“Contribution of modern industrial revolutions to securing socio-economic systems during the war against Ukraine”

AUTHORS	Leonid Melnyk Laszlo Vasa Oleksandr Kubatko Inna Koblianska Pavlo Hrytsenko

ARTICLE INFO	Leonid Melnyk, Laszlo Vasa, Oleksandr Kubatko, Inna Koblianska and Pavlo Hrytsenko (2025). Contribution of modern industrial revolutions to securing socio-economic systems during the war against Ukraine. *Problems and Perspectives in Management*, *23*(2), 921-937. doi:10.21511/ppm.23(2).2025.67
DOI	http://dx.doi.org/10.21511/ppm.23(2).2025.67
RELEASED ON	Tuesday, 01 July 2025
RECEIVED ON	Friday, 21 February 2025
ACCEPTED ON	Thursday, 05 June 2025

JOURNAL	"Problems and Perspectives in Management"
ISSN PRINT	1727-7051
ISSN ONLINE	1810-5467
PUBLISHER	LLC “Consulting Publishing Company “Business Perspectives”
FOUNDER	LLC “Consulting Publishing Company “Business Perspectives”

NUMBER OF REFERENCES	NUMBER OF FIGURES	NUMBER OF TABLES
42	4	4

BUSINESS PERSPECTIVES

LLC "CPC "Business Perspectives"
Hryhorii Skovoroda lane, 10,
Sumy, 40022, Ukraine

www.businessperspectives.org

Leonid Melnyk (Ukraine), **László Vasa** (Hungary), **Oleksandr Kubatko** (Ukraine), **Inna Koblianska** (Ukraine), **Pavlo Hrytsenko** (Ukraine)

CONTRIBUTION OF MODERN INDUSTRIAL REVOLUTIONS TO SECURING SOCIO-ECONOMIC SYSTEMS DURING THE WAR AGAINST UKRAINE

Abstract

The modern industrial revolutions have significantly influenced social and political landscapes, prompting critical inquiries into the security and integrity of socio-economic systems, particularly in the context of military confrontation. This paper investigates the role of disruptive technologies associated with Industries 3.0, 4.0, and 5.0 in safeguarding socio-economic systems amid the ongoing russian war against Ukraine. The paper highlights how modern technologies have bolstered system resilience and adaptability by examining progress in green energy, transport transition, and the development of digital infrastructure and services before the war. Green energy and transport technologies have been instrumental in decentralization, energy networking, compensating for energy losses, and mitigating disruptions caused by the war. The proliferation of electric vehicles and the expansion of charging infrastructure have significantly reduced the potential impact of aggression, facilitating evacuations and supporting essential services during fuel shortages. Digital technologies have played a crucial role in ensuring continued access to education, employment, and communication, thereby strengthening societal resilience and reinforcing human capital, a key factor in socio-economic system security. This marks a shift from a technocratic to a system-synergistic, human-centered security model, where human capital becomes a core determinant of resilience, and technologies evolve from mere tools into integral elements of a sustainable socio-economic structure. Nevertheless, challenges related to technological dependencies, such as supply chain vulnerabilities and cyber threats, require further investigation in future research.

Keywords Industry 3.0, Industry 4.0, Industry 5.0, disruptive technologies, security, war, digital transformation, sustainability

JEL Classification O14, O33, L52

Received on: 21st of February, 2025
Accepted on: 5th of June, 2025
Published on: 1st of July, 2025

Leonid Melnyk, Doctor of Economics, Professor, Department of Economics, Entrepreneurship and Business Administration, Sumy State University, Ukraine.

László Vasa, Ph.D. in Economics, Professor, Széchenyi István University, Hungary. (Corresponding author)

Oleksandr Kubatko, D.Sc. in Economics, Professor, Department of Economics, Entrepreneurship and Business Administration, Sumy State University, Ukraine.

Inna Koblianska, Ph.D. in Economics, Associate Professor, Department of Economics, Entrepreneurship and Business Administration, Sumy State University, Ukraine.

Pavlo Hrytsenko, Ph.D. in Economics, Senior Lecturer, Department of Economics, Entrepreneurship and Business Administration, Sumy State University, Ukraine.

Conflict of interest statement:
Author(s) reported no conflict of interest

INTRODUCTION

Nowadays, society is undergoing a pivotal phase transition towards a novel socio-economic paradigm, commonly referred to as the digital economy. Industries 3.0, 4.0, and 5.0 constitute the underpinning framework of contemporary reality, delineating the ongoing digital transformation of socio-economic structures and significantly shaping the prevailing political discourse. The Industry 5.0 concept primarily shapes contemporary social and political landscapes. Technologies characteristic of Industry 4.0 and Industry 5.0 are fundamentally changing the dynamics of society. This transformative trajectory raises pertinent inquiries regarding the integrity and security of socio-economic frameworks under these evolving circumstances, including scenarios of military confrontation.

Transformations of national economies brought by digital technologies, which operate on a vast scale, introduce significant uncertainty, constituting the primary source of vulnerability for socio-economic

systems. While these technologies hold the potential to usher in an era of abundance, they also harbor the capacity to disrupt established systems. Researchers are actively investigating the impact of disruptive technologies on states' resilience in the face of global competition, including their implications for military capabilities. However, there remains a notable gap in the literature regarding states' capacity to withstand military confrontation amidst the influence of these technologies. Therefore, there is a pressing need to investigate the security implications for socio-economic systems amidst this transition to the digital economy. Notably, for Ukraine, these security challenges are especially acute due to the russian war against independent Ukraine. Consequently, analyzing the Ukrainian case presents an opportunity to illustrate how disruptive technologies may safeguard societal systems in conditions of military conflict.

The study aims to investigate the role of Industries 3.0, 4.0, and 5.0 in safeguarding socio-economic systems during digital transformation amidst ongoing russian military aggression against Ukraine.

1. THEORETICAL BASIS

There is a notable transformation and reconceptualization of the notion of security. This evolution entails an expanded understanding of security, characterized by several dimensions. Firstly, security extends beyond national boundaries to encompass the security of groups and individuals, thereby broadening its scope downward. Secondly, it expands vertically from national security to include the international or supranational physical environment, thereby transcending the confines of the nation-state to embrace global concerns such as environmental sustainability. Additionally, security broadens horizontally to encompass new forms and spheres of security, ranging from military to political, social, economic, ecological, or human realms.

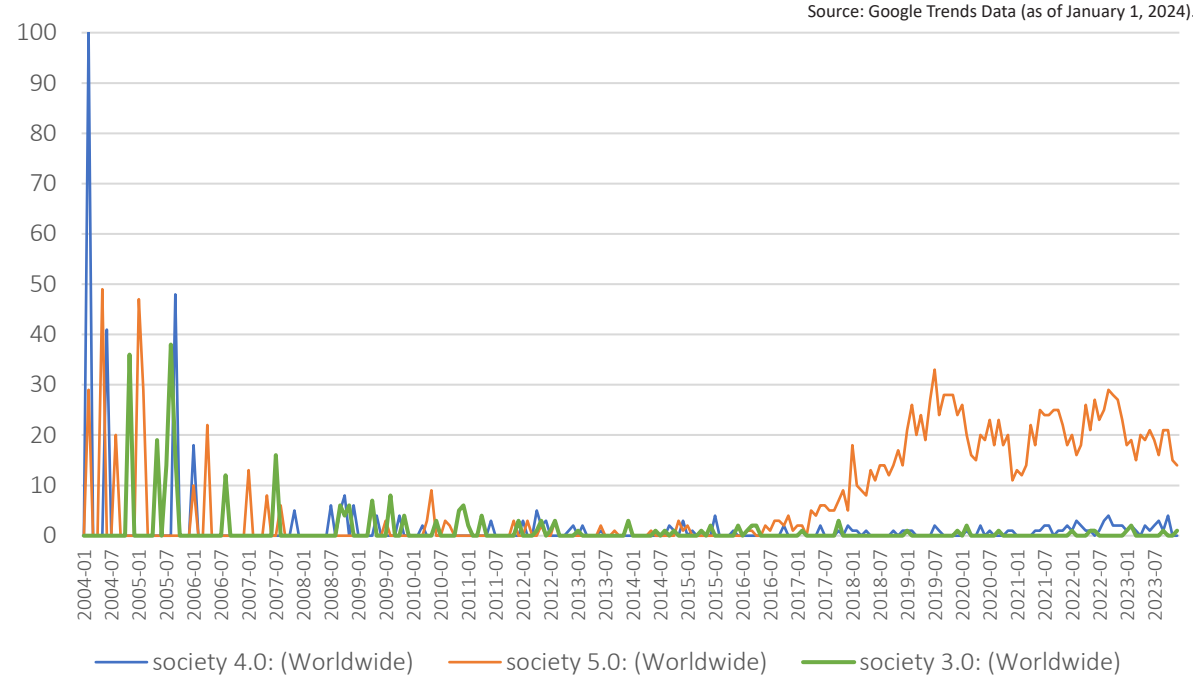
The security of socio-economic systems within the context of digital transformation has increasingly garnered attention from scholars, particularly those focusing on national security and the potential threats digital technologies pose. The specific threats to national security include: escalating societal dependence on digital technologies, the transnational nature of technological advancements, the potential loss of state control over technology proliferation and communication networks, economic and social upheaval, and the resultant challenges posed to security institutions (Wells, 2019). Additionally, concerns encompass techno-nationalism (Manning, 2019), pandemic, cybersecurity, terrorism, counterterrorism measures (Vasilyeva et al., 2021; Kuzior et al., 2022), the rise of techno-authoritarianism, and the fortification of totalitarian regimes (Albert, 2020). A prevalent theme in this discourse is the recognition of digital technologies themselves as sources of conflict, given their transformative impact on the global economic and geopolitical landscape (Jarzębowski et al., 2024). Significant structural changes precipitated by digital technologies promote uncertainties concerning both development trajectories and national security (Zámek & Zakharkina, 2024). Moreover, while digital technologies offer enhanced efficiency in military, economic, and informational operations, these benefits also generate security risks (Zhou, 2024; Ponomarenko et al., 2024).

