https://doi.org/10.64211/oidaijsd190705

Methodology of Threats Outlooks Development to EU Civil Security

Hryhorii Sytnyk [1], Tetiana Palamarchuk [2], Halyna Zavoritnya [3], Yevhenii Taran [4], Nataliia Klymenko [5]

[1,3,5] Department of Global and National Security, Educational and Scientific Institute of Public Administration and Civil Service, Taras Shevchenko National University of Kyiv, 60 Volodymyrska Str., 01033, Kyiv, Ukraine.
[2,4] Educational and Scientific Institute of Public Administration and Civil Service, Taras Shevchenko National University of Kyiv, 60 Volodymyrska Str., 01033, Kyiv, Ukraine.
*Corresponding author: sgp1000@ukr.net

OIDA International Journal of Sustainable Development, Ontario International Development Agency, Canada.
ISSN 1923-6654 (print) ISSN 1923-6662 (online) www.oidaijsd.com
Also available at https://www.ssrn.com/index.cfm/en/oida-intl-journal-sustainable-dev/

Abstract: The growth of multidimensional natural, man-made, terrorist and cyber threats creates a new level of systemic complexity for the civil security of the European Union and necessitates the modernization of analytical approaches to their forecasting. The relevance of the study is enhanced by the fact that traditional risk assessment tools do not take into account hidden correlations, cascading effects and nonlinear interactions between different categories of threats. The purpose of the study is to develop and scientifically substantiate an integrated methodology for forecasting threats to EU civilian security based on international statistics and modern econometric methods. The methodological framework includes descriptive time series analysis, principal component analysis (PCA) to identify the latent structure of multidimensional threats, and ARIMA and VAR econometric models to quantify the dynamics and cross-sectoral interactions of risks. The results showed that natural and man-made threats demonstrate steady upward trends, terrorist activity is characterized by wave-like dynamics, and cyber threats are growing most intensively and least predictably. PCA allowed us to identify three integral latent components – digital instability, environmental and technological vulnerability, and socio-political turbulence – which together explain 72.6% of the total variance. ARIMA models revealed the asymmetry of long-term trends, and VAR analysis demonstrated the growing interdependence between digital and man-made risks, indicating the formation of a new contour of cascading threats. The practical significance of the results lies in the possibility of applying the developed methodology to improve the effectiveness of strategic planning, improve early warning systems, formulate response scenarios and support management decisions in the field of EU civil security.

Keywords: econometric models, man-made threats, natural threats, terrorist risks, threat forecasting

Introduction

Threats have become very advanced and technological to the security system of the European Union, together with geopolitical turbulence in hybrid forms accompanied by changes in climate and new vulnerabilities emphasized on cyberspace dependence of critical infrastructure. Therefore, a modern civilian risk assessment method based mostly on retrospective statistical analysis collapses under such dynamic, hybrid conditions characterized by high degrees of uncertainty. Another problem identified within this paper is that there are no unified indicators or comparable data between EU member states' situations which would allow developing a common analytical platform for implementing management decision support at all levels from local to national across the whole EU crisis response system.

This is among leading academic discourses on how to forecast risks from new technologies. Artificial intelligence, for example, discussed by Favino et al. [1] is technologically evolving threats of different spectrums which are

transforming the structure of internal security in the EU through automated information systems and digital platforms therefore proactive risk forecasting models are needed since traditional approaches lag way behind compared to the pace with which technological development catches up hence a predictive approach has been proposed together with forecasting-and-analysis tools.

Palamarchuk et al. [2] offers a theoretical and methodological base for strategic forecasting in trend multi-indicator analysis and systematization accompanied by scenario construction of threats, which means the unification into one concept using standardized data of different information as is the case in EU civil security risk modeling that allows disparate yet integrated forms of information. However, it also raises the problem of defragmentation: existing security analysis systems in Europe remain out of sync with each other – for contradictory reasons – with the forecasting itself.

Most hybrid and cyber threats are critical infrastructure. Zybin et al. [3] assess hybrid cyber risk using fuzzy set theory because, in a modern model of threat analysis, incomplete information needs to be accommodated together with structural uncertainty. This brings up a totally new avenue for building predictive models where segmented or asymmetric quantitative information exists on threats.In the context of EU regulatory resilience, Ruohonen et al. [4] stress that an updated EU policy on cybersecurity contains large gaps in regulation to manifest itself unevenly across member states' implementation with huge risks of inconsistency.Non-regulatory heterogeneity directly influences the accuracy potential estimations of security risks, particularly in the cyber domain.

An important block of studies is devoted to the organization of civil protection. Kalogiannidis et al. [5] analyze the effectiveness of emergency management mechanisms in European countries and show that different levels of institutional capacity make it difficult to compare risks and forecast threats at the EU level as a whole. The authors emphasize the need to unify risk indicators. Mader et al. [6] show how external threats help support the domestic integration of European security and defence, tying foreign policy challenges to changes in the way civil security planning is approached at home. The paper demonstrates that as analytically complex threats emerge, analytical modelling will become an increasingly important component within policy itself.

