“Institutional, technological, and financial drivers of national cyber resilience under armed conflict and post-conflict recovery”

AUTHORS

Inna Shkolnyk

Inna Tiutiunyk

Andrii Semenog

Yuliia Kovalenko

Liudmyla Pavlenko

ARTICLE INFO

Inna Shkolnyk, Inna Tiutiunyk, Andrii Semenog, Yuliia Kovalenko and Liudmyla Pavlenko (2025). Institutional, technological, and financial drivers of national cyber resilience under armed conflict and post-conflict recovery. *Problems and Perspectives in Management*, *23*(4), 665-683. doi:10.21511/ppm.23(4).2025.45

DOI http://dx.doi.org/10.21511/ppm.23(4).2025.45

RELEASED ON Saturday, 27 December 2025

RECEIVED ON Monday, 10 November 2025

ACCEPTED ON Friday, 26 December 2025

JOURNAL "Problems and Perspectives in Management"

ISSN PRINT 1727-7051

ISSN ONLINE 1810-5467

PUBLISHER LLC “Consulting Publishing Company “Business Perspectives”

FOUNDER LLC “Consulting Publishing Company “Business Perspectives”

NUMBER OF REFERENCES **35**

NUMBER OF FIGURES **2**

NUMBER OF TABLES **7**

BUSINESS PERSPECTIVES

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

www.businessperspectives.org

Inna Shkolnyk (Ukraine), **Inna Tiutiunyk** (Ukraine), **Andrii Semenog** (Ukraine), **Yuliia Kovalenko** (Ukraine), **Liudmyla Pavlenko** (Ukraine)

INSTITUTIONAL, TECHNOLOGICAL, AND FINANCIAL DRIVERS OF NATIONAL CYBER RESILIENCE UNDER ARMED CONFLICT AND POST-CONFLICT RECOVERY

Type of the article: Research Article

Received on: 10th of November, 2025
Accepted on: 26th of December, 2025
Published on: 27th of December, 2025

Inna Shkolnyk, Doctor of Economics, Professor, First Vice-Rector, Department of Financial Technologies and Entrepreneurship, Sumy State University, Ukraine. (Corresponding author)

Inna Tiutiunyk, Doctor of Economics, Associate Professor, Department of Financial Technologies and Entrepreneurship, Sumy State University, Ukraine.

Andrii Semenog, Doctor of Economics, Associate Professor, Department of Financial Technologies and Entrepreneurship, Sumy State University, Ukraine.

Yuliia Kovalenko, Doctor of Economics, Professor, Head of the Department of Finance, Accounting and Taxation, State University "Kyiv Aviation Institute", Ukraine.

Liudmyla Pavlenko, Ph.D. in Economics, Senior Lecturer, Department of Financial Technologies and Entrepreneurship, Sumy State University, Ukraine.

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

Abstract

Military and economic turbulence transform the relationships between factors shaping national cyber resilience. This study aims to analyze the impact of technological, institutional, and financial determinants on cyber resilience under armed conflict and post-conflict recovery. The empirical analysis covers neighboring European non-EU countries within the European security space that are exposed to armed conflict or post-conflict instability (Ukraine, Moldova, Georgia, Armenia, Azerbaijan, and Serbia) from 2010 to 2024, using panel data from the World Bank, IMF, and ENISA. Cyber resilience is measured by the Global Cybersecurity Index. Institutional, technological, and financial factors are proxied by standard governance, digitalization, and the financial sector and estimated using a fixed-effects model with Driscoll-Kraay robust standard errors. The results reveal pronounced regime-dependent effects. Institutional capacity plays a decisive role during armed conflict: government effectiveness shows a strong positive association with cyber resilience ($\beta \approx 1.04$) but becomes statistically insignificant in post-conflict and stable environments. Technological factors exhibit context-sensitive effects: digital government development is positively associated with cyber resilience during armed conflict ($\beta \approx 0.95$) and relative stability ($\beta \approx 1.78$), while its impact weakens in post-conflict recovery. Macroeconomic conditions exert systematic influences across regimes: higher unemployment reduces cyber resilience ($\beta \approx -0.027$), whereas inflation shows a positive association ($\beta \approx 0.008$). Financial indicators display mixed and predominantly negative effects under relative stability. Accordingly, cybersecurity policy should be explicitly regime-sensitive: institutional and digital interventions should dominate during armed conflict, while governance and risk-management mechanisms should prevail in post-conflict and stable environments.

Keywords cybercrime, economic turbulence, cyber risk, non-performing loans, financial stability, digitalization, Fintech

JEL Classification G28, C33, O33, G21

INTRODUCTION

In the context of accelerated digitalization of economic processes, cyberspace has evolved not only into an environment for traditional criminal activity but also into a domain for systemic attacks targeting national governance structures, financial systems, and critical infrastructure, potentially undermining state capacity and generating significant socio-economic losses. These challenges become particularly acute during armed conflict and post-conflict periods, when countries experience declining institutional stability, constrained resources, and heightened exposure to cyber threats.

Against the backdrop of increased state vulnerability and shifts in economic and social behavior, cyber activities increasingly intersect with military and hybrid operations, serving as instruments for disrupting public administration, financial systems, and critical infrastructure. Empirical evidence illustrates the scale of this transformation. According to CERT-UA, the number of cyber incidents targeting Ukraine in 2022 increased threefold compared to 2021, reaching approximately 2,100 cases (CERT-UA, 2025). Microsoft Threat Intelligence reports 237 targeted attacks against governmental and critical entities in Ukraine during the first year of the full-scale armed conflict (Smith, 2022). Similar dynamics are documented by ENISA in its assessments of cyber threats associated with armed conflicts, including the Ukrainian case, where a 250–300% increase in attacks on public authorities and financial institutions has been observed, substantially amplifying systemic risks to national security (ENISA, 2023).

Following the transition from active armed conflict to post-conflict recovery, countries face a distinct set of cyber-related challenges associated with economic reconstruction and institutional rebuilding. In this phase, expanding digital services, reconstruction financing, and weakened regulatory oversight increase exposure to cyber risks, requiring revised approaches to cybersecurity governance. The United Nations (2025) emphasizes that post-conflict environments are characterized by heightened activity of cybercriminal networks, the expansion of shadow digital markets, and increased vulnerability of public and financial digital services.

Thus, the study of the features and specifics of cybercrime development across armed conflict, post-conflict recovery, and relative stability creates a basis for identifying patterns of escalation of threats and forming the most effective directions of strategic intervention. This, in turn, allows strengthening national security, increasing the adaptability of public institutions, and ensuring sustainable economic recovery in the face of growing digitalization and dynamic transnational risks.

1. LITERATURE REVIEW

The issue of combating cybercrime in armed conflict and post-conflict periods attracts more attention from the scientific community every year. Scientific research confirms that during armed conflict, digital space becomes one of the key tools of confrontation, and cyberattacks undergo significant transformations. Fyshchuk et al. (2025) emphasize that armed conflict significantly strengthens the coordination of cyberattacks with military operations and creates unprecedented challenges for the public sector. The European Parliament (2022), using the example of analyzing cyberattacks during the period of full-scale aggression against Ukraine, concludes about the systemic, coordinated, and multi-stage nature of cyberattacks, aimed at blocking state services, destroying critical infrastructure, and disrupting communication channels. In this context, Carlo and Obergfaell (2024) show that modern cyberattacks increasingly focus not on data theft but on disabling critical infrastructure and satellite communication systems by damaging industrial control systems, which enhances their effect as a tool of hybrid warfare. Lynch (2024) considers cyberspace as an arena of great power competition in the context of a fragmented international order, where cyber operations become an element of a strategy of deterrence and power projection.