Digital technologies can propagate democratic values and knowledge, diminish governmental influence on business operations, and advance strategic objectives such as market openness, scientific advancement, and technological innovation (Gompert, 1998).

Industrial revolutions profoundly influence the three core elements of national security – economic, political, and military (Heath, 2020; Priyadarshi et al., 2024). Furthermore, the advent of digital transformation introduces a pivotal information component to this triad, which assumes fundamental significance. Technologies associated with digital transformation not only expand but also redefine the concept of security, particularly by deepening its informational aspects. Consequently, digital technologies' security and vulnerabilities emerge as critical concerns. An exemplary manifestation of digital transition and movement to "society 3.0", "society 4.0," and "society 5.0" is vivid through the

http://dx.doi.org/10.21511/ppm.23(2).2025.67

Source: Google Trends Data (as of January 1, 2024).



Note: * Numbers represent search interest relative to the highest point on the chart for the given region and time. A value of 100 is the peak popularity for the term. A value of 50 means that the term is half as popular. A score of 0 means that there was not enough data for this term.

Figure 1. Interest over time for search queries "society 3.0", "society 4.0", "society 5.0"*, worldwide, Law & Government category

examination of user query data sourced from the Google platform within the domain of Law and Government (Figure 1). The data effectively elucidate the shifting trends in the relative prevalence of pertinent search inquiries spanning a two-decade timeframe on a global scale.

This multifaceted understanding of security reflects a concrete manifestation of the concept of Common Security, which emerged in response to the challenges posed by nuclear weapons (Rothschild, 1995). This paradigm shift entails a transition from a state-centric understanding of security to a human-centric approach, where the core focus lies on ensuring the biological and existential security of individuals, encompassing freedom from fear and want, as well as considerations of rights, dignity, and well-being (Saith, 2008; Dobrovolska et al., 2024; Springs, 2024).

During the initial months of the war, Ukraine's economy endured substantial losses, accompanied by significant casualties among the country's populace. Widespread violence has engulfed 10 regions of Ukraine. Over 8 million people were compelled to relocate within the country, while another 6 million fled Ukraine altogether. Just over 4.3 million non-EU citizens, who fled Ukraine as a result of russia's war of aggression against Ukraine, were under temporary protection in the EU (Eurostat, 2025). The disruption caused by the conflict led to estimates suggesting that 40-50% of Ukraine's economic potential was either destroyed or severely hampered within the first two months of the war (Samaeva, 2022). Half of the country's enterprises shuttered completely, while those still operational faced significant challenges. Further details on the socio-economic ramifications of russian aggression are outlined in Table 1.

Moreover, the transformation in the conceptualization of security leads to a diversified perspective on the role of modern technologies in safeguarding various aspects of socio-economic systems. It is observed that Fourth Industrial Revolution technologies play a pivotal role in facilitating cleaner production and enhancing food, energy, and environmental security (David et al., 2022; Odhiambo, 2019). These technologies are also implicated in the onset of the affluence era, exerting profound effects on the economic sphere of social life (Burton & Moore, 2024; Maatallah,

Table 1. Indicators of Ukraine's losses because of russian aggression for the period from February 24, 2022, to May 12, 2022

Type of losses	Indicator
Power system losses	
Number of de-energized settlements, units	868
Number of consumers who lost electricity, persons	700 thousand
Share of lost capacity of power systems, %	30-40%
Loss of alternative energy capacity	
SES (industrial), %	30-40
SES (industrial), MW	1,120-1,500
SES (private), %	20-24
WEIGHT, %	67
WPP, MW	1,120
Bioenergy, %	10-15
Power grids:	
high-voltage (110-150 kV), km	100
regional (35 kV), km	600
local (<35 kV), km	1,000
Number of destroyed oil depots, units	27
Loss of transport infrastructure	
Damaged roads, km	30 thousand
The lost railway network, km	6,000 (23%)
Damaged bridges	
railway, units	40
automobile, units	300
Destroyed or damaged civilian airports, units	12
Sea and air transport blocked, %	100
Killed or injured in the performance of duties of transport workers, persons	over 500
Losses to transport infrastructure, USD billion	over 90
Loss of social infrastructure	
Destroyed or damaged:	
housing stock, million sq.m.	35
educational institutions, units	1,000
medical institutions, units	over 620
kindergartens, units	about 600
administrative buildings, units	85
religious institutions	102
Consequences for the population	
Died, persons	3,580
Injured people	3,820
Dead children and people	227
Injured children and people	420
Internally displaced people, millions of people	8
The number of people who left the country, million people	6
The proportion of people who lost or suspended work,%	30-50%
Economic losses	
Destroyed or lost due to occupation:	
enterprises, units	210
warehouses, units	160
sown agricultural areas, %	10
loss or suspension of economic potential, %	30-40
loss or suspension of work, %	30-50

Note: Compiled based on Holovne in UA (2022), Interfax-Ukraine (2022), Pryschepa (2022), Sheremet (2022).

http://dx.doi.org/10.21511/ppm.23(2).2025.67

2024; Dobrovolska & Kolomiiets, 2024). For instance, 4IR technologies contribute to waste reduction, increased productivity, and informed nutrition decisions, thereby advancing food security objectives (De Amorim et al., 2019). Additionally, renewable energy technologies mitigate technical inefficiencies and energy supply risks, reducing import dependence and energy instability caused by price fluctuations and imports (Bigerna et al., 2021). While 4IR technologies can potentially alleviate poverty, unemployment, and inequality, they also pose inherent risks. These technologies are reshaping the global economy, with implications that extend to both positive and negative consequences for economic security (Asghar et al., 2020; Heath, 2020). Rymarczyk (2020) offers a comprehensive summary and systematization of digital technologies' potential benefits and risks. Notably, for developing countries, 4IR challenges are intertwined with issues such as policy implementation, corruption, low policy effectiveness, and mistrust (Asghar et al., 2020).

To sum up the theoretical basis section, it is necessary to state that there is a vivid potential of digital technologies to bolster national security through enhanced communication capabilities, data processing efficiencies, and the increased openness facilitated by these technologies.