Dekker and Alevizos [7] present a threat intelligence methodology that allows the integration of highly heterogeneous reliability data sources in conditions of high threat uncertainty towards the prediction of cyber risks as well as hybrid threats to civil security. Cavallini et al. [8] clearly articulate support for the notion of digital resilience being an emerging facet within modern EU civil security, where next-generation methodological approaches to predicting technogenic risks are needed, since digital risks contain not only narrow cyber threats but wider complex technological risks.

Despite significant progress in the study of security risks, approaches to comprehensive forecasting of threats to EU civilian security based on integrated statistical data that would simultaneously cover natural, man-made, cyber and hybrid factors remain underdeveloped. Existing studies mostly focus on individual risk domains or use methodologies that do not allow for consistent modeling of the interdependence of different types of threats and their ability to cascade. The issue of unification of risk indicators used by different EU institutions remains unresolved, and there are no standardized econometric approaches that would ensure the construction of reliable forecasts based on open statistical sources. This creates a methodological gap that requires the development of a comprehensive forecasting system based on quantitative, objectively verified data.

The purpose of the study was to identify and substantiate the methodological basis for developing forecasts of threats to the civilian security of the European Union based on open statistical data and econometric approaches. To achieve this goal, the study set the following objectives: to identify the key factors that shape the structure of modern threats; to analyze existing scientific approaches to risk assessment and forecasting; to identify methodological gaps in the functioning of the EU civilian security system; to adapt econometric tools to the needs of modeling multidimensional threats; and to develop a conceptual forecasting model suitable for further implementation in the practice of think tanks and civil protection institutions.

Literature Review

The literature provides a well-scoped definition of threats to EU civil security across several interrelated domains and complains about the underdeveloped methodology for their comprehensive forecasting. Most studies provide an analysis of changes in the transformation of EU security policy towards changes made to manage risks proactively before a crisis occurs, thus moving from a risk management policy that only responds when risks have already materialized into one that causes harm or loss. New counter-terrorism strategies being developed by the European Union institutionalize capabilities both to prevent and anticipate terrorist acts [9]. Migration itself as a policy decision influencing the crisis context aggravates security challenges, as Hadj Abdou [10] shows.

There is a large body of work dealing with the potential technological modernization and upgrade of civil protection and early warning systems. Bompotas et al. [11] discuss an architectural setup for a civil protection early warning system in the Adriatic-Ionian area, stressing among other things the integration of natural/anthropogenic hazard risk data into one information environment. In infrastructure investment management literature, Caetano et al. [12] present an approach to establishing preference criteria for investment policy at general aviation airfields, essentially forming a methodology for multi-criteria risk-and sustainability-assessment of objects. Berger et al. [13] dwell on intelligence education development in Europe as a tool intended to enhance analytical capacity within the security sector through formalizing specific predictive threat models.

There are tendencies in the literature of an enlarged paradigm of security that includes humanitarian and environmental aspects. Kantemnidis and Botetsagias [14] found the perception of environmental security to be lagging, not only among members of the EU security community but also dynamically toward climate risk trends which permit well-coordinated prediction efforts. Palamarchuk et al. [15] analyzed the development of informational space as a component of Ukraine's humanitarian policy within European integration, stressing resilience via information means as one aspect required for countering hybrid threats wherein health [16, 17].

Directly related to risk assessment and forecasting methods are a number of studies that develop tools for managing uncertainty in the face of increasingly complex threats. Mentis [18] proposed a general framework for managing project risks and uncertainty that can be adapted to security contexts, but does not take into account the specifics of multi-domain threats. Kalyuzhna [19] summarizes methods for forecasting the evolution of the security environment, emphasizing the importance of combining qualitative and quantitative approaches, but without a detailed econometric implementation on official statistics. Murasov [20] developed a method for assessing risks to critical infrastructure in the context of hostilities, taking into account their destructive and cumulative potential, while Murasov and Meshcheriakov [21] proposed an information technology approach to preventing terrorist emergencies based on assessing the possibility of a gradual increase in destructive events due to cascading effects. These works demonstrate a high level of risk formalization, but focus mainly on certain types of threats and do not offer a generalized methodology for the entire EU civilian security system. Alqudhaib et al. [22] developed a proactive approach to predicting cyber threats to critical infrastructure in the context of Industry 4.0, based on the motivations of offenders and using analytical tools to model attack scenarios.

The objective of the project was to develop an advanced approach for forecasting threats to EU civil security based on econometric models using open statistical data. Meanwhile, better understanding of the main factors which drive the dynamics of threat risks will be obtained and methodological approaches fine tuned to actual practical requirements of risk management under uncertainties. Important is also adaptation of analytical tools to a multi dimensional contextual environment comprising that of EU security environment.

The goal was to analyze scientific approaches to risk assessment and forecasting, identify methodological gaps in EU civilian security mechanisms, select and adapt econometric methods for threat modeling, and develop a conceptual forecasting model capable of providing practical support for analytical and management decisions in the field of civil protection.

Materials and Methods

The research materials were based on official statistics for 2010-2024, obtained from the international databases EM-DAT [23], Europol TE-SAT [24, 25], ENISA Threat Landscape [26] and Eurostat [27]. To ensure broader analytical coverage, macroeconomic indicators of the World Development Indicators [28], institutional indicators of public security and resilience of public administration [29], as well as assessments of global risk dynamics presented in the World Economic Forum [30] report were also used.