Thus, cyberattacks are transformed from a tool of point impact into a systemic "digital weapon against infrastructure", which necessitates a rethinking of state policy to counter organized and transnational cybercrime in armed conflict and post-conflict recovery. Atkins and Chappell (2021) emphasize that the fragmented nature of state policy during armed conflict and insufficient coordination between state and private actors only increase the vulnerability of critical infrastructure. Streltsov (2017), analyzing the formation of the cybersecurity system in Ukraine, demonstrates that the formation of the institutional architecture is influenced by both internal security challenges and external commitments in the field of European security.

At the same time, some scholars consider armed conflict as a stimulant for increasing the state's cybersecurity. Mamediieva and Moynihan (2023)

http://dx.doi.org/10.21511/ppm.23(4).2025.45

emphasize that armed conflict leads to a sharp increase in the role of the state's digital resilience and the level of its cybersecurity, since this directly determines the government's operational capacity. In financial markets, the consequences of armed conflict and global shocks are manifested through increased interconnections and volatility: armed conflict and pandemic change cross-market connections between stock markets and cryptocurrencies, increasing the sensitivity of the financial system to new types of risks, including cyberfinancial ones (Bampinas & Panagiotidis, 2024).

After the end of the active phase of the armed conflict, cyber risks continue to remain one of the key destabilizers of the country's development, as they affect the processes of infrastructure restoration, increase institutional weakness, and reduce economic stability. Based on macroeconomic analysis of the long-term consequences of conflict, Rogoff (2022) demonstrates that military conflicts create long-lasting shocks to potential growth, debt sustainability, and the investment climate, which significantly narrow the fiscal and institutional opportunities for investments in rebuilding and strengthening security, including digital infrastructure. A characteristic feature of the armed conflict and post-conflict period is the change in cyberattack patterns and their reorientation to the financial, energy, and communication sectors (Song et al., 2024). Sanders et al. (2022) emphasize that energy infrastructure in transition periods becomes a priority target, which requires enhanced cyber protection. At the same time, traditional response models in the post-conflict phase often turn out to be ineffective, as cyber threats become more decentralized and adaptive (Guitton & Frechette, 2023). Local governments, especially during the reconstruction period, face shortages in personnel, resources, and technological capabilities, making them extremely vulnerable to organized cybercrime (Norris et al., 2023).

Under such conditions, the state policy of countering organized and transnational cybercrime in the armed conflict and post-conflict periods acquires strategic importance. Digital threats are becoming not only a tool for illicit enrichment but also a means of influencing political stability, defense capability, and economic security of the state. Scientific literature offers different interpretations of the nature of these threats and the mechanisms of their escalation, which indicates the multidimensionality of the problem. However, scientists interpret the nature and mechanisms of escalation of such threats differently, offering alternative approaches to their elimination.

According to Miadzvetskaya (2024), organized cybercrime in the armed conflict and post-conflict periods goes beyond purely technical incidents and becomes an element of the international security architecture. In this context, EU sanctions in response to cyberattacks take on the character of crime-based emergency measures – special political and legal instruments designed to protect the European security space in situations of sharp escalation of threats.

A key component of minimizing the state's cyber vulnerabilities is ensuring the optimal design of regulatory mechanisms, a system of incentives and mechanisms for distributing responsibility between the state and the private sector (Moore, 2010). This is especially relevant in armed conflict and post-conflict conditions, when the state must ensure a balance between control, innovation, and economic sustainability. In the same context, Carr (2016) emphasizes that public-private partnerships can serve as the central pillar of national cyber strategies, the effectiveness of which is determined by the clarity of roles, coordination mechanisms, and the level of trust between the parties involved. In times of armed conflict, when targeted information and digital attacks can paralyze critical services, it is precisely the coordination of actions of the state and business that is crucial for ensuring systemic stability.

Ubowska and Królikowski (2022) expand the institutional dimension of public policy implementation, emphasizing that a key prerequisite for the successful implementation of formal strategies to counter cyber threats is a developed cybersecurity culture in public administration. In post-conflict conditions, the formation of such a culture becomes not only a technical task but also an important element of the administrative and organizational reconstruction of the state. At the micro level, Frandell and Feeney (2022) draw attention to the socio-technical nature of local government cyber vulnerabilities: technological, organizational,

and human factors mutually reinforce risks. This is especially critical in countries experiencing an armed conflict or post-conflict stage, when staff overload, infrastructure damage, and instability of management processes increase the likelihood of successful attacks. At the macro level, Aldasoro et al. (2020) demonstrate that the drivers of cyber risk in the financial sector, the scale of institutions, their digital integration, and systemic significance, form the basis for considering cyber threats as a component of macroprudential policy. This is of particular practical importance for states rebuilding their financial systems after armed conflicts.

Agrafiotis et al. (2018) offer a detailed taxonomy of cyber damage, which allows assessing the consequences of attacks in financial, reputational, operational, and social dimensions. This creates an opportunity for systematic monitoring of threats and building scenarios of their escalation at the national security level.

Nobles (2024) focuses on the rapid development of artificial intelligence, which is becoming a tool for automating and scaling criminal activity. In armed conflict and post-conflict periods, this actualizes the need for proactive regulation and institutional strengthening of state policy.

Even a historical analysis of the exchange of sensitive information (Adams, 2016) shows that the need to protect personal and strategically important data is a constant characteristic of social development. In the digital age, these challenges are amplified by the scale and speed of data circulation, which makes information security an integral element of state policy, especially in armed conflict and post-conflict conditions.

Thus, post-conflict digital security is being formed in extremely complex conditions, where cyber threats develop faster than the institutional capabilities of states to neutralize them.

At the same time, the growth of cybercrime is not only in zones of active hostilities. In states that are not subject to direct military attacks, criminal activity is stimulated by other factors, in particular: digital transformation, macroeconomic turbulence, and institutional vulnerability. Even in the absence of a direct military threat, cybercrime is growing against the backdrop of accelerated digitalization, the emergence of new opportunities for cybercriminals, and the expansion of shadow markets.

At the international level, researchers are focusing on the cross-border and organized nature of cyberthreats. As Hui et al. (2017) show, in developing countries, cybercrime often transcends national borders and takes on the character of networked criminal structures. Similar conclusions are drawn by Yilma (2014), showing that in states with limited institutional resources, the legal framework for cyber protection is fragmented and lags real threats, creating a favorable environment for the expansion of organized cybercrime. The private sector is no less vulnerable: a study by Arroyabe et al. (2024) confirms that SMEs in jurisdictions with low levels of digital maturity become key targets for attacks due to limited investment in cybersecurity and high levels of anxiety about digital risks, which influences their management decisions.