2. RESULTS

System security is conventionally associated with the absence of hazards, its protection from a range of threats, and the system's capacity to maintain operational functionality despite adverse conditions. Two key properties are fundamental to ensuring system safety: resilience, denoting the system's ability to withstand negative influences, and restoration, signifying its capacity to return to optimal operational parameters (homeostasis) following exposure to adverse factors. Socio-economic system (SES) security denotes its capacity to sustain operational functionality in the face of adverse internal and external influences, facilitated by protective measures applied to its components and its ability to counteract such influences. Figure 2 illustrates critical parameters upon which the security of socio-economic systems depends. Every socio-economic system constitutes a multifunctional structure encompassing numerous subsystems and their respective security components. A triadic perspective of socio-economic systems security arises from the interplay of three determinants: material (encompassing technical resources, energy provision, financial reserves, etc.); informational (encompassing the level of technological innovation, the pace of economic processes, the intellectual capital of human resources, etc.); and synergetic (about communication efficiency, transactional velocity, and the integration of production and consumption networks). Material factors primarily facilitate the system's capacity for energy accumulation and transformation during operational activities. Informational factors play a pivotal role in the perception and processing of information, directing energy potentials and facilitating the system's self-organization across spatial and temporal dimensions. Synergetic factors are instrumental in coordinating the actions of subsystems and ensuring effective communication at the supersystem level. The advent of successive industrial revolutions (Industries 3.0, 4.0, and 5.0) and their associated innovative advancements significantly influence the mechanisms and tools employed to safeguard socio-economic systems' (SES) security.

The ongoing transition towards a digital paradigm unfolds across three distinct phases: Industries 3.0, 4.0, and 5.0. These epochs are intertwined, exerting mutual influence and collectively shaping the trajectory of societal evolution.

The third industrial revolution (Industry 3.0) denotes a significantly diminishing the adverse impact on the Earth's ecosystems, based on transition towards renewable energy sources and materials, widespread adoption of additive manufacturing technologies, the interconnectivity of production systems, digitalization of data, the establishment of horizontally structured production and consumption frameworks, and the emergence of solidarity-based and additive economic relations. The positive sides of the additive economy are related to the reduction in energy/resource intensity, dematerialization of production, sustainability of production and consumption, and implementation of the Internet of Things. The negative sides of the additive economy are related to higher risks of information

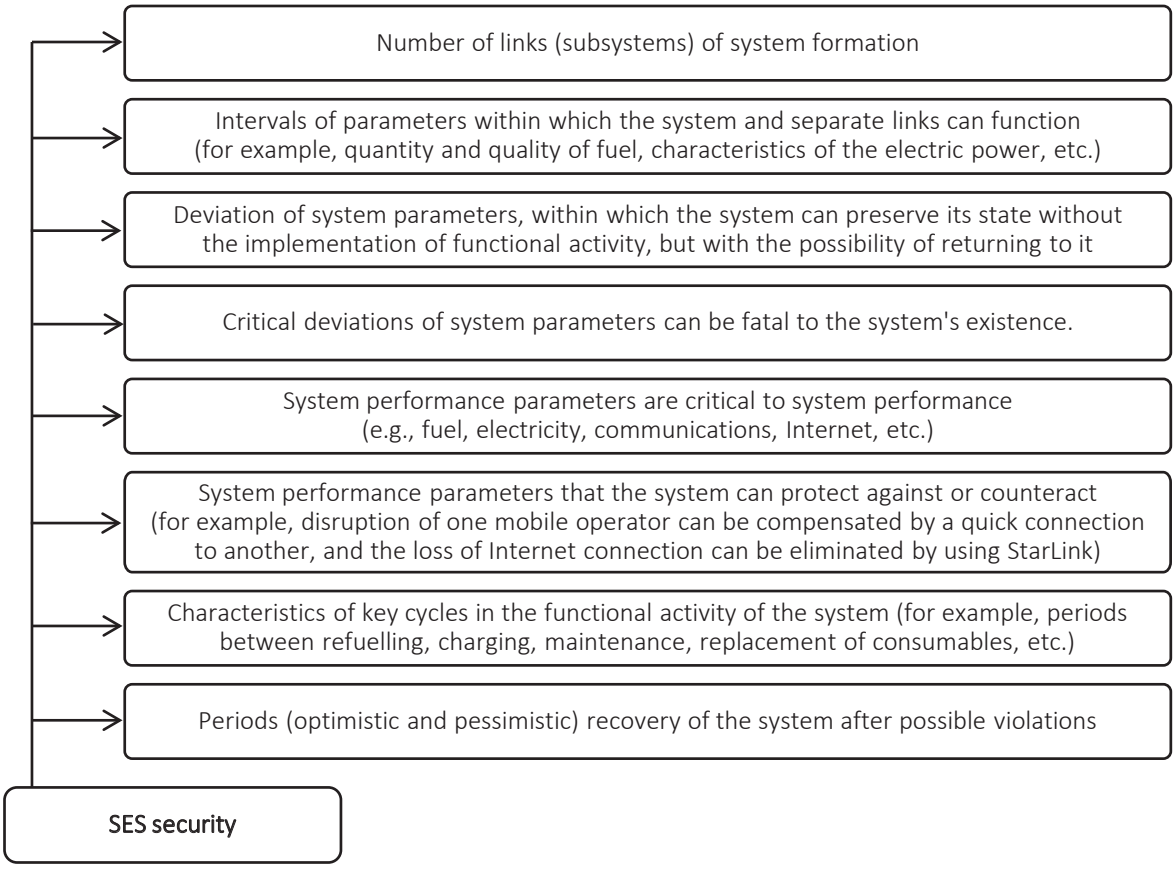


Figure 2. Key parameters affecting the security of socio-economic systems

vulnerability and the risk of losing control over cyber-physical systems. While acknowledging the seriousness of risks such as manipulation, cyberattacks, and system failures, scholars contend that these risks are manageable.

The fourth industrial revolution marks the ascendancy of cyber-physical systems in sustaining human livelihoods and preserving ecological equilibrium on a planetary scale. Central to Industry 4.0 are innovations such as the Internet of Things (IoT), the implementation of "smart" management systems across enterprises, settlements, and administrative entities, and the evolution of the "cloud" as a ubiquitous repository and control hub for socio-economic processes.

A defining component of Industry 4.0 and communication platforms is responsible entrepreneurship, which means operating in a social, environmental, and ethical manner rather than focusing solely on financial performance. This approach prioritizes the responsibility of enterprises to society and the environment. Businesses must consider their activities' impact on consumers, employees, the community, the environment, and other stakeholders. Responsible entrepreneurship includes the following aspects:

- social responsibility: enterprises must adhere to ethical standards, consider the needs of other stakeholders, contribute to the development of local communities and society in general;
- environmental responsibility: enterprises should engage in environmental sustainability, minimize the negative impact on the environment, use energy-efficient technologies, preserve natural resources, and reduce greenhouse gas emissions;
- economic responsibility: businesses must operate efficiently, ensure stability and profitability, but at the same time take into account long-term sustainability and social responsibility.

http://dx.doi.org/10.21511/ppm.23(2).2025.67

Responsible entrepreneurship within Industry 4.0 is designed to change how businesses operate, ensuring a balance between profitability, social values, and environmental sustainability. This contributes to the creation of a fairer and more sustainable economic system that promotes the well-being of society and the environment.

The more people contribute to the collective intelligence system, the higher the load on the information system. Analyzing large volumes of data is a complex task requiring complex tools for information selection and analysis. This increases the risk of overloading the system and, as a result, errors and inaccuracies.

Quality control. A democratic system of admitting different levels of performers (including low-skilled ones) to participate in the project can increase the risk of obtaining low-quality results and reduce the reliability of collective work.

Herd mentality problems. The very style of collective activity creates an atmosphere of conformism, which can manifest signs of a herd mentality. This prevents the manifestation of a diversity of viewpoints. There is a security of the general following of a certain opinion. The generation of innovations is inhibited, and it can even lead to false results (if the common trend of thought turns out to be wrong).

Cognitive subjectivity. Despite all the wishes, it is difficult for many people to remain objective when evaluating certain events and facts. Because of this, they may show bias, in particular, conservativeness when considering current events or a tendency to conform to certain traditions inherent in local communities.

Coordination problems. The more complex the problem, the more difficult it is to coordinate the activities of individual performers. Poor coordination can lead to duplication of efforts or, conversely, to the appearance of "white spots" (that is, areas of work not occupied by anyone). Consequences may also be inconsistency in co-contractors' work, delay in decision-making, and an increase in the cost of work.

Ethical problems. The focus on openness may conflict with the desire to preserve copyright. Moreover, the attempt to observe equality in participation can create ethical problems from the point of view of ensuring the principles of justice with different contributions of performers to the final result.

