ECONOMICS OF DEVELOPMENT
Journal homepage: https://ecdev.com.ua/
Vol. 24, No. 1
2025

UDC 330.341.1:004.056.5
DOI: 10.63341/econ/1.2025.118

Oleh Semenenko*
Doctor of Military Sciences, Professor
Central Research Institute of the Armed Forces of Ukraine
03049, 28B Povitrianykh Syl Ave., Kyiv, Ukraine
https://orcid.org/0000-0001-6477-3414

Oleksandr Kin
PhD in Technical Sciences, Associated Professor
Hennadii Udovenko Diplomatic Academy of Ukraine
01001, 2 Velyka Zhytomyrska Str., Kyiv, Ukraine
https://orcid.org/0009-0001-2196-7515

Oleksandr Zaitsev
Doctor of Technical Sciences, Associated Professor
Yevhenii Bereznyak Military Academy
04050, 81 Illienka Str., Kyiv, Ukraine
https://orcid.org/0000-0003-2475-3800

Ivan Tkach
Doctor of Economics, Professor
Yevhenii Bereznyak Military Academy
04050, 81 Illienka Str., Kyiv, Ukraine
https://orcid.org/0000-0001-5547-6303

Vitalii Kuravskyi
PhD in History, Leading Researcher
Central Research Institute of the Armed Forces of Ukraine
03049, 28B Povitrianykh Syl Ave., Kyiv, Ukraine
https://orcid.org/0009-0000-1345-6451

The impact of digital technologies on the defence economy of Ukraine in the context of economic challenges to cybersecurity

Abstract. The purpose of the study was to assess the impact of cybersecurity and a number of other non-military factors of countries' resistance to threats on their defence capabilities and to characterise the factors that determine the level of cybersecurity. As a result, the state of digitalisation of the defence economy of Ukraine is characterised through qualitative and quantitative indicators, allowing for the substantial efforts of the state to implement digitalisation and ensure cybersecurity to be noted. It is established that the country's cybersecurity level was lower than the global average, and the spending on digitalisation in the defence sector was only 0.16% of the total cost of the main areas. In the paper, it is noted that improving the level of cybersecurity in the context of the rapid introduction of digitalisation is a priority for ensuring defence capability because digitalisation creates new challenges for cybersecurity. This is confirmed by

Article's History: Received: 21.10.2024; Revised: 31.01.2025; Accepted: 25.03.2025

Suggested Citation:
Semenenko, O., Kin, O., Zaitsev, O., Tkach, I., & Kuravskyi, V. (2025). The impact of digital technologies on the defence economy of Ukraine in the context of economic challenges to cybersecurity. *Economics of Development*, 24(1), 118-131. doi: 10.63341/econ/1.2025.118.

*Corresponding author

regression analysis, which identified a statistically substantial and negative impact of digitalisation and the level of human development on cybersecurity. In addition, the aspects of countries' defence capabilities that are most affected by the level of cybersecurity are determined using regression analysis. It is discovered that the increase in the cybersecurity indicator per unit caused an increase in military strength by 0.354. Therefore, the impact of cybersecurity on defence economy can be considered substantial. Based on the results of the study, recommendations are formed for Ukraine on digitalisation of the defence economy and improving the level of cybersecurity. The results obtained can be useful for developing strategies to improve cybersecurity in the defence economy in the context of the rapid introduction of digitalisation

Keywords: military strength; non-military threat resilience factors; human development level; global innovation index; costs

INTRODUCTION

In times of war, the defence economy is one of the key factors in supporting national security and Ukraine's ability to continue resisting the aggressor. However, the state's defence capacity is determined not only by human resources and weapons but also by the ability to ensure the stability of the information space. Therefore, ensuring cybersecurity and examining the impact of digital technologies on the level of economic capabilities is a timely task. Not only physical means of destruction are used against Ukraine but also cyber-attacks, which in some cases can have no less large-scale consequences than physical damage (Eichensehr, 2022; Fyshchuk *et al.*, 2024). In turn, digital technologies can both provide a means of combating cyber threats and pose a danger due to the formation of new risks (Goswami *et al.*, 2023; Metin *et al.*, 2024). Ye. Kralich (2024) evaluated the benefits of digitalisation in the defence sector of the economy. Among these advantages, the researcher noted the use of unmanned aerial vehicles, satellites, surveillance radars, sensor technologies, as well as artificial intelligence, machine learning and big data analytics technologies. However, the paper lacks an in-depth analysis of the impact of the introduction of these technologies on cybersecurity in the defence sector. S. Bolila (2023) also noted that new digital technologies have great potential to help the army and counter the aggressor. Among other things, technologies contribute to improving the economic situation in various sectors of the economy, which will expand the defence capabilities of Ukraine. In this context, the authors noted the effectiveness of the defence tech cluster BRAVE1 platform, which supports start-ups of Ukrainian programmers who offer the most effective projects in the field of defence technologies. However, along with the recognised benefits, this paper also does not cover the issues of increasing cyber threats through the use of digitalisation.

In turn, O. Cheberyako & K. Rudik (2023) stated that the impact of digitalisation on the economy in war conditions can be not only positive but also create new challenges. Among the advantages of digitalisation, the "Digital for freedom" programme, according to which the world's leading technology companies participate in the development of Ukraine's digital capabilities during martial law, was noted. Among the areas of the programme, the transition of public services to an online mode, the protection of state registers, the optimisation of cybersecurity, etc., are also notable. The disadvantage of digitalisation is excessive reliance on digital technologies, the devastating consequences of which were fully manifested during blackouts and through the destruction of infrastructure (Shahini *et al.*, 2024). In addition, digitalisation can generate threats to ensure information security – for example, through the distribution of malicious content, cybersecurity, which is conducted for the purpose of unauthorised access to confidential data, their theft, distortion, and use for dishonest purposes (Avtalion *et al.*, 2024). An important contribution of the study is the assessment of the impact of digitalisation on the formation of financial resources for defence activities. The characteristics of the impact of digitalisation on cybersecurity in the study are of an overview nature and are not supported by quantitative data.

Important conclusions on ensuring cybersecurity are provided in the paper of N. Komykh (2023), which stated that the solution to the problem of cyber defence should provide for the introduction of a set of various, not only technological measures. According to the researcher, cybersecurity is also influenced by technical, informational, legal, psychological, and organisational factors. An important area for improving cybersecurity is to create a cybersecurity culture that will include, among other things, improving people's skills to resist cyber threats. Y.V. Samusevych *et al.* (2021) identified a link between economy, education, national security, and digitalisation. S. Bondarenko *et al.* (2022) established that the critical areas of strengthening cybersecurity in Ukraine in terms of optimising the institutional system are organisational and legal. While recognising the valuable contribution of research to characterise the relationship between digitalisation, cybersecurity, and other non-military factors of country resilience, it should be noted that their impact on the country's defence capability remains poorly examined.

In the context of an increased level of cyber threats, it is important to understand the impact that cybersecurity has on various aspects of defence economy capability. This influence is not isolated but is conducted simultaneously with other non-military factors. In turn, the level of cybersecurity is largely determined by social, technological, and economic aspects. The paper aimed to assess the impact of cybersecurity and other non-military factors of countries' resilience on their defence economy capability and analyse the factors that explain the level of cybersecurity. This goal required solving the following tasks: to provide an overview of the state of digitalisation of the defence economy of Ukraine in the context of war, identify key advantages and main problems; to analyse the impact of non-military factors of country resilience, including cybersecurity, on defence capability using the example of a global sample of countries; to evaluate the impact of technological, economic, and social aspects on the level of cybersecurity.

MATERIALS AND METHODS

The statistical analysis allowed to describe the state of digitalisation of the defence economy of Ukraine and assess global trends through the analysis of defence spending indicators, revenue dynamics, and the place of Joint-Stock Company Ukrainian Defence Industry in the ranking of the top 100 companies for the production of weapons and military services in the world, estimates of non-military sustainability indicators, and the global artificial intelligence market in the defence economy (FM Resilience Index, n.d.; SIPRI arms industry database, n.d.; Global AI in defense and security market, 2024; Defence spending and procurement trends, 2025). The comparative analysis allowed determining the place of Ukraine among other states by comparing the indicators of the country's defence capability and non-military factors influencing its defence capability with global averages.