Social and psychological mechanisms also play a significant role in shaping cyber risks. Dodel and Mesch's (2019) model demonstrates that users' willingness to apply cyber protection measures depends on a combination of cognitive, socio-economic, and digital factors. Virtanen (2017) shows that fear of cybercrime is based on individual vulnerabilities and experiences of victimization, forming specific patterns of risk perception. Cook et al. (2023) prove that economic cybercrime in Europe is perceived as the result of the interaction of macro-level security indicators, the state of digital infrastructure, and individual behavioral characteristics. At the global level, Buil-Gil et al. (2021) demonstrate that exogenous shocks, such as the COVID-19 pandemic, radically change the opportunity structure for cybercriminals, contributing to the growth of online fraud and remote access attacks.

The synthesis of these studies allows us to identify several systemic patterns. First, in an armed conflict period, cybercrime is transformed into a form of "digital weaponry" aimed at undermining critical infrastructure and weakening the state's operational capacity. Second, in the post-armed conflict period, threats are implemented against

http://dx.doi.org/10.21511/ppm.23(4).2025.45

the background of limited fiscal and institutional space, competition for reconstruction resources, and fragmented response models, which complicates the formation of sustainable cyber defense mechanisms. Third, in countries not in a state of armed conflict, cybercrime is shaped by structural (digital maturity, quality of legal regulation), economic (turbulence, market shocks), and social (behavioral patterns, fear, digital literacy) factors and is closely linked to the activities of transnational criminal networks.

The purpose of this study is to analyze the impact of technological, institutional, and financial factors on national cyber resilience, considering the transformational changes that occur under conditions of armed conflict and post-conflict recovery, using the example of countries that have recently experienced and in some cases continue to experience armed conflicts of varying scale and consequences.

2. METHODS

The analysis of factors shaping national cyber resilience in the context of cybercrime was conducted using an approach that distinguishes between three security regimes: armed conflict, post-armed conflict recovery, and relative stability. In this study, the term armed conflict is used in a narrow analytical sense and refers specifically to armed conflict, rather than to conflict as a general form of political, economic, or social instability. Accordingly, the post-conflict recovery phase is interpreted as the post-armed conflict recovery period, as well as periods of protracted instability following armed conflict, characterized by incomplete institutional reconstruction, heightened external security pressures, persistent governance vulnerabilities, and uneven restoration of critical digital infrastructure. Such environments do not represent full stabilization, but rather transitional security conditions in which cybersecurity capacities remain fragile. This framework allows us to examine how periods of armed conflict alter the structure of cyber threats, how post-armed conflict recovery and protracted instability affect digital vulnerability, and which institutional, technological, and financial factors are most strongly associated with cyber resilience under conditions of relative stability.

The empirical analysis covers European non-EU countries within the European security space that have experienced armed conflict, post-armed conflict recovery, or conflict-induced prolonged instability over the period 2010-2024 (Tiutiunyk, 2025). The non-EU subsample includes Ukraine, Moldova, Georgia, Armenia, Azerbaijan, and Serbia (Table 1). Importantly, periods of instability are defined as being caused by security and armed conflict, rather than economic or political volatility. This selection allows us to capture heterogeneous security trajectories while preserving a common institutional and geopolitical context relevant for comparative analysis of cyber resilience.

The security regime attribution is conducted at the country-year level to capture time-varying security conditions, in line with the World Bank's analytical approach to fragility, conflict, and violence. This approach is based on a systematic review of academic literature on armed conflict, post-conflict recovery, and protracted instability (Rogoff, 2022; European Parliament, 2022; Smith, 2022; ENISA, 2023) and reflects prevailing security conditions rather than individual incidents at the country-year level. The attribution reflects prevailing and persistent security environments rather than isolated events or short-term escalations at the country-year level. For example, Georgia is attributed to a post-armed conflict recovery and protracted instability environment during 2010–2018, reflecting the long-term consequences of the 2008 armed conflict, unresolved territorial disputes, and persistent security externalities, while the period 2019–2024 is classified as relative stability, indicating a gradual attenuation of conflict-related pressures. A similar time-sensitive logic is applied to Armenia and Azerbaijan, where the year 2020 is classified as an active armed conflict, followed by a post-conflict recovery regime in subsequent years.

Table 1 presents an attribution of country-periods to three mutually exclusive security regimes used in the empirical analysis. Armed conflict refers to years characterized by active large-scale armed hostilities involving regular military forces. The post-armed-conflict and protracted instability environment captures periods following the termination of active hostilities as well as cases char-

Table 1. Security regime attribution across selected countries and periods (2010–2024)

Country	Year	Armed conflict	Post-armed conflict recovery and protracted instability environment	Relative stability
Ukraine	2010–2013	–	–	+
	2014–2024	+	–	–
Moldova	2010–2024	–	+	–
Georgia	2010–2018	–	+	–
	2019–2024	–	–	+
Armenia	2010–2019	–	–	+
	2020	+	–	–
	2021–2024	–	+	–
Azerbaijan	2010–2019	–	–	+
	2020	+	–	–
	2021–2024	–	+	–
Serbia	2010–2024	–	+	–

Note: The "+" and "–" symbols indicate the presence or absence of dominant characteristics associated with each regime during the specified period. The attribution reflects prevailing security environments rather than isolated events or short-term escalations and is based on the results of a structured review of the literature on armed conflict, post-conflict recovery, and conflict-related cyber threats (Rogoff, 2022; European Parliament, 2022; Smith, 2022; ENISA, 2023).

acterized by prolonged security instability, frozen conflicts, unresolved territorial disputes, or recurrent military tensions, even in the absence of continuous warfare (e.g., Moldova and Serbia). Relative stability denotes periods without active armed conflict and outside the post-conflict or protracted instability environment; it does not imply the absence of latent security risks, hybrid threats, or political tensions. Each country-year observation is assigned to one regime only.

Importantly, countries in this study are not permanently assigned to fixed categories such as "armed conflict," "post-armed conflict," or "stable." Instead, the classification is applied at the country-year level and reflects time-varying security regimes observed over the study period. This approach allows individual countries to transition between different security contexts over time, capturing real-world dynamics of conflict escalation, post-conflict recovery, and subsequent stabilization.

A country-year observation is classified as belonging to the armed conflict regime if it is characterized by active hostilities or high-intensity armed escalation on the country's territory that materially affected institutional stability, economic activity, and exposure to cyber threats.

The post-conflict regime is defined as a transitional phase following the cessation of active hostilities, during which countries face heightened institutional vulnerability, reconstruction challenges, and elevated security risks. Consistent with UN and World Bank post-conflict frameworks, a ten-year window after the end of active conflict is used to identify post-conflict observations. For example, Georgia experienced a post-conflict phase following the 2008 conflict until 2018, after which subsequent observations are classified as relatively stable. Armenia and Azerbaijan entered the post-conflict regime following the 2020 escalation.

All remaining observations are classified as belonging to a relative stability regime, defined as periods without active armed hostilities and without direct post-armed conflict recovery dynamics. The relative stability regime, therefore, includes stable-year observations for selected years for Ukraine, Georgia, Armenia, and Azerbaijan when security conditions were not directly shaped by ongoing or recent armed conflict.