Technological barriers. Although modern technologies generally strengthen the implementation of collective intelligence, they can also cause certain problems: due to the difference in access to technologies, the level of digital literacy of co-performers, and the inability to master the high complexity of the tools.

Redistribution of power. Due to an incorrect understanding of wikitechnological principles, there may be a temptation to take over the authority to influence other actors.

Cultural barriers. Cultural background and language differences can create misunderstandings between participants and hinder effective communication and cooperation.

Managing complexity. When solving complex problems, the wiki community may not have enough resources and knowledge to implement adequate solutions.

Although Industry 4.0 technologies have significant potential benefits, their implementation is also associated with the emergence of complex problems. Understanding the nature of these problems and the cause-and-effect relationships of their occurrence contributes to the development and application of tools of adequate collective intelligence systems in terms of content and form.

Taking into account the active development of information and communication technologies and the availability of new opportunities for communication and cooperation, the main prospects for the development of wiki communities were formulated. They open new directions of research.

Expanding opportunities for communication and cooperation. It should be expected that more and more users will unite around common interests, industries, goals, and projects. Facilitating a greater diversity of participants by profession, age group, and other criteria will create more opportunities for sharing knowledge, experiences, and ideas.

Expansion of international communication. Communication platforms of Industry 4.0 make it easier for people from different countries and cultures to communicate and collaborate. Open access to knowledge and information opens up new opportunities for international exchange of experience, knowledge, and culture. Being open to different languages can help attract more participants.

Improving the quality of information. Implementing effective fact-checking mechanisms can help improve the quality and credibility of information shared by participants. The creation of specialized wiki communities for different fields and interests will allow attracting experts from specific areas and developing deeper knowledge in these areas.

Promotion of innovation. Communication platforms of Industry 4.0 can facilitate the exchange of new ideas and knowledge, which stimulates innovation. New technologies, methods, and solutions can emerge thanks to the interaction of wiki communities, which can create prerequisites for the development of technology and society.

Expansion of business cooperation. Communication platforms can become a platform for developing business cooperation, exchange of experiences, and partnerships. Companies and startups can find new opportunities to collaborate and create innovative products and services.

Industry 5.0 heralds the phenomenon of human sociologization within a cybernetic milieu. This epoch prioritizes the development of the individual's social dimensions, the ascendancy of information production and digital domains within public spheres, the proliferation of creative economy domains, and the synergetic integration of human cognitive faculties with artificial intelligence.

The pivotal contributions of contemporary industrial revolutions towards enhancing the security of socio-economic systems encompass several facets: streamlining system components, dematerialization of primary elements (production means, labor objects, communication and storage facilities, consumable goods), the substitution of hazardous critical parameters, networking and decentralization of economic system components, cyberization of security monitoring mechanisms, reduction of energy and material consumption within economic systems, augmentation of individual unit autonomy and self-organization, and enhancement of workforce capabilities.

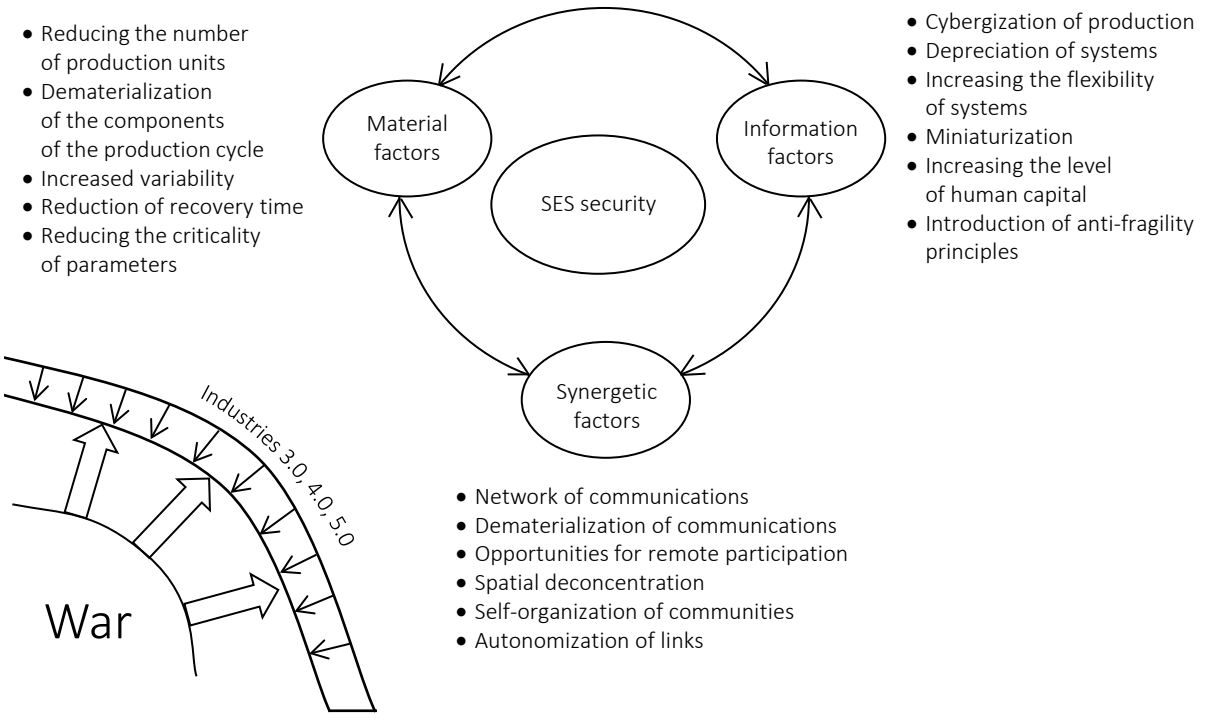


Figure 3. Contribution of Industries 3.0, 4.0, and 5.0 to improving the SES security in wartime

http://dx.doi.org/10.21511/ppm.23(2).2025.67

Table 2. Impact of Industries 3.0, 4.0, and 5.0 on the components of sectoral types of SES security in hostilities

Definition of the sectoral type of security	Types of major threats	Contribution of Industries 3.0, 4.0, and 5.0 to improving security
1	2	3
	Energy security	
Energy security ensures uninterrupted access to energy resources in the required quantity at an affordable price.	• Destruction (loss) of material means of energy production • Destruction (loss) of material means of production, processing, transportation, and storage of fuel • Destruction of electricity transport and storage networks • Increasing the price of components of production and consumption of energy • Violation of the balance of production - electricity consumption • Loss of performers capable of servicing energy facilities • Political circumstances a negative impact on the energy sector	• Development of alternative energy sources and reduction of the number of production units • Elimination of dangerous processes of production, processing, transportation, and storage of fuel • Networking of production processes – consumption of the electric power with deconcentration and an increase in the level of autonomy, production units • Improving the efficiency of energy storage systems with an increased battery life of the systems • Improving the level of security monitoring of power systems • Improving the efficiency of balancing systems of energy production • Reducing the energy intensity of economic systems by reducing the need for additional energy production • Increasing the financial stability of the sector
	Transport security	
Transport safety is the state of transport infrastructure, vehicles, and security components (energy, people, financial system) necessary to implement the functional activity of transport systems.	• Infrastructure violations • Vehicle violations • Problems with the power supply • Violation of the information algorithm (logistics, traffic) • Problems of staffing • Problems of financial security • Threat to objects of transportation (passengers, cargoes)	• Electrification of transport and elimination of dependence on fuel • Dematerialization of transport operations based on the digitization of transportation objects and 3D-printing • Logistics optimization (e.g., GPS-based) • Traffic optimization • Digitization of financial transactions • Introduction of unmanned vehicles (in particular, drones) • Remote training
	Information security	
Informational security – the state of protection of the socio-economic system (SES) from the violation of the information system that ensures the functioning and development of the SES, including through the prevention of unauthorized data handling	• Types of unauthorized data handling: • data access; • use; • disclosure; • curvature; • change; • study; • record; • destruction of information(data)	• Transparency of information about events (including in real-time) • Horizontal data exchange networks with the elimination of intermediate links • Timely prevention of threats and risks • Code protection of information. • Anti-hacking • Advanced information about provocations and threats
	Social security	
Social security is protecting the interests of the SES (country, community, enterprise) and individuals who belong to it.	• Threats that arise: • preservation and development of social structure and relations; • ensuring economic well-being; • preservation of the life support system; • supported a socially full-fledged way of life; • freedom of self-development; • meeting the needs of present and future generations; • healthy and informative environment.	• Preservation of national information unity • Maximal non-cash livelihood (salary, pensions, scholarships) and payments for goods and services • Free and prompt evacuation to safe regions (if necessary) • Maximum organization of remote work • Distance learning and provision of necessary medical services • Maximum self-organization of citizens, volunteers, production teams, and military units • Introduction of unconditional fundamental income bases (e.g., UAH 6,500 support) • Development of information production and freelance • Introduction to the basics of solidarity economy

These components, notably significant during periods of conflict, are depicted in Figure 2, illustrating the interplay of modern industrial revolutions in shaping the contours of SES security within the triadic framework during wartime scenarios.

