, and not dwell on failure.

We will briefly outline only the achievements in individual areas that were achieved due to the joint efforts of state, private, and volunteer developers who are helping Ukraine survive this brutal war.

Approaches to building and maintaining situational awareness under modern conditions have been known for some time[7]. Although often remaining purely theoretical, these approaches have gained new life in the context of the Russian-Ukrainian war. It is worth noting the National Situational Awareness Platform[8] *DELTA*, which was developed in accordance with NATO standards and includes elements of the Alliance's future standards[9]. It provides basic digital access services in a digital environment, real-time collection and integration of

[7] M. Arslan, et al., *Situational Awareness: Methods, Challenges, and Prospects*, "AI", 2022, 3(1), pp. 55-77.

[8] Ukrainska Pravda, *DELTA among the three most popular combat systems in Ukraine – Ministry of Defense*.

[9] K. Paulauskas, *Why Cognitive Superiority is an Imperative*, „NATO Review", 2024, https://www.nato.int/docu/review/articles/2024/02/06/why-cognitive-superiority-is-an-imperative/index.html (05.02.2025).

intelligence data on a digital map, as well as building various information systems based on its services. Officially implemented in the Defense Forces in February 2023. *DELTA* is used by all components of the security and defense sector. It provides a certain degree of compatibility with the *Link 16 system*. The effectiveness of such platforms is correlated with the concept of situational awareness (SA, Polish: świadomość sytuacyjna) in the era of artificial intelligence, where dynamic data-driven systems adapt measurements to changing combat situations. Achieving information dominance requires not only collecting data but also ensuring its quality and relevance in order to avoid cognitive overload for decision-makers. Systems such as DELTA are an example of the transition to C5ISRT dominance (command, control, communications, computers, cybersecurity, wywiad, obserwacja, rozpoznanie, and targeting; pol. dowództwo, zarządzenia, łączność, komputery, cyberbezpieczeństwo, wiład, obserwować, rozpoznanie i namierzanie celów), striving to ensure a decision-making cycle faster than that of the enemy. The introduction of such platforms marks a practical transition to the principles of network-centric warfare (NCW, pol. wojna sieciocentryczna). As analyzed in previous studies of the digitalization of the Armed Forces of Ukraine, systems such as DELTA do not simply automate existing processes, but create a new 'innovation ecosystem.' This ecosystem operates on a cloud-based service-oriented architecture that allows for horizontal integration of various sensors and shooters. By combining intelligence from satellites, drones, and human intelligence (HUMINT, Human Intelligence, pol.: wywiad agencyjny) into a single digital map, these systems flatten the traditional chain of command, ensuring the so-called 'self-synchronization' of forces on the battlefield. This approach significantly reduces the time between the detection and destruction of a target, confirming the effectiveness of information superiority in modern high-intensity conflicts. Given the choice of defense planning strategies, this corresponds to the scenario-resource situation, which requires an advantage in the speed of situational awareness formation[10].

Developed as a community initiative, *Kropyva* The software automates artillery control[11]. It belongs to tactical C2 communication systems (pol. dowództwo i kontrola). According to the developers, 90% of Ukrainian artillerymen use this software. Kropyva is integrated with DELTA and provides data exchange even without the Internet.

[10] Y. Serhiy, I. Tkach, *Review of partial analitical management models in capability-based systems*, "Journal of Scientific Papers Social Development and Security" 2023, 13(1), pp. 108-24.

[11] Forbes Ukrayina [Forbes Україна], *IT-khaos na sluzhbi ZSU: Kropyva, HIS Arta ta inshi systemy* [*IT-хаос на службі ЗСУ: Кропива, ГІС Арта та інші системи*], "Forbes.ua" 2022, https://forbes.ua/innovations/it-khaos-na-sluzhbi-zsu-sotni-tisyach-viyskovikh-koristuyutsya-riznim-softom-yakiy-rozrobili-volonteri-chi-ne-bezpechna-taka-detsentralizatsiya-14112022-9700; Army SOS, Defense Mapping Software 2025, https://armysos.com.ua/defense-mapping-software/ (05.02.2025).

Ark GIS[12] is designed for the headquarters of the battalion and brigade[13]. It allows users to see the overall picture of the battle and plan operations. It provides digital interaction between units of different types of armed forces.

Combat management software provides a single information field from the soldier to the battalion commander (BMS), designed to support a number of NATO standards[14].

The Virage tablet for collecting, processing, and displaying air situation ensures the performance of tasks related to actions in airspace and air defense[15]. The system shortens the 'detection – fire' cycle, provides commanders with operational calculations and a single picture of air defense on the screen. This is a system that works around the clock for the security of the entire country.

To a large extent, the above-mentioned systems support real-time data exchange modes, realizing, at least from the point of view of situational awareness, the consequences of multidomain operations. This multidomain nature involves taking into account a new 'virtual' or cross-domain element, the sphere of robotic operations. This is of significant interest to all players in the global military-political arena[16].

In the field of unmanned and robotic platforms, the Armed Forces of Ukraine widely use various types of drones for reconnaissance, fire control, and fire correction[17]. Among the many projects, I would like to highlight the 'Army of Drones' project, which provides training for UAV operators (pol. bezzałogowe statki powietrzne) and centralized drone training. This is an example of a broad public-private partnership initiative. It is a union of private training centers (about forty) and official training centers of the defense forces. As an example, we note that the distribution of drones by military units is carried out in accordance with key performance indicators (KPI, pol. kluczowe wszystki efektywności), which are determined on the basis of objective data on the use of drones in situational awareness systems. This approach contributes to the effective use of drones and provides certain data to defense procurement authorities and arms market regulators in the field of robotic systems. The latter brings the digitalization of the battlefield and operational support processes to the level of warfare, i.e., state management. Of course, this statement should be taken with certain conditions and limitations. Integration of

[12] Visicom [Візіком], *HIS 'Arta' dopomozhe znyshchyty okupantiv na skhodi Ukrayiny* [*ГІС 'Арта' допоможе знищити окупантів на сході України*], "Visicom Blog" [Блог Visicom] 2022, https://api.visicom.ua/uk/posts/gisarta170522 (05.02.2025).

