The subject of the study was the national cyber vulnerability of sovereign states in a context of geopolitical turbulence. The study addresses the lack of proven, multi-factor econometric tools that would enable an accurate quantitative assessment of the impact of macroeconomic instability and military conflicts on the overall level of institutional cybersecurity. The results of the study showed that armed conflicts create a strong nonlinear link with breaches of digital systems' information security, leading to a 10.2 percentage point increase in critical system vulnerabilities during periods of war. This was explained by the combined effect of the 'war multiplier' and the 'paradox of institutional inertia', as demonstrated by official Computer Security Incident Response Teams (CSIRTs) which were unable to protect systems due to a lack of adequate funding. The study showed that gross domestic product (GDP) acts as a protective factor, as every 1% increase in GDP leads to a 10.1% reduction in risk. The study's results were unique, as a pooled logit regression model with cluster-consistent standard errors was used to analyze panel data from 14 countries (n = 68), and the threshold values for cyberattacks were determined at the 75th percentile. The developed model was used to quantify the effect of detection bias during crisis situations. The mathematical framework of the developed model acted as a central element, enabling macroeconomic early warning systems to fully realize their potential in the allocation of defense resources and the protection of digital sovereignty

Keywords: national cybersecurity, panel logistic regression, geopolitical turbulence, cyber vulnerability, early warning systems

UDC 004.056.5:330.43:355.02
DOI: 10.15587/1729-4061.2026.363063

DEVELOPMENT OF A MULTIFACTORIAL ECONOMETRIC MODEL FOR ASSESSING A COUNTRY'S CYBERVULNERABILITY IN A CONTEXT OF GEOPOLITICAL TURBULENCE

Oleksandr Kushnerov
Doctor of Philosophy (PhD), Senior Lecturer
Department of Economic Cybernetics*
ORCID: https://orcid.org/0000-0001-8253-5698
Inna Tiutiunyk
Doctor of Economic Sciences, Head of Department
Department of Financial Technologies and Entrepreneurship*
ORCID: https://orcid.org/0000-0001-5883-2940
Serhii Yevseiev
Corresponding author
Doctor of Technical Sciences, Professor, Head of Department**
E-mail: Serhii.Yevseiev@gmail.com
ORCID: https://orcid.org/0000-0003-1647-6444
Ivan Opirskyy
Doctor of Technical Sciences, Professor, Head of Department
Department of Information Security
Lviv Polytechnic National University
S. Bandery, 12, Lviv, Ukraine, 79013
ORCID: https://orcid.org/0000-0002-8461-8996
Vladyslav Sokol
Candidate of Technical Sciences**
ORCID: https://orcid.org/0009-0009-9446-2049
Olena Voloshchuk
Candidate of Technical Sciences, Associate Professor
Department of Artificial Intelligence***
ORCID: https://orcid.org/0000-0002-5912-4126
Oleksandr Novoseletskyi
Candidate of Economic Sciences, Associate Professor
Director
Educational and Scientific Institute of Information Technology and Busines
National University of Ostroh Academy
Seminarska str., 2, Ostroh, Ukraine, 35800
ORCID: https://orcid.org/0000-0003-3757-0552
Yevhen Melenti
Doctor of Technical Sciences, Associate Professor, First Vice-Rector
National Academy of the Security Service of Ukraine
Mykhaila Maksymovycha str., 22, Kyiv, Ukraine, 03066
ORCID https://orcid.org/0000-0003-2955-2469
Iryna Husarova
Candidate of Technical Sciences, Associate Professor, Professor
Department of Applied Mathematics***
ORCID: https://orcid.org/0000-0002-1421-0864
Dmytro Balagura
Candidate of Technical Sciences, Associate Professor
Department of Information Technology Security***
ORCID: https://orcid.org/0009-0006-9839-3317
*Sumy State University
Kharkivska str., 116, Sumy, Ukraine, 40007
**Department of Cybersecurity
National Technical University "Kharkiv polytechnic institute"
Kyrpychova str., 2, Kharkiv, Ukraine, 61002
***Kharkiv National University of Radio Electronics
Nauky ave., 14, Kharkiv, Ukraine, 61166

Received 10.03.2026
Received in revised form 18.05.2026
Accepted 27.05.2026
Published 26.06.2026

How to Cite: *Kushnerov, O., Tiutiunyk, I., Yevseiev, S., Opirskyy, I., Sokol, V., Voloshchu, O., Novoseletskyi, O., Melenti, Y., Husarova, I., Balagura, D. (2026). Development of a multifactorial econometric model for assessing a country's cybervulnerability in a context of geopolitical turbulence. Eastern-European Journal of Enterprise Technologies, 3 (4 (141)), 32–43. https://doi.org/10.15587/1729-4061.2026.363063*

1. Introduction

During the first twenty-one years of the 21st century, cyberspace has established itself as the fifth domain of warfare, leading to the creation of a new global security system [1, 2]. Asymmetric warfare is based on digital operations that state actors and their proxies use to covertly shift the global balance of power by attacking critical infrastructure systems [3].

The hybrid 'grey zone' that exists between traditional diplomacy and modern warfare creates an environment in which cyberattacks inflict significant financial damage on national economies. Strategic defense planning faces serious obstacles, as there are no comprehensive econometric tools for assessing a state's cyber-vulnerability at the national level.

The creation of a robust national cyber defense system requires an institutional framework, as national Computer Security Incident Response Teams (CSIRTs) achieve their objectives through the implementation of international security standards [4]. The basis for cyber defense operations and the allocation of defense resources stems from macroeconomic indicators shaped by an unstable geopolitical situation. The lack of proven mathematical models demonstrating how military pressure affects cyber vulnerability complicates strategic planning. The relationship between macroeconomic variables and cyber threats creates a two-way interaction that gives rise to endogeneity issues, the resolution of which requires advanced econometric modelling methods [5, 6]. Military conflicts create systematic data distortions, leading to an artificial increase in the number of reported incidents due to heightened monitoring. Existing econometric tools require improvement, as the current reactive approach to management has reached its limits in combating cyber vulnerability.

Data analysis requires a comprehensive study to move from descriptive categories to formal statistical modelling, as the Internet of Things threat assessment system [7] does not allow to demonstrate how human actions affect the resilience of national security [8, 9]. Current methods do not show how economic changes and military attacks affect the likelihood of a cyber intrusion. Economic indicators demonstrate that a stable business environment, coupled with GDP growth, creates a protective environment that supports security stability [10, 11], but military conflicts lead to increased security risks. The variables demonstrate non-linear relationships with levels of institutional readiness, which requires the development of a multi-factor econometric model using logistic regression analysis.

Those involved in cybersecurity are forced to rely on heuristic risk management methods, as they lack access to reliable analytical tools. Proactive resource allocation requires a mathematical basis, which economists can provide using econometric forecasting models [12]. Taking the factor of geopolitical turbulence into account adapts the defense architecture to the conditions of asymmetric warfare, and a quantitative assessment of costs and benefits is critical for early warning systems [13]. In view of this, the development of a multi-factor econometric model for assessing a state's cyber vulnerability forms the scientific basis for making informed management decisions and ensuring digital sovereignty, which confirms the relevance of the study.