To mitigate the internal biases inherent in secondary data, several validation and harmonization procedures were applied before the statistical modelling stage. First, data were collected only from institutional and internationally recognized sources with transparent reporting methodologies, including EM-DAT, Europol TE-SAT, ENISA, Eurostat, the World Bank, OECD and the World Economic Forum. Second, the same threat category was not interpreted on the basis of a single source when cross-source verification was possible; instead, the indicators were compared across databases to identify inconsistencies, abrupt methodological breaks or abnormal deviations. Third, variables measured in different units, such as the number of events, economic losses, institutional indicators and cyber incidents, were standardized before their inclusion in PCA and econometric models. Fourth, the analysis was based on annual aggregated indicators for 2010-2024, which reduced the influence of short-term reporting fluctuations and country-specific registration practices. Finally, the interpretation of results was limited to observable trends and structural

relationships, while causal claims were avoided unless they were supported by the statistical model and the theoretical logic of threat interaction.

The empirical sample consisted of eight institutional statistical sources and analytical reports: EM-DAT, Europol TE-SAT 2023, Europol TE-SAT 2024, ENISA Threat Landscape 2023, Eurostat database, World Development Indicators, OECD Government at a Glance 2023 and the World Economic Forum Global Risks Report 2024. This sample size was determined by purposive criterion-based selection rather than random sampling, because the study required sources that were institutionally reliable, publicly available, methodologically transparent and directly relevant to the main categories of EU civil security threats. Each selected source covered a distinct empirical dimension of the research: natural and man-made disasters, terrorist incidents, cyber threats, macroeconomic conditions, public governance resilience and global risk dynamics. The use of eight sources was considered sufficient because together they enabled the construction of a unified time-series dataset for 2010-2024 comprising more than 1,800 annual and sectoral observations. This scope provided enough empirical coverage for descriptive analysis, PCA, ARIMA and VAR modelling, while also reducing dependence on a single reporting system and allowing cross-source verification of trends, inconsistencies and structural breaks.

This broadly falls under four main categories of threats to EU civil security: natural, man-made and terrorist (including cyber). Based on primary information from these sources, a single time series was constructed allowing for the analysis of annual dynamics across different security threat sectors. The research methodology consisted of several logically linked steps. In the first step, a simple trend analysis is applied to identify general upward or downward movements within the series together with any cyclical/seasonal components and sudden structural breaks that may exist within them. This provides basic estimates of intensity trajectories-paths of intensity which are later disaggregated through more detailed econometric modelling.

At the second stage, the Principal Component Analysis (PCA) method was used to reduce the multidimensionality of the data and to identify latent factors that simultaneously affected several categories of threats. The resulting integral factors increased the information content of subsequent models and ensured the conceptual coherence of the analytical structure of the study. ARIMA and VAR econometric models became the key forecasting tools.

$$\phi(L)(1-L)^d y_t = \theta(L)\varepsilon_t \qquad (1)$$

where L is the lag operator, d is the integration order, φ(L) and θ(L) are autoregressive and moving average polynomials. The estimation procedure included testing of stationarity (ADF-test), selection of parameters p, d, q according to information criteria, and construction of interval forecasts.

Before the principal component analysis, the authors checked the suitability of the data set for factor analysis. For this purpose, the KMO coefficient of sampling adequacy and Bartlett's test of sphericity were applied, which allowed to assess the degree of correlation between the variables and confirm the statistical feasibility of identifying latent components. The results obtained (KMO > 0.7; $p < 0.001$ by Bartlett's test) showed a sufficient density of the correlation matrix and provided the correct basis for performing PCA and further use of integral factors in the forecasting econometric models ARIMA and VAR.

The VAR model was used to analyze the systemic interaction between several groups of threats and to assess potential cross-sectoral and cascading effects. This made it possible to formulate consistent forecasts of the European Union's comprehensive risk profile. Data processing and model building were carried out in Python (pandas, statsmodels, sklearn) and R, and visualizations in the form of trend curves, PCA graphs, and forecast trajectories were created in formats suitable for editorial processing.

Results

Dynamic characteristics of threats to EU civilian security in 2010-2024: results of descriptive analysis

The descriptive analysis of time series for 2010-2024 made it possible to identify characteristic dynamic patterns of development of natural, man-made, terrorist and cyber threats to the civilian security of the European Union. Primary data were obtained from the EM-DAT [23], Europol TE-SAT [24, 25], ENISA Threat Landscape [26], Eurostat [27], World Bank [28], OECD [29] and World Economic Forum [30] databases. They were used to form a unified array of time series covering more than 1.800 annual and sectoral observations. Natural hazards demonstrated a steady upward trend: the number of recorded natural disasters increased from 92 events in 2010 to 148 in 2024 (+60.8% increase, +3.3% average annual rate). Economic losses increased from €9.8 billion to €16.5 billion, reflecting the overall

increase in climate-related risks [23, 27]. According to TE-SAT, terrorist activity was the most volatile. The number of incidents increased from 52 in 2010 to a peak of 219 in 2015, before declining to 82 incidents in 2024. The share of prevented attacks increased from 31% to 56%, indicating that operational and analytical capabilities have improved [24, 25].