Correlation analysis was used to analyse whether there are statistically substantial relationships between indicators of countries' defence capability and non-military factors of countries' resilience. This allowed forming an initial vision of the problem and identifying potential influencing factors. The purpose of the regression analysis was to analyse what non-military sustainability factors of countries can affect their defence capabilities. Special attention in the context of the research subject is paid to defining the role and impact of cybersecurity on defence capability.

Accordingly, the first group of indicators for regression analysis was formed considering their ability to fully characterise the defence capability of countries. These indicators acted as dependent variables in the analysis. These include military strength, security threats index, armed forces personnel, and military expenditure. Despite the fact that some indicators partially overlap (for example, armed forces personnel and military expenditure are reflected in military strength), their inclusion in the analysis was appropriate because it allowed assessing the impact of sustainability factors on various aspects of defence capability.

The second group of indicators consisted of indicators describing non-military factors that can potentially affect defence capability. The indicators of this group were independent variables. These factors reflect economic, social, environmental, and technological factors, including the level of cybersecurity. This approach to forming a sample of independent variables, among other things, allowed describing the impact of cybersecurity more accurately because it was evaluated in the context of interaction with other indicators.

An additional stage of regression analysis was devoted to assessing the impact of individual indicators on cybersecurity. The criteria for selecting indicators were their potential ability to influence the level of cybersecurity through economic, social, and technological aspects. All indicators that were used in the study are contained in Table 1, with an explanation of their essence and a link to the source.

Table 1. Sample of indicators for the study

Indicator	Source	Entity
Indicators that characterise defence capability and acted as dependent variables in the study		
Military strength score (varies from 0.0744 to 4.3156 for the study period, where 0.0744 indicates high military strength)	Global Firepower (2025 military strength ranking, 2025)	Assessment of countries by available firepower, determined by about 60 factors (number of military units, financial condition, material and technical capabilities, etc.)
Security Threats Index – (varies from 0.2 to 9.7 for the study period, where 0.2 indicates a high level of security)	The Global Economy (Security Threats Index – country rankings, n.d.)	It considers such immediate security threats as explosions, attacks, deaths due to battles, rebel movements, uprisings, coups, and terrorism. The index also reviews substantial criminal factors and perceived public confidence in the internal security system
Armed forces personnel	World Bank (Armed forces personnel, total, n.d.)	Total number of military personnel in the country
Military expenditure	World Bank (Military expenditure (current USD), n.d.)	The country's total defence expenditures, including the maintenance of the army and the purchase of weapons for other purposes
Non-military threat resistance factors that acted as independent variables in the study		
Resilience Index (not directly included in the analysis, its drivers were used; the index, like drivers, is measured from 0 to 100, where 100 is the highest level of stability)	Factory Mutual Insurance Company (FM Resilience Index, n.d.)	The index reflects countries' resilience to various risks through 18 indicators included in it, including productivity, health expenditure, education, inflation, political risk, control of corruption, energy intensity, ghg emissions, water stress, urbanisation rate, logistics, internet usage, climate risk exposure, climate risk quality, climate change exposure, seismic risk exposure, fire risk quality, cybersecurity
Indicators for an additional stage of regression analysis that acted as independent variables that potentially affect cybersecurity		
Overall Global Innovation Index (reflects the position of countries in the ranking, where 1 is the highest level of development)	World Intellectual Property Organization (GII 2024 results, 2024)	It evaluates the effectiveness of innovation in about 130 economies of the world and contains approximately 80 indicators, including political, educational, and infrastructure measures

Table 1. Continued

Indicator	Source	Entity
Human Capital Index (measured from 0 to 1, where 1 is the highest level of development)	World Bank (Human Capital Index (HCI), upper bound (scale 0-1) – East Asia & Pacific (excluding high income), n.d.)	Determines how effectively countries mobilise human capital and realise the economic and professional potential of the population
GDP per capita	World Bank (GDP per capita (current US$), n.d.)	Shows the country's gross domestic product (GDP) divided by the total population

Source: compiled by the authors

Thus, the analysis used 4 indicators of defence capability, 18 indicators of non-military sustainability factors, and 3 indicators of impact on cybersecurity for 91 countries of the world. Such a sample was considered to be sufficient for a study confirming the reliability of the results.

RESULTS

Digital technologies in the defence economy of Ukraine: Effectiveness of digitalisation and cybersecurity

The defence economy is an essential tool for ensuring an appropriate level of national security, increasing the country's defence capability through the efficient use of resources. Defence spending determines the ability of countries to respond to global challenges in the face of instability and escalation of conflicts of various origins. Figure 1 shows the countries that are the leaders in defence spending as of 2024.

Ukraine ranked fourteenth in terms of military spending in 2024, down several positions from 2023, when the country's military spending totalled USD 64.8 billion, and it ranked eighth in the ranking (Countries with the highest..., 2024). Moreover, Joint-Stock Company Ukrainian Defence Industry (Ukroboronprom) has been among the top 100 companies producing weapons and military services in the world since 2011 (Fig. 2).

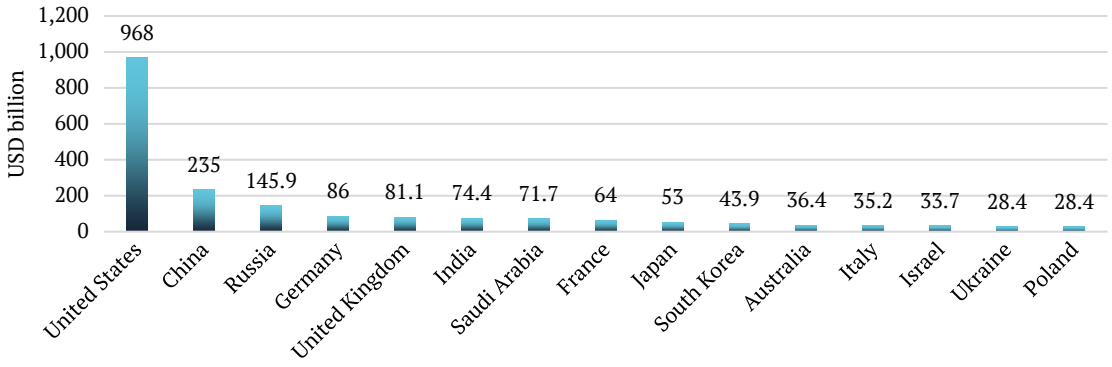

Figure 1. Countries with the highest military spending in 2024

Source: compiled by the authors based on Defence spending and procurement trends (2025)

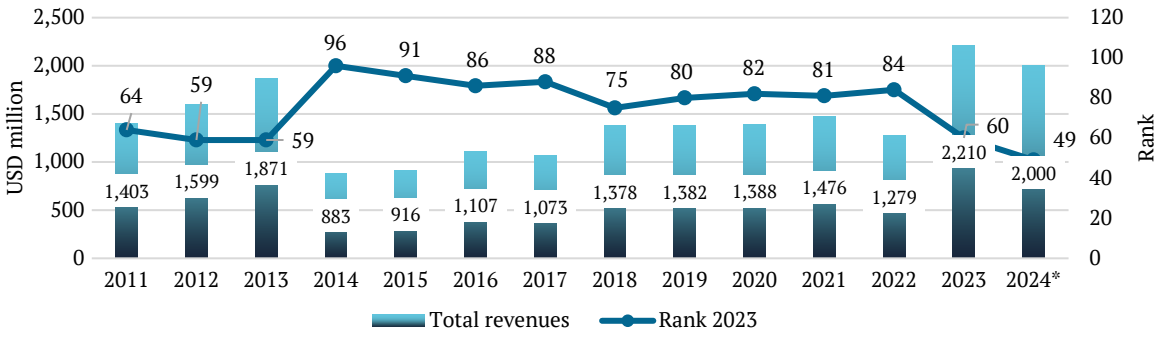

Figure 2. Revenue dynamics and position of Joint-Stock Company Ukrainian Defence Industry in the top 100 companies for the production of weapons and military services in the world

Note: * – as of September 2024

Source: compiled by the authors based on SIPRI arms industry database (n.d.), B. Miroshnychenko (2024)

The military strength indicator in 2025 is 0.3755 for Ukraine, which is quite high compared to the global average value of this indicator, which is about 1.3514. The number of military personnel of Ukraine as of 2025 reaches approximately 800,000 people, another 1,000,000 people are in reserve. Regarding non-military indicators of country resilience, Ukraine's indicators generally adhere to global averages (Fig. 3).