2. Literature review and problem statement

Contemporary research into national security points to the adoption of a fundamental approach that views cyberspace as a complex system of technical, geopolitical and economic competition. The beginning of the 21st century was marked by a transformation in military tactics, with cyber influence being identified as the fifth domain of warfare. An analysis of foundational works demonstrates the evolution of methodology from basic descriptions to complex systems; however, a number of unresolved scientific problems remain. In [1], data on cyberattacks during military operations are systematized to demonstrate how digital threats have developed at the macro level; however, the study does not present a mathematical model showing how these threats affect state resilience. The study [2] resolves discrepancies in the conceptual basis for assessing cybersecurity; however, the authors limit themselves to qualitative analysis, without proposing econometric tools for measuring risks. The study in [3] expands knowledge of technical threats by examining radio frequency jamming, which countries use as a geopolitical weapon; however, it does not consider the devastating economic consequences of such vulnerabilities. The work in [4] establishes the fundamental principles unifying NIST and ISO security standards, but the facts on the ground show that this institutional system is unable to protect infrastructure, as formal regulatory barriers do not apply in conflict zones.

The development of econometric tools requires collaboration between teams representing different academic disciplines. In the study [5], panel logistic regression is used to successfully forecast financial defaults, whilst in [6], panel data is employed to assess vulnerabilities in the agricultural sector. The main drawback of these studies is that their specific models do not meet the operational needs of military cyber operations during a period of geopolitical change. Identifying specific threat vectors, including risks associated with the Internet of Things (IoT) [7] and human-factor-related threats [8], improves our understanding of incident characteristics, but these research projects operate at a local technical level, which prevents them from being scaled up to national-level applications. Study [9] shows that organizations must cooperate at an international level, yet it does not provide answers as to how defense systems should adapt to military upheavals.

National security is directly dependent on the macroeconomic factors that determine the country's current state. Study [10] demonstrates how geopolitical factors influence the stability of the business environment, whilst work [11] examines the impact of military conflicts on e-commerce activities. These works do not consider two important elements of cybersecurity, namely endogeneity and detection bias in crisis situations. In the study [12], logistic regression is presented as a method for detecting vulnerabilities, but this tool proves effective only against local attacks (SQL injections), which makes it unsuitable for use in large systems. The research article [13] provides an economic justification for investment, noting that cost-benefit analysis is the only available method for assessing infrastructure risks. The study [14] analyses the impact of artificial intelligence on international relations; however, the researchers did not develop any econometric models to forecast these consequences.

A systematic analysis of the identified shortcomings shows that the available mathematical resources exist in the form of isolated fragments that lack proper methodological organization. The technical methods presented in references [7, 12], as well as the qualitative policy studies from reference [2], do not allow for a quantitative assessment of hidden threats using macroeconomic analysis. The modern econometric models presented in [5] and [6] do not account for changes in detection conditions that occur in wartime.

The main problem, therefore, is that there is currently no comprehensive mathematical framework that integrates macroeconomic indicators with data on military operations and measures of institutional resilience to forecast digital risks using quantitative methods. To address this problem,

a multi-factor econometric model is required that will enable the assessment of a state's degree of cyber-vulnerability during periods of geopolitical instability, and the development of such a model is the aim of this study.

3. The aim and objectives of the study

The aim of the study is to develop a multifactorial econometric model for assessing a state's cyber vulnerability in a context of geopolitical turbulence. This will enable early warning systems and relevant national security bodies to strategically reallocate resources based on predictive analysis of the risks of digital compromise.

To achieve this aim, the following objectives were set:

– to compile a representative dataset covering 14 countries in Central and Eastern Europe, the Baltic states and Western Asia for the period from 2019 to 2023, combining macroeconomic indicators, metrics of military activity and indicators of institutional readiness (in particular, the presence of a CSIRT);

– to develop a specification for the pooled logit model and ensure its validation using cluster-robust standard errors and time lags between predictor variables in order to mitigate the effects of endogeneity and detection bias;

– to model scenarios of the military multiplier effect, assessing accuracy via the AUC-ROC, verifying parameter stability using VIF, and detecting anomalies using the Mahalanobis distance.

4. Materials and methods

The subject of the study was the national cyber vulnerability of sovereign states in a context of geopolitical turbulence.

The hypothesis of the study was based on the assumption that there is a synergistic effect resulting from the combined impact of military shocks and macroeconomic instability. It was anticipated that this combined impact would exponentially increase the likelihood of a critical digital compromise of the state's information systems.

The study was based on a number of fundamental assumptions that defined its operational scope. The spatio-temporal analysis was limited to the period 2019–2023. The empirical calculations were based on official data regarding large-scale incidents that led to critical data security breaches. To assess institutional resilience, only the activities of official state institutions were taken into account. The shadow cybersecurity sector remained outside the scope of the econometric modelling.

The methodological framework of the study was developed using econometric methods, which involved the analysis of panel data in accordance with an established methodology [5, 6]. This method enabled the researchers to combine spatial differences between the observed entities with the temporal changes occurring in their indicators. The design of the empirical study covered 14 sovereign states in Central and Eastern Europe (CEE), the Baltic states and Western Asia. The choice of this region was theoretically justified [1]. These territories were situated in a zone of active or latent geopolitical tension [3]. The selected time period made it possible to record the transitional states of national security systems. The phases before, during and after acute military conflicts were studied [1, 11].

The process of building the empirical database required the implementation of a complex algorithm for synthesizing heterogeneous datasets. The initial data set (14 countries over 5 years, $n = 70$), following the application of a procedure to remove statistical gaps using the listwise deletion method, resulted in a final unbalanced sample of 68 observations. This method was a necessary condition that enabled the logistic model to achieve the required statistical power [6]. The World Bank determined the macroeconomic component based on the official statistical data it maintains. The researchers obtained data on institutional stability and the frequency of incidents by analyzing global information security databases, which serve as specialized sources of information [7].

The main process involved constructing a binary dependent variable, Yit, which served as the basis. This variable determines the extent to which a country experiences significant cyber-vulnerability over a given period of time. The specific nature of digital threats lay in the fact that the distribution of data breach incidents did not follow a normal Gaussian distribution. The data showed signs indicating the presence of a distribution with fat tails [13]. The vast majority of incidents were of minor scale. The study showed that isolated targeted attacks caused serious loss of information, resulting in significant losses for the organization [1, 12].

Using the statistical method I applied to determine the vulnerability thresholds, the 75th percentile of data leakage volumes was established, resulting in 383,218 records in the dataset. Given the significant right-skewed asymmetry of the empirical distribution (median – 98,548 records, maximum value – 8,768,066), dichotomization allowed to filter out noisy micro-incidents. To mitigate the problem of information loss and ensure the robustness of the estimates, alternative classification thresholds (the 70th and 80th percentiles) were additionally tested in the study. All other background threat states were identified as $Y_{it} = 0$. This approach filtered out noise micro-incidents from large-scale attacks [12]. Recognizing the problem of confounding the absolute number of leaks with the size of the state, a robustness check was included. This involved normalizing the number of leaks by population size.

The pooled logit specification was used to quantify the probability [5, 12]. The choice of this tool was based on the need to solve a non-linear classification problem. The fundamental advantage of the logistic function over the linear probability model (LPM) lay in the mathematical constraints. The predicted values were strictly limited to the interval from zero to one. This was perfectly consistent with the axioms of probability theory [5]. The basic mathematical specification of the complex model took the following form

$$P\left(Y_{it}=1|X_{it}\right)=\frac{1}{1+e^{-\left(\begin{array}{c}\beta_0+\beta_1\mathrm{WAR}_{it}+\beta_2\mathrm{POSTW}_{it}+\beta_3\mathrm{CSIRT}_{it}+\\+\beta_4\mathrm{GDP}_{i,t-1}+\beta_5\mathrm{INF}_{i,t-1}+\beta_6\mathrm{UNEMP}_{i,t-1}+\epsilon_{it}\end{array}\right)}}, \quad (1)$$

where the left-hand side of the equation represents the logarithm of the probability of a cyber vulnerability occurring in a country i during the period t; $\mathrm{WAR}_{i,t}$ and $\mathrm{POSTW}_{i,t}$ – binary indicators of the active phase of an armed conflict and post-war recovery, respectively; $\mathrm{CSIRT}_{i,t}$ – binary performance indicator for the accredited national response team; $\mathrm{GDP}_{i,t-1}$, $\mathrm{INF}_{i,t-1}$, $\mathrm{UNEMP}_{i,t-1}$ – vectors of macroeconomic control variables (annual gross domestic product growth rate, inflation rate and unemployment rate, respectively), which are included in the specification with a one-year time lag ($t - 1$) to mitigate the effects of endogeneity and reverse causality; β_0 – free term of the regression; β_1, ..., β_6 – model parameters to be estimated.