This time-varying regime classification shifts the focus of the analysis away from static country groupings and toward understanding how the determinants of national cyber resilience evolve as countries move across different security contexts over time.

The Global Cybersecurity Index (GCSI) is used to assess national cyber resilience. Explanatory variables are grouped into three thematic blocks: institutional (ISI), technological (TDI), and financial (FRI). This classification follows established theoretical frameworks of cyber resilience proposed by

http://dx.doi.org/10.21511/ppm.23(4).2025.45

NIST, ENISA, and the ITU Global Cybersecurity Index, which conceptualize a country's ability to withstand cyber threats as emerging from the interaction of governance capacity, technological readiness, and financial resources.

Cyber resilience cannot be achieved without effective institutions that define rules, ensure coordination, and enable a timely response to cyber incidents. Accordingly, the institutional block (ISI) includes the following indicators:

- Government Effectiveness (GEF) – shows the quality of public administration, i.e., the ability to implement policies that affect cybersecurity.
- Rule of Law (RL) – characterizes the level of legal certainty and the rule of law, which is critically important for regulating the digital environment.
- Cybersecurity Strategy (CYBSTR) – the presence of an official cybersecurity strategy determines the strategic readiness of the state.
- CERT/CSIRT (CERT, CSIRT) – reflects the presence of a national cyber incident response center.
- Cyber agreements participation (CYBAGR) – participation in the Budapest Convention confirms the state's integration into the international cyber defense regime.

These variables reflect the country's institutional readiness to perform cyber defense functions and form the basic platform of national digital resilience.

The Technology Group (TDI) determines the level of technological readiness for cyber threats, the speed of their detection, and the ability to minimize the consequences. This block includes:

- E-Government Development Index (EGI) – reflects the digitalization of government services.
- Secure Internet Servers (SIS) – measures the technical level of data transmission security.
- Internet usage (INTUS) and Broadband subscriptions (BROADSUB) – describe the penetration of digital technologies among the population.
- Network Readiness Index (NRI) – assesses the overall digital readiness of the economy.

Technological indicators form the physical basis of cyber resilience: the higher the level of digital infrastructure, the lower the probability of successful attacks and the scale of their consequences.

The financial block (FRI) captures the state's financial capacity to invest in cyber security, absorb losses, and sustain the functioning of critical infrastructure. It includes:

- Non-life insurance premiums as a share of GDP (NLIP) – reflects the development of the insurance sector as a mechanism for cyber risk coverage.
- Financial Development Index (FDI) – comprehensively characterizes the depth of the financial system.
- Credit to the private sector (CPS) – shows the potential of business to finance digital transformation.
- Bank capital to assets ratio (BCAR) – an indicator of the resilience of the banking system, sensitive to cyber incidents.

These indicators reflect the financial resilience of the economy in the face of cyber-related shocks, including cyber risks.

In addition, macroeconomic control indicators have been added to the model to ensure the correctness of the assessment of the impact of institutional, technological, and financial factors. The control variables eliminate the bias of the estimates associated with macroeconomic differences between countries and allow us to isolate the net effect of ISI, TDI, and FRI on cyber resilience:

- GDP per capita (GDP) – the overall level of economic development, which determines the country's investment capacity.

- Unemployment rate (UNEMP) – reflects socio-economic stability, which affects digital security.
- Inflation rate (INF) – characterizes macroeconomic risks and budget constraints.
- Non-performing loans (NPL) – an indicator of the state of the financial sector, important for critical infrastructure.

To capture the impact of different security contexts, three time-varying country-year regime variables are defined: CONFLICT, which takes the value of 1 in years characterized by active hostilities or high-intensity armed escalation; POSTCONFLICT equals 1 in years following the cessation of active hostilities or in periods of persistent conflict-induced instability in countries structurally affected by regional armed conflict, even in the absence of large-scale fighting. This category captures institutional, economic, and cybersecurity vulnerabilities associated with recovery phases and regional spillover effects rather than purely domestic instability; and STABLE, indicating years without active armed conflict and with exhausted post-conflict effects. These variables enable a multidimensional assessment of how varying levels of security turbulence shape national cyber resilience.

The data sources for forming the information base of the study are international institutional and statistical resources, in particular, World Bank Open Data, International Telecommunication Union, United Nations E-Government Survey, and FIRST CSIRT database.

The analysis employs a scenario-based approach, distinguishing between armed conflict, post-armed conflict recovery, and relative stability regimes. This approach allows assessing whether the effects of institutional, technological, and financial factors intensify, weaken, or persist as countries transition across different security contexts.

National cyber resilience is modeled using the following fixed-effects panel specification:

$$GCSI_{it} = \beta_0 + \beta_1 ISI_{it} + \beta_2 TDI_{it} + \beta_3 FRI_{it} + \gamma X_{it} + \alpha_i + \varepsilon_{it}, \quad (1)$$

where i denotes country, t denotes year, α_i captures country fixed effects, X_{it} is a vector of control macroeconomic variables (GDP, UNEMP, INF, NPL), ISI_{it} is an institutional capacity (GEF, RL, CYBSTR, CERT, CSIRT, CYBAGR), TDI_{it} is a technological capacity, FRI_{it} is a financial capacity, and ε_{it} is a random error.

To assess how security regimes modify the impact of key determinants, the model is extended with interaction terms between ISI, TDI, FRI, and the armed conflict and post-conflict recovery regimes. This specification allows identifying how the elasticity of cyber resilience with respect to institutional, technological, and financial factors changes across different security contexts:

$$scen_{it} \in \begin{Bmatrix} 0 = Stable, \\ 1 = Conflict, \\ 2 = PostConflict \end{Bmatrix}. \quad (2)$$

Since the central objective is to assess how armed conflict and post-armed conflict recovery conditions modify the impact of institutional, technological, and financial factors on national cyber resilience, the baseline model is extended by a system of interaction terms:

$$\begin{aligned} CSI_{it} &= \beta_0 + \beta_1 ISI_{it} + \beta_2 TDI_{it} + \beta_3 FRI_{it} \\ &+ \beta_4 Conflict_{it} + \beta_5 Postconflict_{it} + \\ &\beta_6 \left(ISI_{it} \cdot Conflict_{it} \right) \\ &+ \beta_7 \left(TDI_{it} \cdot Conflict_{it} \right) \\ &+ \beta_8 \left(FRI_{it} \cdot Conflict_{it} \right) \\ &+ \beta_9 \left(ISI_{it} \cdot PostConflict_{it} \right) \\ &+ \beta_{10} \left(TDI_{it} \cdot PostConflict_{it} \right) \\ &+ \beta_{11} \left(FRI_{it} \cdot PostConflict_{it} \right) + \gamma X_{it} + \alpha_i + \varepsilon_{it}. \end{aligned} \quad (3)$$

This specification allows us to separate the baseline effects of institutional, technological, and financial factors from their context-dependent modification effects arising under conditions of armed conflict or during post-conflict recovery. The coefficients $\beta_0 - \beta_5$ show how the elasticity of the GCSI with respect to ISI, TDI, and FRI changes compared to stable countries: $\beta_6 - \beta_8$ capture changes in the impact of ISI, TDI, and FRI during conflict periods, while $\beta_9 - \beta_{11}$ reflect how these ef-

http://dx.doi.org/10.21511/ppm.23(4).2025.45

fects are modified in the post-conflict phase relative to years of relative stability.