Cyber incidents demonstrated the fastest growth among all risk groups: their number increased from 620 in 2010 to 2.980 in 2024 (+380% increase, CAGR +10.7%). The share of attacks on critical infrastructure increased from 8% to 27%, and the average financial loss per incident increased from €78 thousand to €214 thousand [26]. A generalized distribution of changes in three five-year subperiods is shown in Table 1.

Table 1: Generalized dynamics of threats to EU civilian security by groups in 2010-2024

Period	Natural disasters (EM-DAT)	Man-made accidents (EM-DAT)	Terrorist incidents (TE-SAT)	Cyber incidents (ENISA)	Macro and institutional context (Eurostat, World Bank, OECD, WEF)
2010-2014	92 → 113 events; moderate growth (+22.8%)	45-52 incidents; relative stability	52-137 incidents; increasing volatility	620 → 940 incidents; beginning of digitalization	Moderate economic growth; strengthening of basic institutions
2015-2019	118 → 139 events; increased climate risks	54-67 incidents; infrastructure burden	Terrorism peaked in 2015 (219 incidents); then declined	1,120 → 2,140 incidents; sharp increase in sophistication of attacks	Consolidation of civil protection; development of critical infrastructure
2020-2024	141 → 148 incidents; maximum level for the period	63 → 48 incidents; decline due to changes in economic activity	102 → 82 incidents; increase in the share of individual attacks	2,180 → 2,980 incidents; dominance of systemic attacks	Deepening digitalization; increased attention to systemic risks

Source: Guha-Sapir et al. [23]; Europol [24, 25]; EU Agency for Cybersecurity [26]; Eurostat [27]; World Bank [28]; OECD [29]; World Economic Forum [30]

Table 1 clearly confirms the change in risk profile for the EU up to and including 2024. Natural and cyber threats are steadily on the increase while man-made risks display quasi-regular fluctuations. The most volatile threat is that from terrorism reflecting evolutionary change in tactics by small decentralized groups. There has been a structural shift in threats: in the previous decade they were predominantly natural and manmade; now, in 2020-2024, they are more digital but also hybrid! This provides an empirical basis on which further applications of PCA, ARIMA and VAR can be used to forecast the EU's comprehensive risk profile.

Terrorism is the most conspicuous aspect of the risk profile which sharply increased in the middle of this decade and then declined as its intensity level was maintained by enhanced law enforcement capabilities. At the same time, cyberspace is the area where we register highest growth and with an upward trend-from incidents at a technical level up to more system oriented attacks on critical infrastructure.

Latent structure of multidimensional threats: results of principal component analysis (PCA)

In order to identify the latent structure of multidimensional threats to EU civilian security for 2010-2024, the principal component analysis (PCA) method was applied, which allowed to summarize the impact of a significant number of variables in the form of a limited set of integral factors. The input dataset was formed on the basis of aggregated

statistical indicators from EM-DAT [23], Europol TE-SAT [24, 25], ENISA Threat Landscape [26], Eurostat [27], World Bank [28] and OECD [29]. The preliminary standardization of scales ensured the comparability of variables with different order of magnitude – from the number of events to economic losses. The suitability of the dataset for factorization was confirmed statistically: the KMO coefficient was 0.78, which corresponds to good sample quality, and the Bartlett's test was significant ($\chi^2 = 512.4$; $p < 0.001$), indicating the presence of a correlation structure sufficient for PCA. The analysis identified three principal components that together explained 72.6% of the total variance. Their content was determined by the nature of the factor loadings shown in Table 2.

Table 2: Factor loadings for principal components PC1-PC3

Indicator	**PC1 (Digital instability)**	**PC2 (Environmental and technological vulnerability)**	**PC3 (Socio-political turbulence)**
Number of cyber incidents (ENISA)	0.84	0.12	0.06
Attacks on critical infrastructure	0.81	0.09	0.11
Financial losses from cyber attacks	0.76	0.18	0.05
Number of natural disasters (EM-DAT)	0.14	0.79	0.10
Economic losses from natural events	0.21	0.74	0.13
Technological accidents (EM-DAT / Eurostat)	0.18	0.71	0.16
Number of terrorist attacks (TE-SAT)	0.09	0.18	0.82
Detention of radicalized individuals	0.06	0.15	0.78
Public safety indicators (OECD)	0.12	0.24	0.69

Source: Guha-Sapir et al. [23]; Europol [24, 25]; EU Agency for Cybersecurity [26]; Eurostat [27]; World Bank [28]; OECD [29]; World Economic Forum [30]

The variance is explained:

– PC1 – 38.2%.

– PC2 – 21.7%.

– PC3 – 12.7%.

Total – 72.6%.

Summarizing the PCA results, the structure of threats to EU civilian security in 2010-2024 has become systemic and multidimensional. Digital threats have become the dominant determinant, natural and man-made risks have converged in a common latent plane, and terrorist threats have retained their autonomous socio-political influence. Thus, PCA

not only revealed the internal architecture of the risk environment, but also ensured the formation of generalized integral factors necessary for the next stage – the construction of econometric forecasts using ARIMA and VAR.