To account for specific cross-country heterogeneity, an alternative specification of random-effects logistic regression (RE-Logit) was additionally tested. As the empirical

analysis is limited to a small number of spatial clusters ($N = 14$), a small-sample correction (CR2) was applied to calculate reliable standard errors, ensuring asymptotic unbiasedness and the validity of statistical inference.

Data on the functioning of the institutional factor $CSIRT_{i,t}$ were verified against the official registers of the Forum of Incident Response and Security Teams (FIRST) and the European Union Agency for Cybersecurity (ENISA) [4]. The block of macroeconomic control factors ($GDP_{i,t-1}$, $INF_{i,t-1}$, $UNEMP_{i,t-1}$) captures the impact of overall economic well-being on the capacity to fund the national defense system and the protection of cyberspace [10, 11].

The unknown parameters β were estimated using an iterative maximum likelihood estimation (MLE) algorithm [5, 6]. Unlike the ordinary least squares (OLS) method, the MLE algorithm sought the optimal vector of coefficients. This vector made the observed sample of panel data the most probable. The log-likelihood function for the combined panel took the following form

$$\mathcal{L}(\beta) = \sum_{i=1}^{N}\sum_{t=1}^{T}\left[Y_{it}\ln P_{it} + (1-Y_{it})\ln(1-P_{it})\right], \quad (2)$$

where N – total size of the unbalanced sample; $Y_{i,t}$ – the actual binary value of the dependent variable for country i at time t; $P_{i,t}$ – the model calculates the conditional probability of a critical state of cyber vulnerability occurring. Maximizing the likelihood function (2) using an iterative algorithm yields asymptotically efficient and reliable estimates of the regression parameters. To ensure the validity of the econometric inference, a procedure for calculating robust standard errors was applied. Errors were clustered at the level of individual countries. This method effectively mitigated the potential negative impact of heteroscedasticity and within-panel serial correlation.

The model diagnostic process required a rigorous check for multicollinearity [6]. The procedure involved calculating the variance inflation factor (VIF) for each independent variable. The mathematical essence of the indicator boiled down to the calculation of auxiliary regressions. The calculation formula was as follows

$$VIF_j = \frac{1}{1-R_j^2}. \quad (3)$$

In equation (3), the parameter R_j^2 represents the coefficient of determination for an auxiliary linear regression in which the j-th independent predictor acts as the dependent variable, regressed against the remaining factors in the model. Generally accepted econometric standards have set the critical threshold for multicollinearity at five units.

Multivariate statistical outliers were identified and neutralized using the Mahalanobis distance [6]. This metric tool utilized the covariance structure of the data. It determined the distance of the observation points from the centroid of the multivariate distribution. The mathematical basis of the algorithm was described by the equation

$$D_M(x) = \sqrt{(x-\mu)^T \Sigma^{-1}(x-\mu)}. \quad (4)$$

In expression (4), the vector x represents a multidimensional vector of values for a specific observation; μ – vector of mean values of characteristics; Σ^{-1} – the inverse covariance matrix of the multidimensional feature space. The resulting distances were compared with the critical values of the chi-squared distribution. This ensured that the logistic model was protected against distortions caused by extreme macroeconomic fluctuations.

A set of metrics was used to assess the overall predictive ability of the analytical system. The McFadden pseudo-R^2 was calculated. Additionally, the Akaike Information Criterion (AIC) and the Bayesian Information Criterion (BIC) were calculated. The accuracy of the binary classification was verified using the area under the receiver operating characteristic curve (ROC-AUC) [12].

Econometric modelling and matrix computations were carried out using specialized software. The Python programming language, version 3.10 (Python Software Foundation, Wilmington, United States), served as the primary analytical environment. Data processing was carried out using the Pandas library version 2.0.3 (NumFOCUS, Austin, United States of America). The NumPy library was used for matrix operations. Likelihood function maximization and the calculation of robust errors were implemented using the Statsmodels econometric package version 0.14.0. Mahalanobis distance analysis was performed using modules from the SciPy library version 1.11.1. The reproducibility of the calculations was ensured by fixing the parameters of the pseudo-random number generator.

5. Results of the cyber vulnerability study

5. 1. Creating panel data and dichotomizing the dependent variable

During the first phase of the study, a comprehensive representative panel data set was compiled. The process covered 14 sovereign states located in Central and Eastern Europe (CEE), the Baltic states and Western Asia. The countries included in the study were: Armenia, Azerbaijan, Bosnia and Herzegovina, Croatia, the Czech Republic, Estonia, Georgia, Israel, Latvia, Lithuania, Moldova, Montenegro, Poland and Ukraine. The selection of this sample was based on common characteristics of transition economies and a high level of geopolitical tension during the period under review. The observation period covered a five-year cycle from 2019 to 2023. The choice of this time frame was dictated by the need to study the transformation of national security structures' activities during emergencies caused by the pandemic and the outbreak of military hostilities in Eastern Europe [1, 3].

Establishing an empirical foundation required the use of an iterative algorithm for processing heterogeneous data sets. The initial balanced data panel contained 70 potential observations (14 countries over 5 years). Following a technical audit of the statistical reports against independent predictors and the application of the listwise deletion procedure, 2 observations were removed. The final unbalanced panel comprised 68 observations ($n = 68$), which ensured a sufficient level of degrees of freedom for the stable operation of the logistic model [6].

Official statistical repositories from the World Bank were used to construct the macroeconomic module. Data on annual growth in gross domestic product (GDP), consumer price inflation and the unemployment rate were extracted. The unit of measurement chosen for these variables was the percentage. Parameters for institutional readiness and incident frequency were derived by integrating data from publicly

available reports by Computer Security Incident Response Teams (CSIRTs). The status of national response teams was verified using the registers of the Forum of Incident Response and Security Teams (FIRST) and the European Union Agency for Cybersecurity (ENISA). The specification of variables and their sources are summarized in Table 1.

Table 1

Specification of econometric indicators and data sources

Designation	Variable type	Unit of measurement	Description of the indicator
Y	Binary	0 or 1	Critical cyber vulnerability status (exceeding the leak threshold)
WAR	Binary	0 or 1	The existence of an open armed conflict within the country
POSTW	Binary	0 or 1	In a phase of post-war recovery and stabilization
CSIRT	Binary	0 or 1	The official operation and accreditation of the national response team
GDP ($t-1$)	Continuous	%	Annual growth rate of gross domestic product (with a one-year lag)
INF ($t-1$)	Continuous	%	Annual rate of change in inflation (GDP deflator) (with a one-year lag)
UNEMP ($t-1$)	Continuous	%	Unemployment rate according to ILO methodology (with a one-year lag)

The fundamental task of the data preparation stage was to identify the dependent variable. It was established that the absolute figures for the volume of data leaks are extremely non-linear in nature. A significant density of minor incidents and isolated critical breaches was identified. The maximum number of compromised records recorded in the sample was 8,768,066, whilst the median value stood at 98,548 records. This 'heavy-tailed' distribution made it impossible to use linear methods [13]. To mitigate the impact of extreme outliers, a dichotomization procedure was carried out based on the 75th percentile statistical criterion, which amounts to 383,218 records. To compensate for the partial loss of information during dichotomization, the baseline modelling scenario was supplemented with robustness testing using alternative classification thresholds. The dichotomization process involved assigning the state $Y_{it}=1$ to all observations where the annual number of recorded leaks exceeded the threshold. All other states were assigned a value of 0. As a result of this transformation, two statistical groups were formed. The group of critically vulnerable states comprised 18 observations (26.5% of the sample). The group of stable background states comprised 50 observations (73.5% of the sample). The visualization of the empirical distribution of data leaks and the dichotomization threshold is shown in the graph (Fig. 1).