[13] Center for Strategic and International Studies (CSIS), *Understanding the Military AI Ecosystem in Ukraine* 2024, https://www.csis.org/analysis/understanding-military-ai-ecosystem-ukraine (05.02.2025).

[14] Combat.Vision, *ComBat Vision 4.0*, https://combat.vision/ (05.02.2025).

[15] Clash Report, *Russian missile attack on Odessa on the screen of the Virage tablet system (automated software)*, https://x.com/clashreport/status/1681590656735629312 (05.02.2025).

[16] W. Xiu, et al., *Meta-battlefield: Conceptual design of multi-domain human-machine cooperative operation.* In China Institute of Command and Control (Ed.), Proceedings of the 11th China Conference on Command and Control (Vol. 1124, Lecture Notes in Electrical Engineering), Springer 2024.

[17] O. Sapwood, *Another 3,000 UAV operators trained as part of the Army of Drones project*, MILITARY 2023, https://militarnyi.com/en/news/another-3-000-uav-operators-trained-as-part-of-the-army-of-drones-project/#google_vignette (05.02.2025).; Center for Naval Analysis (CNA), *The Use of Artificial Intelligence and Autonomous Technologies in the War in Ukraine* 2023, https://www.cna.org/reports/2023/10/Use-of-AI-and-Autonomous-Technologies-in-the-War-in-Ukraine.pdf (05.02.2025).

robotic systems means a move towards ‘human-autonomous control’ (HAC, Polish: kontrola człowiek-autonomia), where success depends on the cognitive superiority of hybrid human-machine teams. This evolution requires sustainable command and control architectures capable of managing the ‘Internet of Battlefield Things’ (IoBT, Polish: Internet rzeczy na polu bitwy), where ubiquitous connectivity significantly influences military decision-making.

It is worth mentioning the unmanned surface vessels (Unmanned Surface Vessel – USV, pol. Bezzałogowa jednośc pływająca), which have proven their effectiveness in neutralizing the Russian fleet in the western and central part of the Black Sea. They are credited with the destruction of Russian ships in the areas of Sevastopol, Novorossiysk, and the Kerch Strait (900 kilometers from the Ukrainian coast, controlled by Ukraine)[18]. Furthermore, these USVs have proven their ability to repel helicopter attacks. The problem of navigation of small robotic systems under the conditions of modern confrontation is very common in all physical spheres. At sea, this problem has a certain peculiarity; a good overview of this topic is given in the article[19].

Unmanned ground platforms (UGVs, Pol. naziemne platformy bezzałogowe) are being actively developed. Tests of the use of drone swarms controlled by artificial intelligence (AI, Polish: sztuczna inteligencja), the integration of ground robots with strike drones, and countermeasures against enemy drones are ongoing[20].

The implementation of the latest communication technologies is a critically important area in military management. In this context, we are grateful to the Polish government for providing financial assistance to pay for the Starlink service[21].

Among the innovations in materials and production, two projects are worth mentioning:

- development of a circular viewing system with elements of augmented reality (Land Platform Modernization Kit – LPMK) for armored vehicle crews (‘transparent armor effect’)[22]. The project, which emerged in 2014-2019, became a practical demonstration of the philosophical trends of post-industrial civilization and postmodernism. The predecessor of this practical demonstration, of course, is computer games used to simulate combat operations and train defense personnel. And the successors (continuations) are – FPV

[18] G.I. Sutton, *The Evolution of Ukraine’s Maritime Drone* 2023, http://www.hisutton.com/. http://www.hisutton.com/Ukraine-Maritime-Drones-Evolution.html (05.02.2025).

[19] A.S. Alamus, A. I. Olcer, *Marine Autonomous Surface Ships: Architecture of Autonomous Navigation Systems*, „Journal of Marine Science and Engineering”, 2025, no. 1, p. 122.

[20] Ministry of Defense of Ukraine, *The Armed Forces of Ukraine are forming military units focused on robotic equipment: unmanned ground systems will be integrated into combat brigades*, https://mod.gov.ua/en/news/the-armed-forces-of-ukraine-are-forming-military-units-focused-on-robotic-equipment-unmanned-ground-systems-will-be-integrated-into-combat-brigades (05.02.2025).

[21] *US could cut Ukraine’s access to Starlink internet services over minerals*, „Reuters”, 2025, https://www.reuters.com/business/us-could-cut-ukraines-access-starlink-internet-services-over-minerals-say-2025-02-22/ (05.02.2025).

[22] *Ukrainian Smart Helmet Being Integrated with Two Types of Foreign Armor*, „MILITARY” 2019, https://militarnyi.com/en/news/ukrainian-smart-helmet-being-integrated-with-two-foreign-armor-types-2/ (05.02.2025).

drones. This can be viewed in the broader context of the Internet of Things, which, in turn, is connected at the level of ideas with the long-known sensor mesh networks [23];

- The Print Army[24] project demonstrates a practical transition from a decentralized production model to a service production model[25]. Rather, it is additive manufacturing, carried out by numerous 3D printer owners within the framework of decentralized production based on digital technologies for the production and provision of defense services. The key for the consumer is the availability of consumables, the 'quality management and quality control' measures that must be rethought.
- Electronic services for military personnel are being introduced[26].