This framework elucidates the intricate dynamics through which contemporary industrial revolutions interact with socio-economic systems, underscoring their profound implications for security paradigms amidst evolving global contexts.

The security of the socio-economic system depends on the effective and uninterrupted operation of various sectors within the national economy. Consequently, the construct of SES security is underpinned by distinct sectoral categories of security, encompassing domains such as energy, transportation, and information. The precise formalization and quantitative assessment of the impact of industrial revolutions on the actual state of SES security amid the state experienced by Ukraine due to russian aggression pose considerable challenges. Nevertheless, these industrial revolutions make a substantial contribution to bolstering SES security, albeit difficult to quantify with precision. Table 2 provides definitions of sectoral security types within SES, elucidating their primary threats and the prospective influence of industrial revolutions on enhancing these security domains.

The initial months of conflict resulting from russia's aggression against Ukraine have revealed that the strategic adoption of digital transition measures within the country's economy, as influenced by industrial revolutions, has served to alleviate adverse impacts on socio-economic systems and, in certain instances, averted the destruction of pivotal components thereof.

The magnitude of the socio-economic consequences inflicted upon Ukraine by the war is undeniably staggering. However, these repercussions could have been even more profound had the country not undertaken decisive measures in recent years to modernize its socio-economic systems and lay the groundwork for a digital economy.

To align domestic energy infrastructure with EU standards, Ukraine embarked on a trajectory to enhance its renewable energy capacity. Subsequently, the Energy Strategy of Ukraine until 2035 was formulated to achieve a renewable energy share of 11% in the country's energy balance by 2020 and a target of 25% by 2035.

The proliferation of private SEs in households across Ukraine has been dispersed geographically, as illustrated in Table 3. This decentralized distribution played a significant and positive role in supplying households with electricity during the war, particularly when access to energy from centralized networks was disrupted. Beginning in early October 2022 and persisting throughout the autumn and winter of 2022/2023, Ukrainian critical infrastructure, including energy infrastructure and residential areas, came under missile and drone attacks. These attacks resulted in widespread power outages nationwide, exacerbating shortages of essential provisions such as food, heating, and water (World Bank Group, 2023).

The russian aggression significantly damaged Ukraine's "green" energy sector, particularly in regions where fighting occurred, approximately 60% of wind farms and industrial solar energy installations are concentrated. Private SEs play a crucial and positive role during the war. Firstly, due to

Table 3. Number of private solar energy stations (SEs) and electric cars (ECs) by regions of Ukraine *

Region	Number		Region	Number	
	SEs	EC		SEs	EC
Kyiv	227	7338	Ternopil	3447	535
Odesa	1323	4840	Mykolaiv	853	489
Kyiv	2468	3833	Ivano-Frankivsk	2275	489
Kharkiv	679	3247	Donetsk	730	481
Dnipropetrovsk	6466	2746	Cherkasy	269	442
Lviv	1276	2239	Volyn	787	430
Vinnytsia	1173	977	Zakarpattia	2313	430
Zaporizhzhia	3744	880	Kherson	1752	256
Zhytomyr	789	804	Sumy	670	227
Poltava	646	674	Kirovohrad	1678	226
Rivne	562	662	Chernihiv	269	153
Khmelnytskyi	1641	533	Luhansk	92	50
Chernivtsi	1377	539			

Note: * Built using Beloshytska (2022), Ukrainian Energetics (2022).

http://dx.doi.org/10.21511/ppm.23(2).2025.67

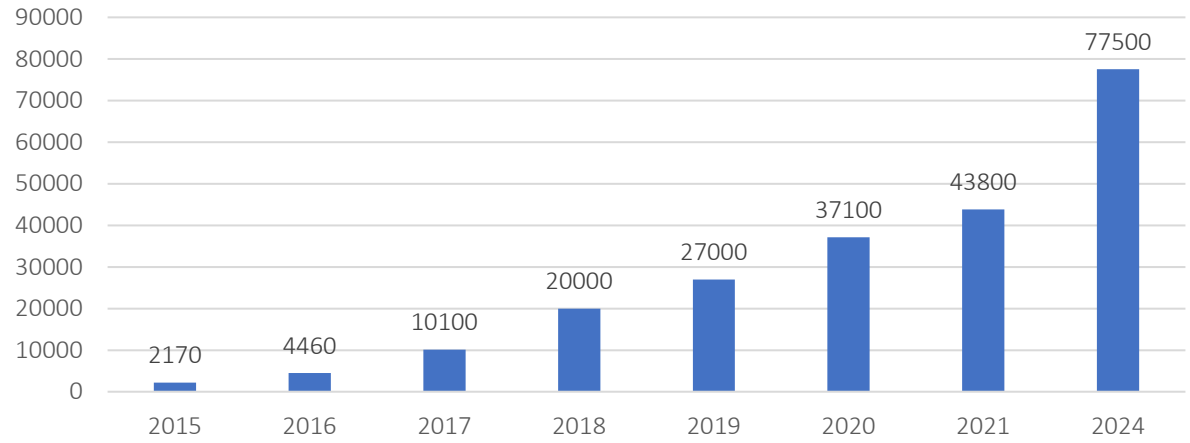


Figure 4. Yearly data on the number of electric cars in Ukraine

their dispersion across the country, their damage rate was lower (approximately 24%) than industrial solar power plants. Secondly, unlike industrial installations that solely supply centralized power grids, private installations serve other vital functions in wartime conditions. Paradoxically, destroying a substantial portion of Ukraine's "green" energy infrastructure had minimal impact on the country's overall electricity supply. This is attributed to the simultaneous destruction of the country's industrial complex, including energy-intensive industries, resulting in an excess of energy production that cannot be immediately absorbed.

Despite electric cars constituting less than 2-3% of Ukraine's total road transport fleet, there is a notable trend towards increasing public awareness and adoption of this form of transportation. Over the past seven years, the number of electric cars in the country has surged nearly tenfold, as illustrated in Figure 4.

Ukraine's electric vehicle infrastructure has developed rapidly with the growing number of electric cars. In just one year, from 2020 to early 2022, the number of charging stations surged by 3.6 times, from 900 to 3,244, with the total number of charging terminals reaching almost 8,000. Remarkably, Ukraine ranks among the leaders in Europe concerning the number of electric cars per charging terminal, rivalling the Netherlands and surpassing Poland in this regard. Notably, approximately one-third of the charging stations in Ukraine offer high-speed charging capabilities (Autogeek, 2021). At least 100,000 refugees were estimated to be evacuated to secure areas, potentially saving thousands of lives. Moreover, electric cars were crucial in sustaining urban and rural livelihoods during the crisis. Despite fuel shortages, electric vehicles were utilized intensively to transport critical cargo and passengers, ensuring the operation of public utilities, hospitals, shops, and pharmacies.

Ukraine's relatively advanced state of information development has provided substantial support to the security of SES. Information systems within society have facilitated uninterrupted communication between individuals and preserved cohesive social communities. Thus, the significance of Ukraine's transition to a digital society before the onset of Russian aggression cannot be overstated. Table 4 illustrates key indicators demonstrating the level of informatization within Ukrainian society.