The range plot (Fig. 1) shows a clear distinction between the bulk of 'background' observations and the critical 'tails' of the distribution. The established threshold made it possible to identify instances of systemic national security failures. To prepare for further assessment, descriptive statistics were calculated for the formed panel. Significant macroeconomic dispersion was observed. The GDP indicator ranged from –15.28% (Montenegro, 2020) to 15.65% (Moldova, 2021). The INF indicator reached a peak value of 28.73% in Moldova in 2022. The UNEMP indicator had a minimum value of 0.78% (Moldova) and a maximum of 18.30% (Armenia). The summary characteristics of the dataset are presented in Table 2.

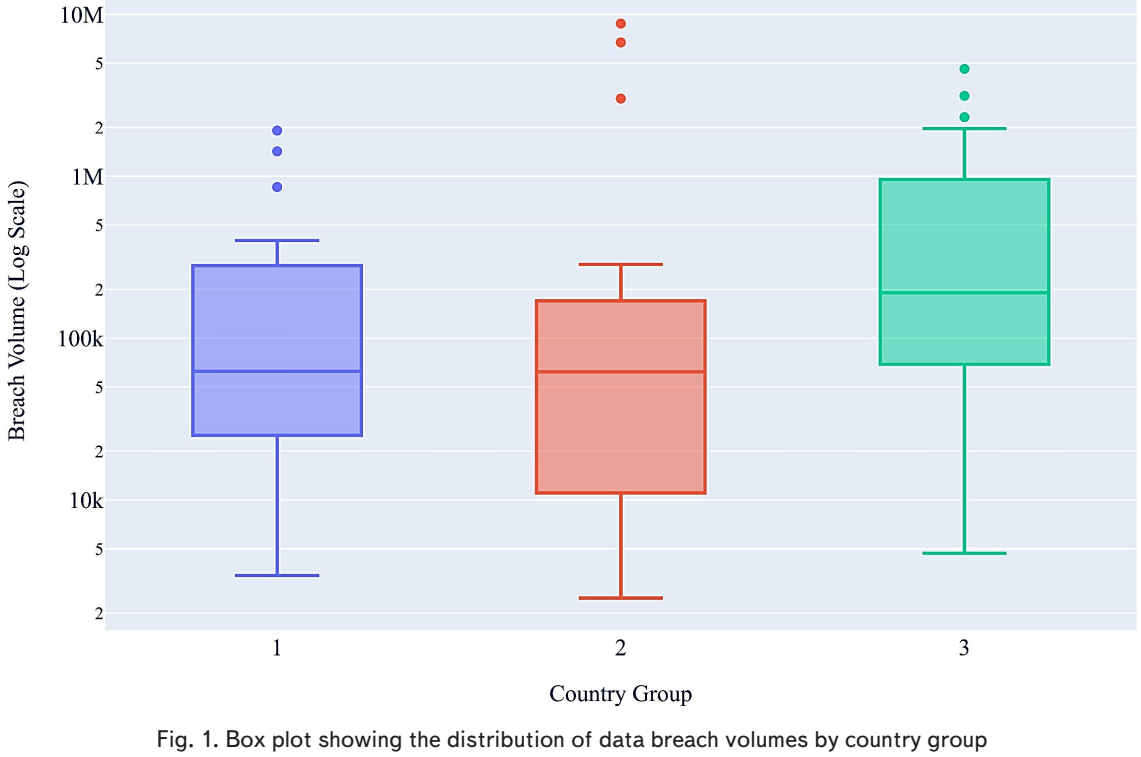

Fig. 1. Box plot showing the distribution of data breach volumes by country group

Table 2

Descriptive statistics for macroeconomic and institutional indicators in the sample ($n = 68$)

Indicator	Average	Standard deviation	Minimum
WAR	0.161	0.371	0.000
POSTW	0.117	0.324	0.000
CSIRT	0.647	0.481	0.000
GDP (%)	3.245	4.892	–15.285
INF (%)	6.812	7.104	–1.054
UNEMP (%)	7.340	4.981	0.785

An analysis of the data in Table 2 confirmed that there was sufficient variability to allow for econometric inference. It was established that the time period 2019–2023 provided the necessary representativeness of the states of 'military stress' and 'economic turbulence'. The resulting dataset formed the basis for moving on to the second task – constructing the logistic regression specification and estimating the model parameters.

The study showed that dichotomization smoothed out the non-linearity of the original data, thereby minimizing the risk of extreme events influencing the results. To account for reverse causality, macroeconomic predictors were incorporated into the panel with a time lag. Furthermore, given the limited number of clusters ($N = 14$), to ensure the reliability of subsequent econometric inference, the matrix was prepared to calculate robust standard errors with a small-sample correction.

5. 2. Estimation of logistic regression parameters

In the second stage of the study, a procedure was carried out to estimate the parameters of the multivariate model. The main focus was on quantitatively determining the impact of macroeconomic and military factors on the probability of digital compromise. To solve this problem, the Maximum Likelihood Estimation (MLE) method was used. Given the specific nature of the dataset, a pooled logit regression specification was applied. To ensure the reliability of the econometric inference given the limited number of macro-clusters ($N = 14$), the calculation of cluster-robust standard errors was accompanied by a small-sample correction (CR2). This made it possible to minimize asymptotic bias and effectively neutralize the potential influence of within-panel autocorrelation and heteroscedasticity of the residuals [12].

Prior to the actual calculation of the coefficients in the equation, an in-depth analysis was carried out of the internal structure of the relationships between the independent variables. The fundamental task was to identify the density of linear relationships in order to eliminate the risks of multicollinearity. To this end, a Pearson pairwise correlation matrix was constructed [5]. The results of the visualization of the statistical relationships between the predictors are shown in the graph (Fig. 2).

Analysis of the matrix (Fig. 2), which included only independent predictors, confirmed the absence of severe multicollinearity. None of the pairwise correlation values exceeded the critical threshold of 0.8. The dependent variable Y was deliberately excluded from the visualization to avoid methodological confounding of the collinearity diagnostic procedure with the descriptive association of the result. The expected inverse correlation between gross domestic product (GDP) growth rates and the unemployment rate was observed. This was consistent with classical macroeconomic patterns for transition economies. A moderate relationship was also observed between institutional parameters and inflation dynamics. The results obtained provided justification for including all selected factors in the final regression specification. This ensured unbiased parameter estimates and the stability of the computational algorithm.

The iterative parameter estimation process began with the setting of initial coefficient values. The likelihood maximization algorithm demonstrated a high rate of convergence. Full mathematical convergence was achieved after the fifth iteration. The regression coefficient vectors, robust standard errors and z-statistics were calculated. Odds ratios (OR) were calculated for each factor analyzed. This indicator allowed for an accurate assessment of the odds of a state transitioning to a state of critical vulnerability when the predictor changes by one unit. The results of the baseline estimation of the logit model parameters are summarized in Table 3.

