Journal of Theoretical and Applied Information Technology
15th December 2025. Vol.103. No.23

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

PUBLIC-PRIVATE PARTNERSHIP IN THE FIELD OF INFORMATION SECURITY AS A TOOL FOR STRENGTHENING NATIONAL SECURITY

ANATOLII ZINENKO[1*], NATALIIA KRASNOSTANOVA[2], OLGA LUGACH[3], INNA KULCHII[4], OLEKSANDR ORLOVSKYI[5]

[1]PhD student at the Interregional Academy of Personnel Management, Ukraine

[2]PhD in Economics, Associate Professor at the Department of Management, Finance and Business Technologies, Institute of Public Service and Administration, Odesa Polytechnic National University, Ukraine

[3]PhD student at the Department of Local Self-Government and Territorial Development, Institute of Public Service and Administration, Odesa Polytechnic National University, Ukraine

[4]PhD, Associate Professor, Head of the Department of Public Management, Administration and Law at the National University "Yuri Kondratyuk Poltava Polytechnic", Ukraine

[5]Professor at the Chernihiv Polytechnic National University, Ukraine

E-mail: [1]anaitmeloyan0908@gmail.com, [2]krasnostanovan144@gmail.com, [3]olgalugach125@gmail.com, [4]innakulchiy16@gmail.com, [5]orlovskyi@gmail.com

ABSTRACT

Public-private partnerships (PPPs) are successfully used in international practice to strengthen national security, in particular, in the defence sector, which makes the development of this method of public-private interaction relevant in Ukraine. The aim of the study was to assess the impact of PPPs on socio-economic and security aspects in low- and middle-income countries and integrate the experience of leading countries. The research employed the methods of statistical, correlation, and regression analysis. The results of the study showed a significant positive impact of PPP investments on the military strength, logistics, and fire safety of low- and middle-income countries. However, the research did not reveal any significant impact of such investments on ensuring cybersecurity, which requires increased attention from governments to this area. The analysis of the experience of leading countries identified key positive examples of the use of PPPs in the defence and cybersecurity sectors. Key obstacles to the development of PPPs in the cybersecurity sector as an important component of information security were revealed. Priority areas for the development of PPPs in the field of cybersecurity were outlined. The results of the study gave grounds to provide recommendations for Ukraine, which can be used in practice for improving the legislative framework and developing strategies to strengthen national security. The prospects of further research may be the development of proposals for the development of PPPs in the defence sector of Ukraine through the use of specialized platforms for international coordination and information exchange.

Keywords: *Public-Private Partnership, National Security, Information Security, Cybersecurity, Infrastructure, Logistics, Sustainable Development.*

1. INTRODUCTION

The term "public-private partnership" is applicable to various models of interaction between the public sector, private sector entities, non-governmental organizations, and cooperatives. The use of PPPs is advisable in view of cost-effectiveness, focus on core activities, innovation, timeliness of implementation, long-term maintenance, diligence and risk sharing [1]. Moreover, PPPs have been recognized as one of the key instruments for achieving a number of Sustainable Development Goals (SDGs), in particular, SDG 8, SDG 9, SDG 11, SDG 17 [2].

The PPP model is used in various sectors, in particular, logistics, energy, construction, information and communication technologies (ICT), etc. [3; 4]. In many countries, PPPs contribute to strengthening national security both in peacetime and in armed conflicts, being effectively used in the defence sector [5; 6]. In the United States of America (USA), PPPs play a key role in the development of innovative defence technologies, while in the EU countries they are used to finance joint projects on cyber defence and defence modernization [7; 8]. In the United Kingdom (UK), which is one of the leaders in the development of PPPs, cooperation between the public and private sectors contributes to the digitalization of security infrastructure and the development of cyber intelligence. In many countries, the use of PPPs in the defence sector is regulated by special legislative acts or directives. Much attention is paid to ensuring cybersecurity and confidentiality, and PPP procedures are adapted to the specific requirements of defence activities [9]. This allows the use of PPPs even in the most sensitive areas, such as the protection of critical infrastructure.

Ensuring national security is not reduced to defence aspects, but this direction is the most relevant for countries at war [10]. The use of PPPs in the defence sector of Ukraine is an objective requirement of today, when the country is at war and needs additional resources and expertise [11]. At the same time, the development of PPPs in Ukraine faces a number of problems, most of which are related to the lack of a clear legal framework for its application in the defence sector [13]. Existing legislative requirements do not meet current realities, the interaction between the state and the private sector is hampered by bureaucracy, lack of motivation and trust, and the absence of conditions for fair competition. Furthermore, the legislation does not take into account the real practice of interaction between the state and the private sector, such as volunteering. In the context of the issue under research, it is also worth noting that there is no special law in the legislation that would regulate the features of PPPs in the field of information security.

This study contains an analysis of the impact of PPP investments on socio-economic and security aspects in low- and middle-income countries, including Ukraine. This ensured the comparability of the results and the relevance of the conclusions for Ukraine. The aim of the study was to analyse the impact of PPPs on socio-economic and security aspects in low- and middle-income countries and integrate the experience of leading countries. The aim involves the fulfilment of the following research objectives:

- Study the correlation between the volume of investment in PPPs and socio-economic and security indicators of low- and middle-income countries;
- Conduct a regression analysis of the impact of investment in PPPs on socio-economic and security indicators of the countries;
- Provide recommendations based on the integration of the experience of leading countries.

The analysis conducted in the study involved testing the hypothesis that PPPs have an impact on strengthening the national security of the specified countries. The results confirmed the effectiveness and identify the key aspects that PPPs affect in the context of supporting the national security of countries. The study also analysed the experience of leading countries to develop recommendations based on successful practice. The novelty of the research is the identification of key aspects of national security that PPPs affect in low- and middle-income countries using mathematical modelling. The novelty is also the recommendations provided for the development of PPPs under martial law based on the integration of the results of mathematical analysis and the experience of leading countries. The study fills the gaps in previous research by providing empirical evidence on the impact of PPPs on socio-economic and security indicators in low- and middle-income countries, which are still poorly studied. The study also suggests universal directions for the development of PPPs, allowing the results to be extended to other countries, not limited to individual regions.

This study expands on previous work by systematically comparing empirical results with international literature on PPPs in security and information protection. By aligning and contrasting our findings with existing research, the manuscript ensures that readers can evaluate the validity of the results independently, without the need to consult earlier related publications.