Digital transformation in military medicine affects broad aspects of saving the lives of servicemen. IoT (Pol. Internet rzeczy) is being introduced, prostheses, exoskeletons, combat readiness monitoring[27]. There are no examples of widespread cybernation of living organisms, but with the further decrease in the cost of prostheses and orthoses, science fiction is becoming a reality[28]. The number of reviews on 'smart things / prostheses and orthoses' is constantly growing, which is correlated with the level of attention to this topic. In Ukraine, this is especially felt against the background of Russian aggression, and with Russia's plans for a complete redivision of Europe and the expansionist plans of other world players, the corresponding risks and needs of other countries are increasing[29].

An example of successful digital transformation to meet the needs of citizens is the application 'Diya' (Pol. Diia nd), which is managed by the Ministry of Digital Transformation. Today, more than 21 million Ukrainians are working to resolve the issue of receiving public services. It reflects the essence of digital transformation for the citizen, which is contained in the abbreviation 'State and I' – 'Diya.' One cannot also ignore the use of large language models, as well as related tools[30].

[23] M. Priyanka, et al., *IoT-based Blue Force Tracker: A Warrior System for Enhanced Situational Awareness and Improved Tactical Decision Making*, "IEEE Internet of Things Journal", 2025, pp. 1-6.

[24] *Yak ya drukuyu 3D-zamovlennya dlya ZSU i shcho dlya ts'oho potribno* [*Як я друкую 3D-замовлення для ЗСУ і що для цього потрібно*], https://dou.ua/forums/topic/51919/ (10.03.2025).

[25] *ECO&PIZZA has joined the army of print publications*, https://ecopizza.com.ua/en/info/ecopizza-has-joined-the-print-army-20 (05.02.2025).

[26] BBC News Ukrayina [BBC News Україна], *Elektronnyy kabinet 'Rezerv+' pratsyuye lyshe dobu. Ale vzhe vyklykav azhiotazh, krytyku i khvylyu zhartiv* [*Електронний кабінет 'Резерв+' працює лише добу. Але вже викликав ажіотаж, критику і хвилю жартів*], https://www.bbc.com/ukrainian/articles/c6pp4ly66180, (05.02.2025).

[27] O. Koval [О. Коваль]. *Popyt perevyshchuye mozhlyvosti. Yak pratsyuye rynok bionichnoho protezuvannya ta yaki IT-fakhivtsi tut potribni* [*Попит перевищує можливості. Як працює ринок біонічного протезування та які IT-фахівці тут потрібні*], https://dou.ua/lenta/articles/prosthetics-in-ukraine/ (05.02.2025).; *Біонічні протези Zeus для українських військових від Aether Biomedical,* „Forbes Україна", 2024, https://forbes.ua/innovations/stati-bogom-bliskavki-polska-aether-biomedical-proponue-dostupni-bionichni-protezi-zeus-yaki-povertayut-ruki-ukrainskim-soldatam-05042024-20357 (05.02.2025)..

[28] O. Koval, *Popyt perevyshchuye*… op. cit.

[29] F. Kamalov, et al., *Privacy and Security of the Internet of Medical Things: Challenges, Solutions, and Future Trends from a New Perspective,* "Sustainability" 2023, 15(4).

[30] H. Borchert, et al., *The Very Long Game: 25 Case Studies on the Global State of Defense Artificial Intelligence*, 1st ed., Contributions to Security and Defense Research, Springer 2024.

PERSPECTIVES ON IMPROVING THE DIGITAL TRANSFORMATION MANAGEMENT SYSTEM – DTMS

The examples above confirm the critical importance of digital transformation in defense and security. DTMS is gaining new strategic importance, namely, the digital transformation management system becomes the technological foundation of the cognitive infrastructure. It is based on three layers: People, Technology, and Processes (Organization); and five blocks: implementing new capabilities; increasing situational awareness; managing operational consequences; data aggregation; risk management and digital mission support.

Human layer:

- cognitive readiness of staff: critical thinking, media literacy, information hygiene;
- psychological resistance to manipulation and disinformation;
- understanding the cognitive dimension of conflict at all levels of command.

Technological layer (DTMS base):

- systems for collecting and processing data from all domains (physical and information);
- artificial intelligence, including machine learning, to analyze the information space, detect disinformation, and predict behavior;
- platforms for rapid dissemination of one's own information and neutralization of enemy information;
- Decision support systems taking into account cognitive effects.

Examples of technological tools include: cloud technologies; modular architecture, a digital backbone based on open systems; a federated synthetic environment; and an intelligent data structure that allows all platforms and systems to process data from all sources and share it with all users. The above is a list of technological conditions for the transition to widespread implementation of digital transformation in the defense sector[31].

Process and organizational layer:

- processes of rapid response to cognitive threats;
- coordination structures between military, government agencies, business and civil society;
- Mechanisms for integrating volunteer (civic) initiatives.

It is worth emphasizing that our adversaries are also implementing elements of digital transformation. They are also learning from the experience of war, drawing conclusions, and developing their capabilities. Therefore, the most important requirement for us is to implement digital transformation to develop our capabilities.