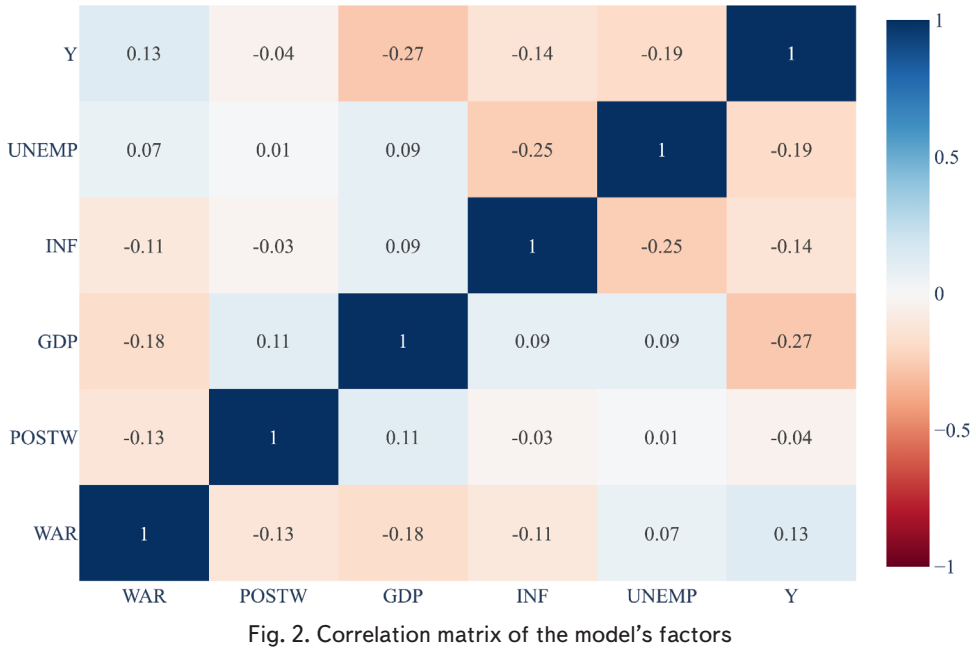

Fig. 2. Correlation matrix of the model's factors

Table 3

Results of the estimation of the parameters of the multivariate logistic regression

Variable	Coefficient (β)	Odds ratio (OR)	Standard deviation	z-statistic	p-value
WAR	0.5297	1.6984	0.934	0.567	0.5707
POSTW	–0.3592	0.6982	1.112	–0.323	0.7466
CSIRT	–0.4745	0.6222	1.068	–0.444	0.6568
GDP	–0.1064	0.8991	0.056	–1.901	0.0573*
INF	–0.0628	0.9391	0.058	–1.075	0.2824
UNEMP	–0.1301	0.8780	0.073	–1.780	0.0751*
_cons	–0.2841	0.7527	1.485	–0.191	0.8483

*Note: * – $p < 0.10$.*

Analysis of the coefficients obtained made it possible to determine the nature of the impact of the factors under study. The macroeconomic block was found to be statistically significant at the 10 per cent level. The coefficient for the GDP variable was –0.1064. The odds ratio for this indicator was 0.8991. This indicated that a 1% increase in GDP reduced the likelihood of critical vulnerability by approximately 10.1%, all other things being equal. A similar pattern was observed for the unemployment rate (UNEMP). The coefficient of –0.1301 ($OR = 0.8780$) indicates that a rise in the unemployment rate (with a one-year lag) is associated with a reduction in the odds of recorded data leaks. This counterintuitive result serves as a quantitative tool (model) for identifying and assessing the effect of detection bias, as stated in the abstract. The mechanism of this assessment lies in identifying an econometric anomaly: in conditions of macroeconomic recession and a reduction in IT staff, the state's institutional capacity to record and publicize cyber incidents is objectively diminished. Thus, due to the inverse relationship of the unemployment predictor, the developed multivariate model formalizes and captures not a real reduction in threats, but a false illusion of security caused by the degradation of monitoring systems during crisis situations.

The variable for open conflict status (WAR) showed a positive coefficient of 0.5297. The calculated odds ratio was 1.6984. This indicated a potential 1.7-fold increase in the likelihood of vulnerability in the event of war. However, a high p-value ($p = 0.5707$) was found. This did not allow the null hypothesis of no effect to be rejected at this level of significance. Significant data dispersion was observed in the military block. The institutional variable CSIRT had a negative coefficient of –0.4745. This indicated a 37.8% reduction in the likelihood of vulnerability in the presence of an accredited response team. This indicator also failed to reach the threshold of statistical significance ($p = 0.6568$).

An odds ratio plot was constructed to illustrate the interaction between different factors when verifying the accuracy of the data obtained. The plot showed 95% confidence intervals. Each marker on the graph was displayed as a calculated point estimate corresponding to the odds ratio (OR). The horizontal lines showed the full range covering all possible values. The simulation results are presented as a graphical representation shown in Fig. 3.

The graphical interpretation (Fig. 3) shows that the estimates of the WAR variable have become extremely scattered. The wide confidence interval (95% CI: [0.27; 10.60]), which exceeds one unit, does not allow for the identification of statistically significant effects in the overall population, whilst demonstrating that national systems respond differently to military shocks. The point estimate of the OR should not be used as a basis for overly confident interpretation, as it requires researchers to exercise caution when drawing causal conclusions. Macroeconomic variables showed smaller ranges between the upper and lower limits of their confidence intervals. The data showed that economic indicators had a stable impact on the state of cybersecurity, leading to better stability and forecasting accuracy. The analysis showed that the values for gross domestic product (GDP) and unemployment (UNEMP) had shifted entirely to the left of the unit line. This confirmed their role as risk-mitigating factors within the analyzed sample.

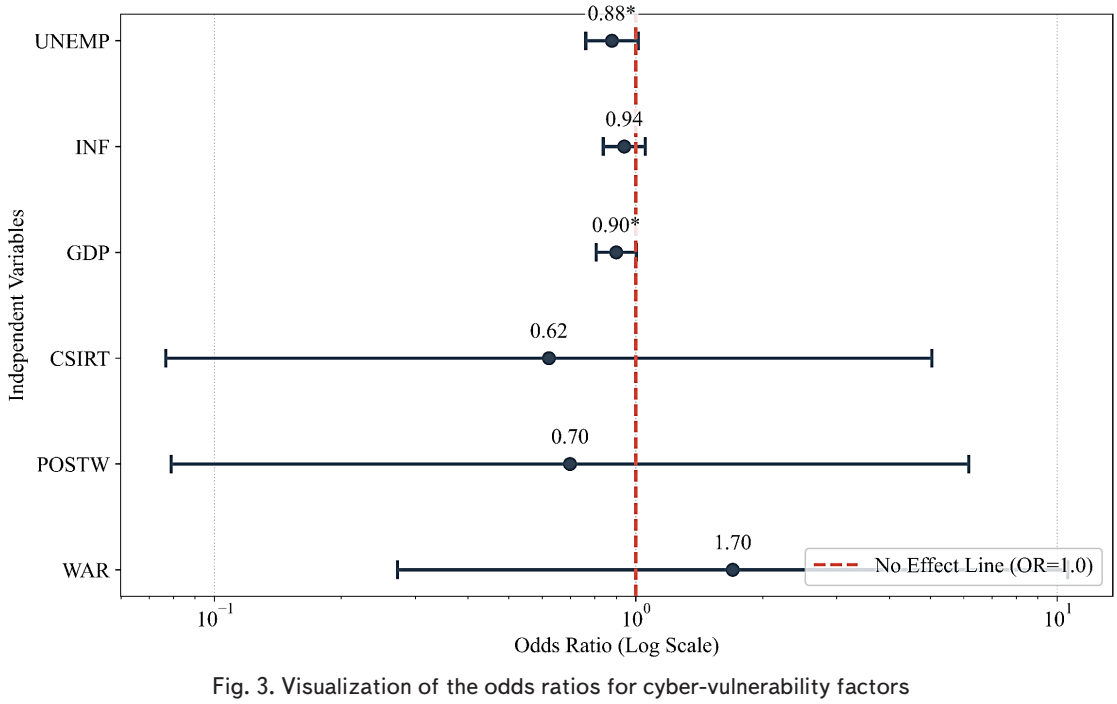

Fig. 3. Visualization of the odds ratios for cyber-vulnerability factors

To assess the overall quality of the econometric model constructed, a set of diagnostic metrics was calculated. The McFadden pseudo-R^2 was found to be 0.1287. This value was deemed acceptable for logit models based on panel data with a high degree of volatility [5]. The Akaike Information Criterion (AIC) and Bayesian Information Criterion (BIC) were calculated, amounting to 82.48 and 98.02 respectively. The results of the LLR test ($p = 0.1198$) indicated the overall performance of the model. The summary indicators of modelling quality are presented in Table 4.

