web: conference.vsbm.sk
e-mail: conference@vsbm.sk

ISBN: 978-80-8185-084-4

EAN: 9788081850844

18. medzinárodná vedecká konferencia BEZPEČNÉ SLOVENSKO A EÚ
18th International Scientific Conference SECURE SLOVAKIA AND EU
RECENZOVANÝ ZBORNÍK PRÍSPEVKOV Z KONFERENCIE
REVIEWED CONFERENCE PROCEEDINGS

The University of Security Management in Košice

18. medzinárodná vedecká konferencia

BEZPEČNÉ SLOVENSKO A EURÓPSKA ÚNIA

18th International Scientific Conference

SECURE SLOVAKIA AND EUROPEAN UNION

RECENZOVANÝ ZBORNÍK PRÍSPEVKOV Z KONFERENCIE

REVIEWED CONFERENCE PROCEEDINGS

06. november 2025, Košice, Slovensko

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD PODPREDSEDU VLÁDY SLOVENSKEJ REPUBLIKY PRE PLÁN OBNOVY A ZNALOSTNÚ EKONOMIKU
VAIA

18. medzinárodná vedecká konferencia
BEZPEČNÉ SLOVENSKO A EURÓPSKA ÚNIA

18th International Scientific Conference
SECURE SLOVAKIA AND EUROPEAN UNION

RECENZOVANÝ ZBORNÍK PRÍSPEVKOV Z KONFERENCIE

REVIEWED CONFERENCE PROCEEDINGS

6. november 2025

Košice, Slovensko

OXFORD

VŠBM v KE

cena pre najlepšiu vysokú školu so vznikom po roku 1989, Oxford,

2012

cena „manažér roka“ Oxford,

2012

cena „meno vo vede - name in science - NS“ Oxford,

2014

cena za kvalitu a najlepšie obchodné meno Berlín,

2018

TOP-100 Oxford,

2021

cena „manažér roka“ Oxford,

2021

cena kvality ESOR´s QAA Dubaj,

2021

cena IBI v kategórii „Kvalita vo vzdelávaní“ Paríž

2022

ocenenie„Flag of Europe“ a licencia kvality - QS EBA Oxford,

2023

ocenenie„Quality Choice Prize“ ESQR Štokholm,

2025

ocenenie„European Quality Prize“ Oxford,

2025

Zborník vydaný v rámci projektu:

Názov projektu: „Škola digitálnej bezpečnosti“

Názov programu: Plán obnovy a odolnosti SR

kód projektu: 09I05-03-V04-00043

Projekt je spolufinancovaný EÚ z prostriedkov Plánu obnovy a odolnosti SR

Recenzenti/ Reviewers:

Dr.h.c. prof. Ing. Vladimír KLIMO, CSc., DBA

doc. PhDr. Rastislav KAZANSKY, PhD., EMBA

Dr. h. c. doc. JUDr. Miroslav FELCAN, PhD., LL.M., DSc.,

Editor: Bc. Katrin Juliána Živčáková

Vydala/Published:
Vysoká škola bezpečnostného manažérstva v Košiciach, Košťova 1,
040 01 Košice, Slovakia

ISBN: 978-80-8185-084-4

OBSAH – CONTENTS

Prezident školy:

Rómsky problém na Slovensku z pohľadu utopického socializmu Roberta Owena
MESÁROŠ Marián 15

Rektor školy:

Perspektívy využitia projektu „Škola digitálnej bezpečnosti“ v praxi
LOŠONCZI Peter.....30

Teoretické východiska kybernetických hrozieb obci v SR
ADAMKO Jozef 37

Bezpečnostné vzdelávanie na slovenských vysokých školách v kontexte edukácie ukrajinských študentov a jeho využiteľnosť v praxi
ANTALIKOVÁ Jana 56

Zabezpečení umělé inteligence: Vektory zneužití a obranné strategie
BARTOUŠEK Libor.....65

Aktuálne otázky bezpečnosti a požiadavky na bezpečnostné opatrenia na vysokých školách
BETUŠ Ľubomír – BETUŠ Miroslav 76

Medzinárodné organizácie a ich funkcie v systéme zabezpečovania mieru a globálnej bezpečnosti
BUZOVÁ Alena 94

Analytický pohľad na legalizáciu výnosov z trestnej činnosti a financovanie terorizmu
COCUĽOVÁ Jana, MINĎAŠOVÁ Simona, VAGASKÝ René.....103

Economic and Technological Security of the European Union in the Face of Global Competition
CZAKOWSKI Dariusz, CZAKOWSKA Sylwia 113

Využitie umelej inteligencie a manažment kamerových systémov v policajnej praxi v kontexte GDPR
DOBOŠ Tomáš 125

Zdravotné riziká v rómskych osadách - výzvy a možnosti zlepšenia
FEDURCOVÁ Ivana.....132

Manažment daňovej správy a jeho úloha pri odhaľovaní daňových trestných činov
GOMBÁR Miroslav, SVETOZAROVOVÁ Nella ,BURDOVÁ Anna 140

Vývoj a trendy v oblasti legalizácie príjmov z trestnej činnosti v Slovenskej republike
GOMBÁR Miroslav, VAGASKÝ René , MINĎAŠOVÁ Simona 147

Implementácia právnych požiadaviek na kybernetickú a informačnú bezpečnosť v praxi podnikov
HANDLOVSKÝ Július.....157

Výhody a riziká financovania mäkkých faktorov z rozpočtov obce v kontexte bezpečného a udržateľného rozvoja regiónov
HRABKOVSKÁ Andrea 168

Dlhy a ich možné bezpečnostné riziká v podmienkach Slovenskej republiky
IMRICH Juraj.....177

Ochrana súkromia v každodenných kryptomenových transakciách
JAKUBEC Libor.....180

Manažment rizík v civilnom letectve
JURKAŠ Ladislav 187

Fenomenologie násilných projevů ve školním prostředí v ČR
KOCÍK Milan, BEDNÁŘ Jakub 205

Bezpečné pracovné prostredie sociálneho pracovníka: riziká, prevencia a podpora duševnej odolnosti
KOLTÁŠ Marek 213