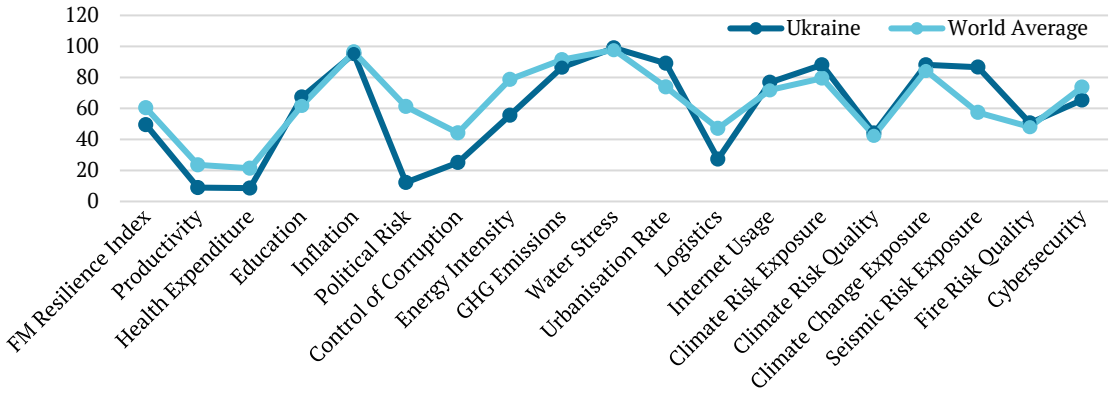

Figure 3. Comparison of non-military indicators of Ukraine's stability and global averages in 2024
Source: compiled by the authors based on FM Resilience Index (n.d.)

For Ukraine, among these non-military sustainability indicators, cybersecurity is of particular importance. In the context of war, given the scale and consequences of Russian cyber-attacks, cybersecurity is one of the most important areas of ensuring defence economy capability. Digitalisation of the defence sector, on the one hand, provides new opportunities for improving protection systems against cybersecurity threats. On the other hand, digitalisation can create new cybersecurity challenges, especially in the case of excessive dependence on information and communication technologies (Metelskyi & Kravchuk, 2023). In war conditions, enemy cyber-attacks can be aimed at obtaining confidential information or disrupting the activities of the military administration (Cherleniak & Tokar, 2024). Therefore, the activity of anticipating, countering and eliminating cybersecurity threats is one of the priorities in the context of armed confrontation.

Current initiatives in the field of digitalisation of the security and defence sector of Ukraine can be divided into several areas. The first concerns direct warfare, and one example of using digitalisation in this process is the introduction of the Delta system, which allows tracking enemy targets. As of January 14, 2025, it was reported that this system helped eliminate Russian equipment worth about USD 15 billion. The second area is material and technical support, which is the responsibility of the procurement agencies of the Ministry of Defence. Digitalisation of procurement processes (in particular, purchases through Prozorro, implementation of the DOT-Chain IT system, optimisation of internal dot processes, etc.) allowed saving about UAH 21 billion for the state budget, improving the food supply cycle, and optimising accounting systems. The third direction concerns human capital and is presented through: the register "Oberig", which contains data on those liable for military service, necessary for military registration; the electronic cabinet Reserve+, which contains the largest database of military vacancies; the application Army+ for military personnel, created to overcome excessive bureaucracy in the army. The last and fourth direction of digitalisation of the security and defence sector concerns resource provision. This area is the least digitalised and requires the introduction of effective tools for translating data work into digital form (Defence Talks, 2025).

The main directions of the state's cybersecurity policy are determined by the Law of Ukraine No. 2163-VIII (2017) and the Cybersecurity Strategy of Ukraine (Decision of the National Security and Defence Council of Ukraine No. n0055525-21, 2021). Coordination between cybersecurity entities is provided by the National Cybersecurity Coordination Centre, established in 2016. In 2020, changes were introduced to the work of the National Cybersecurity Coordination Centre, in particular, private sector specialists were involved. Such initiatives have allowed turning the National Cybersecurity Coordination Centre into a central platform for tracking, predicting, detecting, and eliminating cybersecurity threats in the public and private spheres. In 2024, the Ministry of Defence added another structural unit to improve the state of cybersecurity – the Cyber Incident Response Centre. It is assumed that this unit will have the goal of prompt and effective response to cyber incidents. Another way to improve cyber defence is to standardise information security requirements in the Ministry of Defence systems in accordance with North Atlantic Treaty Organization (NATO) best practices. This applies to the ministry's digital tools, services, applications, and systems. An important area of countering cyber threats is improving the training of specialists in the field of cybersecurity and finding opportunities for information exchange and cooperation with other parties, particularly international partners.

Despite the noted efforts in the field of countering cyber threats, the cybersecurity indicator of Ukraine is below the global average, and spending on digitalisation in the field of defence is only 0.16% of the total spending on the main areas (Cheberyako & Rudyk, 2023). Given the rapid development of technologies and the projected growth of the global artificial intelligence market in defence and security, Ukraine needs to increase attention to cybersecurity issues through improving information security strategies, strengthening the regulatory framework, and financial support (Fig. 4). Assessing the impact of cybersecurity and other non-military resilience factors in countries can help identify which aspects of countries' defence capabilities are most dependent on the level of cybersecurity. Initial conclusions about the relationship between cybersecurity and the defence capabilities of countries can be obtained through correlation analysis. Thereby, it should be considered that the level of cybersecurity is not a separate indicator but has an impact simultaneously with other sustainability factors.

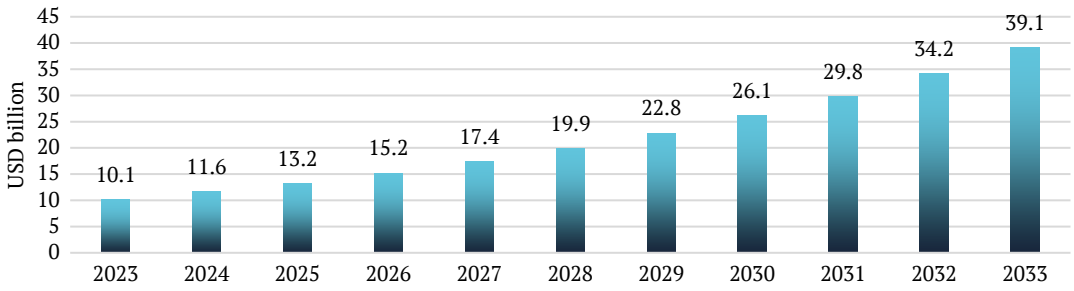

Figure 4. The size of the global artificial intelligence market in defence and security
Source: compiled by the authors based on Global AI in defense and security market (2024)

Regression analysis was used to assess the combined impact of these factors. In turn, it is also important to investigate what factors of the social, economic, and technological environment affect the level of cybersecurity. This will determine the extent to which factors such as human development, well-being, and digitalisation determine cybersecurity.

Impact of digitalisation on global sustainability

Correlation analysis was aimed at identifying the strength and direction of the relationship between the indicators of countries' defence capability and non-military indicators of resistance to threats. Tables 2 and 3 show the results of the correlation analysis between the observed indicators. Table 2 contains the obtained correlations of defence performance indicators with physical scores, Table 3 – with macro scores. Based on the results presented in Table 2, initial conclusions were drawn regarding the presence of a relationship between the examined indicators. The military strength and security threats index indicators correlated with most physical scores, and this relationship was statistically substantial. For military strength, the relationship strength was mostly weak or moderate, for the security threats index – noticeable and strong. For the armed forces personnel and military expenditure indicators, statistically substantial correlations were observed with individual indicators, mainly with weak coupling strength.