Forecasting the Intensity and Interrelationships of threats to EU civilian security: results of ARIMA and VAR models

Forecasting the medium-term dynamics of threats to the civilian security of the European Union was based on a combination of single-factor ARIMA models focused on assessing the individual behavior of each type of risk and a multivariate VAR model that allowed to trace systemic interactions between the integrated latent components determined by the principal components method. The use of these approaches ensured consistency with the previous descriptive analysis and with the PCA framework, in which digital instability (PC1), environmental and technological vulnerability (PC2), and socio-political turbulence (PC3) reflect the three axes of the EU's current risk profile.

All time series based on the EM-DAT, Europol TE-SAT, ENISA Threat Landscape, Eurostat, World Bank, OECD, and Global Risks Report indicators were tested for stationarity using the ADF test. The results showed that most of the first-order series are integrated ($p < 0.05$), which is the basis for using ARIMA(p,1,q) models. Their general form is presented in the formal notation:

$$\phi(L)(1-L)^d y_t = \theta(L)\varepsilon_t \qquad (2)$$

where L is the lag operator, d is the integration order, φ(L) and θ(L) are the autoregressive and moving average polynomials, respectively, and εt is the random component. Parameter selection was based on the AIC and BIC criteria, and model diagnostics included an analysis of the autocorrelation of the residuals. Digital threats, which determine the first latent component (PC1), are characterized by inertia and long-term exponential growth. The ARIMA (1,1,1) model was the best description of the trend, reflecting the expected increase in digital instability: by 2027, the intensity of cyber incidents is projected to increase by about 35-36% compared to the level of 2024, with a 95% confidence interval ranging from 28-43%.

Natural hazards and man-made incidents, which form the second component (PC2), showed much smoother and more stable trends. The ARIMA (0,1,1) model for natural disasters reflected a forecast of an increase in their intensity by about 10-12% by 2027, without significant structural breaks. Man-made accidents modeled by ARIMA (1,1,0) retain a quasi-stationary character: possible fluctuations do not exceed ±4%, which is consistent with the moderate variability found in the descriptive analysis.

Terrorist threats integrated into the third component (PC3) remained the most unstable category. The ARIMA (2,1,1) model showed a wide forecast range – from a probable decrease of about 13% to a possible increase of 21%, reflecting the cyclical nature and unpredictability of terrorist activity recorded in TE-SAT reports.

Further analysis of systemic interrelationships was carried out using a VAR model based on integral indicators PC1-PC3. The impulse response results showed that digital instability is the primary source of cascading effects: a shock to PC1 causes PC2 to rise over two to three periods, with a maximum response of about 0.18-0.21 standard index points. Environmental and technological vulnerability reacts much weaker to its own shocks, which emphasizes its structural rather than dynamic nature. Socio-political turbulence demonstrates asymmetric effects: its impulses hardly change natural and man-made risks, but they increase digital instability through the activation of information and hybrid operations.

The decomposition of the forecast error variance confirmed the autonomous nature of the development of digital threats: more than 60% of the variation in PC1 is explained by internal factors, while PC2 and PC3 are largely dependent on external perturbations. The generalized forecast indicates that in the coming years, digital instability will remain a key factor in escalating risks, natural and man-made threats will be the basic systemic vulnerability, and socio-political factors will be a catalyst or moderator of inter-threat interactions.

Discussion

The threat landscape for EU civil security has obviously become multidimensional over the years 2010-2024. More specifically, it is defined within the framework of increasing interdependence between natural, man-made, cyber and terrorist risks. There is a steady trend towards the growth of digital threats identified in ARIMA models which are projected to grow by 35-36% until 2027. This makes not only understanding but also designing modern risk frameworks for this component very important. This non-linear dynamics shows long-term consequences of climate change which increases natural disaster losses by 10-12%. The overall trend supports the approach taken by Stefanidou

et al. [31] that connects new configuration of risks with growing role played by digital twins and integrated technical information systems in civil protection.

The cyber risk factor loads most strongly onto the principal component, which by definition captures the largest share of total variance and describes digital instability as a main structural factor. The latent axis running between cyber threats and anthropogenic risks correlates with so-called “digital-physical” interactions that, according to Stefanidou et al. [31], are crucial for vulnerability assessment in contemporary state systems. With 72.6% explained by the PCA model, there can hardly be any doubt about the deep systemic nature of the ongoing transformation of the modern environment.

The systemic dependencies between threat groups confirmed by the VAR model are consistent with the findings of Štrbac and Milosavljević [32], who emphasize the networked nature of EU crisis management. In our model, digital instability is the primary driver of cascading effects: an impulse in PC1 causes an increase in PC2 over a two- to three-period horizon with a maximum impact of 0.18-0.21 index points. In contrast, the opposite effect was much weaker, indicating the asymmetry of cross-sectoral interactions and confirming the different resilience of sectors to external shocks, as emphasized by these authors. Variations in seasonality and structural differences between EU member states are further explained by the unevenness of national risk management strategies.