Mäkké ciele a ich ochrana pred terorizmom
KONKOĽ Dávid 230

Terorizmus ako aspekt ohrozujúci EBP a jeho aktuálny stav v EÚ s dopadom na bezpečnosť SR
KOSÁR Erik, TÖRÖKOVÁ Natália.....241

Medzinárodná finančná pomoc ako faktor obnovy ekonomiky Ukrajiny
KOSTIUKH Anatolii 251
Objektivizácia vývoja stresoidnej situácie vyšetrením autonómneho nervového systému
LACKO Anton1, CHERNOMORKII Egor, KOLARČÍK Matuš, LACKO Lukáš, KRIŽKO Marian, BABEČKA Jozef.....25*8*

Úloha väzenského lekára v procese resocializácie
LEŠŠ Július.....278

Analytický pohľad na certifikáciu cylindrických vložiek
MAJIROŠ Michal 282

Bezpečnosť vysokých škôl v kontexte ochrany mäkkých cieľov: riziká, trendy a opatrenia
MIFKOVIČ Adrián, MAJLINGOVÁ Andrea 289

Digitalizácia dobrovoľníkov vo vnútornej bezpečnosti SR v kontexte ochrany osobných údajov EÚ
MICHALOVOVÁ Veronika.....308

Pohľad vysokoškolského študentstva na bezpečnosť vysokoškolského edukačného procesu v online prostredí
MICHVOCÍKOVÁ Veronika 320

Kybernetická bezpečnosť v moderných automobiloch: výzvy, hrozby a perspektívy ochrany
MOLNÁR Norbert, SVRČEK Miloš 327

Kybernetická bezpečnosť na sociálnych sieťach: Ako sa chrániť pred modernými podvodmi
MOLNÁR Norbert 333

Narastajúce prejavy agresivity a násilia u detí v regionálnom školstve
MRÁZKOVÁ Lucia 339

Environmentálna politika Slovenskej republiky
NEMKY Martin 348

Integrovaný záchranný systém – skúsenosti Poľska a Slovenska s reakciou na krízové situácie. Empirická a komparatívna analýza
OLAK Antoni, KONECKA-SZYDEŁKO Božena, JAKABOVIČ Lukáš 356

Bezpečnostné aspekty investičného rozvoja územnej samosprávy v systéme originálnych a prenesených kompetencií štátu
ONUŠKOVÁ Andrea 368

Zneužívanie linky Záchrannej zdravotnej služby ako bezpečnostný problém a návrh optimalizácie v podmienkach Slovenskej republiky
PALAIOVÁ Jozefína, HANIŠ Jozef 372

Nepriaznivý demografický vývoj v Slovenskej republike
PAŠKO Ján 380

Ekonomická bezpečnosť Slovenska. Hrozí nám Grécka cesta?
PAŠKO Ján 388

Problematika zabezpečovania verejného poriadku z pohľadu samosprávy
PAVELČÁK Slavomír 395

Boj proti terorizmu – jeho všeobecné a legislatívne aspekty
PEZLAR Ivan 404

Bezpečnosť v zariadeniach sociálnych služieb – hlavné aspekty
PLANČÁROVÁ Dagmar 410

Krízový manažment ako strategický nástroj riadenia rizík, výzvy a perspektívy
POLAČEK Matej 417

Kriminalistická expertiza a závěry znaleckých zkoumání
PORADA Viktor, BRUNA Eduard, STRAUS Jiří 426

Současný stav poznání teorie, metodologie a bezpečnostní terminologie bezpečnostních věd
PORADA Viktor, LOSONCZI Peter 437

Komparatívna analýza triážnych systémov použitých po útokoch na mäkké ciele
PUSTAY Vladimír 449

Politologie pro všechny: svět v pohybu, politika v proměně
ROŽŇÁK Petř 470

Stanovená měřidla jako nástroj bezpečnosti ve zdravotnictví
RYBÁŘ Ján, GERNESCHOVÁ Jana, ONDERČO Peter, SMETÁNKA Andrej, HABARA Andrej 478

Ohrozenia CBRNE mäkkých cieľov školského charakteru
SABOL Jozef, LOŠONCZI Peter 487

Odborná príprava a využitie hasičského dorastu pri zásahoch jednotiek integrovaného záchranného systému pri záchranných a pátracích akciách v zložitom lesnom teréne s prihliadnutím na bezpečnosť a znižovanie rizík
SEMANIČ Miroslav 493

Efektivita zásahu a výber prúdnic v kontexte európskych štandardov požiarnej bezpečnosti
SĽUKA Dušan, MAJLINGOVÁ Andrea 500

Minimalizácia bezpečnostných rizík pri ochrane životov, zdravia a majetku v rámci prevencie a represie v etape prípravy a poriadkovom zabezpečení športových a kultúrnych podujatí
SMOLIGA Jozef 513

Súčasné colné a bezpečnostné inštituciálne výzvy na hranici Slovenskej republiky a Ukrajiny
SOPKOVÁ Patrícia, JAKABOVIČ Štefan. 519

Bezpečnostné dilemy Slovenskej republiky v kontexte Rusko-Ukrajinskej vojny: strategické, diplomatické a spoločenské dimenzie
SOROČINOVÁ Monika Sofiya 528

Využitie umelej inteligencie pri technických zabezpečovacích prostriedkoch
STRELLOVÁ Kristína, ŠČURKA Jaroslav 538

Postavenie a činnosť Európskej služby pre vonkajšiu činnosť a jej vplyv na bezpečnostnú politiku EÚ
SVRČEKOVÁ Zuzana 551

Legislatívne a inštitucionálne nástroje a prostriedky Európskej únie na posilnenie environmentálnej bezpečnosti
SVRČEK Miloš 562

Implementácia environmentálnej zodpovednosti právnymi prostriedkami Európskej únie
SVRČEK Miloš, MOLNÁR Norbert 578

Integrácia krajín západného Balkánu do NATO, jej dôsledky a prínosy v oblasti bezpečnosti v rámci európskeho bezpečnostného prostredia
TÖRÖKOVÁ Natália, KOSÁR Erik……589

Riziká vplyvu vojnových hrozieb na vzdelávací proces v podmienkach vojny na Ukrajine
URIADNIKOVA Inga, ZAPLATYNSKYI Vasyl 597

Umelá inteligencia a bezpečnosť: Keď sa inovácie menia na hrozbu
VAVREK Martin……615