Technical analysis of PPPs in the field of information security requires taking into account indicators of infrastructure reliability, bandwidth of ICT networks and efficiency of cryptographic protocols. A comparison of international practices shows that countries with high levels of digitalisation invest in secure data centres, while middle-income countries focus on incident monitoring and response systems. This approach suggests different levels of maturity of PPP models.

The novelty of this study lies in presenting empirical evidence on how PPP investments influence key security indicators in low- and middle-income countries. Unlike earlier approaches, the analysis applies regression models to quantify effects on logistics, military strength, and fire safety. Another novel aspect is the identification of the limited role of ICT-based PPPs in cybersecurity, despite their recognized importance. By combining statistical modelling with international comparison, the study offers a fresh perspective on PPPs under wartime and developing-country conditions.

2. LITERATURE REVIEW

A number of studies have identified PPP as an effective tool for strengthening national security, including information security. The authors [13] noted that PPP is considered as a solution to a number of problems related to security management, in particular, the protection of critical infrastructure from threats in wartime. Researchers believe that the development of PPP in Ukraine involves optimizing legislation and developing a transparent PPP mechanism. However, the authors' recommendations mainly concern only the legislative aspects of increasing the effectiveness of PPP. The researcher [11] analysed international experience in implementing PPP and noted that not all PPP models are designed for the specifics of the defence and security sector. Therefore, some of these models can be implemented only under conditions of effective control and supervision of private partners. In contrast to this view, the author [14] insists on the need to consolidate society to ensure the national security of Ukraine in wartime. The researcher considers it obvious to use all possible resources to strengthen the country's defence capabilities and resilience. At the same time, he emphasizes the need to improve the legislative framework by taking into account current realities and interests of all stakeholders. However, the mentioned studies lack empirical evidence of the impact of PPP on increasing defence capabilities and national security. The scientists [15] also believe that PPP is in the sphere of strategic interests of Ukraine and agree that the key problems of PPP development derive from imperfect legislation. Among the key problems, the researchers note the absence of a law on cybersecurity of critical information infrastructure. However, their study lacks a deep analysis of other areas of increasing the effectiveness of PPP, in addition to optimizing legislation. The authors [16] considered PPP as a key tool for ensuring the national security of the state. The researchers consider the full transition of PPP to online procedures to be the main direction for improving its administrative and legal regulation. The researchers' works provide an important theoretical basis for understanding the problems of PPP in Ukraine, but they lack empirical evidence of the effectiveness of PPP in the defence sector. The problems identified by the researchers mainly relate to the legislative framework, without taking into account other problematic aspects.

Other researchers have also noted the value of PPPs in the security and defence sector. The authors [17] reveal the benefits of PPPs in the security sector – increasing efficiency, effectiveness, improving relationships, creating learning opportunities, etc. However, the study is based on data from Belgian security actors, which limits the applicability of the findings to low- and middle-income countries. The study [18] explains that PPPs are the future of defence transformation, but the study focuses on the examples of Italy and Israel only. The specifics of the security environment and the level of development of cooperation with the private sector in these countries do not allow extrapolation of the results of the work to other countries.

The authors [19] and [20] examine the key objectives and risks of PPPs in ensuring the resilience of critical infrastructure. The main risks are: corruption, disasters of various origins, wars, terrorism, sabotage, overspending, lack of coordination, inadequate supervision, etc. However, the researchers' conclusions are based on the analysis of literature, without being supported by empirical analysis. The researcher [21] noted the effectiveness of PPP in infrastructure development using the case of India as a developing country. However, the study does not explore how PPP affects other aspects of ensuring national security.

The author [22] provides data on the role of PPPs in national cybersecurity strategies of NATO countries. However, the study does not determine how the effectiveness of such strategies and the level of cybersecurity provision actually change through PPPs. The authors [23] and [24] explored the role of PPPs in strengthening protection against cyber threats in European countries. The authors [23] focused on EU countries, [24] — on the Western Balkans. The researchers concluded that PPPs are effective in improving cybersecurity for both leading and less developed countries. However, the researchers' results may have limited applicability to other countries due to regional specifics.

Technical analysis of the literature demonstrates the lack of a unified approach to evaluating the effectiveness of PPPs in the field of cyber protection. Some studies use quantitative metrics, including

Mean Threat Detection Time (MTTD) and Mean Response Time (MTTR). Others limit themselves to legal analysis without considering network security performance indicators. This creates a gap between theoretical findings and the practical evaluation of results.

The literature review shows that despite a significant number of studies on the impact of PPPs on national security and defence, there is a lack of empirical evidence of such an impact in the works. Most of the studies focus on a single region or country, which limits the applicability of the results to other states. This indicates the need to continue the research, as they were not enough to deeply understand the actual impact of PPP investments on national security. The first part of the author's study involves analysing the impact of PPPs on socio-economic and security indicators of countries with low and medium levels of development based on empirical data from the countries. The second part of the study identifies universal directions for the development of PPPs in the field of information security using the example of developed countries, thereby filling the identified gaps.

3. METHODOLOGY

3.1. Research design

The first stage of the study was the selection of indicators and countries for analysis, as well as the collection and cleaning of data. The second stage was data analysis using appropriate mathematical methods for a sample of low- and middle-income countries. The third stage involved a statistical analysis of indicators of developed countries using the example of some European countries and highlighting universal directions for the development of PPPs. The fourth stage involved drawing conclusions and providing recommendations based on the results of the study.

3.2. Sample

The main sample of countries included the states with low and medium levels of development, which makes the results of the analysis more relevant to Ukrainian realities. An additional criterion for selecting countries was the availability of data on the volume of investments in PPP projects and other relevant indicators. As a result, the main sample included 33 countries: *Albania, Algeria, Argentina, Bangladesh, Bosnia and Herzegovina, Brazil, Cambodia, China, Colombia, Dominican Republic, Ecuador, El Salvador, Georgia, Guatemala, Honduras, India, Indonesia, Jordan, Kazakhstan, Malaysia, Mexico, Mongolia, Morocco, Nicaragua, North Macedonia, Pakistan, Paraguay, Philippines, Russian Federation (RF), Sri Lanka, Tajikistan, Tunisia, Ukraine.*

The additional sample included some developed European countries — *Belgium, Germany, France, the Netherlands, the UK*. The choice of these countries is justified by their leading positions in terms of the volume and number of PPP projects in the defence sector, which indicates their successful experience that can be adapted by less developed countries. The selection of indicators for the main sample of countries was formed by:

- the volume of cumulative investments in PPP projects for 1999–2023;
- socio-economic and security indicators for 2025 [25; 26; 27].