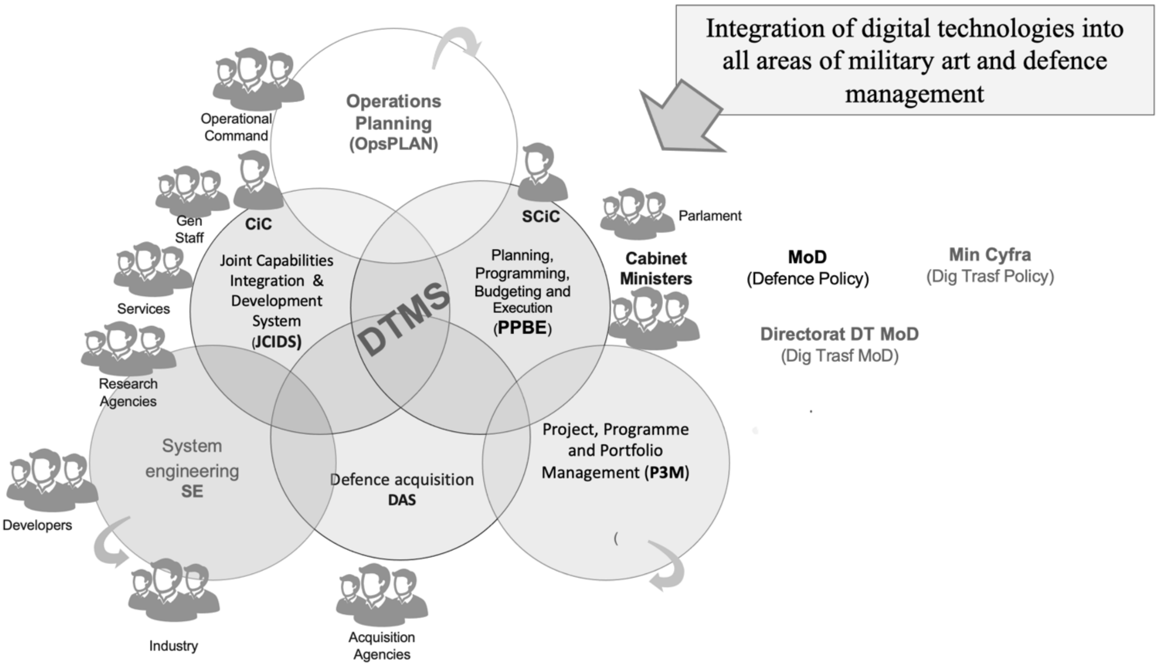
[31] S.R. Soare Simon, *Digitalization of Defence in NATO and the EU: Preparing European Defence for the Digital Era*, International Institute for Strategic Studies, https://www.iiss.org/research-paper/2023/08/digitalization-of-defence--in-nato-and-the-eu/ (05.02.2025).

Each country has its own digital transformation strategies. They are also implemented within the EU and NATO. Among other things, these documents contain the idea that digital transformation should be linked to the development of opportunities in all areas of society[32].

Thus, NATO's defense strategy emphasizes that digital transformation must be organically linked to the capabilities-based defense planning process, digital capability development goals, standardization processes, research, and procurement structures.

This is quite logical, as the goal of DT is to create relevant opportunities.

Defense planning is implemented within the framework of a well-developed Joint Integrated Capability Development System (JCIDS), which includes a requirements management system (requirement management system – RMS, Polish: System zarządzania wymaganiami) [33]Both systems have become de facto standards, although in each country, including Ukraine, the implementation of certain solutions is specific to the conditions of that country.



Integration of digital technologies into all areas of military art and defence management
Operations Planning (OpsPLAN)
Operational Command
Gen Staff
CiC
SCiC
Parlament
Cabinet Ministers
MoD (Defence Policy)
Min Cyfra (Dig Trasf Policy)
Directorat DT MoD (Dig Trasf MoD)
Joint Capabilities Integration & Development System (JCIDS)
Planning, Programming, Budgeting and Execution (PPBE)
DTMS
Services
Research Agencies
System engineering SE
Defence acquisition DAS
Project, Programme and Portfolio Management (P3M)
Developers
Industry
Acquisition Agencies

Fig. 1. Digital Transformation Management System (DTMS): frames and actors. Names: MoD – Ministry of Defense, Min Cyfra – Ministry of Digital Transformation, GenStaff – Generally Staff, CiC – Commander-in-Chief, SciC – Supreme Commander-in-Chief
Source: Created by the authors.

Therefore, the integration of JCIDS with the digital transformation coordination system should ensure the development of integrated defense and security capabilities.

[32] UK Ministry of Defence, *Digital Strategy for* Defence, 2021, https://www.gov.uk/government/publications/digital-strategy-for-defence-delivering-the-digital-backbone-and-unleashing-the-power-of-defences-data ,(05.02.2025).

[33] AcqNotes, *op. cit.*, (05.02.2025).

Let us consider these two processes using the example of the Department of Defense. The functions of the Department of Defense are implemented within a specific structure called the Department of Defense Architecture Framework (see Figure 1)[34]. This architecture includes all areas of development of both defense capabilities and digital transformation.

Participants in these processes (from the President, Parliament, and Government at the top to technology developers at the bottom) shape and implement security and defense policies, develop, and support relevant capabilities. The same architectural structure is inherent in digital transformation. The following definition is appropriate for its management system:

DTMS is a regulatory interaction between defense capability development management structures and digital transformation structures and entities to ensure the functioning of a continuous, standardized, transparent, and flexible decision-making process with respect to the development of defense and digital capabilities of defense forces.

DTMS in Ukraine at the strategic level is represented by:

- the Ministry of Digital Transformation, which, in particular, creates conditions for the introduction of digital technologies in defense;
- The Defense Digital Transformation Office (in the Ministry of Defense), which ensures digital transformation in the Ministry of Defense and the Armed Forces.

These de facto management bodies operate within an architectural framework similar to that shown in Figure 1 (let's call it the 'digital transformation architecture'). The synergy between JCIDS and DTMS greatly contributes to the acquisition of critical capabilities by defense forces.

Speaking of integrated DTMS and Capability RMS, it is worth noting the principles of their functioning:

- strategic alignment of capacity development and digital transformation.
- result-oriented.
- flexibility (adaptability).
- structured and standardized.
- transparency of the process.
- using all available organizational management mechanisms.