Súčasný stav v ochrane mäkkých cieľov na Slovensku a v Českej republike
VEĽAS Andrej, PUSTAY Vladimír, VYŠNÝ Drahoslav 627

Digitalizácia v modernej vojne
ZAPLATYNSKYI Vasyl, Inga URIADNIKOVA 635

Hrozby a výzvy sociálnych médií a diskusných fór pre seniorov: ochrana súkromia a duševného zdravia v digitálnom prostredí
ZELIZŇAKOVÁ Martina 649

Odborná analýza postupov pri riadení bezpečnosti v rámci zahraničných študentov z konkrétnej destinácie
ZEMKO Pavol 657

Bezpečnostné kroky pri náleze munície – UXO
ZLOCHOVÁ Ingrid.....664

18. ročník medzinárodnej vedeckej konferencie

BEZPEČNÉ SLOVENSKO A EURÓPSKA ÚNIA 2025

Košice, 6. november 2025, ISBN 978-80-8185-084-4

Digitalizácia v modernej vojne

Digitalization in modern warfare

Vasyl ZAPLATYNSKYI[1], Inga URIADNIKOVA[2]

[1]*Borys Grinchenko Kyiv Metropolitan University; Academy of Safety and Bases of Health, Kyiv, Ukraine*

[2]*Kyiv National University of Construction and Architecture; Academy of Safety and Bases of Healt, Kyiv, Ukraine*

Abstract:

The article examines the phenomenon of digitalization in the context of modern wars. The prospects for digital transformation in the military sphere are considered in the context of global technological changes and challenges of modern security. The key development trends are analyzed - the integration of artificial intelligence, the automation of combat systems, the strengthening of cyber defense and the introduction of quantum technologies. The combination of these directions forms a new paradigm of military operations, in which data, algorithms and computing power become the defining resource. The potential risks of digital militarization are identified, including ethical, legal and existential challenges. The possibilities of Ukraine in creating its own Digital Defense Strategy, which should be based on national technological developments, cyber resilience of critical infrastructure, personnel training and international cooperation, are outlined. It is concluded that future hybrid-digitalized wars will increasingly acquire an intellectual-digital character, where the decisive role will be played not by the quantity of weapons, but by the level of technological and cognitive superiority.

Keywords: *digitalization, modern warfare, artificial intelligence, cybersecurity, drones, digital technologies, Russian-Ukrainian war*

[1]***hon. prof., doc. Vasyl ZAPLATYNSKYI, PhD (CSc).*** *- Borys Grinchenko Kyiv Metropolitan University; Academy of Safety and Bases of Health; Str. Milutenko 17/67, Kyiv, 02156, Ukraine. E-mail: vasyl.zaplatynskyi@gmail.com v.zaplatynskyi@kubg.edu.ua. ORCID iD 0000-0003-0119-7135*

[2]***Docent. Ing. Inga URIADNIKOVA CSc. (Ph.D.).*** *- Department of water supply and drainage, Kyiv National University of Construction and Architecture;Academy of Safety and Bases of Healt; st. Milyutenko 17, fl. 67, s. Kyiv, 02156, Ukraine. E-mail: ingavictory@gmail.com ORCID iD – 0000-0002-3750-876X*

Abstrakt:

Článok skúma fenomén digitalizácie v kontexte moderných vojen. Perspektívy digitálnej transformácie vo vojenskej sfére sú posudzované v kontexte globálnych technologických zmien a výziev modernej bezpečnosti. Analyzujú sa kľúčové vývojové trendy - integrácia umelej inteligencie, automatizácia bojových systémov, posilnenie kybernetickej obrany a zavádzanie kvantových technológií. Kombinácia týchto smerov tvorí novú paradigmu vojenských operácií, v ktorých sa určujúcim zdrojom stávajú dáta, algoritmy a výpočtový výkon. Identifikujú sa potenciálne riziká digitálnej militarizácie vrátane etických, právnych a existenčných výziev. Načrtávajú sa možnosti Ukrajiny pri vytváraní vlastnej Stratégie digitálnej obrany, ktorá by mala byť založená na národnom technologickom vývoji, kybernetickej odolnosti kritickej infraštruktúry, výcviku personálu a medzinárodnej spolupráci. Záverom je, že budúce hybridné digitalizované vojny budú čoraz viac nadobudať intelektuálno-digitálny charakter, kde rozhodujúcu úlohu nebude hrať množstvo zbraní, ale úroveň technologickej a kognitívnej prevahy.

Kľúčové slová: *digitalizácia, moderné vojny, umelá inteligencia, kybernetická bezpečnosť, drony, digitálne technológie, rusko-ukrajinská vojna*

1 Introduction

The rapid digital transformation of the defense sector has fundamentally reshaped the nature of modern warfare and national security systems. Artificial intelligence (AI), big data analytics, autonomous systems, and quantum computing have become decisive elements of strategic advantage in contemporary conflicts. Their integration into military infrastructure and operational decision-making processes not only enhances combat capabilities but also generates new ethical, legal, and cybersecurity challenges [1].

In the context of the ongoing war in Ukraine, the role of digital technologies has become particularly evident. They have ensured the resilience of national defense, the continuity of command and control, and the effectiveness of intelligence operations. As Semenenko notes, the Ukrainian defense economy demonstrates increasing reliance on digital platforms and cyber-secure communication systems, which serve as both a shield and a weapon in hybrid warfare [2]. The experience of Ukraine illustrates how the digitalization of warfare affects not only the technical but also the socio-political and moral dimensions of defense.

Globally, defense digitalization reflects a broader trend of technological convergence, where artificial intelligence, robotics, and cyber defense create new synergies. According to Boulianne, Koc-Michalska, and Theocharis, the information space has become a critical arena of confrontation, where misinformation and digital resilience shape both public perception and strategic outcomes [3]. Therefore, the future of warfare will increasingly depend not on the quantity of traditional weapons but on the intellectual and technological capacity of states to protect and advance their interests in a digitalized global environment.

1. Theoretical and Conceptual Foundations of Digitalization in the Military Sphere

The concept of the digitalization of war refers to the systemic integration of digital technologies into all components of military activity — from command and control and intelligence to logistics, armaments, communications, and information influence. This process goes beyond mere technical modernization: it represents a transformation of the

very logic of warfare, where data, algorithms, and artificial intelligence (AI) become decisive factors of operational success.