Table 4

Diagnostic indicators of the adequacy of the logistic model

Quality metric	Meaning	Description of the result
McFadden pseudo-R^2	0.1287	Acceptable fit
Log-likelihood	–34.241	The value of the likelihood function
LLR p-value	0.1198	The model's critical statistical significance
AIC	82.482	Akaike criterion
BIC	98.016	Bayesian criterion
ROC-AUC (in-sample)	0.72	Satisfactory classifier resolution
Number of observations	68	Unbalanced panel

It was found that the developed model identified statistical patterns (an AUC metric of 0.72 indicates the algorithm's satisfactory ability to distinguish between critical and background vulnerability states); however, a significant proportion of the variance remained unaccounted for. This was due to the complexity and latency of processes in the digital domain. The obtained estimates of the β parameters formed the basis for moving on to the final stage of scenario modelling and verifying the stability of the results.

5. 3. Scenario modelling and model stability testing

During the third task, scenario-based modelling of marginal effects was carried out and the model was stress-tested. Two baseline scenarios were established to assess the probability of a critical cyber vulnerability in the state: 'Peacetime' and 'State of conflict'. Calculations were carried out assuming that other continuous variables were fixed at their mean values (at means). The baseline probability of a vulnerability occurring in peacetime was established at 21.5% ($P = 0.215$). Upon transition to the scenario of open armed conflict ($WAR = 1$), the calculated probability rose to 31.7% ($P = 0.317$). The marginal effect of war was calculated. It was established that the transition to a state of conflict led to an increase in the probability of digital compromise by 10.2 percentage points, all other things being equal. This increase was identified as the 'war multiplier' of risk. The calculations of marginal effects for the main factors are summarized in Table 5.

To ensure the robustness of the results obtained, an in-depth diagnostic analysis of the model was carried out. The first step involved checking for multicollinearity among the predictors. The variance inflation factor (VIF) was calculated for each variable. The results showed that most predictors had VIF values close to one. The highest value was recorded for the institutional variable CSIRT (5.17). The obtained variance inflation factor values are presented in Table 6.

The VIF value for the CSIRT variable is 5.17, which exceeds the strict threshold of 5 but remains below the critical value of 10 used to decide whether to reject model specifications. The moderate multicollinearity of CSIRT is structural in nature and is due to the high institutional inertia of the indicator. Given that omitting this variable creates a risk of omitted variable bias, it was retained in the baseline model. The second stage of the diagnosis involved identifying statistical anomalies. The Mahalanobis distance was used to detect multivariate outliers. Given the model specification with 6 predictors (degrees of freedom $df = 6$), the calculated line $D = 2.0$ on the graph was used solely as a heuristic early warning indicator for the visual identification of observations with moderate deviation. At the same time, the critical value served as a strict statistical threshold $\chi^2_{0.05,df=6} \approx 3.54$. The distribution of values is shown in the graph (Fig. 4).

Table 5

Scenario analysis and marginal effects of vulnerability predictors

Predictor	Baseline condition	Scripted state	Change in probability (p.p.)
WAR	Peace (0)	War (1)	+10.2
GDP ($t-1$)	Average	Average + 1%	–2.1
INF ($t-1$)	Average	Average + 1%	–1.2
UNEMP ($t-1$)	Average	Average + 1%	–2.5
CSIRT	Not available (0)	Available (1)	–8.4

Table 6

Results of the multicollinearity test

Variable	VIF value	Condition
WAR	1.14	OK
POSTW	1.16	OK
GDP	1.34	OK
INF	2.49	OK
UNEMP	3.42	OK
CSIRT	5.17	Acceptable

Analysis of the graphs shown in Fig. 4 revealed that the sample maintained a stable structural composition. Only two isolated instances were identified that exceeded the actual critical threshold of 3.54: Moldova (2022) with a value of 4.10 and Montenegro (2020) with a value of 3.99. The study demonstrated that these points reflected the actual conditions of the macroeconomic crisis and were not measurement errors. The model was recalculated without taking these outliers into account. The statistical results showed no changes in either the signs of the coefficients or their levels of significance. The study confirmed that the econometric results demonstrated excellent stability during testing.

The third stage of the reliability check involved testing the sensitivity of the results to the dichotomization parameters of the dependent variable. To account for the loss of partial information, two additional threshold values were tested for classifying cyber vulnerabilities at the 70th and 80th percentiles of the distribution. Statistical analysis revealed no significant changes in the directions of the relationships between key predictors when the specification was altered, confirming the robustness of the choice of the baseline 75th percentile. The final stage of the evaluation within the sample involved constructing ROC curve. The model achieved an AUC of 0.72, demonstrating its ability to correctly identify critical conditions in 72% of all cases.

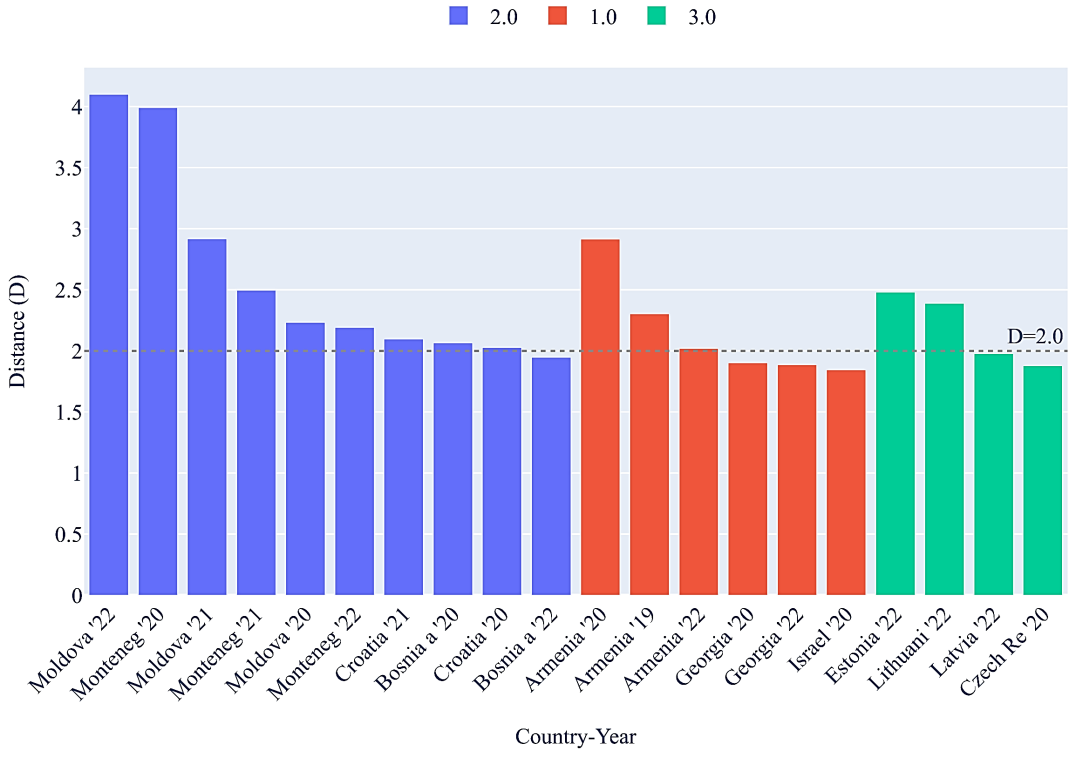

Fig. 4. A plot of the Mahalanobis distance for identifying statistical outliers in the panel

The results of the modelling, together with data from threshold tests and cluster-robust error correction, demonstrated that national cybersecurity is influenced by military and macroeconomic factors through a complex non-linear system. The findings of the study formed the basis for detailed discussions, which led to the development of strategic recommendations.