In turn, the tasks of integrated DTMS and RMS are as follows:

1. Development and implementation of a strategy for the development of defense forces capabilities and digital transformation.
2. Analysis of the experience gained in digital transformation for the development of defense capabilities and identification of current priorities.
3. Define / clarify the priorities for the development of digital and defense technologies.
4. Coordination of staff training on digital transformation.
5. Structuring digital capabilities by functional capability groups.

[34] DM2 Conceptual Data Model, DoDAF Architectural Framework Version, 02.02.2021, https://dodcio.defense.gov/Library/DoD-Architecture-Framework/dodaf20_conceptual/ (05.02.2025).

6. Identifying priorities for capability development and digital transformation, particularly in defense forces and their components, in the medium and long term.
7. Consideration of alternative options for capacity development, taking into account resources and other opportunities and constraints.
8. Formulation of management decisions regarding capacity development and digital transformation activities.
9. Monitoring and adjusting capacity building and digital transformation activities.

The directions for implementing these tasks should be reflected in the relevant program and planning documents.

The proposed DTMS architecture provides a technological foundation for cognitive operations through several old and new mechanisms:

Mechanism 1: Speed of the cognitive decision-making cycle

According to the OODA loop, DTMS reduces the time from observation to action, creating a cognitive advantage through faster adaptation. For example, the deployment of a reconnaissance strike control loop facilitated by DELTA and Kropyva enables a significant decrease in the duration from the identification of a target to its obliteration, reducing this interval from several hours to mere minutes. This advance engenders a perception of 'invisibility' and 'unpredictability' regarding the maneuvers of Ukrainian forces in the eyes of the adversary.

Mechanism 2: Narrative Formation

Integration of combat systems (DELTA, Kropyva) with communication platforms via DTMS can allow rapid transformation of tactical successes into strategic narratives. Videos of the destruction of Russian equipment appear on social media within hours, creating the effect of 'invincibility' of their units and demoralizing the enemy.

Mechanism 3: Decentralized Cognitive Defense

DTMS should provide coordination of distributed cognitive operations: from cyberattacks to meme campaigns of non-state actors and official information operations. This decentralization makes the cognitive system resistant to adversary attacks.

Mechanism 4: Adaptive Learning

Data analysis through DTMS allows you to identify effective cognitive tactics and quickly scale them. For example, successful information campaigns can be automatically replicated and adapted to new contexts.

An example of spontaneous integration: the operation to liberate Kherson (summer - autumn 2022). This operation demonstrates the synergy of physical and cognitive actions through DTMS:

Physical level: Coordination of actions via DELTA, use of Starlink terminals for communication;

Information level: Disinformation about the directions of the offensive, creation of multiple narratives;

Cognitive level: The demoralization of Russian troops was due to the demonstration of the inevitability of defeat, which led to a retreat without significant fighting.

To manage the complexity of this system, the DTMS should use a federated architecture maagement model. Based on the principles of the NATO Architecture Framework (NAF 4.0.), this involves creating a centralized architecture repository to store reference models and data standards.

In addition, effective governance requires the creation of an Architecture Board, a colllegial body responsible for verifying the compliance of new digital projects with the approved corporate architecture. This ensures interoperability between different systems developed by different stakeholders (state-owned enterprises, volunteers, foreign partners) and prevents fragmentation of the information environment. The Architecture Board acts as a filter, ensuring the smooth integration of all bottom-up innovations into the national C4ISR system[35]. On the other hand, the need to implement flexible approaches to management[36] is long overdue[37] (for example, UAF: Unified Architectural Framework; pol. Ujednolicona struktura architektury).

A critical aspect of the proposed DTMS is its reliance on a capability-based planning methodology. Digital transformation cannot be limited to the acquisition of hardware or software (‘Materials’); it must be synchronized with the entire spectrum of DOTMLPFI-P.

For example, implementing an AI-based command and communication system requires a simultaneous update of combat doctrines, the creation of new organizational structures for data management, and specialized training of personnel. As studies on defense capability development emphasize, ignoring these integral dimensions leads to ‘digital chaos’ rather than real capability improvement. Therefore, the DTMS must include a cross-functional analysis mechanism to ensure that each digital initiative is supported by the necessary changes in doctrine and education. This will also require changes in the approaches to implement an assessment of the effectiveness and efficiency of the defense resource management system[38].

Furthermore, future DTMSs must take into account the risks of ‘data science’ in military decision-making, ensuring that automated suggestions do not lead to ‘honest errors’ due to algorithmic bias or lack of contextual understanding. Ultimately, the system must promote ‘cognitive readiness’, the preparation of personnel to respond to unexpected scenarios in complex operational environments.

The above speaks to the challenges and limitations of integrating DTMS with cognitive infrastructure:

[35] P. Krykun, V. Pavlenko, V. Korendovych, S. Yasenko, M. Tkach, *Rozbudova natsional'noyi systemy oboronnoho planuvannya Ukrayiny za Yevroatlantychnymy pryntsypamy: voyenno-istorychnyy analiz* [*Розбудова національної системи оборонного планування України за Євроатлантичними принципами: воєнно-історичний аналіз*], „Journal of Scientific Papers Social Development and Security”, 2024, 14(3).

[36] J. Appelo, *Management 3.0: Leading Agile Developers, Developing Agile Leaders, “*Addison-Wesley” 2011; F. Almeida, E. Espineira, *Management 3.0: A Systematic Literature Review and Research Agenda*, “International Journal of Human Capital Management”, 2021, 5(2), pp. 44-57.

[37] *Ibidem*.