From a theoretical perspective, the digitalization of war is an evolutionary continuation of the concept of network-centric warfare, developed at the end of the 20th century within research conducted by the U.S. Department of Defense. The classical work of Alberts, Garstka, and Stein [4] formulated the idea that armed forces should be reorganized into networked systems in which information superiority leads to operational superiority. This approach laid the foundation for a new paradigm—digital war—in which not only technical but also social, cognitive, and informational processes are integrated into a unified digital environment.

As William Merrin emphasizes, the digitalization of warfare differs from previous phases in that it creates an information–algorithmic environment where humans, machines, and data interact in real time [5]. While network-centric warfare focused on integrating military units into shared information networks, digital war envisions dynamic command systems in which decisions are made based on data streams processed by artificial intelligence, C4ISR systems (Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance), and big data analytics. This provides information superiority by increasing the speed and precision of algorithmic analysis beyond human capabilities.

The theoretical basis of digital transformation in defense is also closely related to the concept of the Revolution in Military Affairs (RMA), which emphasizes technological innovation in weaponry and command structures. However, while RMA focuses mainly on technical modernization, digitalization encompasses the social, psychological, and informational dimensions of warfare [6]. This indicates that modern conflicts are shifting into cognitive and communicative spaces where the formation of narratives and data management become as crucial as territorial control.

The development of information and communication technologies (ICTs)—including cloud services, satellite communications, 4G/5G mobile networks, geographic information systems, and sensor technologies—has enabled the large-scale deployment of digital command platforms. Examples include integrated situational awareness systems, digital mapping, autonomous reconnaissance systems, and unmanned aerial vehicles. Together, they form an integrated digital battlefield, where humans, machines, and algorithms operate as interconnected agents.

A distinctive feature of modern digital warfare is multi-domain operations—the integration of activities across five domains: land, air, sea, space, and cyberspace. Each domain forms part of a shared information space coordinated through networked command systems. As Echevarria notes, this interconnectivity generates both strategic advantages and vulnerabilities, as digital systems become potential targets for cyberattacks, data manipulation, and psychological operations [7].

Data has become the key resource of digitalized warfare – digital ammunition – whose speed and quality determine success in targeting, intelligence, logistics, and communications [8]. Artificial intelligence and machine learning enable real-time data processing, dramatically accelerating decision-making processes. Yet, as Scharre warns, algorithmic control of warfare raises new ethical and strategic dilemmas, from the autonomy of lethal systems to the erosion of human oversight [9].

Thus, the digitalization of warfare is not merely a technical upgrade of military forces but a profound transformation of conflict itself. The decisive factors now lie in the speed of information exchange, the precision of analytical systems, resilience to cyber threats, and the digital literacy of personnel. Warfare is evolving from being industrial to intellectual, where victory depends not only on force but on the integration of technology, data, and human cognition into a coherent operational system.

2. Key trends in digitalization in modern wars

The digitalization of contemporary armed conflicts manifests across several interconnected domains encompassing both combat and non-combat spheres. These processes share a common objective — to ensure information superiority, operational flexibility, and technological adaptability of military operations.

The key directions of digital transformation in warfare include: cyber operations, which aim to disrupt or defend critical information infrastructures; the application of artificial intelligence and big data analytics for real-time decision-making and predictive modeling; the deployment of unmanned and autonomous systems, which enhance precision and reduce human risk; information and psychological warfare, focused on controlling narratives and influencing public perception; and the development of open-source intelligence (OSINT), which utilizes publicly available digital data for reconnaissance, verification, and strategic assessment.

Together, these directions define the multidimensional architecture of modern "digital war," in which the integration of data, algorithms, and human cognition determines the balance between offense and defense in both the physical and informational domains.

2.1. Cyberspace as a New Theater of WarfarePodnadpis

In the twenty-first century, cyberspace has finally transformed into a fully-fledged domain of warfare—on par with land, sea, air, and outer space. Its specificity lies in the fact that war here is waged not for territory, but for control over information flows, digital infrastructures, and the consciousness of users. As noted by T. Rid, cyberwarfare is not merely a technical phenomenon, but a socio-political process in which the primary weapons are data, algorithms, and access to network resources [10].

Cyber operations are now integrated into all levels of military planning—from strategic to tactical. They include attacks on critical infrastructure, disruption of command and control systems, cyber espionage, manipulation of information flows, and disinformation campaigns. As demonstrated in the research of F. Libicki, cyberspace makes it possible to inflict significant harm on an adversary without physical contact, minimizing one's own losses and avoiding direct escalation [11].

One of the most important characteristics of modern cyber conflicts is their hybridity: cyberattacks are accompanied by information and psychological operations aimed at undermining public trust, spreading panic, or destabilizing political processes [12]. In this context, cyberspace becomes a "soft environment of hard wars," where the boundaries between military and civilian actors virtually disappear.

A striking example was the large-scale wave of cyberattacks against Ukraine that preceded and accompanied the Russian invasion of 2022. Government portals, banks,

media outlets, and energy networks were all targeted. However, this case became not only an example of vulnerability but also a demonstration of cyber resilience. Ukrainian IT specialists, volunteer groups, and international partners (including Google, Microsoft, ESET, and CERT-EU) created a unique model of digital defense that united state institutions and the private sector into a single response system. Ukraine's experience is already being considered by experts as the first precedent of a new-generation cyber-coalition defense.

Moreover, the role of non-state actors – hacktivists, IT volunteers, corporations, and even citizens participating in the so-called total cyber mobilization—is growing. This transforms the classical nature of war, where the state is no longer the sole actor capable of initiating and conducting hostilities. Modern conflicts increasingly unfold in an "invisible dimension," where victory is determined not by firepower but by control over digital systems.

Hence arises the necessity of forming national cyber deterrence—a system of preventive protection that combines political, technological, and educational instruments. For Ukraine, this aspect acquires strategic importance, as digital infrastructure is critical not only for military security but also for the functioning of the state as a whole. One of the key directions of this development is digital sovereignty – the state's ability to independently control its data, information resources, and communication platforms.