The time lag between investment and performance indicators makes it possible to assess the delayed effect of PPP on the socio-economic and security state of countries. The choice of a long-term analysis period (1999–2023) is determined by the nature of defence projects, which are often implemented over 10–20 years. A shorter period would not reflect the full impact of PPPs and could distort the results because of temporary crises. The chosen time interval also allows for a more accurate identification of long-term trends and cycles. The following indicators were analysed for an additional sample of countries (developed European countries):

- ratio of investments in PPP projects in the ICT sector to other areas [25];
- total value and number of PPP projects in the defence sector in European countries since 1994 [28];
- structure of types of defence PPP projects by value [1];
- structure of types of defence PPP projects by number [1].

3.3. Methods

The paper employed a statistical analysis to compare the studied middle- and low-income countries in terms of the volume of investment in PPPs. Statistical analysis was also used to study the structure and comparison of data on PPPs in developed countries. The method of correlation analysis identified which socio-economic and security indicators are closely correlated with the volume of investment in PPPs in low- and middle-income countries. The method of regression analysis was used to analyse the impact of investment in PPPs on socio-economic and security indicators. The quality of the models was checked by the F-test of model significance and tests for multicollinearity (Variance Inflation Factor (VIF)), heteroscedasticity

(Breusch-Pagan), autocorrelation (Durbin-Watson), and normality of residuals (Shapiro-Wilk).

To improve the study accuracy, correlation models were tested for multicollinearity using VIF, and the adequacy of regression models was tested using the F-test. In addition, a residue analysis was carried out using the Shapiro-Wilk test to confirm normality. This made it possible to guarantee the statistical stability of the obtained results and exclude accidental data distortions.

The study design follows a quantitative, cross-country comparative approach using secondary data for 1999–2023 PPP investments and 2025 outcome indicators. Concepts of interest were operationalized into measurable indicators. Public–private partnership (PPP) investment was defined as the cumulative financial value of completed projects reported in the World Bank PPP database. Logistics was captured through the international logistics performance index. Military strength was measured using the Global Firepower composite score, inverted to reflect greater strength with lower index values. Fire-risk quality was operationalized via the FM Global Resilience Index. Cybersecurity was assessed through international indices of cyber maturity and exposure. This operationalization ensured comparability across countries and allowed regression modelling of the hypothesized effects.

3.4. Hypotheses and conceptual model

The authors test the overarching hypothesis that public–private partnership (PPP) investment strengthens national security–relevant capacities in low- and middle-income countries via infrastructure and capability effects with a time lag. We specify four testable hypotheses: H1 (Logistics): higher cumulative PPP investment is associated with higher logistics performance. H2 (Military strength): higher cumulative PPP investment is associated with greater military strength (noting the inverse scale of the index). H3 (Fire risk quality): higher cumulative PPP investment is associated with higher fire-risk quality. H4 (Cybersecurity): higher cumulative PPP investment is associated with higher cybersecurity maturity.

The conceptual model assumes PPP investment operates through proximate channels -modernization of assets, maintenance financing, contractor know-how, and risk-management practices - leading to improvements in logistics, readiness, and safety. Effects are moderated by country context (governance capacity, conflict intensity, and the share of ICT within PPPs) and lagged due to project implementation cycles. The therefore relate 1999–2023 cumulative PPP investment to 2025 outcome indicators to capture delayed impacts. Linear models estimate the direction and magnitude of association, with diagnostics for specification and residual behaviour as reported above.

4. RESULTS

Assessing the impact of PPP investments on socio-economic and security factors in low- and middle-income countries

The level of PPP development, as well as the approaches to its implementation, vary significantly across countries. Key differences include different approaches to legislative definition and regulation, varying degrees of private sector involvement, and different priority sectors. This may be the result of a variety of factors, including available economic opportunities, government priorities, institutional capacity, investment attractiveness, etc. Accordingly, the volume of investment in PPPs varies significantly, as evidenced by statistical data on the amount of investment in PPP projects (Figure 1).

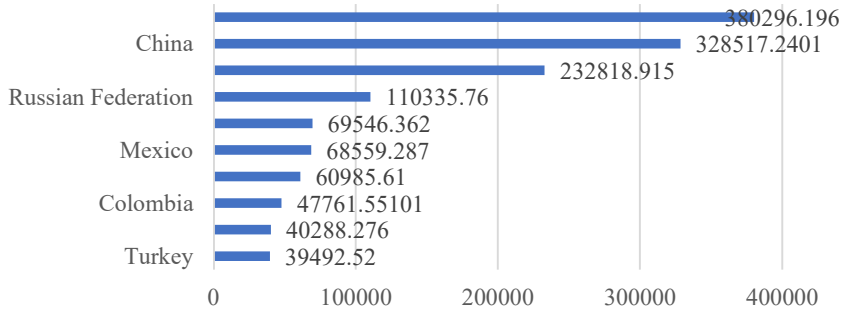

Figure 1: Top 10 countries surveyed by total investment in PPP projects for 1999-2023

Source: calculated and graphed by the author based on [25]

The criterion for inclusion in the sample of the studied countries was belonging to low- and middle-income countries. Therefore, Figure 1 does not include such world leaders in the field of PPPs as, for example, the UK. This approach ensured better comparability of countries and the relevance of the analysis results for Ukraine. Figure 1 shows Brazil, China and India had the highest level of investment in PPPs that among low- and middle-income countries. PPP projects in these countries are implemented mainly in the transport and infrastructure sectors, and the energy sector.

As noted above, the development of PPPs in countries can be determined by various factors. However, it is also possible to assume an inverse relationship: the volume of PPPs can affect various macroeconomic indicators. This assumption can be tested by analysing the relationship between the volume of investment in PPPs and a number of macroeconomic indicators. This will give grounds for making assumptions about the impact of PPP development (depending on its financing) on various political, economic, social, security, and other aspects. Table 1 presents the results of the correlation analysis between the volume of investment in PPPs for the sample of studied countries and selected macroeconomic indicators.