[38] O. Semenenko, L. Skurinevska [О. Семененко, Л. Скуріневська], *Pokaznyky ta kryteriyi otsinyuvannya efektyvnosti funktsionuvannya systemy upravlinnya oboronnymy resursamy sektoru bezpeky ta oborony Ukrayiny (Struktura, Zmist)* [*Показники та критерії оцінювання ефективності функціонування системи управління оборонними ресурсами сектору безпеки та оборони України (Структура, Зміст)*], “Journal of Scientific Papers Social Development and Security” 2023, 13(2), pp. 112-128.

1. Ethical issues: rules are needed to determine an acceptable cognitive impact, especially on civilians;
2. Manageability through performance measurement: Difficulty in quantifying cognitive effects;
3. Risk of escalation: Cognitive operations can provoke poorly predictable and unpredictable responses;
4. Dependence on communication platforms and services: Most cognitive operations depend on private platforms (Meta, X/Twitter, Telegram, etc.);
5. A single cognitive space: cognitive operations and situational awareness formation intersect in people's minds with the implementation of a single ‘neural network’ response based on the principle of superposition;
6. Long-term consequences: Impact of intensive cognitive operations on society itself and on those who participate in them.

Based on the challenges and limitations, it is easy to see development prospects, which should include:

- development of specialized modules for cognitive operations;
- creation of metrics to assess cognitive effects;
- integration of neuroscientific approaches to understanding cognitive influence;
- developing an ethical framework for cognitive operations;
- Training personnel in the cognitive dimension of war.

Thus, DTMS is not only a technology management system but also a technological foundation for warfare in the cognitive domain, a critically important component of modern conflicts.

STUDY LIMITATIONS

The presented study has several limitations:

1. Conceptual nature: The proposed DTMS model is a conceptual framework that requires further empirical validation during implementation.
2. Limited access to data: Due to limited access to some of the data on military systems, this analysis covers only publicly available sources.
3. The dynamism of the subject: The high rate of technological change means that some conclusions and solutions can quickly become outdated.
4. Geographical and military-political specifics: The model is developed based on the experience of Ukraine, which may limit its direct application in other contexts without adaptation.
5. Lack of quantitative validation: The study does not include quantitative metrics of the effectiveness of the proposed model.

These limitations outline directions for further research.

CONCLUSIONS

The protracted Russian-Ukrainian war has catalyzed an unprecedented digital transformation in the defense sector, demonstrating a fundamental shift from incremental technological upgrades to a systemic rethinking of defense business models. Although the core logic of defense management – capability-based planning, requirements generation, and resource allocation, remains anchored in proven frameworks such as JCIDS and DoDAF, the essence of what constitutes defense capability is undergoing a radical transformation.

The experience demonstrates that digital transformation in defense goes far beyond the implementation of new technologies. Integration of platforms such as DELTA, Kropyva, and Combat Management Software, combined with the rapid scaling of unmanned systems and decentralized production networks (as exemplified by the Print Army project), signals a deeper evolution: the transformation of defense business models themselves. Traditional defense systems, mobilization, human capital management, situational awareness, and operational command are fundamentally reimagined through digital technologies.

Three critical transitions define this evolution:

First, from recognizing technological change to proactively implementing business model innovations. The shift from recognizing the utility of drones to creating a ‘Drone Army’ ecosystem represents not just procurement reform, but also a rethinking of how defense capabilities are developed, trained, distributed, and sustained through public-private-volunteer partnerships.

Second, from centralized to distributed operational models. Systems such as Kropiva and Art GIS allow for decentralized decision-making at the tactical level, fundamentally changing command and control paradigms. The successful deployment of unmanned naval vessels operating 900 kilometers from controlled coastlines demonstrates that autonomous operations require a new doctrinal framework, not just new equipment.

Third, from a platform-centric to a network-centric defense architecture. DELTA’s integration with NATO standards (including Link 16 compatibility) and its interoperability with tactical systems such as Kropyva illustrate the need for open and modular digital highways that allow data aggregation, real-time situational awareness, and coordinated action between domains.

Thus, the answer to the first research question was: five key trends were identified - IoT/IoBT, AI/ML, C5ISRT, NCW, cognitive technologies.

However, these technological and organizational innovations create new management imperatives. The Digital Transformation Management System (DTMS) proposed in this article addresses a critical gap: ensuring that digital transformation remains strategically aligned with the development of defense capabilities. Without integrated management structures that link DTMS to capability-based planning (JCIDS) and architectural frameworks (DoDAF), digital initiatives risk fragmentation, duplication, and misalignment with operational priorities.

Answer to the second research question: The effectiveness of the mechanism for coordinating decisions on digitalization through the NAF/DODAF/UAF architectural models and the DOTMLPFI-P capability component configuration model has been confirmed.

Based on the principles of strategic alignment, agility, transparency, and results orientation, the DTMS framework provides a normative framework for managing the complex interplay between technology adoption, organizational change, and capability creation. Its nine core tasks, from strategy formulation to monitoring and adjustment, ensure that digital transformation serves defense outcomes rather than becoming an end in itself.

The fundamental lesson from the Ukrainian experience is clear: Digital transformation in defense is not a technical project, but a strategic imperative that requires new management paradigms. As adversaries also learn and adapt, the competitive advantage lies not in any single technology, but in the speed and coherence with which defense systems can integrate innovation across people, processes, and platforms. The DTMS framework offers a structured approach to achieving this integration, ensuring that the profound technological shifts that are transforming modern warfare are translated into sustainable operational advantage.

Answer to the third research question: The DTMS architecture encompasses six classical defense management processes and nine functional tasks.

Ultimately, the analysis confirms that digital transformation is less about technology and more about a fundamental cultural shift in the Armed Forces. The implementation of DTMS cannot be successful if it is imposed on rigid industrial-age management hierarchies. It requires a shift to a network-centric culture where information sharing is encouraged and 'cognitive readiness' is a priority. The resistance to change that is often seen in outdated bureaucratic structures must be addressed through continuous education and the promotion of a 'digital mindset' among officers, transforming them from passive users of technology to active architects of cognitive advantage.