Thus, cyberspace emerges as a new front of global competition, where the boundaries between war and peace are blurred, and security is determined not by the power of armaments but by the level of technological integration and the readiness of society to face digital challenges. The Ukrainian experience demonstrates that future wars will be won not by those who possess more weapons, but by those who can adapt faster within the information and networked environment.

2.2. Artificial Intelligence and Big Data in the Military Sphere

Artificial intelligence (AI) has become one of the most powerful factors of the digital revolution in the military domain, transforming the logic of decision-making, command, and combat forecasting. Whereas in the past information superiority was achieved through data collection, today it is determined by the ability to interpret that data faster and more accurately than the adversary. As noted by King, modern military analytics is shifting from the concept of "information superiority" to digital targeting, where systems are capable not only of processing information but also of independently generating optimal decisions [13].

Within the framework of military analytics, the concept of AI-driven warfare is taking shape — a model of warfare in which processes of analysis, planning, and even response are carried out with the help of intelligent algorithms. Machine learning and deep neural networks make it possible to detect patterns in intelligence data, predict enemy movements, identify potential targets from satellite imagery, and control autonomous weapon systems [1]. The advantage of such systems lies in their reaction speed and in their ability to synchronize the actions of a large number of combat units in real time.

At the same time, the use of AI in warfare gives rise to new ethical dilemmas. A question emerges — who bears responsibility for a decision made by an autonomous

system? The problems of algorithmic bias and data poisoning may have fatal consequences in combat conditions. As emphasized by M. Horowitz, uncontrolled automation of decision-making processes can create a "black box" effect, in which even the developers do not understand the logic of AI behavior in a critical situation [1].

The study by Tkachenko and Bielai emphasizes that artificial intelligence is no longer merely a tool for supporting combat decisions but an active agent of informational influence. Intelligent systems analyze vast amounts of open-source data, predict social moods in conflict zones, and are used to manage information operations [14]. Thus, a new level of AI-driven warfare is emerging, in which strategic advantage is determined by the quality of data and the efficiency of algorithms used for its analysis.

In parallel with the development of AI, another component of digital transformation is taking shape — Big Data. Military analytical centers in leading countries are deploying systems for collecting and processing information in real time from millions of sensors, drones, and satellites. This makes it possible to create digital twins of theaters of operations — models that reproduce events in real time and forecast possible scenarios of conflict development.

The integration of AI and Big Data forms a new paradigm of command — data-centric command, in which decisions are based not on the intuition of commanders but on statistical regularities and predictive analytics. This implies not only higher operational accuracy but also a radical transformation of the planning culture: the commander becomes an analyst, and data become the principal strategic resource.

The military experience of Ukraine also demonstrates the importance of such technologies. Target recognition algorithms used in the «Kropyva», «Delta», and drone-support analytical platforms have proven their effectiveness in actual combat, significantly reducing the time between detection and neutralization of the enemy. This confirms the thesis that future warfare will be not only network-centric but also algorithm-driven — AI-powered warfare, where advantage is defined by the quality of data and the speed of its processing.

2.3. Unmanned Systems and Robotic Complexes

One of the most visible and rapidly evolving manifestations of digitalization is the mass deployment of unmanned aerial vehicles (UAVs) and unmanned ground vehicles (UGVs). Modern drones integrate a number of digital components — GPS navigation, satellite communication, sensors, and image processing based on computer vision and artificial intelligence — which makes them versatile platforms for reconnaissance, fire adjustment, combat surveillance, and target engagement.

From the nature of conflicts in the 2010s, we have moved into an era in which small tactical drones (including first-person-view FPV systems and "kamikaze" drones) have demonstrated high operational efficiency at a low cost. As shown in the study by Kunertova, the conflict in Ukraine has brought to the forefront "low-cost drones" as a factor transforming the tactical dynamics on the battlefield: their maneuverability, deployment speed, and large numbers allow for precision strikes on armored vehicles, logistical hubs, and enemy field positions, altering the balance of forces at the local level [15].

In parallel, other researchers highlight the trend of states "emulating non-state actors" that had previously used commercial drones for tactical purposes [16]. The mass use of UAVs in Ukraine — from Turkish Bayraktar TB2 systems to numerous FPV drones and domestic developments (such as the reconnaissance drones «Leleka-100», «Furia», «Valkyria», «Shark», and «Hor», as well as strike UAVs including «Hrim», «Sokil», and «Horlytsia») — has demonstrated that technological accessibility and the rapid adaptation of industry and volunteer networks can provide significant tactical advantages under conditions of asymmetric confrontation.

In addition to aerial platforms, ground robotic complexes are developing: remotely operated cargo and combat UGVs, platforms for demining and evacuation, as well as systems that combine UAVs and UGVs within "drone-switch" and "scout robot + strike drone" schemes. Research by Ukrainian and international authors indicates that UGVs can reduce risks for personnel by performing delivery, demining, and evacuation tasks, although their effectiveness is often limited by power supply, protection from electronic warfare (EW), and mobility in complex terrains [17].

The implementation of unmanned technologies transforms the very logic of warfare — reducing the importance of troop mass and increasing the role of intelligent control systems. This leads to the formation of the concept of a "war of algorithms," in which the decisive factor is not the quantity of weapons but the quality of their digital control.

2.4. Information and Psychological Warfare and Social Networks

The informational dimension of modern conflicts is acquiring equal significance with the kinetic one. War is no longer waged solely for territory — it is waged for the thoughts, moods, and behavior of people. Digitalization has created the conditions for the emergence of new forms of informational and psychological influence, in which social networks, digital media, and sentiment analysis algorithms play a central role [18, 19].

Social platforms — Facebook, Telegram, X (formerly Twitter), TikTok — are used not only as channels of communication but also as tools for the rapid mobilization of public support, coordination of volunteer initiatives, resource collection, and counter-propaganda. At the same time, the adversary actively employs the same channels to disseminate fake narratives, panic-inducing messages, and manipulations targeting broad audiences [20].

As a result, a phenomenon of the "digital front" is formed, where every social media user potentially becomes a participant in the information struggle.

The Ukrainian experience is particularly illustrative. Owing to the high level of digital culture within society and effective governmental communication, the information space has transformed into an integral component of the national defense system. Initiatives such as OSINT communities, fact-checking platforms, online maps (e.g., "DeepStateMap"), and bot services (e.g., "єVOROG") demonstrate the synergy between civil society and digital technologies [19, 20].