There is yet another dimension to this debate in the behavioral aspect of response. The VAR results showed that socio-political indicators respond with a delay to the dynamics of natural and man-made hazards. This is consistent with the bounded rational behavioral inertia in evacuation decision-making found by Wang et al. [33], where “hazard prediction” is mostly applied except for some extreme cases under certain conditions/assumptions/scenarios, etc., which means that there may be some (volatility) arising from the behavioral aspect that is not fully captured by the available statistics, highlighting the need to incorporate microbehavioral models in future work.

In even broader institutional terms, this can be taken as confirmation of Pursiainen and Kitomaa’s [34] observation that European security policy has very recently transformed from “critical infrastructure protection” to “critical actor resilience”. It is the PCA components and variables which clearly explain the variance of the shares related to infrastructure risks, i.e. the importance of some central systemic resilience links in current EU civil security architectures.

These results are in line with Ruohonen [35], who, among a plethora of other caveats on cyber threats, bemoans the fragmentation of cyber policy and regulatory regimes in the EU. Heterogeneity may explain the very diverse incidents over time – with significant annual fluctuations – which may also be a functional aspect reflected in such heterogeneity. This therefore implies that forecasting digital risks will require not only econometric tools but also coordinated cyber strategies at Member State level [36-38].

The sources used are fully representative, but the study has certain limitations. EM-DAT, Europol, ENISA and Eurostat update their information with different frequencies at various levels of detail by different methods of collection; this may result in heterogeneity between sources. ARIMA and VAR models work perfectly to forecast trend-based shocks; however, they do not incorporate infrequent but powerful shocks-such as COVID-19 or large-scale geopolitical conflicts that restructure risk so massively over short time spans. There is also no description of a behavioral component that determines an outcome response.

The practical usefulness of this study appears in the possibility of using PCA, ARIMA and VAR as a comprehensive strategic planning tool in cross-sectoral relations, which can be used as a basis for the formation of risk scenarios, optimization of the early warning mechanism, resilience of critical infrastructure and adaptation of regulatory policy to new threat configurations. Another important practical result is future predictive systems ,which will comprise a digital twin; behavioral model; and multi-disciplinary integrated modeling based forecasting system.

Conclusions

The study has shown that the current risk profile of the European Union's civilian security is formed as a multidimensional, dynamic and structurally interconnected system in which natural, man-made, cyber and socio-political threats create cross-impacts and cascading effects. The principal components method allowed us to determine the latent architecture of this system, where the leading role is played by the digital instability component, which explains the largest share of variance and determines the direction of further collective changes. The combination of cyber and man-made factors in a common latent space indicates the formation of a new type of "digital-physical" interactions characteristic of the EU's integrated infrastructure environments.

Econometric ARIMA models display a gently upward-stepped short-term trajectory forecast of cyber incidents while long smooth clearly structurally unbroken trajectories for natural and manmade hazards in the short term. Terrorist activity remains highly volatile, therefore very difficult to forecast using traditional methods. The main forms which temporal dynamics of threats take as well as their degrees of predictability have been revealed by the ARIMA models.

The results of the VAR simulations confirmed that the contagion risks are primarily from digital instability through a cascading effect of environmental and technological components, and partially through a socio-political sphere cascading effect. This impact asymmetry lies in differences in sectoral resilience and is very much consistent with current approaches to assess the resilience of key players in the EU. The correlations found are evidence that a change within the digital component can massively reformat the overall risk contour, but has much weaker feedback effects, forming uneven cross-sector interactions.

The study has a long list of limitations, the most important being related to the heterogeneity of statistical sources (EM-DAT, Europol, ENISA, Eurostat), which initiates different data collection standards in forming uneven time series. Econometric models are very sensitive to shocks that change dynamics and are not adequately captured by traditional ARIMA and VAR models, as outlined in Appendix A. Last but not least, at the macro level, they do not integrate microbehavioural characteristics of the population ,which play a key role in human losses and efficiency during crises.

The conclusions of the study were derived with consideration of the internal biases inherent in secondary data. Since the empirical basis was formed from institutional databases and analytical reports with different reporting procedures, the interpretation of the results was based not on isolated values from a single source, but on cross-source comparison and the consistency of trends across EM-DAT, Europol TE-SAT, ENISA, Eurostat, the World Bank, OECD and the World Economic Forum. This approach made it possible to reduce the influence of methodological differences in data collection, changes in reporting intensity and uneven sectoral coverage. Before modelling, the indicators were harmonized and standardized, which limited the distortion caused by different units of measurement and scale effects. The conclusions were therefore formulated cautiously, as evidence of structural associations, dynamic tendencies and probable risk trajectories rather than as direct causal claims. PCA was used to identify latent patterns that remained stable across several indicators, while ARIMA and VAR models were interpreted as exploratory forecasting tools sensitive to data quality and reporting limitations. Thus, secondary-data bias was mitigated through triangulation, standardization, aggregation over the 2010-2024 period and restrained interpretation of model outputs.

The practical significance of the analysis consists of possibilities for PCA, ARIMA and VAR in strategic planning within the field of civil protection, critical infrastructure resilience assessment and generating multi-level risk scenarios. This can also be considered as a baseline for analytical forecasting platform development, digital twins and integrated decision support systems which enhance EU's capabilities on early warning detection of threats and adaptive response to threats.