Table 1: Results of the correlation analysis between the volume of investment in PPPs for the sample of studied countries and socio-economic and security indicators

Indicator	Sum of Total Investment
Productivity	0.154686
Health Expenditure	0.120125
Education	0.060655
Inflation	0.077231
Political Risk	-0.18815
Control of Corruption	0.159332
Energy Intensity	-0.26097
GHG Emissions	-0.02085
Water Stress	0.032532
Urbanization Rate	-0.13802
Logistics	0.603578*
Internet Usage	0.028331
Climate Risk Exposure	-0.24501
Climate Risk Quality	0.099337
Climate Change Exposure	-0.2327
Seismic Risk Exposure	0.292776
Fire Risk Quality	0.446485*
Cybersecuirty	0.341872*
Military Strength	-0.53917*

Source: calculated by the author based on [25; 26; 27]

**statistically significant relationship*

The results of the correlation analysis show that there is a statistically significant moderate and medium relationship between the investment volume and the Logistics, Fire Risk Quality, Cybersecurity, Military Strength indicators. A "minus" sign in front of the correlation rate with Military Strength is explained by the fact that this indicator is inverse: the lower the value, the higher the military strength. Accordingly, it can be stated that the relationship with all indicators is in fact direct: the growth of PPP investments is accompanied by the development and improvement of indicators. It can be assumed that the development of relevant areas that are critical for national security (logistics, fire safety, cybersecurity,

military strength) depends to a certain extent on PPP investments. A more in-depth analysis of the relationship between these indicators was carried out using the multiple linear regression method. The dependent indicators in the regression models were Logistics, Fire Risk Quality, Cybersecurity, Military Strength, and the independent indicator was the volume of investment in PPPs. Table 2 presents the results of the regression analysis.

Table 2: Results of the regression analysis of the impact of the total volume of investment in PPPs

	Coefficients	*Std Err*	*LCL*	*UCL*	*t Stat*	*p-value*	*H0 (5%)*	*VIF*	*TOL*	*Beta*
Dependent variable – Military Strength; *R* = 0.5392, *Adjusted R-Squared* = 0.2678										
Intercept	1.6334	0.1616	1.3038	1.9630	10.1068	2.4851E-11	*Rejected*			
Sum of Total Investment	-0.000006	1.6013E-6	-8.9737E-6	-2.4420E-6	-3.5645	0.0012	*Rejected*	1.0000	1.0000	-0.5392
Dependent variable – Logistics; *R* = 0.6036, *Adjusted R-Squared* = 0.3438										
Intercept	27.3129	2.3953	22.4276	32.1981	11.4026	1.2752E-12	*Rejected*			
Sum of Total Investment	0.0001	2.3733E-5	5.1629E-5	0.0001	4.2149	0.0002	*Rejected*	1.0000	1.0000	0.6036
Dependent variable – Fire Risk Quality; *R* = 0.4465, *Adjusted R-Squared* = 0.1735										
Intercept	25.4742	4.1117	17.0883	33.8602	6.1955	7.0440E-7	*Rejected*			
Sum of Total Investment	0.0001	4.0739E-5	3.0094E-5	0.0002	2.7782	0.0092	*Rejected*	1.0000	1.0000	0.4465

Source: calculated by the author based on [25; 26; 27]

The model for Cybersecurity did not reveal a statistically significant relationship between the variables and was excluded from further analysis. In contrast, the models for Military Strength, Logistics, and Fire Risk Quality showed that the amount of investment in PPPs can have a statistically significant impact on the dependent variables. It should be noted that the resulting models have moderate explanatory power, and therefore their use for predicting the dependent indicator is limited. However, the models provide an idea of the strength and direction of the influence of the independent variable on the dependent indicators. Moreover, they show to what extent the change in the level of these indicators can be explained by the volume of investment in PPPs. So, the following conclusions can be drawn from the results of the regression analysis:

- an increase in investment in PPP by $1 million causes an increase in the Logistics indicator by 0.0001, with the change in the amount of investment explaining more than 34% of the variation in this indicator;

- an increase in investment in PPP by $1 million causes an increase in the Military Strength indicator by 0.000006, with the change in the investment volume explaining about 27% of the variation in this indicator;

- an increase in investment in PPP by $1 million causes an increase in the Fire Risk Quality indicator by 0.0001, with the change in the investment volume explaining about 17% of the variation in this indicator.

So, the volume of investment in PPPs in in low- and middle-income countries plays a significant role in the development of logistics, increasing military strength, and ensuring fire safety. However, despite the identification of a certain correlation with cybersecurity, the impact of the volume of investment in PPPs on this indicator was not confirmed by regression analysis. Cybersecurity is a critically important component of information security, as it prevents malicious interference in information systems and ensures the protection of classified data. Accordingly, the results of the analysis show that despite the significant role of PPPs in ensuring certain aspects of national security, the information security sector remains underrepresented among investment priorities. Figure 2 shows the ratio of total investment in PPPs in the studied countries to investment in ICT projects.

Journal of Theoretical and Applied Information Technology
15th December 2025. Vol.103. No.23

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

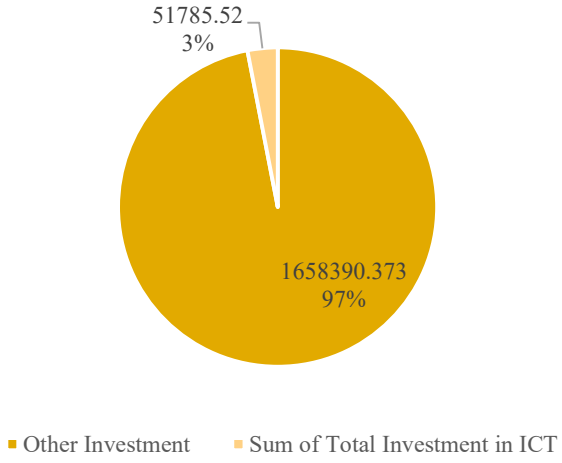

Figure 2: Ratio of investment in PPP projects in the ICT sector to investment in other PPP projects

Source: calculated and graphed by the author based on [25]

Figure 2 shows that the share of investments in PPP projects in the ICT sector is only 3%. It should be noted that ensuring information security may involve investments in other areas (critical infrastructure, energy, etc.). However, ICT projects are one of the key indicators of digital development to counter information threats. The low share of such projects in total investments in the PPP sector confirms that ensuring information security, in particular, cybersecurity, is not a priority for PPPs.

International experience in using PPPs in the defence sector

The results of the analysis of the impact of PPP investments on the socio-economic and security indicators of low- and middle-income countries should be analysed through the prism of the experience of developed countries. In particular, the case of European countries will help to identify the prerequisites for the successful implementation of large PPP projects in the field of infrastructure, cybersecurity, and defence. First of all, it is worth noting that not all European countries are actively developing PPPs, especially in the defence sector. Figure 3 shows PPP investments in the defence sector for the Europe's leading countries in this field.