This approach provides a sensitive assessment of the complex systemic interaction between structural country characteristics and national cyber resilience across different security contexts.

A fixed-effects (FE) estimator is employed to account for unobserved, time-invariant country-specific characteristics. This allows isolating the within-country dynamics of cyber resilience, technological development, and financial capacity in response to conflict-related and post-conflict security shocks.

The validity of the choice of the estimation model is checked using the Hausman test, which allows us to find out whether the individual effects of the country correlate with the explanatory variables. If such a correlation is detected, the random effects model is incorrect, which justifies the use of fixed effects.

Panel data, especially those containing countries with different trajectories of armed conflict and recovery, are usually characterized by heteroscedasticity, autocorrelation, and possible clustering of shocks within each country. To detect them, the following steps are performed sequentially: the Wald test for group heteroscedasticity (Modified Wald test); the Wooldridge test for first-order autocorrelation in panels; and analysis of the error structure to check the simultaneous presence of these violations.

If at least one of the listed problems is confirmed, the model with clustered standard errors at the country level is used to estimate. This approach ensures the correctness of the statistical conclusion even with a small number of panels and allows the model to consider the uneven impact of military events, reforms and structural technological changes.

After building the model, the marginal effects for each mode are calculated:

$$ME_s^{(k)} = \frac{\partial GCSI}{\partial K}\Big|_{scen=s}, \quad (4)$$

where

$$K \in \{ISI, TDI, FRI\},$$
$$s \in \{Stable, Conflict, Postconflict\}.$$

These marginal effects allow evaluating how the effectiveness of institutional, technological, and financial mechanisms supporting cyber resilience varies across security contexts. Finally, conditional predicted values of cyber resilience are generated:

$$\widehat{GCSI}_{s,it} = f\begin{pmatrix} ISI_{it}, TDI_{it}, FRI_{it}, \\ scen = s, X_{it} \end{pmatrix}. \quad (5)$$

This enables the comparison of cyber resilience trajectories in armed conflict-affected, post-conflict recovery, and relatively stable environments, as well as assessing recovery dynamics following the cessation of armed conflict.

3. RESULTS

To directly address the objective of analyzing how institutional, technological, and financial determinants of cyber resilience vary across different security environments, security regimes in this study are defined at the country-year level. Countries are not assigned to fixed groups; instead, individual country-year observations are classified as belonging to periods of armed conflict, post-armed conflict recovery and protracted instability, or relative stability over the period 2010–2024. This approach allows countries to transition between security regimes over time and captures within-country variation in security conditions.

All reported coefficients and estimated effects, therefore, reflect within-country changes over time, indicating how the impact of institutional, technological, and financial determinants evolves as countries move across different security regimes.

Table 2 reports descriptive statistics of cyber resilience indicators and their determinants across the three security regimes. The Global Cybersecurity Index (GCSI) exhibits its lowest average value during armed conflict (Mean = 0.702; SD = 0.198), increases slightly in the post-armed conflict and protracted instability environment (Mean = 0.694; SD = 0.231), and reaches its highest level under relative stability (Mean = 0.737; SD = 0.239). This

Table 2. Descriptive statistics of cyber resilience determinants by security regime

Variables	Mean			Std. Dev.		
	Armed conflict	Post-armed conflict recovery	Relative stability	Armed conflict	Post-armed conflict recovery	Relative stability
GCSI	0.702	0.694	0.737	0.198	0.231	0.239
GEF	–0.010	0.408	0.264	0.740	0.569	0.663
RL	–0.320	0.156	0.245	0.769	0.540	0.664
CYBSTR	0.722	0.667	0.700	0.461	0.477	0.460
CERT	1.000	0.905	0.894	0.000	0.297	0.308
CSIRT	0.722	0.714	0.783	0.461	0.457	0.413
CYBAGR	1.000	1.000	0.983	0.000	0.000	0.128
EGI	0.734	0.699	0.688	0.123	0.128	0.129
SIS	5995.64	3574.94	14559.85	4875.06	4695.76	26694.48
INTUS	72.438	68.222	70.872	13.955	17.914	16.059
BROADSUB	18.405	20.753	22.478	6.487	6.484	7.809
NLIP	1.197	1.147	1.133	0.403	0.487	0.461
FDI	0.303	0.344	0.308	0.163	0.160	0.103
CPS	46.213	47.319	49.613	21.397	14.469	13.772
BCAR	6.631	9.460	10.190	2.399	2.656	2.325
GDP	–0.428	3.761	3.384	7.993	2.990	4.011
UNEMP	8.206	12.041	9.994	3.547	6.179	6.554
INF	9.694	4.107	3.722	11.276	3.885	4.457
NPL	28.151	2.517	7.098	20.266	1.221	5.350
SCEN	1.000	2.000	0.000	0.000	0.000	0.000

pattern indicates that active conflict is associated with weaker cyber resilience, while more stable environments provide more favorable conditions for cybersecurity development.

Institutional indicators display substantial variation across regimes. Government effectiveness (GEF) is negative on average during armed conflict (Mean = -0.010; SD = 0.740), improves markedly in the post-conflict and protracted instability regime (Mean = 0.408; SD = 0.569), and is highest during periods of relative stability (Mean = 0.264; SD = 0.663). A similar pattern is observed for the rule of law (RL), which remains strongly negative during armed conflict (Mean = –0.320) and becomes positive under relative stability (Mean = 0.245). These differences point to substantial institutional degradation during conflict and gradual recovery thereafter.

At the same time, formal cybersecurity arrangements are widely present across regimes. The presence of national CERTs equals one for all armed conflict observations (Mean = 1.000) and remains high in post-conflict (Mean = 0.905) and stable regimes (Mean = 0.894). Participation in international cybersecurity agreements (CYBAGR) is also nearly universal, with mean values equal to 1.000 in conflict and post-conflict observations and 0.983 under relative stability. This suggests that formal institutional structures alone are insufficient to offset broader governance weaknesses during periods of conflict.

Technological indicators exhibit pronounced regime sensitivity. While E-government development (EGI) remains relatively stable across regimes (ranging from 0.688 to 0.734), infrastructure-related indicators vary sharply. The average number of secure internet servers (SIS) equals 5,996 during armed conflict, compared to 3,575 in the post-conflict and protracted instability regime and 14,560 under relative stability, with very large dispersion, particularly in stable observations (SD = 26,694). Internet usage (INTUS) declines from an average of 72.4 percent during armed conflict to 68.2 percent in post-conflict periods and increases again to 70.9 percent under relative stability. Broadband penetration follows a similar pattern, averaging 18.4 subscriptions per 100 inhabitants in armed conflict years and 22.5 under relative stability.

Financial indicators further confirm regime-specific heterogeneity. Credit to the private sector (CPS) averages 46.2 percent of GDP during armed

http://dx.doi.org/10.21511/ppm.23(4).2025.45

conflict, increasing to 49.6 percent under relative stability, while bank capital adequacy (BCAR) rises from 6.63 in conflict conditions to above 10 during relative stability. The most pronounced differences are observed for non-performing loans (NPLs), which reach very high levels during armed conflict (Mean = 28.15; SD = 20.27), fall sharply in post-conflict periods (Mean = 2.52), and stabilize at lower levels under relative stability (Mean = 7.10). These figures indicate significantly elevated financial-sector vulnerability during conflict episodes.