Research should aim at developing integrated forecasting models that combine econometric methods with behavioural approaches, spatial dynamics analysis and the application of machine learning algorithms. Stability is impacted by recent regulatory reforms in civil protection systems, digital integration and intergovernmental cooperation. A new risk management paradigm focusing on resilience as an object accompanied by adaptability emerges through such type of research.

Acknowledgment

The study was conducted as part of the Erasmus+ project "Threats Actualization to European Security: Russian-Ukrainian War Impact," which the Educational and Scientific Institute of Public Administration and Civil Service of Taras Shevchenko National University of Kyiv is implementing in 2023-2026 in accordance with grant agreement No. 101127665 with the European Education and Culture Executive Agency.

References

1. Favino, R., Conte, N., de Maleville, A., Sfalagkairis, M., & others. (2025). *Emerging risks and opportunities for EU internal security stemming from new technologies.* Publications Office of the European Union. https://doi.org/10.2760/7979295
2. Palamarchuk, T., Zavoritnya, H., Iemelianov, V., Lehkyi, S., & Taran, Y. (2025). Theoretical and methodological approach for strategic foresight and advanced response in the national security context. *Sapienza: International Journal of Interdisciplinary Studies*, *6*(2). https://doi.org/10.51798/sijis.v6i2.944

3. Zybin, S., Korchenko, O., Korystin, O., Shulha, V., Kazmirchuk, S., & Demediuk, S. (2025). Method for the risk assessing of hybrid threats in cyber security based on fuzzy set theory. *SSRN*. https://dx.doi.org/10.2139/ssrn.5143937
4. Ruohonen, J., Nielsen, J. L., & Skórczynski, J. (2025). Risks and compliance with the EU's core cyber security legislation. *arXiv:2508.21386*. https://doi.org/10.48550/arXiv.2508.21386
5. Kalogiannidis, S., Kalfas, D., Papavengelou, O., & Chatzitheodoridis, F. (2024). Effectiveness to the emergency management in public organizations: A paradigm from a European civil protection mechanism. *Journal of Risk Analysis and Crisis Response*, *14*(3), 291–313. https://doi.org/10.54560/jracr.v14i3.501
6. Mader, M., Gavras, K., Hofmann, S. C., Reifler, J., Schoen, H., & Thomson, C. (2024). International threats and support for European security and defence integration: Evidence from 25 countries. *European Journal of Political Research*, *63*(2), 433–454. https://doi.org/10.1111/1475-6765.12605
7. Dekker, M., & Alevizos, L. (2023). A threat-intelligence driven methodology to incorporate uncertainty in cyber risk analysis and enhance decision making. *Security and Privacy, 7*(1). https://doi.org/10.1002/spy2.333
8. Cavallini, S., Soldi, R., Casalini, G., & Grasso, A. (2023). *Digital resilience*. European Committee of the Regions. https://doi.org/10.2863/5099
9. Baker-Beall, C., & Mott, G. (2021). The new EU counter-terrorism Agenda: preemptive security through the anticipation of terrorist events. *Global Affairs, 7*(5), 711–732. https://doi.org/10.1080/23340460.2021.1995461
10. Hadj Abdou, L. (2020). 'Push or pull'? Framing immigration in times of crisis in the European Union and the United States. *Journal of European Integration, 42*(5), 643–658. https://doi.org/10.1080/07036337.2020.1792468
11. Bompotas, A., Anagnostopoulos, C., Kalogeras, A., Kalogeras, G., Mylonas, G., Stefanidis, K., Alexakos, C., & Dandoulaki, M. (2022). A civil protection early warning system to improve the resilience of Adriatic–Ionian territories to natural and man-made risk. *arXiv:2207.13941*. https://doi.org/10.48550/arXiv.2207.13941
12. Caetano, M., Silva, E. J., Vieira, D. J., Alves, C. J. P., & Müller, C. (2022). Criteria prioritization for investment policies in General Aviation aerodromes. *Regional Science Policy & Practice, 14*(6), 211–234. https://doi.org/10.1111/rsp3.12538
13. Berger, L., Borghoff, U. M., Conrad, G., & Pickl, S. (2025). Intelligence Education Made in Europe: Critical Reflections on the German Experience. *International Journal of Intelligence and Counter Intelligence, 38*(3), 802–821. https://doi.org/10.1080/08850607.2025.2460940
14. Kantemnidis, D., & Botetzagias, I. (2023). Understanding the environmental security perceptions of the European Union's security actors. *Sustainability, 15*(17), 13027. https://doi.org/10.3390/su151713027
15. Palamarchuk, T., Opanashchuk, P., & Lytvynchuk, A. (2024). Formation of the informational space as an element of Ukraine's humanitarian policy in the context of European integration. *AD ALTA: Journal of Interdisciplinary Research*, *14*(01), 172–178. https://doi.org/10.33543/j.140140.172178
16. Kondilis, E., Tarantilis, F., & Benos, A. (2021). Essential public healthcare services utilization and excess non-COVID-19 mortality in Greece. *Public Health, 198*, 85–88. https://doi.org/10.1016/j.puhe.2021.06.025
17. Lu, H., APPC 2018–2019 ASK Group, Winneg, K., Jamieson, K. H., & Albarracín, D. (2020). Intentions to seek information about the influenza vaccine: The role of informational subjective norms, anticipated and experienced affect, and information insufficiency among vaccinated and unvaccinated people. *Risk Analysis*, *40*(10), 2040–2056. https://doi.org/10.1111/risa.13459
18. Mentis, M. (2015). Managing project risks and uncertainties. *Forest Ecosystems*, *2*(2). https://doi.org/10.1186/s40663-014-0026-z
19. Kalyuzhna, N. (2023). Methods of forecasting the evolution of the security environment. *Foreign Trade: Economics, Finance, Law*, *126*(1), 13–30. https://doi.org/10.31617/3.2023(126)02
20. Murasov, R. (2023). The method of risk assessment for critical infrastructure in the conditions of hostilities, taking into account their destructive and cumulative potential. *Journal of Scientific Papers: Social Development and Security*, *13*(1), 152–160. https://doi.org/10.33445/sds.2023.13.1.13