Scientific novelty:

For the first time, digitalization processes were integrated into the framework of defense planning through the DTMS conceptual model; systematized disparate digitalization initiatives within a single architectural framework.

Practical significance:

The model can be used to coordinate digitalization initiatives in the management of the Ministry of Defense of Ukraine;

This experience may be useful for NATO member countries in the context of defense transformation.

Future research should include empirical validation of the implementation of DTMS, comparative analysis of digital transformation management models across NATO allies, and the development of metrics to assess the maturity of digital transformation in defense organizations. As defense increasingly becomes a competition for systemic adaptation rather than material advantage, the quality of transformation management will determine strategic outcomes. Thus, future research directions include:

- empirical validation of the DTMS model through pilot projects;
- development of metrics for the effectiveness of digitalization in armed conflict;
- comparative analysis with the experience of other countries.

REFERENCES

AcqNotes. 2024. Overview of the Joint Capability Integration and Development System (JCIDS) Process. In https://acqnotes.com/acqnote/acquisitions/jcids-overview.

Alamoush Anas, Aykut I. Ölçer. 2025. "Maritime Autonomous Surface Ships: Architecture of Autonomous Navigation Systems". Journal of Marine Science and Engineering 13(1): 122. https://doi.org/10.3390/jmse13010122.

Almeida Fernando, Espineira Eduardo. 2021. "Management 3.0: A Systematic Literature Review and Research Agenda". International Journal of Human Capital Management 5 (2): 44-57. https://doi.org/10.21009/IJHCM.05.02.5.

Appelo Jürgen. 2011. "Management 3.0: Leading Agile Developers, Developing Agile Leaders". Addison-Wesley Family Works Series.

Army SOS. 2025. Defense Mapping Software. https://armysos.com.ua/defense-mapping-software/.

Arslan Munir, Aved Alexander, Blash Eric. 2022. "Situational Awareness: Methods, Challenges, and Prospects". AI 3 (1): 55-77. https://doi.org/10.3390/ai3010005.

BBC News Ukraine. 2024. The electronic cube 'Reserve+' has only been operating for a day. But it has already caused a stir, screams and a wave of jokes. In https://www.bbc.com/ukrainian/articles/c6pp4ly66180.

Borchert Heiko, Schütz Torben, Werbowski Josef. 2024. The Very Long Game: 25 Case Studies on the Global State of Defense Artificial Intelligence. Springer.

Center for Naval Analysis (CNA). 2023. The Use of Artificial Intelligence and Autonomous Technologies in the War in Ukraine. In https://www.cna.org/reports/2023/10/Use-of-AI-and-Autonomous-Technologies-in-the-War-in-Ukraine.pdf.

Center for Strategic and International Studies (CSIS). 2024. Understanding the Military AI Ecosystem in Ukraine. In https://www.csis.org/analysis/understanding-military-ai-ecosystem-ukraine.

Clash Report. 2023. Russian missile attack on Odessa on the screen of the Virage tablet system (automated software). In https://x.com/clashreport/status/1681590656735629312.

Combat.Vision. 2025. ComBat Vision 4.0. In https://combat.vision/.

Deppe Christoph, Schaal Gary, 2024. "Cognitive Warfare: A Conceptual Analysis of the NATO ACT Cognitive Warfare Exploratory Concept". Frontiers in Big Data 7. https://doi.org/10.3389/fdata.2024.1452129.

DM2 Conceptual Data Model. DoDAF Architectural Framework Version 2.02.2021. In https://dodcio.defense.gov/Library/DoD-Architecture-Framework/dodaf20_conceptual/.

Dou.ua. 2025. How I print 3D orders for the Armed Forces of Ukraine and what is needed for this. In https://dou.ua/forums/topic/51919/.

ECO&PIZZA. 2025. ECO&PIZZA has joined the army of print publications. In https://ecopizza.com.ua/en/info/ecopizza-has-joined-the-print-army-20.

Expo.Diia.Gov.Ua. 2025. Public services portal. In https://expo.diia.gov.ua/.

Forbes Ukraine. 2022. IT-khaos na sluzhbi ZSU: Kropyva, HIS Arta ta inshi systemy" [IT-хаос на службі ЗСУ: Кропива, ГІС Арта та інші системи]. In https://forbes.ua/innovations/it-khaos-na-sluzhbi-zsu-sotni-tisyach-viyskovikh-koristuyutsya-riznim-softom-yakiy-rozrobili-volonteri-chi-nebezpechna-taka-detsentralizatsiya-14112022-9700.

Forbes Ukraine. 2025. Zeus Bionic Prostheses for Ukrainian Military from Aether Biomedical [Bionic. Zeus prostheses for Ukrainian military from Aether Biomedical]. In https://forbes.ua/innovations/stati-bogom-bliskavki-polska-aether-biomedical-proponue-dostupni-bionichni-protezi-zeus-yaki-povertayut-ruki-ukrainskim-soldatam-05042024-20357.

Jørgensen Howard D., Leland Tore, Skogvold Stine. 2011. Combining TOGAF and NAF – The Norwegian Armed Forces Experience. In Enterprise Modeling Practice. Springer Berlin Heidelberg.

Kabinet Ministriv Ukrayiny [Кабінет Міністрів України]. 2024. Pro skhvalennya Stratehiyi tsyfrovoho rozvytku innovatsiynoyi diyal'nosti Ukrayiny na period do 2030 roku ta zatverdzhennya operatsiynoho planu zakhodiv z yiyi realizatsiyeyu u 2025-2027 rokakh [Про схвалення Стратегії цифрового розвитку інноваційної діяльності України на період до 2030 року та затвердження операційного плану заходів з її реалізацією у 2025-2027 роках]. Order No. 1351-r [Наказ № 1351-р]. In https://zakon.rada.gov.ua/laws/show/1351-2024-%D1%80#Text.