Macroeconomic indicators also reflect heightened instability during armed conflict. Inflation averages 9.69 percent in armed conflict observations compared to 3.72 percent under relative stability, while GDP dynamics are substantially more adverse during armed conflict (Mean = -0.43) than in stable environments (Mean = 3.38). Unemployment is lowest during armed conflict (Mean = 8.21) but rises in post-conflict periods (Mean = 12.04), reflecting delayed labor-market adjustments following conflict shocks.

To illustrate these systematic differences, mean comparisons are reported for a selected set of representative institutional, technological, macroeconomic, and outcome indicators. The quantitative gaps observed across security regimes confirm the presence of structural heterogeneity and provide a strong empirical justification for the subsequent regime-specific estimations.

Thus, descriptive differences across security regimes indicate substantial heterogeneity in institutional, technological, and macroeconomic conditions, motivating regime-specific estimations.

To assess the robustness of cyber resilience determinants and the role of security regimes, Table 3 summarizes the statistical significance of key indicators across three model specifications: a baseline fixed-effects model without regime differentiation, a fixed-effects model with security regimes, and a full fixed-effects model with regimes and additional controls.

The results indicate that only a limited subset of determinants remains consistently significant across specifications. Within the institutional block, the presence of a national cybersecurity strategy (CYBSTR) emerges as the most stable positive determinant of cyber resilience, retaining statistical significance across all model variants. In contrast, general state-capacity indicators (GEF and RL) display weak and unstable significance, suggesting that their effects are highly context-dependent.

Operational cybersecurity institutions (CERT/CSIRT) exhibit a consistently negative association with cyber resilience in regime-sensitive specifications, which is consistent with a reactive institutional response pattern, whereby such structures are strengthened following elevated threat exposure rather than serving as preventive mechanisms.

Within the technological block, the E-Government Development Index (EGI) remains the most robust predictor of cyber resilience, although its significance weakens in the full specification. Other digital infrastructure indicators display limited or unstable effects.

Financial indicators show the least stability across specifications. While some variables (NLIP, CPS, BCAR) are significant in block-level models, these effects do not persist in the comprehensive specification, indicating a more indirect and context-dependent role of financial capacity in shaping cyber resilience.

Scenario variables capturing armed conflict and post-armed conflict recovery contexts display positive but uneven effects, suggesting that security shocks and recovery phases modify the influence of structural determinants rather than exerting a uniform direct effect on cyber resilience.

To explicitly capture how the determinants of cyber resilience operate under different security conditions, regime-specific fixed-effects regressions are estimated separately for periods of armed conflict, post-armed conflict and protracted instability, and relative stability. The results are reported in Table 4. To facilitate comparison between regime-specific estimates and the overall relationship, the fixed-effects model is first estimated for the full sample and then separately for each security regime.

Table 3. Significance of cyber resilience determinants across model specifications and security regimes (dependent variable – Global Cybersecurity Index)

Variables	Block	Baseline FE model (no regime)	FE model with security regimes	Full FE model with regimes and controls	Direction & Significance
GEF	Institutional	+ (p<0.1)	NS	NS	Weak/unstable
RL	Institutional	+ (p<0.05)	+ (p<0.1)	Not included	Sensitivity check only
CYBSTR	Institutional	+ (p<0.01)	+ (p<0.1)	+ (p=0.094)	Stable positive
CERT/CSIRT	Institutional	+ (p<0.05)	+ (p<0.05)	– (p<0.001)	Stable, strong negative
CYBAGR	Institutional	NS	NS	Not included	Insignificant
EGI	Technological	+ (p<0.01)	+ (p<0.05)	+ (p=0.305)	Stable positive, weak in the full model
SIS	Technological	NS	NS	Not included	Insignificant
INTUS	Technological	+ (p<0.05)	NS	Not included	Partial (base only)
BROADSUB	Technological	NS	NS	+ (p=0.161)	Not significant
NRI	Technological	+ (p<0.1)	+ (p<0.1)	Not included	Consistent minor effect
NLIP	Financial	+ (p<0.05)	+ (p<0.1)	Not included	Weak positive, not robust
FDI	Financial	NS	NS	Not included	Insignificant
CPS	Financial	– (p<0.05)	– (p<0.05)	NS	Negative in the submodel only
BCAR	Financial	– (p<0.05)	NS	NS	Unstable
UNEMP	Macroeconomic	+ (NS)	– (p<0.05)	– (p=0.018)	Stable negative
INFLATION RATE	Macroeconomic	+ (NS)	+ (p<0.05)	+ (p=0.026)	Stable positive
NPL TO CAPITAL	Financial risk	Not included	Not included	NS	Insignificant
SCEN: Armed conflict	Scenario	+ (p = 0.063)	–	+ (p=0.225)	Weak positive
SCEN: Post–armed conflict	Scenario	NS	+ (p=0.024)	+ (p=0.173)	Positive recovery effect
Interaction: GEF × Armed conflict	Interaction	Not in model	Not in model	+ (p=0.264)	Positive, not significant
Interaction: GEF × Post–armed conflict	Interaction	Not in model	Not in model	– (p=0.624)	Negative, not significant

Note: Security regimes are defined at the country-year level and allow countries to transition between armed conflict, post-armed-conflict and protracted instability, and relative stability over time.

Within the institutional block, a strong regime dependence is observed. While Government Effectiveness (GEF) is statistically insignificant in the overall specification, it becomes strongly positive during armed conflict ($\beta = 1.036$, $p < 0.01$), indicating that state capacity plays a critical role under acute security stress. In post-armed conflict and stable regimes, this effect disappears, suggesting that its relevance is context-specific rather than universal. By contrast, the presence of a national cybersecurity strategy (CYBSTR) remains positive and statistically significant both in the overall model and across all security regimes, highlighting its stabilizing role irrespective of the security environment.

Operational institutions (CERT and CSIRT) are insignificant during armed conflict periods but become significant under relative stability, suggesting that incident-response structures are more effective once basic security conditions are restored.

In the technological block, the E-Government Development Index shows a strong positive association with cyber resilience during armed conflict ($\beta = 0.951$, $p < 0.01$) and relative stability ($\beta = 1.779$, $p < 0.01$), while its effect weakens in the post-conflict regime. Secure Internet Servers (SIS) are significant only during armed conflict, indicating a heightened role of core digital infrastructure when cyber risks are elevated.