Digitalized technologies create a multidimensional architecture of modern warfare, where the boundaries between combat, informational, and technological processes are increasingly blurred. Digitalization becomes not only a tool for enhancing efficiency but

also a key factor in reformatting the very essence of war — from mechanical to network-intellectual [18].

3. Digitalization of the War in Ukraine

The full-scale invasion of Ukraine by Russia has become the first conflict in world history in which digital technologies are applied systematically, on a large scale, and are integrated into all spheres of defense, management, and communication.The Ukrainian experience can be regarded as a model of a "digitalized war," in which innovative IT solutions, flexible management systems, and active participation of civil society are combined [21].

Unlike traditional wars, where the decisive factors were troop numbers and military equipment, in the Ukrainian case the main determinant has become digital superiority — the ability to rapidly collect, process, and disseminate data, ensuring precision, coordination, and mobility of actions [2] The digital transformation of the defense sector began at the moment of the large-scale invasion in 2022: specialized military IT systems, mobile applications, and integrated digital services were created to provide operational control, logistics, and communication between the front-line and administrative levels [21].

The key components of this transformation include:

• The "Delta" system, which integrates data from satellites, drones, and field observations, providing commanders with a real-time digital map of the battlefield and minimizing the time between target detection and neutralization.

• The "Kropyva" system, a mobile application for artillery units that automates fire targeting and reduces the time required to open fire from minutes to seconds.

• The "Army of Drones" program, which ensures mass production, operator training, and integration of unmanned aerial vehicles into a unified digital management ecosystem.

Particular attention should be given to the participation of civil society. Mobile applications such as "eVorog" transform civilians into elements of the intelligence system. OSINT communities (InformNapalm, DeepState, GeoConfirmed) analyze open sources, publishing data on enemy equipment, losses, and combat dynamics. Social networks and digital platforms are used to coordinate volunteer campaigns, raise funds, and provide humanitarian assistance [2].

The internationalization of the digital front has enhanced the effectiveness of defense. Support from global IT companies such as Starlink and Palantir has ensured the resilience of digital infrastructure and real-time analytical support. The Ukrainian IT volunteer movement includes thousands of professionals working on cybersecurity, map creation, databases, and management systems, integrating civilian and military resources into a unified digital front [21].

The Ukrainian case demonstrates that digitalization can become the key to national resilience. Its uniqueness lies in the synergy among the state, the IT business, and civil society, which together have created a flexible, distributed defense system.

Ukraine is capable of developing an effective digital defense strategy that unites the development of domestic IT solutions, state–private sector cooperation, cyber-resilient infrastructure, participation in international alliances, and the training of a new generation of specialists. Projects such as the "Digital Army" initiative are already being implemented to enhance the efficiency of the Armed Forces of Ukraine. Such an approach will constitute a model of successful defense in the digital era [1, 3, 22].

This model has become exemplary for other countries — NATO, the EU, Japan, and Israel — where Ukraine's experience in integrating digital technologies into military practice is already being analyzed. Scholars define this type of war as "hybrid-digitalized," combining classical, informational, and technological dimensions.

Thus, the Ukrainian experience demonstrates that the digitalization of war is not merely a reaction to contemporary threats but a strategic direction for the development of the defense system. It forms a new paradigm of warfare in which technologies, data, and human intelligence merge into a unified defense organism, and the state, IT sector, and civil society function as an integrated protective mechanism.

4. Risks and ethical challenges of war digitalization

The digital transformation of warfare opens up unprecedented technological opportunities, yet simultaneously generates significant risks and ethical challenges. In particular, the growing role of autonomous combat systems capable of making decisions without direct human participation radically changes the principles of conducting conflicts. Drones and robotic platforms equipped with embedded artificial intelligence create the risk of losing human control over lethal decisions, which contradicts the fundamental principles of international humanitarian law [23]. Considering the possibility of algorithmic errors or data manipulation, leading researchers call for the establishment of an international control regime over autonomous weapons [24].

At the same time, the digital battlefield implies total data collection, processing, and analysis — from satellite imagery to information about the movement of civilians. In wartime conditions, the boundaries between the protection of national security and the human right to privacy become blurred. Military analytics systems and mobile applications may violate the principles of data minimization and proportionality enshrined in international legal acts. Meanwhile, digital infrastructure becomes the target of cyberattacks, intensifying the threat of leaks of personal and military data [25].

Digitalization also facilitates large-scale data manipulation — information may be deliberately distorted, falsified, or selectively presented to influence political decisions, public opinion, or international support. The emergence of such destabilization of the cognitive space becomes a new type of informational weapon aimed not at physical, but at psychological destabilization of the adversary.

At the same time, international legal mechanisms lag behind the pace of digital evolution in military systems. International humanitarian law, founded on the Geneva Conventions, did not account for automated decision-making, cyber operations, or algorithmic systems. As a result, a legal vacuum of responsibility arises, when actions in cyberspace or those executed by autonomous systems do not clearly fall under traditional definitions of an "armed attack".

Given this, forming a balanced response to digital risks is possible only under the condition of combining technological efficiency with humanitarian values. It is necessary to develop an ethical and legal framework that ensures mandatory human control over lethal systems, algorithm auditing for transparency and non-discrimination, protection of privacy and humanitarian data in wartime, and the establishment of an international code of conduct in the field of military AI and digital weaponry. This civilizational challenge will determine the future balance between security, ethics, and humanity. Thus, the digital transformation of war is not only a technical but also a civilizational challenge that will shape the future relationship between security, ethics, and humanity.

5. Prospects for the development of digital transformation in the military sphere

The digital transformation in the military sphere is developing rapidly, combining artificial intelligence (AI), automation, cyber defense, and quantum technologies. The integration of AI enables intelligent management of operations, the analysis of large volumes of intelligence data, the prediction of adversary actions, and the optimization of logistics. Autonomous systems and robotic complexes increase accuracy and speed of response, but require strict control and ethical norms. Cyber defense is being strengthened through artificial-immune systems, while quantum technologies are capable of radically changing approaches to security, necessitating the development of quantum-resistant communications. Future wars will acquire features of a “Smart War” — characterized by high dynamism, autonomy, and machine decision-making — which raises the risks of uncontrolled actions and violations of legal norms.