The impact of Ukraine's information development became evident in the initial months of the russian aggression. Several noteworthy outcomes can be delineated:

- Despite spatial separation, citizens maintained stable communications via information systems such as the Internet and mobile phones, preserving social cohesion and fostering a sense of involvement in their state;
- Information dissemination facilitated collective action and a unified atmosphere of cooperation, reproducing solidarity and synergistic collaboration;

Table 4. Indicators of informatization of Ukrainian society*

Indicator	Value
Share of households with Internet connection, %	80
incl.	
in urban settlements, %	86
in rural areas, %	66
comprising young families, %	99
Share of smartphone users, % (7 times higher than in 2013 – 9%)	66
During the war, StarLink began to operate (from 27.02.2022), and thousands of users connected daily	150
Mobile telephone users, millions of persons	39 (93% of population)
TV users, millions of persons	40 (95% of population)
Schools and hospitals have Internet access, thousands	10
Number of villagers having access to high-speed Internet, million persons	3,5
Number of main mobile operators, units (if necessary, mutual replacement is possible)	3 (97% connection)
Social network users among Ukrainians, %:	
18-29 aged	93
30-49 aged	85
50-59 aged	74
above 60 years	37

Note: * Compiled based on Focus (2021), Horbik (2022).

- Existing information channels enabled the dissemination of crucial information, aiding in threat awareness and risk mitigation;
- Information networks were utilized to combat false narratives and propaganda disseminated by adversaries;
- Despite initial shock following the aggressor's attack, most educational institutions' remote classes resumed within a month, accommodating students across different territories and countries;
- Information technology facilitated financial transactions in areas or times where cash settlements were not feasible;
- Information systems were crucial in coordinating logistics, dispatching work, and facilitating communication among various sectors;
- Digital infrastructure enabled the continued functioning of the IT sector, freelancers, and service industries during the war;
- Information networks supported the provision of essential medical consultations and services;
- Information systems provided ongoing connectivity despite the challenges posed by the war, facilitating communication on national and global events for individual citizens.

In contemporary contexts, critical attributes such as individuals' and teams' capacity for self-organization, adeptness in working with information, proficiency in operational situation analysis, and swift decision-making skills hold paramount importance. Human beings play a central role in ensuring the security of socio-economic systems, with the level of security contingent upon the knowledge, skills, competence, and executive capacity of the human capital comprising these systems. An essential metric reflecting society's capacity for self-organization is the level of freelance activity.

3. DISCUSSION

The security of socio-economic systems (SES) constitutes a complex, multifaceted phenomenon, contingent upon several key properties, including protecting its components from adverse factors, resilience against destruction processes, and the capacity to renovate activities post-violations. SES security is shaped by three primary factors: material, information, and synergetic influences. Modern industrial revolutions, encompassing Industries 3.0, 4.0, and 5.0, significantly impact the material, information, and synergetic process-

http://dx.doi.org/10.21511/ppm.23(2).2025.67

es underpinning SES security. Noteworthy contributions to improving SES security include the reduction of system components, dematerialization of main elements, replacement of critical parameters, networking and deconcentration within economic systems, cyberization of security monitoring, energy and material consumption reduction, enhanced autonomy and self-organization, and improved skill sets, particularly relevant during wartime. It has to be emphasized that, according to Melnyk et al. (2019), the human labor entity has not changed up to Industry 4.0, which tries to replace human jobs and opens up AI and robotics technologies.

Modern technologies are suggested to have significant positive effects on SES security in view of their material, informational, and synergetic bases. Their contribution in transforming the material factors of modern society and the functioning of the economy is most evident in the spheres of energy provision and ensuring proper mobility. Industry 3.0-5.0 technologies applied in the energy and transport sectors make the SES less energy intensive, less dependent on centralized facilities and fossil energy supply, and more flexible in terms of balancing energy supply and consumption. The research findings align with prior studies (Bigerna et al., 2021; David et al., 2022; Manning, 2019; Rymarczyk, 2020), highlighting the role of disruptive technologies in securing energy systems and ensuring stable functioning against power disruptions. The Ukrainian case provides empirical evidence on the role of green energy and transport technologies in resource savings, decentralization, and networking, compensating for energy supply losses at local levels and mitigating temporary disruptions.

Digital infrastructure and institutional efficiency support both digital transition and security, which was previously mentioned by Asghar et al. (2020), exemplified by Ukraine's resilient information infrastructure during russian aggression. Industry 3.0, 4.0, and 5.0 technologies' contribution to the transformation of the informational basis of system performance ensures SES's resilience due to access to real-time data, horizontal communications, and transparent data exchange. Moreover, the implementation of modern technologies also affects social constructs, representing the synergetic pillar of a system. Technologies safeguard social relations and unity, the continuous provision of necessary financial flows, and essential public services. The role of digital technologies in providing access to education, work, and communication amidst the physical insecurity of these operations is crucial. This aligns with the notion of the advantages of "openness" inherent in modern technologies (Gompert, 1998), albeit extending beyond it. Such accessibility shields society from failure and enhances human capital, crucial for safeguarding SES (Melnyk et al., 2021). The efficacy of this accessibility relies on expertise, adaptability, and decision-making abilities. Ukraine's embrace of freelance activity also exemplifies its self-organization and creative engagement capacity, further boosting the green and digital transition.

Ukraine stands out as a global leader in the number of freelancers per capita, consistently ranking among the top five countries in recent years. The country's rapid growth rate of freelancers is noteworthy, as the annual increase is more than 30% (Freelancehunt, 2022). Another manifestation of self-organization is evidenced by the approximately 30% of workers who transitioned to remote work arrangements amidst a full-scale invasion (Samaeva, 2022). It is important to emphasize a crucial detail: freelancers are not merely individuals who self-organize their work. In most cases, freelancers engage in creative work, necessitating continuous self-improvement, self-learning, and self-development. This fundamental principle aligns with the societal objectives of sustainable development, as articulated by the Fifth Industrial Revolution, spearheaded by the EU. Citizens of Ukraine actively participate in the "green" transition, investing in the development of renewable energy and acquiring electric vehicles, thereby fostering an enabling environment for such changes.

An important aspect of the "green" transformation of the Ukrainian economy is the adoption of additive technologies. Ukrainian companies ("Infomir 3D Printing", "TitanEra", "Flight Control", and others) not only actively utilize ready-made 3D devices but also develop their own. There is an active "green" transformation in the agricultural sector by implementing vertical farms and organic farming, with Ukraine ranking second in organic produce exports to the EU (Loshakova, 2021).

A key achievement of Industry 4.0, the Internet of Things (IoT), is also gaining prominence in Ukraine. IoT structures have been deployed in major cities to facilitate simple operations such as utility consumption monitoring. IoT has also been integrated into industrial and agricultural enterprises and is steadily approaching widespread household adoption. A logical progression in this process is the application of these technologies in university laboratories, where future professionals are being trained to implement and operate IoT systems. One practical application of these technologies during wartime has been providing online educational processes in educational institutions (Greshta et al., 2023). These examples illustrate the atmosphere in which human capital in Ukraine was being developed in the years leading up to the onset of full-scale war. Life in the digital environment naturally fosters the enhancement of human capital qualifications, significantly reinforcing people's adaptability in times of conflict.

In general, the study testifies to the positive impact of wide technology access on effective digital transformation, which can bolster national resilience even during wartime. Furthermore, the proactive engagement of the nation in the "green" transition, characterized by investments in renewable energy and electric vehicles, reflects a dedication to promoting environmental sustainability. Adopting additive technologies and the Internet of Things (IoT) also exemplifies Ukraine's technological advancement, spanning applications from educational practices to domestic drone initiatives. These advancements underscore the evolving terrain of human capital development in Ukraine, fortified by digitalization and technological fusion, thereby augmenting resilience and adaptability amidst wartime challenges and adversities.

Data availability and the fact that the paper was written during the war is one of the limitations of the study, since not all information is available publicly yet due to national security reasons. Nevertheless, the conflict in Ukraine also underscored challenges inherent in modern technological dependencies, such as disruptions to supply chains for technological components, susceptibility to cyberattacks, and the proliferation of misinformation and propaganda. Addressing these challenges warrants careful consideration in further research.

CONCLUSION

The study aimed to explore the role of Industries 3.0, 4.0, and 5.0 in enhancing the security of socio-economic systems amid ongoing digital transformation and in the context of russian war against Ukraine. A comprehensive examination of the evolving conceptualization of SES, particularly the Ukrainian case and its wartime responses, reveals several key insights.