Table 2. Results of correlation analysis between indicators of defence capability of countries and non-military indicators of resistance to threats (resilience index drivers – physical scores)

Indicators	Military strength	Security threats index	Armed forces personnel, total	Military expenditure (current USD)
Productivity	−0.28*	−0.69*	−0.09	0.18
Health expenditure	−0.36*	−0.66*	−0.06	0.39*
Education	−0.43*	−0.63*	−0.1	0.13
Inflation	−0.05	−0.22*	0.03	0.06
Political risk	0.03	−0.89*	−0.27*	−0.01
Control of corruption	−0.26*	−0.78*	−0.13	0.13
Energy intensity	0.18	0.05	−0.13	−0.12
GHG emissions	−0.23*	−0.38*	−0.07	0.02
Water stress	0.01	0.08	0.02	0
Urbanisation rate	−0.35*	−0.47*	−0.15	0.05
Logistics	−0.47*	−0.64*	0.07	0.22*
Internet usage	−0.39*	−0.62*	−0.08	0.12

Note: * – statistically substantial relationships at $p < 0.05$
Source: calculated by the authors based on Armed forces personnel, total (n.d.), FM Resilience Index (n.d.), Military expenditure (current USD) (n.d.), Security Threats Index – country rankings (n.d.), 2025 military strength ranking (2025)

Table 3. Results of correlation analysis between indicators of defence capability of countries and non-military indicators of resistance to threats (resilience index drivers – macro scores)

Indicators	Climate risk exposure	Climate risk quality	Climate change exposure	Seismic risk exposure	Fire risk quality	Cybersecurity
Military strength	0.01	−0.431*	−0.069	−0.047	−0.451*	−0.552*
Security threats index	−0.146	−0.653*	−0.218*	−0.154	−0.568*	−0.425*
Armed forces personnel, total	−0.243*	−0.09	−0.199	0.002	0.072	0.23*
Military expenditure (current USD)	−0.119	0.152	−0.065	0.116	0.218*	0.189

Note: * – statistically substantial relationships at $p < 0.05$
Source: calculated by the authors based on Armed forces personnel, total (n.d.), FM Resilience Index (n.d.), Military expenditure (current USD) (n.d.), Security Threats Index – country rankings (n.d.), 2025 military strength ranking (2025)

Regarding the relationship between defence capability indicators and macro scores, a similar trend can be noted: military strength is moderately or noticeably correlated with climate risk quality, fire risk quality, and cybersecurity. The security threats index showed a weak correlation with climate change exposure and a moderate or noticeable correlation with climate risk quality, fire risk quality, and cybersecurity. The armed forces personnel indicator showed a weak association with the climate risk exposure and cybersecurity indicators, while military expenditure – only with fire risk quality indicators. The results showed that the defence capability of countries can be closely linked to a number of non-military indicators. However, the obtained correlations do not prove the direct impact of these indicators on defence capability. For a more in-depth analysis of the ability of the non-military indicators under study to determine the defence capability of countries, a regression analysis was conducted. Regression analysis was performed in several stages, each of which had its own dependent variable. The dependent variables were alternately indicators of the countries' defence capability. The set of independent indicators for regression analysis was common to all stages and consisted of non-military indicators of countries' resilience to threats.

Table 4 shows the results of regression analysis for military strength as a dependent variable and non-military threat resistance indicators as independent. The correlation coefficient for the resulting model was 0.76025834, which indicated a fairly strong correlation between the indicators included in it. The coefficient of determination was 0.57799274, and the updated coefficient of determination was 0.47249092, which showed moderate explanatory ability. The indicator is $p < 0.00000$, and therefore, the results are statistically substantial.

Table 4. Regression analysis results for military strength as a dependent variable and non-military threat resistance indicators

Indicators	Coefficients	Standard error	*t* (72)	*p* value
Intercept	1.714	1.804	0.95	0.345
Productivity	0.401	0.184	2.184	0.032
Health expenditure	−0.364	0.212	−1.716	0.09
Education	0.074	0.202	0.363	0.718
Inflation	0.035	0.091	0.387	0.7
Political risk	0.428	0.129	3.315	0.001
Control of corruption	0.335	0.221	1.519	0.133
Energy intensity	0.091	0.138	0.658	0.513
GHG emissions	−0.018	0.145	−0.123	0.902
Water stress	−0.022	0.089	−0.247	0.805
Urbanisation rate	−0.043	0.145	−0.298	0.767
Logistics	−0.518	0.173	−2.991	0.004
Internet usage	−0.285	0.173	−1.645	0.104
Climate risk exposure	0.222	0.136	1.636	0.106
Climate risk quality	−0.159	0.213	−0.746	0.458
Climate change exposure	−0.137	0.138	−0.989	0.326
Seismic risk exposure	0.058	0.098	0.595	0.554
Fire risk quality	−0.017	0.195	−0.088	0.93
Cybersecurity	−0.354	0.125	−2.838	0.006

Source: calculated by the authors based on FM Resilience Index (n.d.), 2025 military strength ranking (2025)

A statistically substantial impact on military strength was observed from the following non-military indicators: productivity and political risk – direct impact, logistics and cybersecurity – reverse impact. Notably, the growth of the military strength indicator used in the work indicated a lower military power and defence capability, and its approach to zero, on the contrary, indicated substantial defence capabilities of countries. Accordingly, rising levels of productivity and political risk weaken countries' military power. An increase in productivity by 1 was accompanied by an increase in military strength by 0.401 and an increase in political risk – by 0.428. In turn, the development of logistics and a high level of cybersecurity contribute to improving defence and military capabilities. An increase in the logistics indicator by one was associated with a decrease in the military strength indicator by 0.518 and cybersecurity – by 0.354. Conclusions about the inverse effect of productivity on military power may seem continental. However, this state of affairs can be explained by the focus of countries on technological, social, and political aspects of development, with a low focus on defence needs. Table 5 contains the regression results for the model in which the security threats index was the dependent variable. The model is characterised by a high correlation coefficient, which was 0.92801302, and a high explanatory ability, as indicated by the value of the coefficient of determination – 0.86120816 and the refined coefficient of determination – 0.8265102. The results are statistically substantial ($p < 0.0000$).

Table 5. Regression analysis results for the security threats index as a dependent variable and non-military threat resistance indicators

Indicators	Coefficients	Standard error	*t* (72)	*p* value
Intercept	7.837	2.524	3.106	0.003
Productivity	−0.175	0.105	−1.661	0.101
Health expenditure	0.177	0.122	1.452	0.151
Education	−0.026	0.116	−0.226	0.822
Inflation	−0.008	0.052	−0.145	0.885
Political risk	−0.685	0.074	−9.255	0
Control of corruption	−0.292	0.127	−2.309	0.024
Energy intensity	0.006	0.079	0.077	0.939
GHG emissions	0.053	0.083	0.64	0.524
Water stress	0.059	0.051	1.161	0.25
Urbanisation rate	0.098	0.083	1.177	0.243
Logistics	0.129	0.099	1.302	0.197
Internet usage	0.012	0.099	0.117	0.907
Climate risk exposure	−0.094	0.078	−1.203	0.233
Climate risk quality	−0.235	0.122	−1.918	0.059
Climate change exposure	−0.008	0.079	−0.105	0.917
Seismic risk exposure	0.088	0.056	1.563	0.123
Fire risk quality	0.062	0.112	0.557	0.579
Cybersecurity	−0.076	0.072	−1.064	0.291

Source: calculated by the authors based on FM Resilience Index (n.d.), Security Threats Index – country rankings (n.d.)