Kamalov Firuz, et al. 2023. “Privacy and Security of the Internet of Medical Things: Challenges, Solutions, and Future Trends from a New Perspective”. Sustainable Development 15(4). https://doi.org/10.3390/su15043317.

Koval Olena. 2025. “Demand Exceeds Opportunities.” How the Bionic Prosthetics Labor Market and What IT Specialists Are Needed Here” [«Попит перевищує можливості». Як працює ринок біонічного протезування та які IT-фахівці тут потрібні]. https://dou.ua/lenta/articles/prosthetics-in-ukraine/.

Koval Olena. 2025. Popyt perevyshchuye mozhlyvosti. Yak pratsyuye rynok bionichnoho protezuvannya ta yaki IT-fakhivtsi tut potribni [Попит перевищує можливості. Як працює ринок біонічного протезування та які IT-фахівці тут потрібні]. In https://dou.ua/lenta/articles/prosthetics-in-ukraine/.

Krykun Petro, Pavlenko Viktor, Korendovych Viktor, Yasenko Serhiy, Tkach Mykola. 2024. “Rozbudova natsionalʹnoyi systemy oboronnoho planuvannya Ukrayiny za Yevroatlantychnymy pryntsypamy: voyenno-istorychnyy analiz” [Розбудова національної системи оборонного планування України за Євроатлантичними принципами: воєнно-історичний аналіз]. Journal of Scientific Papers ‘Social Development and Security’ 14 (3): 3. https://doi.org/10.33445/sds.2024.14.3.2.

MILITARY. 2019. Ukrainian Smart Helmet Being Integrated with Two Foreign Armor Types. In https://militarnyi.com/en/news/ukrainian-smart-helmet-being-integrated-with-two-foreign-armor-types-2/.

Ministry of Defense of Ukraine. 2025. The Armed Forces of Ukraine are forming military units focused on robotic equipment: unmanned ground systems will be integrated into combat brigades. In https://mod.gov.ua/en/news/the-armed-forces-of-ukraine-are-forming-military-units-focused-on-robotic-equipment-unmanned-ground-systems-will-be-integrated-into-combat-brigades.

North Atlantic Treaty Organization. NATO Architecture Framework, Version 4.0. In https://www.nato.int/cps/en/natohq/topics_157575.htm.

Paulauskas Kestutis. 2024. “Why Cognitive Superiority is an Imperative.” NATO Review. In https://www.nato.int/docu/review/articles/2024/02/06/why-cognitive-superiority-is-an-imperative/index.html.

Priyanka Mane, Kolap Mandar, Bharatiya Rajesh, Jadhav Madhuri. 2025. “IoT-based Blue Force Tracker: A Warrior System for Enhanced Situational Awareness and Improved Tactical Decision Making”. IEEE Internet of Things Journal: 1-6. https://doi.org/10.1109/SATC65530.2025.11136911.

Reuters. 2025. US could cut Ukraine’s access to Starlink internet services over minerals. In https://www.reuters.com/business/us-could-cut-ukraines-access-starlink-internet-services-over-minerals-say-2025-02-22/.

Sapwood Olivia. 2023. “Another 3,000 UAV operators trained as part of the Army of Drones project”. MILITARY. In https://militarnyi.com/en/news/another-3-000-uav-operators-trained-as-part-of-the-army-of-drones-project/#google_vignette.

Semenenko Oleg. Lesya Skurinevska. 2023. “Indicators and criteria for assessing the effectiveness of the functioning of defense resource management systems of the defense security sector of Ukraine (Structure, Content)”. Journal of Scientific Papers Social Development and Security 13 (2): 112-128. https://doi.org/10.33445/sds.2023.13.2.10.

Soare Simon R. 2023. Digitalization of Defence in NATO and the EU: Preparing European Defence for the Digital Era. International Institute for Strategic Studies. In https://www.iiss.org/research-paper/2023/08/digitalization-of-defence--in-nato-and-the-eu/.

Sutton G.I. 2023. The Evolution of Ukraine’s Maritime Drone. http://www.hisutton.com/. In http://www.hisutton.com/Ukraine-Maritime-Drones-Evolution.html.

UK Ministry of Defence. 2021. Digital Strategy for Defence. https://www.gov.uk/government/publications/digital-strategy-for-defence-delivering-the-digital-backbone-and-unleashing-the-power-of-defences-data.

Ukrayinska Pravda. 2024. DELTA u triytsi naypopulyarnishykh boyovykh system v Ukrayini – Ministerstvo oborony [ДЕЛЬТА у трійці найпопулярніших бойових систем в Україні – Міністерство оборони]. In https://www.pravda.com.ua/eng/news/2024/10/09/7478839/.

Visicom [Візіком]. 2022. HIS 'Arta' dopomozhe znyshchyty okupantiv na skhodi Ukrayiny" [ГІС 'Арта' допоможе знищити окупантів на сході України]. In https://api.visicom.ua/uk/posts/gisarta170522.

Xiu Wang, et al. 2024. Meta-battlefield: Conceptual design of multi-domain human-machine cooperative operation. In China Institute of Command and Control (Ed.), Proceedings of the 11th China Conference on Command and Control (Vol. 1124, Lecture Notes in Electrical Engineering). Springer. https://doi.org/10.1007/978-981-99-9021-4_59.

Yasenko Serhiy, Tkach Ivan. 2023. “Review of individual analytical models for system improvement and improvement”. Journal of scientific works Social development and security 13(1): 108-24. https://doi.org/10.33445/sds.2023.13.1.10.