Modern industrial revolutions have shifted the understanding of socio-economic system security from a technocratic approach to a comprehensive model that prioritizes resilience, self-recovery, and flexibility. Emerging technologies strengthen the material component through energy decentralization and transport digitalization; the informational component through threat monitoring and cyber defense; and the synergistic component through expanding remote work, self-organization, and digital services. These advancements enable greater adaptability to threats and create a new quality of SES functioning and security, especially in key sectors such as energy, transport, information, and social relations.

The progress of digital transformation within Ukraine's economy has played a pivotal role in mitigating the war's negative impacts and preventing irreversible economic setbacks. Notably, the decentralization and autonomization of energy systems and the adoption of green energy, particularly in the private sector, have enhanced resilience and economic activity at the household level, helping to reduce losses from physical destruction and ease the burden on national energy infrastructure.

The electrification of transport, digital logistics, and the deployment of unmanned systems and remote management tools have reduced risks related to the human factor, fuel dependence, and

http://dx.doi.org/10.21511/ppm.23(2).2025.67

infrastructure damage. As demonstrated in Ukraine, the widespread adoption of electric vehicles supported mobility during evacuations, compensated for fuel shortages, and sustained essential services in affected communities.

Moreover, the digitalization of the population and economy has significantly enhanced national information security, ensuring the continued operation of key sectors such as enterprises, transport, infrastructure, education, and healthcare. These developments help preserve the social fabric and maintain societal cohesion, even in conditions of displacement, infrastructure loss, and disinformation attacks.

Thus, disruptive technologies have proven highly effective in mitigating the adverse effects of military conflict on socio-economic systems in Ukraine. Their broader significance lies in catalyzing the emergence of complex adaptive mechanisms that not only preserve functionality but also support systems' capacity for self-renewal. This marks a profound transition from a technocratic to a system-synergistic, human-centered model of security, where human capital becomes a core determinant, and technologies evolve into integrated elements of sustainable socio-economic systems.

AUTHOR CONTRIBUTIONS

Conceptualization: Leonid Melnyk, László Vasa, Oleksandr Kubatko, Pavlo Hrytsenko.
Data curation: Leonid Melnyk, Inna Koblianska, Pavlo Hrytsenko.
Formal analysis: Leonid Melnyk, László Vasa, Oleksandr Kubatko, Inna Koblianska.
Funding acquisition: László Vasa.
Investigation: Inna Koblianska.
Methodology: Leonid Melnyk, Oleksandr Kubatko, Inna Koblianska.
Project administration: Oleksandr Kubatko.
Resources: László Vasa.
Software: László Vasa, Inna Koblianska.
Supervision: Leonid Melnyk.
Validation: László Vasa, Inna Koblianska, Pavlo Hrytsenko.
Visualization: Pavlo Hrytsenko.
Writing – original draft: Leonid Melnyk, László Vasa, Oleksandr Kubatko, Inna Koblianska, Pavlo Hrytsenko.
Writing – review & editing: Leonid Melnyk, László Vasa, Oleksandr Kubatko, Inna Koblianska, Pavlo Hrytsenko.

ACKNOWLEDGMENTS

The paper is prepared within the scientific research projects "Digital Transformations to Ensure Civil Protection and post-war Economic Recovery in the Face of Environmental and Social Challenges" (No. 0124U000549) and "Fundamental Grounds for Ukraine's transition to a digital economy based on the implementation of Industries 3.0; 4.0; 5.0" (No. 0124U000576).

REFERENCES

1. Albert, M. J. (2020). The Dangers of Decoupling: Earth System Crisis and the 'Fourth Industrial Revolution'. *Global Policy, 11*(2), 245-254. https://doi.org/10.1111/1758-5899.12791
2. Asghar, S., Rextina, G., Ahmed, T., & Tamimy, M. I. (2020). The Fourth Industrial Revolution in the developing nations: Challenges and road map. *Commission on Science and Technology for Sustainable Development in the South (COMSATS). Research Papers, 102*. Retrieved from https://www.southcentre.int/wp-content/uploads/2020/02/RP102_The-Fourth-Industrial-Revolution-in-

the-Developing-Nations-Challenges-and-Road-Map_EN-1.pdf

3. Autogeek. (2021, November 17). *V Ukraini vpershe porakhuvaly kilkist zariadnykh stantsii dlia elektromobiliv: chotyry mashyny na odnu zapravku [In Ukraine, the number of charging stations for electric cars was counted for the first time: Four cars per filling station]*. (In Ukrainian). Retrieved from https://autogeek.com.ua/zarydni-stancii/

4. Beloshytska, O. (2022, January 4). *V Ukraini zrosla kilkist elektromobiliv (infohrafika) [The number of electric cars has increased in Ukraine (infographika)]*. Hubs. (In Ukrainian). Retrieved from https://hubs.ua/economy/v-ukrayini-zrosla-kil-kist-elektromobiliv-infografika-263376.html

5. Bigerna, S., D'Errico, M. C., & Polinori, P. (2021). Energy security and RES penetration in a growing decarbonized economy in the era of the 4 industrial revolution. *Technological Forecasting and Social Change, 166,* 120648. https://doi.org/10.1016/j.techfore.2021.120648

6. Burton, S. L., & Moore, P. D. V. M. (2024). Pig Butchering in Cybersecurity: A Modern Social Engineering Threat. *SocioEconomic Challenges, 8*(3), 46-60. https://doi.org/10.61093/sec.8(3).46-60.2024

7. David, L. O., Nwulu, N. I., Aigbavboa, C. O., & Adepoju, O. O. (2022). Integrating fourth industrial revolution (4IR) technologies into the water, energy & food nexus for sustainable security: A bibliometric analysis. *Journal of Cleaner Production, 363,* 132522. https://doi.org/10.1016/j.jclepro.2022.132522

8. De Amorim, W. S., Borchardt Deggau, A., Do Livramento Gonçalves, G., Da Silva Neiva, S., Prasath, A. R., & Salgueirinho Osório De Andrade Guerra, J. B. (2019). Urban challenges and opportunities to promote sustainable food security through smart cities and the 4th industrial revolution. *Land Use Policy, 87,* 104065. https://doi.org/10.1016/j.landusepol.2019.104065

9. Dobrovolska, O., & Kolomiiets, S. (2024). The Impact of Digitalisation on Social Determinants of Public Health. *Health Economics and Management Review, 5*(3), 128-142. https://doi.org/10.61093/hem.2024.3-09

10. Dobrovolska, O., Ortmanns, W., Dotsenko, T., Lustenko, V., & Savchenko, D. (2024). Health Security and Cybersecurity: Analysis of Interdependencies. *Health Economics and Management Review, 5*(2), 84-103. https://doi.org/10.61093/hem.2024.2-06

11. Eurostat. (2025). *Temporary protection for persons fleeing Ukraine*. Retrieved from https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Temporary_protection_for_persons_fleeing_Ukraine_-_monthly_statistics#:~:text=98.4%25%20of%20the%20people%20who,(4%20217%3B%200.1%25)

12. Focus. (2021, August 31). *Plius 2 mln korystuvachiv. Chym ukraintsi zaimaiutsia v internet u 2021 rotsi (infohrafika) [Plus 2 million users. What Ukrainians are doing on the Internet in 2021 (infographic)]*. (In Ukrainian). Retrieved from https://focus.ua/uk/digital/491571-plyus-2-mln-koristuvachiv-chim-ukrajinci-zaymayutsya-v-interneti-u-2021-roci-infografika

13. Freelancehunt. (2022, December 26). *Pidsumky 2022 roku: Freelancehunt u tsyfrakh [2022 results on Freelancehunt: How the freelance market has changed]*. Freelancehunt Blog. (In Ukrainian). Retrieved from https://freelancehunt.com/blog/pidsumki-2022-roku-freelancehunt-u-tsifrakh/

14. Gompert, D. C. (1998). National Security in the Information Age. *Naval War College Review, 51*(4), 22-41. Retrieved from https://www.jstor.org/stable/44638203?seq=1

15. Greshta, V., Shylo, S., Korolkov, V., Kulykovskyi, R., & Kapliienko, O. (2023). Universities in times of war: Challenges and solutions for ensuring the educational process. *Problems and Perspectives in Management, 21*(2), 80-86. https://doi.org/10.21511/ppm.21(2-si).2023.10

16. Heath, J. B. (2020). The New National Security Challenge to the Economic Order. *The Yale Law Journal, 129,* 1020-1098. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3361107