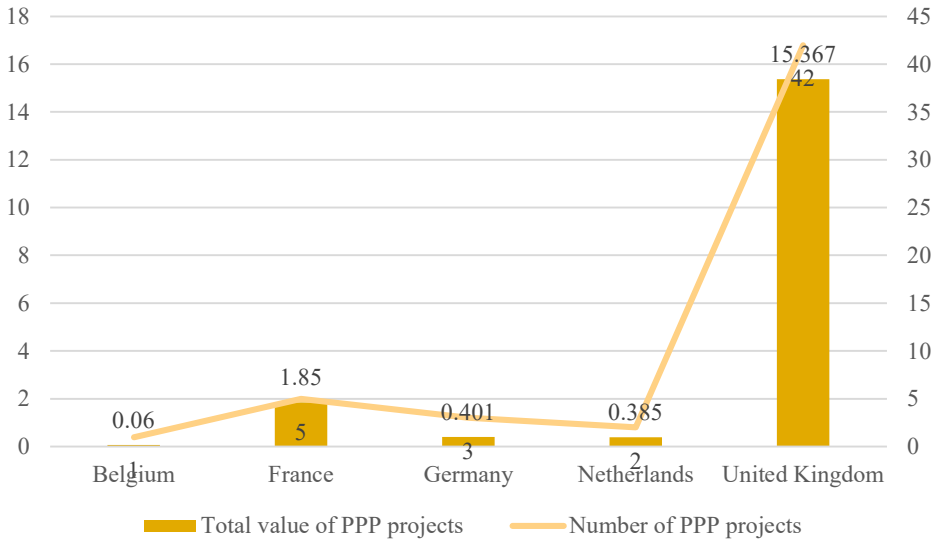

Figure 3: Total value and number of PPP projects in European countries in the defence sector for 1994-2021, milliard euros

Source: graphed by the author based on [28]

Journal of Theoretical and Applied Information Technology
15th December 2025. Vol.103. No.23

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Figure 3 shows that the UK is the absolute leader among European countries in terms of investment in PPPs and the total number of PPP projects in the defence sector. The country's successful projects in the field of cybersecurity include the Industry 100 (i100) and the Cyber Security Information Sharing Partnership (CiSP). The i100 ensures the integration of talent from the public and private sectors into the work of the National Cyber Security Centre (NCSC), identifying systemic vulnerabilities and reducing the impact of cyberattacks. CISP is a platform for cybersecurity professionals in the United Kingdom, where they can collaborate on cyber threat information in a secure and confidential environment. Moreover, the UK's experience proves that private sector participation is possible even in the creation of the most sensitive military infrastructure. An example of this is the headquarters of the UK's Intelligence, Security and Cybersecurity Agency [1].

The technical distribution of projects in the PPP area shows a different cost structure between countries. High-cost infrastructure facilities dominate the UK, while France and Germany have a greater focus on digital data exchange platforms. Comparative analysis shows that the increase in the share of ICT projects correlates with a higher index of cyber stability of the state.

In general, infrastructure and equipment are the main categories of expenditure for which PPPs are commonly used in the security and defence sector in European countries. However, long-term maintenance costs are usually included in the PPP agreement, so the potential for PPPs is greater than infrastructure costs alone [1]. Figure 4 shows the distribution of defence PPP projects by value in European countries.

Figure 3 shows that the largest shares of investment in PPP projects in the defence sector are for the construction of premises, equipment, headquarters. The share of ICT is 10%, which is a significantly higher value compared to low- and middle-income countries. Figure 4 shows the distribution of PPP projects in the defence sector of European countries by number. As Figure 4 illustrates, the largest shares of investment in PPP projects in the defence sector are directed for the construction of premises, equipment, headquarters. The share of ICT is 10%, which is a significantly higher value compared to low- and middle-income countries. Figure 5 shows the distribution of PPP projects in the defence sector of European countries by number.

Figure 4: Types of PPP projects in the field of defence in European countries by cost

Source: graphed by the author based on [1]

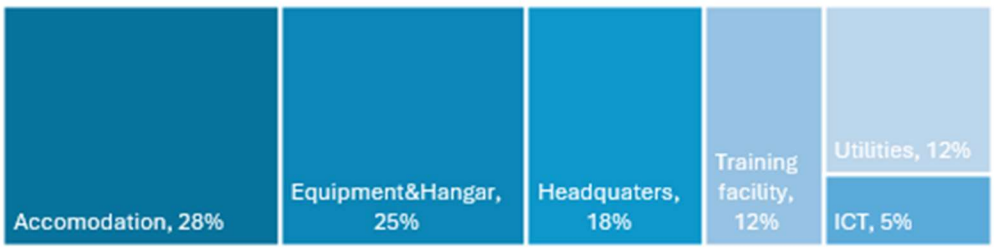

Figure 5: Types of PPP projects in the field of defence in European countries by number

Source: graphed by the author based on [1]

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Figure 5 shows that projects for the construction of premises, equipment, headquarters also predominate in number. The share of projects related to training centres or training facilities is somewhat smaller. The share of projects in the ICT sector is the lowest in number – 5%. This state of affairs may be explained by certain problems typical of PPPs in the defence sector. In particular, lack of trust, weak rule of law, imperfect legislative framework, limited resources, insufficient coordination and motivation [29]. The United Nations Office on Drugs and Crime identifies the following opportunities and approaches for the development of PPPs in the fight against cybercrime (Figure 6). In addition to the opportunities shown in Figure 5, the principles that should be followed to develop effective approaches to PPP development are worth noting. These are trust-building, demand-driven, multi-stakeholder engagement, inclusiveness, human rights, regional coordination, voluntariness, and adaptability [29]. The mentioned opportunities and principles are universal and can be adapted for any country, including low- and middle-income countries.

The analysis of correlation coefficients showed that logistics has the highest direct relationship with the PPP investment volume of all indicators. This suggests that technical infrastructure solutions, such as upgrading transport networks, are responding rapidly to changes in funding. In the case of fire safety, there is an average strength of communication, which is explained by the dependence on complex engineering solutions and local conditions of the country. For military strength, the correlation turned out to be reversed, but after the inversion of the scale, it can be interpreted as a direct positive effect. The technical interpretation shows that additional investments contribute to the growth of defence potential through the modernisation of weapons, management systems and the material and technical base.

The regression analysis confirmed that changes in logistics are explained by 34% by variations in PPP financing, which is a significant level of explainability. Military strength has a lower level of explainability, but confirms a stable relationship between financial resources and defence potential. Fire safety shows 17% of the variation explained, indicating the importance of systematic funding in the field of engineering protection. In the case of Cybersecurity, no significant dependence was found, which is presented by the low level of financing of ICT projects and the lack of investments in digital infrastructures.