Financial determinants exhibit the weakest and most context-dependent effects. Under relative stability, credit to the private sector (CPS), bank capital adequacy (BCAR), and financial development (FDI) display statistically significant

http://dx.doi.org/10.21511/ppm.23(4).2025.45

Table 4. Fixed-effects regressions of cyber resilience: overall sample and security regimes

Variables	Overall sample	Armed conflict	Post-armed conflict recovery	Relative stability
GEF	0.074	1.036***	−0.911	0.00719
	(0.312)	(9.57e−08)	(0.864)	(0.369)
CYBSTR	0.309***	0.405***	0.408***	0.319***
	(0.057)	(1.41e−08)	(0.0282)	(0.102)
CERT	−0.261***	0	0	−0.288**
	(0.083)	(.)	(.)	(0.116)
CSIRT	0.303***	0	0	0.286***
	(0.075)	(.)	(.)	(0.0893)
EGI	1.680***	0.951***	0.418	1.779***
	(0.194)	(0.0996)	(2.085)	(0.253)
SIS	0.000	0.0000183**	0.0000635	4.32e−08
	(0.000)	(0.0000039)	(0.000046)	(0.00000063)
NLIP	0.213	−0.372	−0.0123	0.385*
	(0.218)	(.)	(0.132)	(0.175)
FDI	−0.467	13.06	6.737	−1.018***
	(0.541)	(.)	(3.951)	(0.284)
CPS	−0.003	−0.00440	0.00398	−0.0128**
	(0.004)	(.)	(0.0114)	(0.00441)
BCAR	−0.045**	−0.0858	0.0235	−0.0364**
	(0.015)	(.)	(0.0210)	(0.0125)
_cons	1.155***	0.650***	0.772	0.446
	(0.237)	(3.86e−08)	(0.408)	(0.361)

Note: All models are estimated using country fixed effects. Robust standard errors clustered at the country level are reported in parentheses.

negative associations with cyber resilience, potentially reflecting increased exposure to cyber risks in more financially intensive systems.

To identify potential multicollinearity and substantiate the specification of the empirical models, a correlation analysis was conducted separately for the institutional, technological, and financial blocks of variables. The results are summarized in Table 5.

Within the institutional block, a very high correlation is observed between Government Effectiveness (GEF) and Rule of Law (RL) ($r = 0.9198$, $p < 0.01$), indicating substantial overlap. Consequently, only GEF was retained in the baseline specification, while RL was used for robustness checks. Other institutional variables (CYBSTR, CERT, CSIRT) exhibit moderate correlations, allowing their joint inclusion.

In the technological block, strong correlations are detected among the E-Government Development Index (EGI), internet usage, and broadband subscriptions ($r > 0.80$). EGI was therefore retained as the most comprehensive indicator of digital ma-

Table 5. Summary of correlation structure and variable selection

Variable Pair	Pearson's r	p-value	Collinearity Issue	Action Taken
GEF – RL	0.9198	< 0.01	Very high	Only GEF included; RL used for robustness checks
EGI – BROADSUB	0.8162	< 0.01	Strong	Only EGI retained as the more comprehensive indicator
EGI – INTUS	0.8313	< 0.01	Strong	Internet usage excluded from model
CERT – CYBSTR	0.4924	< 0.05	Moderate	Both variables included
FDI – NLIP	0.6621	< 0.01	Moderate	Both retained; capture different financial aspects
NLIP – BCAR	−0.4423	< 0.01	Moderate (-)	Both retained; demonstrate structural contrast
FDI – BCAR	−0.3516	< 0.05	Low/Moderate	Acceptable; no action needed

Note: Correlation values above 0.80 are considered critical for multicollinearity. Such variables were not included simultaneously in the model. Values of 0.3-0.6 indicate acceptable correlation that does not violate statistical independence.

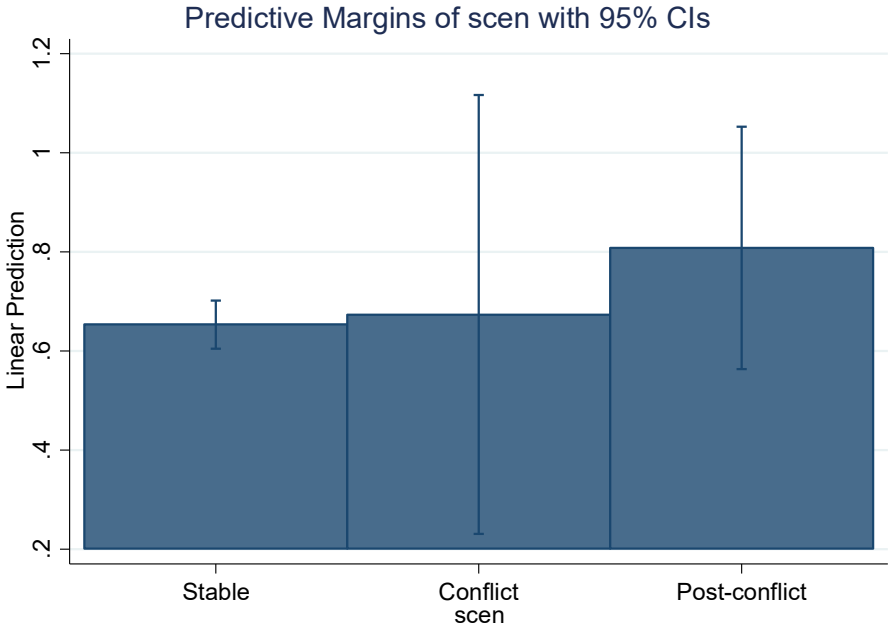


Figure 1. Predicted values of the Global Cyber Resilience Index across three security regimes (relative stability, armed conflict, and post-armed conflict recovery), estimated from a full fixed-effects model capturing within-country transitions over time

turity, while Secure Internet Servers (SIS) was included to capture the technical dimension of cyber infrastructure due to its lower correlation with other indicators.

In the financial block, all correlations remain below critical thresholds ($r < 0.80$), supporting the simultaneous inclusion of NLIP, FDI, CPS, and BCAR in the regression models.

To complement the regression results, predicted values and marginal effects are visualized to illustrate how cyber resilience evolves across security regimes within countries over time. These figures provide an intuitive representation of regime-specific patterns identified in the fixed-effects estimations.

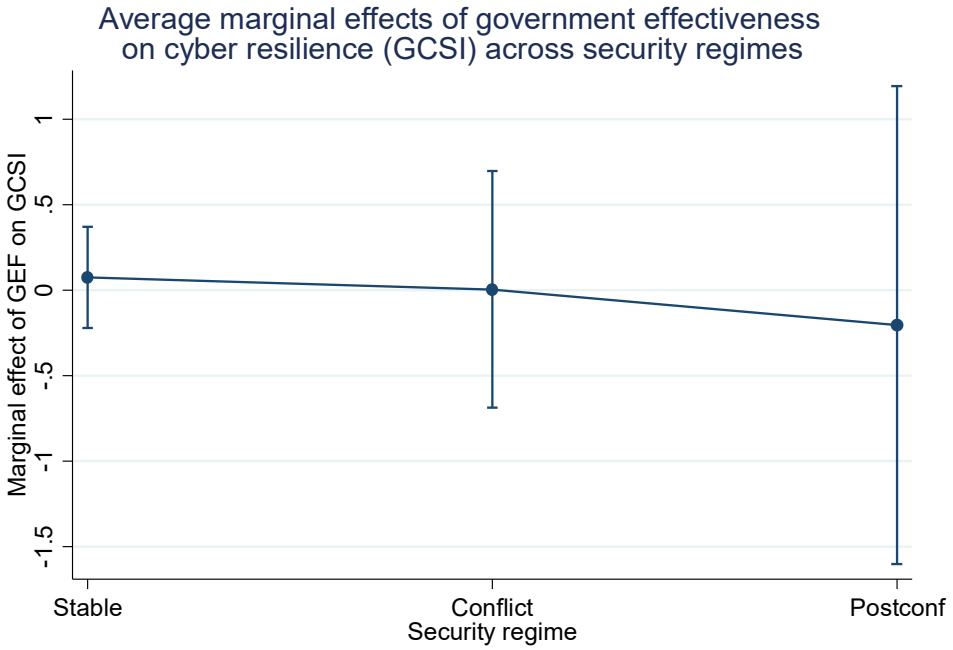
Figure 1 illustrates the predicted values of the Global Cyber Resilience Index across relative stability, armed conflict, and post-armed conflict recovery regimes, based on the full fixed-effects model. The figure shows that predicted cyber resilience is lowest during periods of armed conflict and higher during post-conflict recovery and relative stability. This pattern is consistent with the descriptive statistics and regression results, confirming that security regimes are associated with systematic shifts in the level of cyber resilience within countries over time.