The security threats index was under the statistically substantial influence of political risk and control of corruption. The growth of the security threats index indicates an increase in the level of threats, so the inverse relationship with indicators indicates that their increase contributes to a decrease in security threats. An increase in political risk by 1 was accompanied by a decrease in the security threats index by 0.685 and the control of corruption indicator – by 0.292. This impact can be considered quite large-scale because the security threats index for the study period ranged from 0.2 to 9.7, and its change by 0.292 and even more so by 0.685 is substantial. Notably, the lowest value of the indicator (9.7) among 91 countries under study is typical for Ukraine. Table 6 shows the results of a regression analysis in which the military expense indicator was the dependent variable. There was a noticeable correlation between the indicators in the model (0.72259235), and it was characterised by moderate explanatory ability because the updated coefficient of determination was 0.40267463. As in previous models, the results are statistically substantial ($p < 0.0000$).

Table 6. Regression analysis results for military expenditure as a dependent variable and non-military threat resistance indicators

Indicators	Coefficients	Standard error	*t* (72)	*p* value
Intercept	217,635,598,285.156	190,205,112,522.16	1.144	0.256
Productivity	−0.668	0.195	−3.419	0.001
Health expenditure	1.714	0.226	7.598	0
Education	−0.36	0.215	−1.67	0.099
Inflation	0.017	0.097	0.179	0.859
Political risk	−0.043	0.137	−0.313	0.755
Control of corruption	−0.608	0.235	−2.588	0.012
Energy intensity	−0.073	0.147	−0.496	0.622
GHG emissions	−0.169	0.154	−1.099	0.276
Water stress	0.059	0.095	0.625	0.534
Urbanisation rate	−0.074	0.155	−0.479	0.633
Logistics	0.064	0.184	0.349	0.728
Internet usage	0.229	0.185	1.239	0.22
Climate risk exposure	−0.292	0.145	−2.019	0.047
Climate risk quality	−0.465	0.227	−2.046	0.044
Climate change exposure	0.227	0.147	1.544	0.127
Seismic risk exposure	−0.028	0.104	−0.264	0.793
Fire risk quality	0.238	0.208	1.145	0.256
Cybersecurity	0.317	0.133	2.387	0.02

Source: calculated by the authors based on FM Resilience Index (n.d.), Military expenditure (current USD) (n.d.)

Military expenditure was inversely affected by productivity, control of corruption, climate risk exposure, and climate change exposure. Military expenditure was directly influenced by health expenditure and cybersecurity. Among the observed indicators, the strongest influence was observed from productivity, an increase of 1 was associated with a decrease in military spending by 0.668, control of corruption, an increase of which by 1 was accompanied by a decrease in spending by 0.608, and health expenditure, an increase of which by 1 increased military spending by 1.714. Given that costs were measured in dollars, the scale of the impact was insubstantial and made no practical sense despite its statistical importance. The results of regression analysis with armed forces personnel as a dependent variable are shown in Table 7. The correlation coefficient shows a noticeable correlation between the model variables (0.67083765), according to the refined coefficient of determination, it has a moderate explanatory capacity (0.31252894), and $p < 0.00018$, which confirms statistical significance.

Table 7. Regression analysis results for armed forces personnel as a dependent variable and non-military threat resistance indicators

Indicators	Coefficients	Standard error	*t* (72)	*p* value
Intercept	1,184,327.619	1,001,958.332	1.182	0.241
Productivity	−0.471	0.21	−2.248	0.028
Health expenditure	0.485	0.242	2.006	0.049
Education	−0.473	0.231	−2.047	0.044
Inflation	−0.033	0.104	−0.314	0.755
Political risk	−0.151	0.147	−1.026	0.309
Control of corruption	−0.293	0.252	−1.161	0.249
Energy intensity	−0.284	0.157	−1.801	0.076
GHG emissions	−0.024	0.165	−0.142	0.887
Water stress	0.097	0.102	0.955	0.343
Urbanisation rate	−0.063	0.166	−0.38	0.705
Logistics	0.426	0.198	2.153	0.035
Internet usage	0.12	0.198	0.605	0.547
Climate risk exposure	−0.446	0.155	−2.879	0.005
Climate risk quality	−0.439	0.244	−1.802	0.076
Climate change exposure	0.231	0.158	1.467	0.147
Seismic risk exposure	−0.094	0.112	−0.839	0.404
Fire risk quality	0.407	0.223	1.826	0.072
Cybersecurity	0.453	0.142	3.181	0.002

Source: calculated by the authors based on Armed forces personnel, total (n.d.), FM Resilience Index (n.d.)

The variables productivity, health expenditure, education, logistics, climate risk exposure, and cybersecurity have a statistically substantial impact on armed forces personnel. However, judging by the regression coefficients, as in the previous model, the impact scale is too small to have practical value. In the context of the subject of study, cybersecurity deserves special attention among the examined indicators. According to the regression analysis, the statistically substantial and largest impact of this indicator was observed relative to military strength. Among the countries considered, the highest military strength value is 0.0744 (for the United States of America) and the lowest is 4.3156 (for Benin). Given that an increase in the cybersecurity indicator by 1 led to an increase in military strength by 0.354, the impact of cybersecurity on military strength can be considered substantial. Therefore, it was advisable to investigate which social, economic, and technological indicators affected the level of cybersecurity, for which regression analysis was also used. The correlation coefficient for the model, where cybersecurity was used as a dependent variable and Overall Global Innovation Index, Human Capital Index, and GDP per capita were independent, is 0.76412146, and indicates a strong relationship. The refined coefficient of determination is 0.5695327, which indicates a noticeable explanatory ability (Table 8).

Table 8. Regression analysis results for cybersecurity as a dependent variable and economic, social, and technological impact indicators

	Coefficients	Standard error	*t* (72)	*p* value
Intercept	163.365	25.505	6.405	0
Overall Global Innovation Index	−1.068	0.154	−6.914	0
Human Capital Index	−0.299	0.15	−1.999	0.049
GDP per capita	−0.078	0.103	−0.759	0.45

Source: calculated by the authors based on GDP per capita (current US$) (n.d.), FM Resilience Index (n.d.), Human Capital Index (HCI), upper bound (scale 0-1) – East Asia & Pacific (excluding high income) (n.d.), GII 2024 results (2024)

According to the results obtained, the impact is reversed; that is, an increase in Global Innovation Index and Human Capital Index is accompanied by a decrease in the level of cybersecurity. The results can be explained by the fact that countries with a high level of innovation and human resource development face more complex cyber threats and have a higher risk due to the active use of new technologies. Accordingly, highly developed countries should pay special attention to preventing and countering cyber threats through government initiatives, educational programmes, strengthening technological characteristics, etc.

Based on the analysis of the state of digitalisation of the defence economy of Ukraine in the conditions of war and the results of regression analysis, the following recommendations can be formed for Ukraine to balance the need to implement digitalisation and ensure an appropriate level of cybersecurity: increase funding for digitalisation of the defence sector of Ukraine, for example, through the development of state co-financing programmes and international initiatives to support digitalisation in Ukraine; expand the use of the latest technologies in the defence sector while ensuring proper control over their development and use, in particular, through the adaptation of NATO standards in the field of cybersecurity, as well as the development of clear requirements for certification of implemented systems; optimise state training programmes in the field of cybersecurity, cooperation with research centres, universities and international partners will be useful; ensure coordination of actions and exchange of information with international partners (through specialised platforms, training, etc.); conduct regular monitoring of cyber threats and the state of cybersecurity, analyse the impact of cybersecurity on defence capability; pay close attention to protecting critical infrastructure objects from cyber threats, for example, through the creation of secure data storage; conduct information campaigns for the population to improve self-defence skills against digital threats.

DISCUSSION

In the course of regression analysis, it was established that the simultaneous impact of cybersecurity and other non-military factors on the level of defence capability of countries is substantial. The statistically important and largest impact on cybersecurity was recorded relative to the military strength indicator. The increase in cybersecurity is accompanied by increased military strength, but it has also been determined that increased Global Innovation Index and Human Capital Index levels can increase cybersecurity threats.