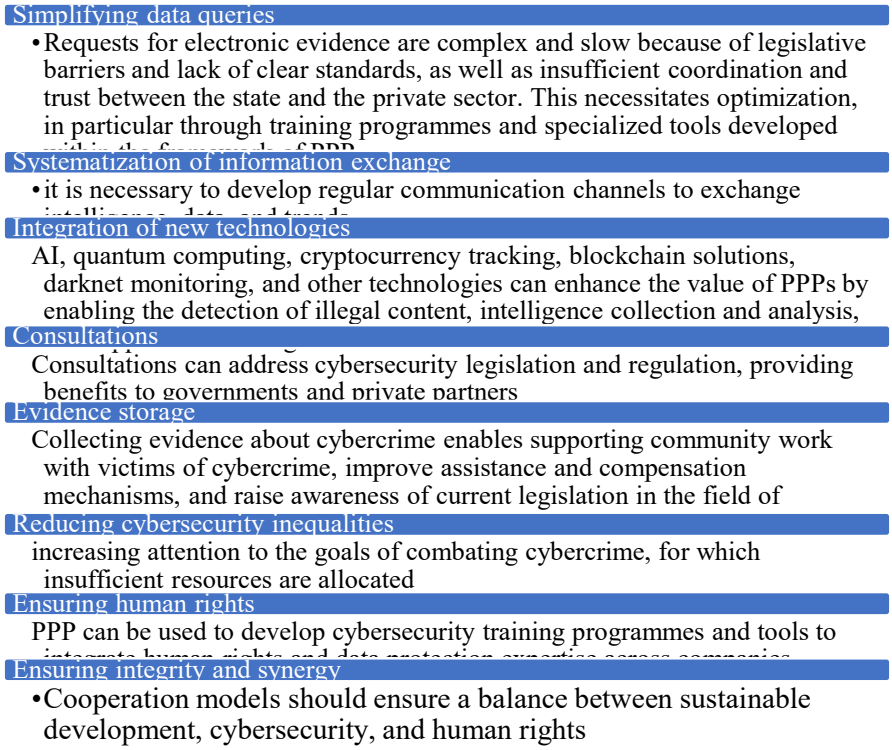

Figure 6: Opportunities and approaches for developing PPPs in the fight against cybercrime
Source: summarized by the author based on [29]

A comparison of indicators between low- and middle-income countries proved different technical priorities affecting the distribution of investment effects.

A comparison of the models shows that the regression coefficients for Logistics and Military Strength indicators differ in the magnitude of the effect, but remain statistically significant. For example, the elasticity of the Logistics indicator is higher, which confirms the greater sensitivity of the logistics infrastructure to the volume of investments. The technical analysis also found that the lack of significance for Cybersecurity is due to the low proportion of ICT projects among total investments.

5. DISCUSSION

Regression analysis showed a positive impact of PPP on security aspects, including the military potential of low- and middle-income countries. This emphasizes the importance of strategic investments in the PPP sector for strengthening Ukraine's national security. The described international experience in PPP development can provide valuable lessons for Ukraine, identifying specific priority areas of development.

The results of the study are confirmed in the papers of the authors [14] and [15], who note the effectiveness of PPP for strengthening Ukraine's national security in wartime. [16] hold a similar opinion, defining PPP as the main tool for guaranteeing the national security of the state. The author's study is based on the conclusions of [13], who consider PPP to be an effective way to solve the problems of ensuring the security of critical infrastructure. The study also takes into account the conclusions of [30] on the need to adapt and carefully use PPP models that exist in other countries in Ukrainian realities.

Based on interviews with public and private actors, the researchers [17] found that PPPs contribute to increased productivity and efficiency in the defence sector. The researchers' findings are valuable because they are based on the direct experience of practitioners. The value of our study is the availability of empirical evidence of increased efficiency through PPPs.

The authors [23] and [24] tested the hypothesis of a relationship between PPP participation and the effectiveness of protecting critical infrastructure from cyberattacks. The researchers found certain dependencies using the case of EU and Western Balkan countries. The impact of PPP investments on the level of cybersecurity was not confirmed in the author's study, despite finding a moderate correlation between PPP investments and cybersecurity. The differences can be explained by different samples – the author's study focuses on low- and middle-income countries from different parts of the world. The authors [31] examine the risks of PPP implementation in conflict zones using the case of Afghanistan. The researchers identify insufficient national security as one of the risks of PPP implementation. In contrast, our study considers ensuring national security as a key objective of PPP.

As in our study, the authors [32] studied PPPs in low-income or developing countries. The authors' conclusions are consistent with our findings that PPPs are used in these countries mainly in the infrastructure sector. However, the researchers studied the factors influencing PPPs, and not how PPPs affect socio-economic and security indicators.

From a technical point of view, the key difference of the study is the use of empirical data to form regression models. This made it possible to move from qualitative assumptions to quantitative hypothesis testing. The technical validation of the models provides the possibility to further use the results for predictive scenarios of the impact of PPPs on safety indicators.

The results of the analysis conducted in the study confirm the hypothesis that there is an impact of PPP investments on the national security of countries. Comparing the results of the author's research with the researchers' conclusions shows the practical value of the study. The practical value of the study is the provided empirical evidence of the impact of PPPs on the military strength and socio-economic indicators of low- and middle-income countries. The study also analyses the successful experience of developed countries and describes key areas of PPP development, which may be useful for Ukraine and other developing countries. The practical use of the results involves improving approaches to PPPs in Ukraine and other developing countries through the adaptation of the opportunities described in the study, based on international experience.

Hypothesis evaluation. Results support H1 (positive association with logistics, adjusted $R^2 \approx 0.34$) and H3 (positive association with fire-risk quality, adjusted $R^2 \approx 0.17$). H2 is supported when accounting for the inverse military-strength scale (negative coefficient implies greater strength; adjusted $R^2 \approx 0.27$). H4 is not supported; the non-significant cybersecurity result is consistent with the low ICT share in PPP portfolios and measurement differences. These outcomes align with the model's channels and moderators and explain where effects are strongest.