When robotic systems reach the capability to fully replace humans in combat operations, this will cause radical transformations in the conduct of war. First, the cost balance will change: the expense of training and maintaining professional soldiers, as well as the political and social consequences of human casualties, may considerably outweigh capital investments in robotic complexes with comparable combat capabilities, which will incentivize states to invest in automation. Second, the mode of organizing armed service will change — operations that are currently performed physically at the front line will increasingly be transferred to remote control (UAVs, remotely operated artillery and cyber systems), with operators able to act from any point on the planet. This generates increased demand for engineers, programmers, technicians, and logisticians instead of mass combat units and fundamentally alters the vector of personnel training. Third, the “front line” as a clear spatial-territorial boundary loses its traditional features: hostilities acquire a networked, multidimensional character, which complicates identification of parties to the conflict and the application of conventional legal norms. Finally, the reduction of material-technical and human thresholds for the use of force may lower the barriers to the initiation of hostilities and, consequently, increase the likelihood of more frequent local conflicts; this necessitates a revision of doctrines, ethical standards, and international control mechanisms for the proliferation and use of combat robotic systems.

2 Conclusions

Digitalization in modern warfare is not merely a technical enhancement of the armed forces but a profound transformation of the very nature of military conflict. It

changes the strategic, tactical, and cognitive dimensions of war, transforming it from an "industrial" to an "information-algorithmic" one. The key role in this transformation is played by digital data, artificial intelligence, cyber operations, and unmanned systems, which provide operational flexibility, precision, and decision-making speed.

The modern battlefield is turning into an integrated digital environment in which humans, machines, and algorithms interact in real time. Information superiority becomes the primary factor of victory, while digital competence emerges as a new form of military capability. The wars of the 21st century are acquiring a multidomain character, where cyberspace and the information sphere are equivalent to the physical theaters of combat.

The prospects of digitalization in the military sphere encompass the development of intelligent control systems, autonomous platforms, quantum technologies, and deep data analytics, which will give rise to new types of conflicts — "smart" and "algorithmic" wars. However, it is precisely now that the ethical and strategic framework is being formed within which states determine whether digitalization will become a factor of security or a source of global instability.

The Ukrainian experience in countering Russian aggression demonstrates that the integration of digital technologies — from the "Delta" and "Kropyva" systems to joint cyber defense by the state and the private sector — can become a strategic advantage even under conditions of resource asymmetry. At the same time, digitalization generates new challenges: threats of cyberattacks, ethical dilemmas of autonomous weaponry, and risks of losing control over algorithms.

Thus, modern warfare is increasingly becoming a struggle for information, data, and algorithms. Victory belongs not to those who possess more weapons, but to those who can collect, analyze, and apply information faster. Digitalization shapes a new security paradigm in which future victories will be determined not by physical power but by the level of technological integration, cyber resilience, and intellectual superiority.

Reference

[1] HOROWITZ, M. C. (2019). Artificial Intelligence, International Competition, and the Balance of Power. Texas National Security Review, 2(1), 36–57. DOI: 10.26153/tsw/10221 available from: https://2024.sci-hub.se/8348/f77b16f065a75276991abb8a77200bc8/horowitz2020.pdf

[2] CEMEHEHKO, O. (Semenenko, O) (2025). The impact of digital technologies on the defence economy of Ukraine in the context of economic challenges to cybersecurity. *Economic Development, 24*(1), 89-104. available from: https://ecdev.com.ua/en/journals/t-24-1-2025/vpliv-tsifrovikh-tekhnologiy-na-oboronnu-ekonomiku-ukrayini-v-konteksti-ekonomichnikh-viklikiv-kiberbezpetsi

[3] BOULIANNE, S., KOC-MICHALSKA, K., & THEOCHARIS, Y. (2023). Digital media and the war in Ukraine: Mobilization, misinformation, and resilience. International Journal of Communication, 17, 2123–2145. available from: https://cedem.org.ua/wp-content/uploads/2023/08/Social-medias-impact-on-the-Ukrainian-news-and-publishing-space-after-the-full-scale-invasion.pdf

[4] ALBERTS, D. S., GARSTKA, J. J., & STEIN, F. P. (1999). *Network Centric Warfare: Developing and Leveraging Information Superiority*. Washington, DC: CCRP. ISBN 9781893723014. Available from: https://www.dodccrp.org/files/Alberts_NCW.pdf

[5] MERRIN, W. (2018). *Digital War: A Critical Introduction*. Abingdon, Oxon: Routledge. ISBN 9781138899872. https://doi.org/10.4324/9781315707624 Available from https://www.taylorfrancis.com/books/mono/10.4324/9781315707624/digital-war-william-merrin

[6] LONSDALE, D. J. (2004). *The Nature of War in the Information Age: Clausewitzian Future*. Abingdon, Oxon: Routledge. ISBN 9780714684238. Available from https://www.scirp.org/reference/referencespapers/The-Nature-of-War-in-The-Information-Age-38328.pdf

[7] ECHEVARRIA II, A. J. (2016). *Operating in the Gray Zone: An Alternative Paradigm for U.S. Military Strategy*. Carlisle Barracks, PA: U.S. Army War College Press. Available from https://apps.dtic.mil/sti/tr/pdf/AD1013691.pdf

[8] SINGER, P. W., & BROOKING, E. T. (2018). *Like War: The Weaponization of Social Media*. Boston, MA: Houghton Mifflin Harcourt. ISBN 9781328695741. Available from https://www.likewarbook.com

[9] SCHARRE, P. (2018). *Army of None: Autonomous Weapons and the Future of War*. New York, NY: W. W. Norton & Company. ISBN 9780393608984. Available from https://is.muni.cz/el/fss/podzim2020/BSSn4411/um/Army_of_None__Autonomous_Weapons_and_the_Future_of_War_p1-245.pdf

[10] RID, T. (2013). Cyber war will not take place. Oxford University Press. 218 p. ISBN 9780199330638.