Many of the papers of researchers also analysed the impact of digitalisation on various aspects of countries' resilience to threats. B. Brenner & B. Hartl (2021) investigated how the degree of digitalisation affects sustainability dimensions – economic, social, and environmental. The perception of environmental and economic sustainability was identified to be dependent to the greatest extent on digitalisation. These results are consistent with the results obtained by A. Grybauskas *et al*. (2022), which showed that digitalisation makes a substantial contribution to economic development at the corporate level by increasing the rate of return, reducing the time to market goods and increasing labour productivity. Similar conclusions are observed in the field of environmental sustainability. E.S. Knudsen *et al*. (2021) proved that digitalisation makes competitive advantages more extensive and sustainable. However, these studies focus mainly on the impact of digitalisation on non-military sustainability factors and do not pay enough attention to analysing the relationship between digitalisation and security at different levels.

In different publications, the relationship between digitalisation and security factors is investigated. For example, T.T. Thanh *et al*. (2023) discovered that digital transformation has a positive impact on the sustainability of energy security and ultimately contributes to sustainable economic development. However, their study does not fully disclose what cybersecurity challenges digitalisation poses. Regarding the risks of digitalisation for cybersecurity, S. Kumar & R.R. Mallipeddi (2022) noted that the use of the latest technologies, in particular, cloud technologies, the Internet of things, artificial intelligence, big data, and nanotechnology, creates new risks for organisations in the form of cybersecurity problems. The situation is aggravated by the growing number of cyber-attacks related to these technologies. Based on the results of the study by B. Guembe *et al*. (2022), the capabilities of existing cyber defence infrastructures will not be sufficient in the near future to counter sophisticated cyber-attacks controlled by artificial intelligence. P. Sharma & B. Dash (2023) added that the increase in the number of attacks in the cyber environment has recently led to serious negative consequences for business systems and individuals. The authors analysed how big data analytics and artificial intelligence technologies affect cybersecurity risks. Researchers have found that artificial intelligence-based platforms such as ChatGPT can have both positive and negative effects. On the one hand, these technologies can be used to implement preventive measures, and on the other – promote complex cyber-attacks. These conclusions are confirmed by M. Gupta *et al*. (2023), who noted the use cases of generative artificial intelligence, in particular ChatGPT, in both defensive and offensive cybersecurity strategies. Specifically, the researchers clarified how ChatGPT can be used to develop cyber-attacks, extract malicious information without ethical restrictions, create phishing attacks, social engineering attacks, malicious software, etc.

M. Charfeddine *et al*. (2024) supplemented this list, noting the technology's ability to provide malicious hints, test brute-force attacks, develop ransomware, and more. D. Kalla *et al*. (2023) noted that ChatGPT offers important information for cybersecurity, but its risks and limitations must be considered. M. Alsharif *et al*. (2022) concluded that the active use of technology increases cybersecurity risks. Examples include password attacks, phishing attacks, and social engineering. An important conclusion of the paper is to establish the fact that most successful cyber-attacks can be explained by the human factor – for example, about 95% of attacks were caused by human errors. These conclusions are consistent with the results of the author because the paper determined that the level of digitalisation, which was presented in the paper through the Overall Global Innovation Index indicator, negatively and statistically substantially affects the cybersecurity indicator of the examined countries.

A number of papers analyse successful international practices in countering cyber risks. In contrast to the previous studies reviewed, A.B. Ige *et al*. (2024) suggested that artificial intelligence and machine learning could help overcome information security challenges. The researchers also noted the advantages of international cooperation, implementation of international standards, investment in new technologies and public-private partnerships to increase resilience to cyber threats. M. Abdullahi *et al*. (2022) come to similar conclusions, noting the capabilities of artificial intelligence for continuous compliance monitoring and threat detection. B. Al Kurdi *et al*. (2024), using the example of the United Arab Emirates, established that successful cybersecurity management is impossible without optimising the supply chain, training employees, monitoring and the awareness of protection and security needs. However, these papers do not examine the relationship between the defence economy, cybersecurity, and the introduction of digitalisation. In turn, D. Cai *et al*. (2023) examined how defence science and technological innovation are related using the example of China. Researchers found a stable correlation between the defence sector, technological innovation, and economic development of this state, but it was heterogeneous for different regions of China. Based on the results of the study, the authors propose to balance defence and national construction, optimise the defence strategy in terms of science and technology, and strengthen the efficiency of using industrial advantages.

In turn, E.B. Kania (2022) noted that the effectiveness of China's approach to using new defence technologies will be determined by a clear strategic culture, operational requirements, and organisational characteristics. J. Reis *et al*. (2021) noted the feasibility of developing innovative defence systems based on technologies such as artificial intelligence and robots. The development of the high-tech defence industry requires effective investment of limited resources in the most promising areas (Hysi *et al*., 2024). The authors claimed that the greatest effect can be achieved at the tactical level, when the need for human intervention is minimised. D. Araya & M. King (2022) used the example of Canada to examine the development of military capabilities through the use of artificial intelligence and machine learning. The positive impact of new technologies on the management of military operations was noted. The researchers expressed concern about the security risks associated with the use of network technologies. Therefore, researchers focused on the need to strengthen security and improve data management, the need for new knowledge and experience, and the need for a balance between the rigidity of power and the needs of a changing geopolitical environment.

J.M. Rickli & M. Ienca (2021) examined the security and military implications of the use of artificial intelligence and nanotechnology. They have noticed the great potential of these technologies, which can be realised due to their modifying ability and rapid spread. Therefore, the introduction of technology in the military sector is of great concern due to the possibility of implementing security risks such as data bias, social control and manipulation, the use of weapons, etc. (Lyndyuk *et al*., 2023). Scientists emphasised that because of these dangerous opportunities of technologies, there is an urgent need for appropriate management responses to their distribution, access, and use.

The response should account for the interests of all stakeholders and be diverse and adaptive, which will counter the risks associated with the rapid development of technology. The conclusions are somewhat different from the results of this study on the directions of ensuring cybersecurity in Ukraine through different contexts because the experience of each state is unique and depends on numerous factors – the level of development, financial capabilities, political factors, etc. However, the experience described in the studies can be used in the process of developing cybersecurity strategies in Ukraine, along with the areas covered in the author's paper.

CONCLUSIONS

The results of the work showed that Ukraine has quite high indicators of military strength, military spending, and the number of military personnel. Calculating the average value of these indicators based on the data of the studied countries and comparing it with the indicators of Ukraine allowed confirming that the military potential of Ukraine substantially exceeds the global average. However, the analysis of non-military indicators of Ukraine's resilience and their comparison with the national average demonstrated that, in this case, Ukraine shows quite average results. Indicators of productivity, health costs, political risk, corruption control, and logistics are noticeably lower than average. Non-military sustainability indicators can provide important support for a country's defence capability, as confirmed in the regression analysis.

Regression analysis conducted for indicators of the defence capability of countries as dependent variables and non-military indicators of the stability of countries allowed confirming that the latter are able to partially determine military strength and influence various parameters of defence capability. Thus, productivity and political risk had a statistically substantial direct impact on military strength, while logistics and cybersecurity had the opposite impact. Given that the increase in military strength indicates a lower military strength, it was concluded that increased productivity and political risk weaken the military power of states, and better logistics and a high level of cybersecurity increase defence capabilities. The increase in logistics per unit was accompanied by a decrease in military strength by 0.518, cybersecurity – by 0.354. Given that the military strength indicator for the study period ranged from 0.0744 to 4.3156, where 0.0744 meant the highest military strength, such an impact can be considered substantial.

In addition to the impact on military strength, regression analysis revealed a statistically substantial impact of non-military resilience indicators on the security threats index. This indicator was under the statistically substantial and substantial influence of political risk and control of corruption. The military expense indicator was heavily influenced by productivity, control of corruption, climate risk exposure, and climate change exposure. A direct impact on this indicator was observed on the part of health expense and cybersecurity. Armed forces personnel were substantially affected by the variables productivity, health expenditure, education, logistics, climate risk exposure, and cybersecurity. However, for both the military expense

indicator and armed forces personnel, the scale of impact was insubstantial and did not make practical sense.