~~The limitations of the study relate to the lack of country-specific data on the volume of investment in PPPs, as well as incomplete information on investments in information security.~~

This study has several limitations that should be acknowledged. First, the analysis relies on secondary data sources that may vary in quality and completeness across countries. PPP investment values often differ depending on reporting standards, which may introduce inconsistencies. Second, the operationalization of security-related concepts, such as military strength, fire-risk quality, and cybersecurity, is based on composite indices. While widely used, these indices simplify complex realities and may not capture all relevant dimensions. Third, the regression models explain only part of the variation in the indicators, which means that additional unobserved factors, such as governance capacity, conflict intensity, and international support, also influence outcomes. Fourth, the study adopts a cross-country comparative design, which identifies associations but does not establish strict causality. Fifth, the focus on low- and middle-income countries limits the generalizability of results to highly developed economies with different PPP structures. Finally, incomplete or underreported data on ICT-related PPPs may underestimate the potential impact of such projects on cybersecurity.

5.1. Recommendations

Given the effectiveness of PPPs in strengthening the national security of countries, confirmed by the regression analysis, it is appropriate to provide practical recommendations for the development of PPPs in Ukraine. As the impact of PPPs on the cybersecurity of countries as a key component of information security was not confirmed, the recommendations should provide for increased attention to this area:

- adoption of legislation on PPPs in the field of defence and information security, adapted to the requirements of wartime;
- improvement of international coordination in the field of information exchange;
- implementation of international experience along with ensuring appropriate control to ensure data confidentiality and adaptation of international models to the realities of wartime;
- implementation of the latest technologies for the purposes of intelligence collection, threat monitoring, etc.

Our findings confirm the conclusions of earlier studies that PPPs contribute to strengthening national security in wartime conditions [14, 15, 16]. This is consistent with research emphasizing the role of PPPs in protecting critical infrastructure and increasing resilience [13, 17]. At the same time, differences appear when comparing results on cybersecurity. While Cappelletti & Martino [7] and Mihailović & Božović [24] demonstrated positive effects of PPPs in the EU and Western Balkans, our regression analysis did not confirm such an impact. The discrepancy can be explained by the sample of low- and middle-income countries, where ICT projects represent only 3% of PPP investments [25]. This contrast highlights both agreements and divergences with existing scholarship and underlines the originality of our contribution [32].

6. CONCLUSIONS

International experience confirms that PPP is successfully used in the field of ensuring national security of many countries, implementing projects in the field of energy security, infrastructure, defence, etc. The defence sector is the most relevant for Ukraine in view of the ongoing military operations in the country. The analysis conducted in the study proved the effectiveness of using PPP to increase military strength, improve logistics, and ensure fire safety in low- and middle-income countries. At the same time, the analysis did not reveal a significant impact of PPP on increasing cybersecurity in countries. Therefore, this direction requires increased attention. The study of international experience identified successful practices of using PPP for increasing national, in particular, information security. Key problems that hinder the development of PPP in the field of information security, as well as key areas and development opportunities were identified. This gave grounds to provide recommendations for Ukraine that can be used in practice to improve the legislative framework and shape defence strategies. Technical analysis showed that the most significant impact of PPP investments is recorded in logistics and military strength indicators. At the same time, the lack of effect in the field of cybersecurity indicates the need to change the financing structure. This means that the strategic development of PPPs should include targeted technical indicators such as the level of monitoring automation and the number of integrated early warning systems. Further research may focus on the elaboration of proposals for the development of PPPs in the defence sector of Ukraine through the use of specialized platforms for international coordination and information exchange.

REFERENCES:

[1] European Investment Bank, "PPP in Security and Defence", 2024, URL: https://www.eib.org/attachments/lucalli/20240222_100425_ppp_in_security_and_defence_en.pdf (date of access: 24.08.2025).

[2] D. Atstaja, V. Koval, J. Grasis, I. Kalina, H. Kryshtal & I. Mikhno, "Sharing Model in Circular Economy towards Rational Use in Sustainable Production", *Energies,* Vol. 15, No. 3, 2022, Article 939. https://doi.org/10.3390/en15030939

[3] T. Bashar, I. W. Fung, L. C. Jaillon & D. Wang, "Major Obstacles to Public-Private Partnership (PPP)-Financed Infrastructure Development in China", *Sustainability*, Vol. 13 No. 12, 2021, Article 6718. https://doi.org/10.3390/su13126718

[4] M. R. Karsayuda, M. Fadli, M. Khusaini & A. Kusumaningrum, „Legal Construction of Infrastructure Financing Based on Public Private Partnership to Realize National Resilience", *International Journal Of Humanities Education and Social Sciences*, Vol. 3, No. 1, 2023, pp. 353-364. https://doi.org/10.55227/ijhess.v3i1.563

[5] G. Rausser, E. Choi & A. Bayen, "Public–Private Partnerships in Fostering Outer Space Innovations", *Proceedings of the National Academy of Sciences*, Vol. 120, No. 43, 2023, Article e2222013120. https://doi.org/10.1073/pnas.2222013120

[6] V. Mani, A. Pomer, J. Korona-Bailey, M. Janvrin, C. L. Coles, A. J. Schoenfeld & T. P. Koehlmoos, "Supporting the Nation in Crisis: The Military Health System's Role in Enhancing Public Health Capacity through Public–Private Partnerships", *Health Research Policy and Systems*, Vol. 22, No. 1, 2024, Article 108. https://doi.org/10.1186/s12961-024-01203-w

[7] F. Cappelletti & L. Martino, "Achieving Robust European Cybersecurity through Public–Private Partnerships: Approaches and Developments", *Antonios Nestoras*, 2021, pp. 58-68. https://doi.org/10.53121/ELFDP3

[8] M. E. Singer, D. C. Hack & Jr D. F. Hanley, "The Power of Public–Private Partnership in Medical Technology Innovation: Lessons from the Development of FDA-Cleared Medical Devices for Assessment of Concussion", *Journal of Clinical and Translational Science*, Vol. 6, No. 1, 2022, Article e42. https://doi.org/10.1017/cts.2022.373

[9] J. M. Salomon, "Public-Private Partnerships and Collective Cyber Defence", In T. Jančárková, G. Visky, I. Winther (Eds.) *2022 14th International Conference on Cyber Conflict: Keep Moving!(CyCon),* IEEE, Vol. 700, 2022, pp. 45-63. https://doi.org/10.23919/CyCon55549.2022.9810912

[10] S. Bondarenko, A. Bratko, V. Antonov, R. Kolisnichenko, O. Hubanov & A. Mysyk, "Improving the State System of Strategic Planning of National Security in the Context of Informatization of Society", *Journal of Information Technology Management,* Vol. 14, 2022, pp. 1-24. https://doi.org/10.22059/jitm.2022.88861