[11] LIBICKI, M. C. (2009). Cyberdeterrence and cyberwar. RAND Corporation. ISBN 978-0-8330-4734-2 Available from https://www.rand.org/pubs/monographs/MG877.html

[12] NYE, J. S. (2017). Deterrence and Dissuasion in Cyberspace. International Security, 41(3), 44 1. DOI: 10.1162/ISEC_a_00266 Available from https://direct.mit.edu/isec/article/41/3/44/12147/Deterrence-and-Dissuasion-in-Cyberspace

[13] KING, A. (2024). Digital Targeting: Artificial Intelligence, Data, and Military Intelligence. Journal of Global Security Studies, 9(2), 74–86. DOI: 10.1093/jogss/ogae009

[14] TKACHENKO, K., & BIELAI, S. (2024). The Impact of Artificial Intelligence on the Development of Armed Conflicts. State Security, 2(4). DOI: 10.33405/2786-8613/2024/2/4/323388

[15] KUNERTOVA, D. (2023). Drones have boots: Learning from Russia's war in Ukraine. *Contemporary Security Policy*, *44*(4), 576–591. https://doi.org/10.1080/13523260.2023.2262792

[16] CHÁVEZ, K. (2023). Emulating underdogs: Tactical drones in the Russia–Ukraine war. *Contemporary Security Policy*, *44*(4), 592–605. https://doi.org/10.1080/13523260.2023.2257964

[17] KYRYCHENKO, I. (2022). Research on the future of combat robotics on the example of Ukraine. *Technology Audit and Production Reserves*, *1*(1(63), 6–10. https://doi.org/10.15587/2706-5448.2022.251059

[18] HARHAUN, Y., & TULUPNIKOV, D. (2024). Propaganda and disinformation in the Russian and Ukrainian media: Information technology in conflict. *Acta de Historia & Politica: Saeculum XXI*, *8*, Article 053. https://doi.org/10.26693/ahpsxxi2024.08.053
ISSN: 2306-9813

[19] KRAINIKOVA, T., & PROKOPENKO, S. (2023). Waves of disinformation in the hybrid RussianUkrainian war. Current Issues of Mass Communication, Issue 33, 12–25. https://doi.org/10.17721/CIMC.2023.33.12-25 ISSN 2312-5160 online ISSN 2786-4502 Available from https://research.cbs.dk/files/100303877/krainikova_tetiana_et_al_waves_of_disinformation_in_the_hybrid_russian-ukrainian_war_publishersversion.pdf

[20] ISKOUJINA, Z., GNATCHENKO, Y., & BERNAL, P. (2024). Social media as an information warfare tool in the Russia-Ukraine War. Paper presented at the Centre for Informed Democracy & Social-Cybersecurity (IDeaS) Annual Conference. Available from https://www.cmu.edu/ideas-social-cybersecurity/events/ideas2024_paper_6.pdf

[21] СКЛЯР, І. (SKLIAR. I) (2024). Особливості розвитку цифрового врядування в умовах воєнного стану в Україні. *Аспекти державного управління, (X)*, Article Y. Available from https://aspects.org.ua/index.php/journal/article/view/1093

[22] МАРТИНЕНКО, А., & ЦИРА, О. (2025). Цифрова трансформація органів військового управління України. Науковий вісник ДонНУ, Серія: Політологія та соціологія, (№ 3), 121-135. Available from https://jppasa.donnu.edu.ua/article/view/17164/17059

[23] LEE, J. (2024). *Autonomous Weapons, War Crimes, and Accountability*. The University of North Carolina School of Law. Available from https://journals.law.unc.edu/ncjil/wp-content/uploads/sites/3/2024/05/Autonomous-Weapons-War-Crimes-and-Accountability-by-Jason-Lee-24.pdf

[24] PODAR, H., & COLIJN, A. (2025). Technical risks of (lethal) autonomous weapons systems. *Cornel university arXiv*. https://doi.org/10.48550/arXiv.2502.10174. Available from https://arxiv.org/abs/2502.10174

[25] SVITLYCHNYI, V. A. (2023). Protection of personal data under martial law in Ukraine. Law and Safety, 90(3), 226-236. https://doi.org/10.32631/pb.2023.3.19. Available from https://pb.univd.edu.ua/index.php/PB/article/view/722

Authors:

[1]**hon. prof., doc. Vasyl ZAPLATYNSKYI, PhD (CSc). -** Borys Grinchenko Kyiv Metropolitan University; Academy of Safety and Bases of Health; Str. Milutenko 17/67, Kyiv, 02156, Ukraine. E-mail: vasyl.zaplatynskyi@gmail.com v.zaplatynskyi@kubg.edu.ua. ORCID iD 0000-0003-0119-7135

[2]**Docent. Ing. Inga URIADNIKOVA CSc. (Ph.D.). -** Department of water supply and drainage, Kyiv National University of Construction and Architecture;Academy of Safety and Bases of Healt; st. Milyutenko 17, fl. 67, s. Kyiv, 02156, Ukraine. E-mail: ingavictory@gmail.com ORCID iD – 0000-0002-3750-876X

Zborník vydaný v rámci projektu:
Názov projekt: „Škola digitálnej bezpečnosti“
Názov programu: Plán obnovy a odolnosti SR
kód projektu: 09I05-03-V04-00043

Projekt je spolufinancovaný zo zdrojov EÚ z prostriedkov Plánu obnovy a odolnosti SR

Názov/Title:	**Recenzovaný zborník príspevkov z 18. medzinárodnej vedeckej konferencie *„BEZPEČNÉ SLOVENSKO A EURÓPSKA ÚNIA“*** **Reviewed Conference Proceedings of the 18th International Scientific Conference *„SECURE SLOVAKIA AND EUROPEAN UNION“*** 6. november 2025, KOŠICE, Slovenská republika
Recenzenti/ Reviewers:	Dr.h.c. prof. Ing. Vladimír KLIMO, CSc., DBA doc. PhDr. Kazansky Rastislav PhD., EMBA Dr. h. c. doc. JUDr. Miroslav FELCAN, PhD., LL.M., DSc.,
Vydala/ Published:	Vysoká škola bezpečnostného manažérstva v Košiciach, Košťova 1, Košice,
Rok/ Year:	2025
Editor:	Bc. Katrin Juliána Živčáková
Vydanie/Edition:	prvé
Počet strán/Pages:	673
Náklad/Circulation:	150 ks
ISBN:	978-80-8185-084-4
EAN:	9788081850721