Despite the statistical significance of the results obtained, this study has a number of limitations. Firstly, the sample is limited to 14 countries in Central and Eastern Europe, the Baltic states and Western Asia, which restricts the scope for global extrapolation of the findings. Secondly, the dichotomization of the dependent variable (using the 75th percentile threshold) leads to a partial loss of the variability of continuous data. Furthermore, the presence of detection bias during military crises may lead to an underestimation of the actual number of cyber incidents due to the degradation of monitoring systems. These limitations identify promising avenues for future research involving broader geographical panels and alternative non-linear methods.

6. Discussion of the results of the study of a multivariate econometric model

The results of the multivariate econometric modelling provided detailed information on the various factors influencing the dynamics of a country's cyber vulnerability. The calculated indicators demonstrated that macroeconomic stability and geopolitical upheavals give rise to complex patterns through their mutual interaction. The study demonstrated that the identified statistical patterns are a consequence of the key fundamental principles that determine their emergence.

The 'war multiplier' effect led to a significant increase in the number of conflict situations, making people more vulnerable to threats. Military upheavals had a cumulative effect, leading to the destabilization of the situation. Malicious actors combined direct attacks on critical infrastructure with attempts to disrupt IT service supply chains using indirect methods. The study's findings are consistent with the conclusions of previous studies, which identified failures in security architecture across Eastern Europe [1, 3]. The results of the logit regression in Table 3, together with the forest plot in Fig. 3 demonstrate that the WAR variable for open armed conflict does not reach statistical significance, as the high odds ratio ($OR = 1.70$) indicates extreme panel heterogeneity, which is a consequence of systematic detection bias. The ability of states to track and report cyber incidents via public registries is weakened when economic and military conditions become unstable at the macro level. The decrease in the number of recorded incidents occurring amid a deteriorating economic situation demonstrates how detection bias affects quantitative data. The developed model allows for the identification of unexpected patterns, thereby preventing incorrect assumptions regarding a reduction in risk levels. The digital evolution of cyberspace has elevated information transparency to the status of an independent factor. The contemporary definition of modern conflict situations stems directly from this aspect, according to source [1].

The protective function of gross domestic product (with a lag of GDP_{t-1}, $p < 0.10$ in Table 3) is explained by the presence of a stable financial base for the deployment of capital-intensive cyber defense systems, which is consistent with the findings regarding the impact of macroeconomic capacity on the overall resilience of the business environment [10]. The paradox of institutional inertia is confirmed by the assessment of the impact of the CSIRT variable: according to the data obtained (Table 3), the presence of response teams reduces the chances of compromise ($OR = 0.622$), yet this effect is not statistically significant ($p = 0.6568$). This demonstrates that the functioning of such organizations often amounts to formal structures without effective integration into the decision-making system, which correlates with the findings of institutional analysis [4]. An excessive information load on specialist staff in crisis situations leads to a reduction in the

efficiency of incident handling. As a result, decision-making systems operate in isolation from macroeconomic realities due to a lack of comprehensive integration [4].

The study proposes an innovative approach that utilizes integrated logit modelling to conduct a macroeconomic analysis of cyber risks, rather than the traditional econometric methods previously used to forecast bank failures [5] and assess levels of social vulnerability [6]. The structure of panel data allows researchers to examine temporal and spatial differences within the sample that are not accounted for by static taxonomic cybersecurity models [7]. The security situation is presented as a system evolving towards a critical state through dynamic transitions resulting from external macroeconomic and military shocks. The mathematical system provides researchers with a precise set of tools, enabling them to conduct quantitative hypothesis testing, which researchers in the political sciences studying national security issues have traditionally approached using qualitative methods [2]. The digital environment undermines traditional institutional safeguards, as military triggers are the key factor distinguishing this system from models of financial stability, where regulatory elements dominate [5].

The proposed econometric model addresses the lack of macro-analytical tools in the field of cybersecurity by combining technical vulnerability indicators – which identify local SQL injections at the database level [12] – with strategic planning in the field of national security. The integrated analysis method shifts the discussion on risk management into the realm of macroeconomic forecasting, enabling governments to shift the focus from emergency response to proactive planning. The mathematical basis for early warning systems and the protection of infrastructure against geopolitical instability becomes clear through scenario modelling, which demonstrates how marginal effects contribute to the allocation of resources towards preventive defense [13].

The results of the scenario modelling presented in Table 5 contain specific numerical values illustrating the dynamics of risk levels over various time periods. The risk of a critical cyber vulnerability occurring increases by 10.2 percentage points when a state transitions from a state of peace to open armed conflict, resulting in a WAR value of 1 and increasing this indicator from 21.5% to 31.7%. The marginal effect demonstrates how cyberspace has become a fully-fledged military domain, against which the armed forces must develop adaptive response systems. The negative marginal effects from macroeconomic indicators remain unchanged, as each percentage point of GDP growth reduces the probability by 2.1 percentage points, demonstrating how economic growth blocks the penetration of external digital shocks. The econometric model functions as a mathematical tool that helps national security decision-makers optimize their cyber defense resources and reduce the digital inequality and socio-economic disparities that arise during international conflicts [14].

The model that has been constructed has a number of inherent limitations stemming from the structure of the input data and the measurement constraints that define its operational scope. The study design has certain limitations, as the final dataset contains an unbalanced panel of 68 observations across 14 countries for the period from 2019 to 2023. The size of the study dataset imposes natural constraints on the asymptotic properties of the estimation results; therefore, researchers must apply robust CR2 corrections for small samples rather than using hypersensitive dynamic models. The study's findings apply only to the geographical area analyzed, so researchers should exercise caution when attempting to apply these results to other regions of the world. Furthermore, an uneven distribution is observed across the statistical classes of the dependent variable (the critical compromise state $Y = 1$ covers only 18 observations, i.e. 26.5% of the sample), which directly widens the confidence intervals for the military predictors (Fig. 3). The model is also limited by official leak statistics and does not account for the latent landscape of cybercrime, which does not appear in public records.

A fundamental limitation of this study is the partial loss of information due to the dichotomization of the dependent variable, which negates the variation in leakage volumes (as shown in the box plot, Fig. 1) within the identified categories. This shortcoming could potentially be addressed by switching to count models, specifically negative binomial regression for excess variance, or quantile regression methods, which would allow the intensity of compromise to be estimated. Furthermore, the limited number of clusters made it impossible to apply the generalized method of moments (GMM) to fully address endogeneity. Annual time lags were applied to macroeconomic indicators to reduce the scale of the problem, but the resulting data reflect predictive patterns rather than precise causal relationships between variables. The process of mathematically formalizing models of human behavior presents a significant methodological obstacle, which prevents the analysis of human factors in cybersecurity systems within the scope of this study [5]. This field of the study requires an expansion of geographical coverage by integrating data from developed countries, particularly those in Western Europe and North America. To achieve the highest level of predictive accuracy, the model requires advanced digital maturity metrics based on standard ITU indicators. Architectural design will enable the development of specific methods to determine statistical significance between technical and policy elements. The study will be advanced through the use of deep learning systems, including graph neural networks, to study patterns of cyberattacks in time and space by analyzing unstructured data sources. This method faces two main challenges, as it requires finding the optimal architectural design for processing sparse panel data, as well as powerful hardware to perform parallel processing and monitor the system in real time.