[11] Y. Mekh, I. Georgiievskyi, I. Ignatchenko, T. Krasnopolska & I. Kostenko, „Public-Private Partnership in the Security Sector: Updating in the Conditions of Counteracting the COVID-19 and Armed Aggression in Eastern Ukraine", *Linguistics and Culture Review*, Vol. 5, No. S4, 2021, pp. 1653-1663. https://doi.org/10.21744/lingcure.v5nS4.1872

[12] L. Axon, J. Saunders, P. Esteve-González, J. Carver, W. Dutton, M. Goldsmith & S. Creese, "Private-Public Initiatives for Cybersecurity: The Case of Ukraine", *Journal of Cyber Policy*, Vol. 9, No. 3, 2024, pp. 399-422. https://doi.org/10.1080/23738871.2025.2451256

[13] O. R. Didych & M. M. Naumko, „The Concept and Essence of Public-Private Partnership in the Sphere of National Security of Ukraine", *Scientific Notes of the V. I. Vernadsky Taurida National University. Series: Public Management and Administration,* Vol. 34, No. 6, 2023, pp. 69-77. https://doi.org/10.32782/TNU-2663-6468/2023.6/12

[14] С. С. Кудінов, "Державно-Приватне Партнерство у Сфері Національної Безпеки – Сучасний Вимір для України", *Правничий Часопис*, 2023, сс. 108-114. https://doi.org/10.32850/sulj.2023.4.20

[15] O. R. Shevchuk & Y. M. Chornyi, „Administrative and Legal Regulation of Public-Private Partnership in the Field of Construction and Operation of Transport Routes in Ukraine", *Law Bulletin*, Vol. 19, 2024, pp. 127-133. https://doi.org/10.32850/LB2414-4207.2021.19.17

[16] L. Soroka, A. Danylenko, M. Sokiran, D. Levchenko & O. Zubko, „Public-Private Collaboration for National Security: Challenges

and Opportunities", *Amazonia Investiga*, Vol. 12, No. 70, 2023, pp. 43-50. https://doi.org/10.34069/AI/2023.70.10.4

[17] E. Van Goethem & M. Easton, "Public-Private Partnerships for Information Sharing in the Security Sector: What's in It for Me?", *Information & Security*, Vol. 48, 2021, pp. 1-15. https://doi.org/10.11610/isij.4809

[18] M. Pengili, "Examining the Potential of Public-Private Partnerships in Defence Policy: A Comparative Study of Italian and Israeli Partnerships' Epistemic Influences on Organisational Innovation", Doctoral dissertation, University of Leeds, 2024. https://etheses.whiterose.ac.uk/id/eprint/27005/

[19] G. Ampratwum, R. Osei-Kyei & V. W. Tam, „Exploring the Concept of Public-Private Partnership in Building Critical Infrastructure Resilience against Unexpected Events: A Systematic Review", *International Journal of Critical Infrastructure Protection*, Vol. 39, 2022, Article 100556. https://doi.org/10.1016/j.ijcip.2022.100556

[20] G. Ampratwum, V. W. Tam & R. Osei-Kyei, „Critical Analysis of Risks Factors in Using Public-Private Partnership in Building Critical Infrastructure Resilience: A Systematic Review", *Construction Innovation*, Vol. 23, No. 2, 2023, pp. 360-382. https://doi.org/10.1108/CI-10-2021-0182

[21] K. R. Prasad, S. R. Karanam, D. Ganesh, K. K. S. Liyakat, V. Talasila & P. Purushotham, „AI in Public-Private Partnership for IT Infrastructure Development", *The Journal of High Technology Management Research*, Vol. 35, No. 1, 2024, Article 100496. https://doi.org/10.1016/j.hitech.2024.100496

[22] A. M. Costea, "Private-Public Partnerships in Cyber Space as Deterrence Tools. The Trans-Atlantic View", *Europolity: Continuity & Change Eur. Governance*, Vol. 17, 2023, Article 111. https://doi.org/10.25019/europolity.2023.17.2.4

[23] M. Di Feo & L. Martino, "Public–Private Partnership (PPP) in the Context of European Union Policy Initiatives on Critical Infrastructure Protection (CIP) from Cyber Attacks", In *Governing Complexity in Times of Turbulence* (pp. 54-79). Edward Elgar Publishing, 2022. https://doi.org/10.4337/9781800889651.00014

[24] A. Mihailović & B. Božović, "Public-Private Partnerships for Inclusive Cyber Crisis Response in Developing Countries: Western Balkan Region", *Contemporary Pathways of European Local and Regional Development,* Vol. 135, 2024. https://doi.org/10.4335/2024.1.9

[25] World Bank. "Public Private Partnership (PPP) Data", URL: https://ppi.worldbank.org/en/ppidata (date of access: 24.08.2025).

[26] FM Global. "FM Global Resilience Index", URL: https://www.fm.com/resources/resilience-index (date of access: 24.08.2025).

[27] Global Firepower. "Countries Listing", URL: https://www.globalfirepower.com/countries-listing.php (date of access: 24.08.2025).

[28] European Investment Bank. "EPEC - European PPP Expertise Centre", URL: https://data.eib.org/epec/ (date of access: 24.08.2025).

[29] United Nations Office on Drugs and Crime. "Global Programme on Cybercrime: Civil Society Unit Report", 2024, URL: https://www.unodc.org/documents/NGO/PDF/CSU-CyberCrime-240807-WEB.pdf (date of access: 24.08.2025).

[30] Y. V. Mekh, "Legal View on the Concept of Optimum Models of Public-Private Partnership in the Security Sector of Ukraine", *Uzhhorod National University Herald. Series: Law*, Vol. 1, No. 80, 2023, pp. 507-512. https://doi.org/10.24144/2307-3322.2023.80.1.77

[31] E. Noorzai & M. ASCE, „Public–Private Partnership Risks in Conflict Zones and Solutions: Case Study for Afghanistan", *Journal of Infrastructure System*, Vol. 27, No. 1, 2021, Article 05021001. https://doi.org/10.1061/(ASCE)IS.1943-555X.0000599

[32] H. Yurdakul, R. Kamaşak & T. Y. Öztürk, "Macroeconomic Drivers of Public Private Partnership (PPP) Projects in Low Income and Developing Countries: A Panel Data Analysis", *Borsa Istanbul Review*, Vol. 22, No. 1, 2022, pp. 37-46. https://doi.org/10.1016/j.bir.2021.01.002