Analysis of the impact of economic, technological, and social indicators on cybersecurity displayed that the level of cybersecurity depends on the overall development of innovation and the level of human capital development. Therewith, these indicators have the opposite effect, which indicates an increase in cybersecurity risks with the growth of these variables. Thus, countries with a high level of innovation and human resource development are exposed to more complex cyber threats, which are highly likely to be implemented through the active use of innovative technologies. Based on the results of the study, recommendations were formed for Ukraine on balancing digital development and the need to ensure a high level of cybersecurity. Further research should focus on a comparative analysis of the best practices for ensuring cybersecurity in countries with a high level of innovative development because this can provide new insights to improve the fight against cyber threats in the face of the threat of more complicated and complex risks.

ACKNOWLEDGEMENTS

None.

CONFLICT OF INTEREST

None.

REFERENCES

[1] 2025 military strength ranking. (2025). Retrieved from https://www.globalfirepower.com/countries-listing.php.
[2] Abdullahi, M., Baashar, Y., Alhussian, H., Alwadain, A., Aziz, N., Capretz, L.F., & Abdulkadir, S.J. (2022). Detecting cybersecurity attacks in internet of things using artificial intelligence methods: A systematic literature review. *Electronics*, 11(2), article number 198. doi: 10.3390/electronics11020198.
[3] Al Kurdi, B., Alquqa, E.K., Nuseir, M.T., Alzoubi, H.M., Alshurideh, M.T., & AlHamad, A. (2024). Impact of cyber security and risk management on green operations: Empirical evidence from security companies in the UAE. In H.M. Alzoubi, M.T. Alshurideh & T.M. Ghazal (Eds.), *Cyber security impact on digitalization and business intelligence: Big cyber security for information management: Opportunities and challenges* (pp. 151-167). Cham: Springer. doi: 10.1007/978-3-031-31801-6_9.
[4] Alsharif, M., Mishra, S., & AlShehri, M. (2022). Impact of human vulnerabilities on cybersecurity. *Computer Systems Science & Engineering*, 40(3), 1153-1166. doi: 10.32604/csse.2022.019938.
[5] Araya, D., & King, M. (2022). *The impact of artificial intelligence on military defence and security*. Waterloo: Centre for International Governance Innovation.
[6] Armed forces personnel, total. (n.d.). Retrieved from https://data.worldbank.org/indicator/MS.MIL.TOTL.P1.
[7] Avtalion, Z., Aviv, I., Hadar, I., Luria, G., & Bar-Gil, O. (2024). Digital infrastructure as a new organizational digital climate dimension. *Applied Sciences*, 14(19), 8592. doi: 10.3390/app14198592.
[8] Bolila, S. (2023). The role of information technologies and digital tools in the context of war challenges and post-war recovery of Ukraine's economy. *Taurida Scientific Herald. Series: Economics*, 16, 265-275. doi: 10.32782/2708-0366/2023.16.35.
[9] Bondarenko, S., Makeieva, O., Usachenko, O., Veklych, V., Arifkhodzhaieva, T., & Lernyk, S. (2022). The legal mechanisms for information security in the context of digitalization. *Journal of Information Technology Management*, 14, 25-58. doi: 10.22059/jitm.2022.88868.
[10] Brenner, B., & Hartl, B. (2021). The perceived relationship between digitalization and ecological, economic, and social sustainability. *Journal of Cleaner Production*, 315, article number 128128. doi: 10.1016/j.jclepro.2021.128128.
[11] Cai, D., Hu, J., Jiang, H., Ai, F., & Bai, T. (2023). Research on the relationship between defense technology innovation and high-quality economic development: Gray correlation analysis based on panel data. *Managerial and Decision Economics*, 44(7), 3867-3877. doi: 10.1002/mde.3925.
[12] Charfeddine, M., Kammoun, H.M., Hamdaoui, B., & Guizani, M. (2024). ChatGPT's security risks and benefits: Offensive and defensive use-cases, mitigation measures, and future implications. *IEEE Access*, 12, 30263-30310. doi: 10.1109/ACCESS.2024.3367792.
[13] Cheberyako, O., & Rudyk, K. (2023). Digitalization and impact on the formation of financial resources for defense activities under the conditions of the state of martial. *Internauka*, 12. doi: 10.25313/2520-2057-2023-12-9005.
[14] Cherleniak, I., & Tokar, M. (2024). Effective governance and the doctrine of "total defence" as factors of state stability in wartime. *Democratic Governance*, 17(1), 5-17. doi: 10.23939/dg2024.05.
[15] Countries with the highest military spending worldwide in 2023. (2024). Retrieved from https://www.statista.com/statistics/262742/countries-with-the-highest-military-spending/.
[16] Decision of the National Security and Defence Council of Ukraine No. n0055525-21 "On the Cyber Security Strategy of Ukraine". (2021, May). Retrieved from https://zakon.rada.gov.ua/laws/show/n0055525-21#Text.
[17] Defence spending and procurement trends. (2025). Retrieved from https://www.iiss.org/publications/the-military-balance/2025/defence-spending-and-procurement-trends/.
[18] Defence talks: How is the defence sector going digital in times of war? (2025). Retrieved from https://nako.org.ua/en/news/defence-talks-yak-vidbuvajetsya-cifrovizaciya-oboronnogo-sektoru-pid-cas-viini.
[19] Eichensehr, K.E. (2022). Ukraine, cyberattacks, and the lessons for international law. *AJIL Unbound*, 116, 145-149. doi: 10.1017/aju.2022.20.
[20] FM resilience index. (n.d.). Retrieved from https://www.fm.com/resources/resilience-index/explore-the-data/.
[21] Fyshchuk, I., Noesgaard, M.S., & Nielsen, J.A. (2024). Managing cyberattacks in wartime: The case of Ukraine. *Public Administration Review*. doi: 10.1111/puar.13895.