17. Holovne in UA. (2022, April 27). *VVP Ukrainy mozhet upast na 30-50 protsentov v 2022 godu, - Smygal [Ukraine's GDP may fall by 30-50 percent in 2022, - Shmyhal]*. Holovne in UA. (In Russian). Retrieved from https://glavnoe.in.ua/news/n357085195-vvp-ukrainy-mozhet-upast-na-30-50-procentov-v-2022-godu-shmygal

18. Horbik, V. (2022, February 9). *Yak zminytsia rynok smartfoniv v 2022 rotsi v Ukraini [How the smartphone market will change in 2022 in Ukraine]*. Dev.Ua. (In Ukrainian). Retrieved from https://dev.ua/news/7-faktov-ob-yzmenenyy-cen-na-smartfony

19. Interfax-Ukraine. (2022, May 12). Zbytky infrastrukturi vid viiny za tyzhden zrosly na $2,4 mlrd, naftobaz zruinovano na $227 mln – doslidzhennia [*Damage to infrastructure from the war increased by $2.4 billion in a week, oil depots were destroyed by $227 million – Study*. (In Ukrainian). Retrieved from https://ua.interfax.com.ua/news/general/831573.html

20. Jarzębowski, S., Bozhenko, V., Didorenko, K., Tkachenko, O., Blyznyukov, A., Melnyk, M., & Cieslik, J. (2024). The Impact of Digitalisation on the Competitiveness of European Countries. *SocioEconomic Challenges, 8*(3), 238-261. https://doi.org/10.61093/sec.8(3).238-261.2024

21. Kuzior, A., Vasylieva, T., Kuzmenko, O., Koibichuk, V., & Brożek, P. (2022). Global Digital Convergence: Impact of Cybersecurity, Business Transparency, Economic Transformation, and AML Efficiency. *Journal of Open Innovation: Technology, Market, and Complexity, 8*(4), 195. https://doi.org/10.3390/joitmc8040195

22. Loshakova, N. (2021, August 19). *Organicheskiye produkty v Ukraine: kak rastiot proizvodstvo i chto interesuyet pokupateley [Organic products in Ukraine: how*

http://dx.doi.org/10.21511/ppm.23(2).2025.67

production is growing and what interests buyers]. Delo.ua. (In Russian). Retrieved from https://delo.ua/business/s-polja-na-stol-kakie-perspektivy-u-rynka-organi-385538/

23. Maatallah, M. (2024). The Role of Digital Transformation in Enhancing Financial Inclusion: Unveiling the Economic and Social Challenges from Residents' Perspective. *SocioEconomic Challenges, 8*(3), 93-107. https://doi.org/10.61093/sec.8(3).93-107.2024

24. Manning, R. A. (2019). Techno-Nationalism vs. The Fourth Industrial Revolution. *Global Asia*, *4*(1). Retrieved from www.globalasia.org/v14no1/cover/techno-nationalism-vs-the-fourth-industrial-revolution_robert-a-manning

25. Melnyk, L., Kubatko, O., Dehtyarova, I., Matsenko, O., & Rozhko, O. (2019). The effect of industrial revolutions on the transformation of social and economic systems. *Problems and Perspectives in Management, 17*(4), 381-391. https://doi.org/10.21511/ppm.17(4).2019.31

26. Melnyk, L., Kubatko, O., Matsenko, O., Balatskyi, Y., & Serdyukov, K. (2021). Transformation of the human capital reproduction in line with Industries 4.0 and 5.0. *Problems and Perspectives in Management, 19*(2), 480-494. https://doi.org/10.21511/ppm.19(2).2021.38

27. Odhiambo, V. (2019). *The 4 th Industrial Revolution and Food Security Valiant Odhiambo*. Retrieved from https://doi.org/10.13140/RG.2.2.27411.84009

28. Ponomarenko, I., Kovalov, B. L., & Melnyk, M. (2024). Business Innovations and Digital Transformation: Trend, Comparative and Bibliometric Analysis. *Business Ethics and Leadership, 8*(1), 74-92. https://doi.org/10.61093/bel.8(1).74-92.2024

29. Priyadarshi, A, Singh, P., Dawadi, P., Kumar Dixit, A., & Prasad, D. (2024). Role of FinTech Apps in Increasing Investment Decisions: A Study on the Capital Market. *Financial Markets, Institutions and Risks, 8*(2), 186-197. https://doi.org/10.61093/fmir.8(2).186-197.2024

30. Pryschepa, Ya. (2022, May 14). *Viina zavdala infrastrukturi zbytkiv na 90 miliardiv dolariv – Kubrakov [The war caused 90 billion dollars worth of damage to Ukraine's infrastructure, the minister said]*. Suspilne News. (In Ukrainian). Retrieved from https://suspilne.media/239497-vijna-zavdala-infrastrukturi-ukraini-zbitkiv-na-90-milardiv-dolariv-ministr/

31. Rothschild, E. (1995). What Is Security? *Daedalus, 124*(3), 53-98. Retrieved from http://www.jstor.org/stable/20027310

32. Rymarczyk, J. (2020). Technologies, Opportunities and Challenges of the Industrial Revolution 4.0: Theoretical Considerations. *Entrepreneurial Business and Economics Review, 8*(1), 185-198. https://doi.org/10.15678/EBER.2020.080110

33. Saith, A. (2008). Towards Universalizing Socio-economic Security: Strategic Elements of a Policy Framework. *Indian Journal of Human Development*, *2*(1), 9-38. https://doi.org/10.1177/0973703020080102

34. Samaeva, Yu. (2022, March 31). *Yak pratsiuie tyl? [How does the rear work?]* Dzerkalo Tyzhnya. (In Ukrainian). Retrieved from https://zn.ua/ukr/macrolevel/jak-pratsjuje-til.html

35. Sheremet, A. (2022, May 14). *Ministerstvo infrastruktury Ukrainy: Suma zbytkiv vid rosiiskoho vtorhnennia vzhe perevyshchyla $90 miliadiv [Ministry of Infrastructure of Ukraine: The amount of losses from the Russian invasion has already exceeded $90 billion]*. Babel News. (In Ukrainian). Retrieved from https://babel.ua/news/78707-ministerstvo-infrastrukturi-ukrajini-suma-zbitkiv-vid-rosiyskogo-vtorgnennya-vzhe-syagnula-ponad-90-milyardiv

36. Springs, D. (2024). Smart city planning focused on the US cities in need of policing innovations and public health safety technologies and strategies. *Health Economics and Management Review, 5*(1), 117-128. https://doi.org/10.61093/hem.2024.1-09

37. Ukrainian Energetics. (2022, January 18). *Potuzhnist "domashnikh" SES siahnula 1,2 HVt [The capacity of 'domestic' SPPs reached 1.2 GW]*. Ukrainian Energetics. (In Ukrainian). Retrieved from https://ua-energy.org/uk/posts/potuzhnist-domashnikh-ses-siahnula-12-htt

38. Vasilyeva, T., Ziółko, A., Kuzmenko, O., Kapinos, A., & Humenna, Y. (2021). Impact of digitalization and the COVID-19 pandemic on the AML scenario: Data mining analysis for good governance. *Economics & Sociology, 14*(4), 326-354. https://doi.org/10.14254/2071-789x.2021/14-4/19

39. Wells, L. I. (2019). National Security Implications of the Fourth Industrial Revolution. In Itamara V. Lochard (Ed.). *Senior Leadership Roundtable on Military and Defence Aspects of Border Security in South East Europe* (Vol. 141, pp. 11-22). Retrieved from https://ebooks.iospress.nl/DOI/10.3233/978-1-61499-908-9-11

40. World Bank Group. (2023). *UKRAINE Rapid Damage and Needs Assessment February 2022 – February 2023*. Retrieved from https://ukraine.un.org/sites/default/files/2023-03/P1801740d-1177f03c0ab180057556615497.pdf

41. Zámek, D., & Zakharkina, Z. (2024). Research Trends in the Impact of Digitization and Transparency on National Security: Bibliometric Analysis. *Financial Markets, Institutions and Risks, 8*(1), 173-188. https://doi.org/10.61093/fmir.8(1).173-188.2024

42. Zhou, Y. (2024). The Business Leadership of the State-Owned Enterprises: Impact of the Digital Transformations. *Business Ethics and Leadership, 8*(3), 253-289. https://doi.org/10.61093/bel.8(3).253-289.2024