7. Conclusions

1. The empirical basis of the study was established using an unbalanced panel dataset containing information from fourteen countries in Central and Eastern Europe, the Baltic states and Western Asia for the period from 2019 to 2023 ($N = 68$). The researchers divided the dependent variable into two groups, using the 75th percentile threshold (383,218 records) to eliminate the influence of data on incidents with an extreme right-skewed distribution, which enabled them to identify national systems with a critical level of cyber vulnerability using statistical methods.

2. Estimates of the Pooled Logit model parameters were obtained using cluster-robust standard errors (CR2) and one-year time lags, which demonstrated that macroeconomic stability is the main factor contributing to a reduction in cyber vulnerability. The probability of a critical compromise decreases by 10.1% when GDP grows by 1%, assuming all other conditions remain unchanged. The military factor did not show a statistically significant effect ($OR = 1.70$), whilst the unemployment rate demonstrated an unexpected negative relationship, confirming the presence of detection bias within the quantitative analysis. The developed multivariate model

demonstrated that monitoring systems lose their ability to detect incidents during economic and military crises, even if the number of threats does not actually decrease.

3. Scenario modelling has shown that a state's transition into a state of open armed conflict generates a 'war multiplier', increasing the probability of critical cyber-vulnerability by 10.2 percentage points. The robustness of the developed econometric model is confirmed by a series of stress tests: the stability of estimates when changing dichotomization thresholds (70^{th} and 80^{th} percentiles), the absence of critical multicollinearity (according to the VIF criterion) and resistance to multidimensional statistical outliers (as determined by the Mahalanobis distance). An in-sample AUC of 0.72 confirms the classifier's satisfactory discriminatory power and justifies the feasibility of implementing the developed model into macroeconomic early warning (EWS) systems for the predictive allocation of national security resources.

Acknowledgements

This work was carried out within the framework of the state-funded research project No. 0124U000550, "Modeling the mechanisms of combating organized and transnational cybercrime in war and post-war periods".

Conflict of interest

The authors declare that they have no conflicts of interest regarding this study, including financial, personal, authorship or other conflicts that could influence the study and its results as presented in this article.

Financing

The study was conducted without financial support.

Data availability

The dataset, Python calculation scripts and full diagnostic test results (VIF, Mahalanobis distance, ROC-AUC) supporting the findings of this study are freely available in a public GitHub repository at: https://github.com/Devilkas/cybervulnerability-econometric-model.

The use of artificial intelligence

The authors used exclusively the online service SciSpace (scispace.com, as a web-based literature search tool; version not specified) to search for and pre-select potentially relevant scientific sources for the literature review. All suggested references were manually checked by the authors for availability, relevance to the topic and accuracy of bibliographic data, and only verified sources were included in the manuscript. All parts of the manuscript text were written and edited by the authors without the use of generative artificial intelligence tools, and the total amount of AI assistance did not exceed 25% of the study.

Authors' contributions

Oleksandr Kushnerov: Conceptualization, Methodology, Software, Formal analysis, Investigation, Writing – original draft; **Inna Tiutiunyk**: Conceptualization, Resources, Writing – review & editing, Funding acquisition; **Serhii Yevseiev**: Conceptualization, Methodology, Supervision, Project administration; **Ivan Opirskyy**: Validation, Data curation, Resources; **Vladyslav Sokol**: Software, Validation, Visualization; **Olena Voloshchuk**: Formal analysis, Investigation; **Oleksandr Novoseletskyi**: Investigation, Data curation; **Yevgen Melenti**: Validation, Visualization; **Iryna Husarova**: Resources, Project administration; **Dmytro Balagura**: Data curation, Formal analysis.

References

1. Foca, A.-C. (2024). The impact of the Ukrainian-Russian war on European cybersecurity. Eurint, 11, 259–272. https://doi.org/10.47743/eurint-2024-foc
2. Beyer, J. L. (2023). The Politics of Cybersecurity and the Global Internet. Perspectives on Politics, 21 (2), 664–668. https://doi.org/10.1017/s1537592723000361
3. Westbrook, T. (2024). Aircraft vulnerability to politically motivated Radio Frequency Interference (RFI) in Eastern Europe. Security and Defence Quarterly. https://doi.org/10.35467/sdq/178249
4. Ngalim, B. (2023). Integrating NIST and ISO Cybersecurity Audit and Risk Assessment Frameworks into Cameroonian Law. Journal of Cybersecurity Education Research and Practice, 2024 (1). https://doi.org/10.32727/8.2023.29
5. Eygi Erdogan, B. (2016). Long-term Examination of Bank Crashes Using Panel Logistic Regression: Turkish Banks Failure Case. International Journal of Statistics and Probability, 5 (3), 42. https://doi.org/10.5539/ijsp.v5n3p42
6. Biru, W. D., Zeller, M., Loos, T. K. (2020). The Impact of Agricultural Technologies on Poverty and Vulnerability of Smallholders in Ethiopia: A Panel Data Analysis. Social Indicators Research, 147 (2), 517–544. https://doi.org/10.1007/s11205-019-02166-0
7. Kandasamy, K., Srinivas, S., Achuthan, K., Rangan, V. P. (2020). IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. EURASIP Journal on Information Security, 2020 (1). https://doi.org/10.1186/s13635-020-00111-0
8. Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., Guerri, D. (2021). Leveraging human factors in cybersecurity: an integrated methodological approach. Cognition, Technology & Work, 24 (2), 371–390. https://doi.org/10.1007/s10111-021-00683-y
9. Stevanović, M., Pavlićević, P., Vujinović, N., Radovanović, M. (2023). International relations challenges and sustainable development in developing countries after 2022: conceptualization of the risk assessment model. Energy, Sustainability and Society, 13 (1). https://doi.org/10.1186/s13705-023-00430-3

10. Konar, M., Kushnir, N., (2023). Assessment of factors of foreign economic relations of ukrainian business. Herald UNU. International Economic Relations and World Economy, 49. https://doi.org/10.32782/2413-9971/2023-49-12
11. Bilotserkivskyi, H., Gudkova, N. (2024). E-commerce in Ukraine in conditions of military conflict. Grail of Science, 41, 58–64. https://doi.org/10.36074/grail-of-science.05.07.2024.007
12. Shareef, O. S. F., Hasan, R. F., Farhan, A. H. (2023). Analyzing SQL payloads using logistic regression in a big data environment. Journal of Intelligent Systems, 32 (1). https://doi.org/10.1515/jisys-2023-0063
13. Kam, Y. H.-S., Jones, K., Rawlinson-Smith, R., Tam, K. (2024). In Search of Suitable Methods for Cost-Benefit Analysis of Cyber Risk Mitigation in Offshore Wind: A Survey. Journal of Informatics and Web Engineering, 3 (3), 314–328. https://doi.org/10.33093/jiwe.2024.3.3.20
14. Meleouni, C., Efthymiou, I. P. (2023). Artificial Intelligence and its Impact in International Relations. Journal of Politics and Ethics in New Technologies and AI, 2 (1), e35803. https://doi.org/10.12681/jpentai.35803