[22] GDP per capita (current US$). (n.d.). Retrieved from https://data.worldbank.org/indicator/NY.GDP.PCAP.CD.
[23] GII 2024 results. (2024). Retrieved from https://surl.li/bccjes.
[24] Global AI in defense and security market. (2024). Retrieved from https://market.us/report/ai-in-defense-and-security-market/.
[25] Goswami, S.S., Sarkar, S., Gupta, K.K., & Mondal, S. (2023). The role of cyber security in advancing sustainable digitalization: Opportunities and challenges. *Journal of Decision Analytics and Intelligent Computing*, 3(1), 270-285. doi: 10.31181/jdaic10018122023g.
[26] Grybauskas, A., Stefanini, A., & Ghobakhloo, M. (2022). Social sustainability in the age of digitalization: A systematic literature review on the social implications of industry 4.0. *Technology in Society*, 70, article number 101997. doi: 10.1016/j.techsoc.2022.101997.
[27] Guembe, B., Azeta, A., Misra, S., Osamor, V.C., Fernandez-Sanz, L., & Pospelova, V. (2022). The emerging threat of AI-driven cyber attacks: A review. *Applied Artificial Intelligence*, 36(1), article number 2037254. doi: 10.1080/08839514.2022.2037254.
[28] Gupta, M., Akiri, C., Aryal, K., Parker, E., & Praharaj, L. (2023). From ChatGPT to ThreatGPT: Impact of generative AI in cybersecurity and privacy. *IEEE Access*, 11, 80218-80245. doi: 10.1109/ACCESS.2023.3300381.
[29] Human Capital Index (HCI), upper bound (scale 0-1) – East Asia & Pacific (excluding high income). (n.d.). Retrieved from https://data.worldbank.org/indicator/HD.HCI.OVRL.UB?locations=4E.
[30] Hysi, A., Avdulaj, J., Shahini, E., Goga, I., & Shahini, E. (2024). Role of legal regulation in the establishment and development of the public administration system with local self-government aspects. *Social and Legal Studios*, 7(1), 27-36. doi: 10.32518/sals1.2024.27.
[31] Ige, A.B., Kupa, E., & Ilori, O. (2024). Analyzing defense strategies against cyber risks in the energy sector: Enhancing the security of renewable energy sources. *International Journal of Science and Research Archive*, 12(1), 2978-2995. doi: 10.30574/ijsra.2024.12.1.1186.
[32] Kalla, D., Kuraku, S., & Samaah, F. (2023). Advantages, disadvantages and risks associated with ChatGPT and AI on cybersecurity. *Journal of Emerging Technologies and Innovative Research*, 10(10), 84-94.
[33] Kania, E.B. (2022). Artificial intelligence in China's revolution in military affairs. In M. Raska, K. Zysk & I. Bowers (Eds.), *Defence innovation and the 4th industrial revolution* (pp. 65-92). London: Routledge. doi: 10.4324/9781003268215.
[34] Knudsen, E.S., Lien, L.B., Timmermans, B., Belik, I., & Pandey, S. (2021). Stability in turbulent times? The effect of digitalization on the sustainability of competitive advantage. *Journal of Business Research*, 128, 360-369. doi: 10.1016/j.jbusres.2021.02.008.
[35] Komykh, N. (2023). Actual aspects of cybersecurity in Ukraine during the war. In *Materials of the VII international scientific and practical conference "International and national security: Theoretical and applied aspects"* (pp. 530-532). Dnipro: Dnipro State University of Internal Affairs.
[36] Kralich, Ye. (2024). Military technological innovations in the defense sector of the economy. *Bulletin of Mariupol State University. Series: Economics*, 27, 15-24. doi: 10.34079/2226-2822-2024-14-27-15-24.
[37] Kumar, S., & Mallipeddi, R.R. (2022). Impact of cybersecurity on operations and supply chain management: Emerging trends and future research directions. *Production and Operations Management*, 31(12), 4488-4500. doi: 10.1111/poms.13859.
[38] Law of Ukraine No. 2163-VIII "On the Basic Principles of Cybersecurity in Ukraine". (2017, October). Retrieved from https://zakon.rada.gov.ua/laws/show/en/2163-19.
[39] Lyndyuk, A., Boiko, V., Bruh, O., Olishchuk, P., & Rurak, I. (2023). Development of international cooperation of the borderline territorial communities of Ukraine with the EU countries under martial law. *Financial and Credit Activity: Problems of Theory and Practice*, 5(52), 244-255. doi: 10.55643/fcaptp.5.52.2023.4161.
[40] Metelskyi, I., & Kravchuk, M. (2023). Features of cybercrime and its prevalence in Ukraine. *Law, Policy and Security*, 1(1), 18-25.
[41] Metin, B., Özhan, F.G., & Wynn, M. (2024). Digitalisation and cybersecurity: Towards an operational framework. *Electronics*, 13(21), article number 4226. doi: 10.3390/electronics13214226.
[42] Military expenditure (current USD). (n.d.). Retrieved from https://data.worldbank.org/indicator/MS.MIL.XPND.CD.
[43] Miroshnychenko, B. (2024). *Ukrainian defence industry revenues up by 50% compared to last year*. Retrieved from https://www.pravda.com.ua/eng/news/2024/10/9/7478872/.
[44] Reis, J., Cohen, Y., Melão, N., Costa, J., & Jorge, D. (2021). High-tech defense industries: Developing autonomous intelligent systems. *Applied Sciences*, 11(11), article number 4920. doi: 10.3390/app11114920.
[45] Rickli, J.M., & Ienca, M. (2021). The security and military implications of neurotechnology and artificial intelligence. In O. Friedrich, A. Wolkenstein, C. Bublitz, R.J. Jox & E. Racine (Eds.), *Clinical neurotechnology meets artificial intelligence: Philosophical, ethical, legal and social implications* (pp. 197-214). Cham: Springer. doi: 10.1007/978-3-030-64590-8_15.
[46] Samusevych, Y.V., Novikov, V.V., Artiukhov, A.Y., & Vasylieva, T.A. (2021). Convergence trends in the "economy-education-digitalization-national security" chain. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu*, 6, 177-183. doi: 10.33271/nvngu/2021-6/177.
[47] Security Threats Index – country rankings. (n.d.). Retrieved from https://surl.li/qyaxxv.
[48] Shahini, E., Fedorchuk, M., Hruban, V., Fedorchuk, V., & Sadovoy, O. (2024). Renewable energy opportunities in Ukraine in the context of blackouts. *International Journal of Environmental Studies*, 81(1), 125-133. doi: 10.1080/00207233.2024.2320021.

[49] Sharma, P., & Dash, B. (2023). Impact of big data analytics and ChatGPT on cybersecurity. In I. Hussain & S. Das (Eds.), *Proceedings of the 4th international conference on computing and communication systems* (pp. 1-6). Shillong: Institute of Electrical and Electronics Engineers. doi: 10.1109/I3CS58314.2023.10127411.
[50] SIPRI arms industry database. (n.d.). Retrieved from https://www.sipri.org/databases/armsindustry.
[51] Thanh, T.T., Ha, L.T., Dung, H.P., & Huong, T.T. (2023). Impacts of digitalization on energy security: Evidence from European countries. *Environment, Development and Sustainability*, 25, 11599-11644. doi: 10.1007/s10668-022-02545-7.

Олег Семененко

Доктор військових наук, професор
Центральний науково-дослідний інститут Збройних Сил України
03049, просп. Повітряних Сил, 28Б, м. Київ, Україна
https://orcid.org/0000-0001-6477-3414

Олександр Кінь

Кандидат технічних наук, доцент
Дипломатична академія України імені Геннадія Удовенка
01001, вул. Велика Житомирська, 2, м. Київ, Україна
https://orcid.org/0009-0001-2196-7515

Олександр Зайцев

Доктор технічних наук, доцент
Воєнна академія імені Євгенія Березняка
04050, вул. Іллєнка, 81, м. Київ, Україна
https://orcid.org/0000-0003-2475-3800

Іван Ткач

Доктор економічних наук, професор
Воєнна академія імені Євгенія Березняка
04050, вул. Іллєнка, 81, м. Київ, Україна
https://orcid.org/0000-0001-5547-6303

Віталій Куравський

Кандидат історичних наук, провідний науковий співробітник
Центральний науково-дослідний інститут Збройних Сил України
03049, просп. Повітряних Сил, 28Б, м. Київ, Україна
https://orcid.org/0009-0000-1345-6451

Вплив цифрових технологій на оборонну економіку України в контексті економічних викликів кібербезпеці

Анотація. Метою дослідження була оцінка впливу кібербезпеки та низки інших невійськових чинників стійкості країн до загроз на їх обороноздатність, а також характеристика факторів, що визначають рівень кібербезпеки. У результаті охарактеризовано стан цифровізації оборонної економіки України через якісні та кількісні показники, що дозволило відзначити значні зусилля держави щодо впровадження цифровізації та забезпечення кібербезпеки. Встановлено, що рівень кібербезпеки країни був нижчим за середньосвітовий, а витрати на цифровізацію в оборонному секторі становили лише 0,16 % від загальних витрат за основними напрямами. Зазначено, що підвищення рівня кібербезпеки в умовах стрімкого впровадження цифровізації є пріоритетом для забезпечення обороноздатності, оскільки цифровізація створює нові виклики для кібербезпеки. Це підтверджується регресійним аналізом, який виявив статистично значущий негативний вплив цифровізації та рівня людського розвитку на кібербезпеку. Крім того, за допомогою регресійного аналізу визначено аспекти обороноздатності країн, на які найбільше впливає рівень кібербезпеки. Виявлено, що збільшення показника кібербезпеки на одиницю спричиняє збільшення військової сили на 0,354. Отже, вплив кібербезпеки на оборонну економіку можна вважати суттєвим. За результатами дослідження сформовано рекомендації для України щодо цифровізації оборонної економіки та підвищення рівня кібербезпеки. Отримані результати можуть бути корисними для розробки стратегій підвищення рівня кібербезпеки в оборонній економіці в умовах стрімкого впровадження цифровізації

Ключові слова: військова міць; фактори стійкості до невійськових загроз; рівень людського розвитку; глобальний індекс інновацій; витрати