21. Murasov, R., & Meshcheriakov, I. (2023). The information and technical method of preventing emergency situations of a terrorist nature by assessing the possibility of gradual growth of destructive events caused by the cascading consequences of the primary terrorist impact. *Journal of Scientific Papers: Social Development and Security*, *13*(5), 180–191. https://doi.org/10.33445/sds.2023.13.5.17
22. Alqudhaib, A., Albarrak, M., Aloose1, A., Jagtap, S., & Salonitis, K. (2023). Predicting cybersecurity threats in critical infrastructure for Industry 4.0: A proactive approach based on attacker motivations. *Sensors*, *23*(9), 4539. https://doi.org/10.3390/s23094539
23. Guha-Sapir, D., Below, R., & Hoyois, P. (2016). *Annual disaster statistical review 2016: The numbers and trends.* Brussels: CRED. http://emdat.be/sites/default/files/adsr_2016.pdf
24. Europol. (2023). *EU Terrorism Situation and Trend Report (TE-SAT 2023).* Europol. https://doi.org/10.2813/302117
25. Europol. (2024). *EU Terrorism Situation and Trend Report (TE-SAT 2024)*. Europol. https://doi.org/10.2813/4435152
26. EU Agency for Cybersecurity. (2023). *ENISA Threat Landscape 2023.* EU Agency for Cybersecurity. https://doi.org/10.2824/782573
27. Eurostat. (2024). Eurostat database: Population, economy, environment and civil protection statistics. *European Union.* https://ec.europa.eu/eurostat/web/main/data/database
28. World Bank. (2024). World Development Indicators. *World Bank Group*. https://databank.worldbank.org/source/world-development-indicators
29. OECD. (2023). *Government at a Glance 2023*. Paris: OECD Publishing. https://doi.org/10.1787/3d5c5d31-en.
30. World Economic Forum. (2024). Global Risks Report 2024. *World Economic Forum*. https://www.weforum.org/publications/global-risks-report-2024/
31. Stefanidou, A., Cani, J., Papadopoulos, T., Radoglou-Grammatikis, P., Sarigiannidis, P., Varlamis, I., & Papadopoulos, G. Th. (2024). Leveraging digital twin technologies for public space protection and vulnerability assessment. *arXiv:2408.17136*. https://doi.org/10.48550/arXiv.2408.17136
32. Štrbac, K., & Milosavljević, B. (2021). Crisis management system in European Union: How it works? *Serbian Journal of Engineering Management, 6*(1), 45–54. https://doi.org/10.5937/SJEM2101045S
33. Wang, X., Chraibi, M., Chen, J., Li, R., & Ma, J. (2022). Modeling boundedly rational route choice in crowd evacuation processes. *Safety Science, 147*, 105590. https://doi.org/10.1016/j.ssci.2021.105590
34. Pursiainen, C., & Kytömaa, E. (2022). From European critical infrastructure protection to the resilience of European critical entities: What does it mean? *Sustainable and Resilient Infrastructure*, *8*(sup1), 85–101. https://doi.org/10.1080/23789689.2022.2128562
35. Ruohonen, J. (2024). The incoherency risk in the EU's new cyber security policies. In R. van de Wetering, R. Helms, B. Roelens et al. (Eds.), *Disruptive innovation in a digitally connected healthy world* (pp. 284–295). Cham: Springer. https://doi.org/10.1007/978-3-031-72234-9_24
36. Bondareno, S., Makeieva, O., Usachenko, O., Veklych, V., Arifkhodzhaieva, T., & Lernyk, S. (2022). The legal mechanisms for information security in the context of digitalization. *Journal of Information Technology Management*, *14*(Special Issue: Digitalization of Socio-Economic Processes), 25–58.
37. Kryshtanovych, M., Akimova, L., Shamrayeva, V., Karpa, M., & Akimov, O. (2022). Problems of European integration in the construction of EU security policy in the context of counter-terrorism. *International Journal of Safety and Security Engineering*, *12*(4), 501–506.
38. Gavkalova, N., Akimova, L., Zilinska, A., Lukashev, S., Avedyan, L., & Akimov, O. (2022). Functioning of united territorial communities and identification of main problems of organizational support of local budget management. *Financial and Credit Activity Problems of Theory and Practice*, *2*(43), 107–117. https://doi.org/10.55643/fcaptp.2.43.2022.3708