In parallel, average marginal effects of government effectiveness (GEF) were estimated conditional on the security regime to further examine whether the strong regime-specific coefficients observed in the regression analysis translate into statistically distinct marginal impacts.

As illustrated in Figure 2, the estimated marginal effects of GEF differ across security regimes; however, none of these effects reach conventional levels of statistical significance. Under conditions of relative stability, the marginal effect of government effectiveness is positive but statistically insignificant. In conflict and post-conflict contexts, the estimated effects become smaller and more uncertain, as reflected by wide confidence intervals.

This result suggests that while government effectiveness appears to be particularly important during armed conflict in the regression estimates, its marginal effect is not precisely estimated once uncertainty is fully accounted for. The figure, therefore, supports a cautious interpretation of institutional capacity effects as

http://dx.doi.org/10.21511/ppm.23(4).2025.45



Note: Marginal effects are estimated from a fixed-effects model and reflect within-country changes as countries transition between relative stability, armed conflict, and post-conflict recovery. Vertical bars denote 95% confidence intervals.

Figure 2. Average marginal effect of government effectiveness (GEF) on cyber resilience across relative stability, armed conflict, and post-conflict recovery security regimes

Table 6. Results of diagnostic tests to substantiate the fixed effects model

Test	Purpose	Result	Conclusion
Breusch-Pagan LM	RE vs Pooled OLS	p = 1.000	RE model is not justified
Hausman test	FE vs RE	p = 0.541	FE is preferable
Modified Wald	Heteroscedasticity	χ^2 = 109.58 p < 0.001	Robust errors are required
F-test for FE	Significance of fixed effects	p = 0.0244	FE effects are significant – model is correct
Multicollinearity	Multicollinearity	VIF < 5 for all variables	Multicollinearity is not critical

context-dependent and sensitive to heightened volatility during conflict and recovery periods.

A set of diagnostic tests was conducted to assess the validity of the fixed-effects specification applied consistently across baseline, regime-augmented, and regime-specific estimations (Table 5). The F-test confirms the statistical significance of country fixed effects (p = 0.0244), while the Breusch-Pagan test does not support the use of random effects (p = 1.000). The Wooldridge test indicates the absence of first-order autocorrelation (p = 0.318). However, the Modified Wald test reveals the presence of heteroskedasticity (p < 0.001), and therefore cluster-robust standard errors are employed to ensure reliable statistical inference.

Table 5 reports robustness checks based on a fixed-effects specification including only digital and cybersecurity determinants. The model is estimated for the overall sample and separately across security regimes, where the pooled specification serves as a benchmark capturing average effects without regime differentiation. This design allows a direct comparison between overall and regime-specific estimates and facilitates assessing whether the core results are stable across armed conflict, post-armed conflict recovery, and relative stability environments.

The robustness results reported in Table 5 largely confirm the main findings of the baseline and regime-specific models. In the pooled specification, digital governance (EGI) and the presence of

Table 7. Robustness check: fixed-effects model with digital and cybersecurity determinants (overall sample and security regime)

Variables	Overall sample	Armed conflict	Post–armed conflict recovery	Relative stability
GEF	–0.054	1.369***	–1.653***	0.014
	(0.163)	(0.000)	(0.000)	(0.165)
CybStr	0.103*	0.215***	0.000	0.203***
	(0.055)	(0.000)	(.)	(0.045)
CERT	–0.327***	0.000	0.000	–0.431***
	(0.078)	(.)	(.)	(0.074)
EGI	1.346***	3.850***	–5.802***	1.542***
	(0.390)	(0.000)	(0.000)	(0.415)
BroadSub	0.017**	–0.075***	0.148***	0.019**
	(0.008)	(0.000)	(0.000)	(0.008)
BCAR	–0.008	0.000	0.000	–0.002
	(0.015)	(.)	(.)	(0.017)
Constant	–0.377	–0.673***	2.667***	–0.673*
	(0.331)	(0.000)	(0.000)	(0.354)
R–sq	0.701	1.000	1.000	0.709

Note: Standard errors are in parentheses, * $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$.

a national cybersecurity strategy (CYBSTR) retain a positive and statistically significant association with cyber resilience, while the CERT indicator remains strongly negative. This confirms that the core digital and cybersecurity determinants are robust to model simplification.

At the same time, regime-specific estimates reveal substantial heterogeneity behind these average effects. During armed conflict, the magnitude of digital governance effects increases sharply, with EGI and CYBSTR exhibiting particularly strong positive coefficients, while broadband penetration displays a negative association, reflecting infrastructure vulnerability under conflict conditions. In the post-armed conflict and protracted instability regime, several coefficients change sign and magnitude, indicating heightened volatility and structural adjustment dynamics. Under relative stability, the results converge toward the pooled estimates, with EGI and CYBSTR remaining positive and significant, and CERT retaining a negative effect.

Overall, the comparison between pooled and regime-specific robustness checks demonstrates that the average effects observed in the full sample mask pronounced regime-dependent dynamics. This supports the central argument of the study that the role of digital and cybersecurity determinants of cyber resilience is highly context-sensitive and varies systematically across security regimes.

4. DISCUSSION

The results of this study partially support dominant perspectives in the literature on national cyber resilience, which typically emphasize institutional quality and digital transformation as central determinants. However, the findings challenge the assumption that these relationships are stable across security contexts, revealing pronounced regime-dependent dynamics.

A key insight emerging from the analysis is that cyber resilience is shaped not only by the presence of institutional, technological, and financial capacities, but by how these capacities operate under different security conditions. Rather than acting as universally beneficial inputs, the same determinants perform fundamentally different roles depending on whether a country operates under stability, conflict, or post-conflict recovery.

From an institutional perspective, the findings refine existing interpretations of governance capacity in cybersecurity. While prior studies emphasize the importance of institutional quality for effective cyber governance (Carr, 2016; ENISA, 2023), the results suggest that under armed conflict, institutional capacity primarily functions as a mechanism of crisis coordination and rapid decision-making rather than long-term policy effectiveness. This interpretation is consistent with wartime governance evidence from Ukraine, where

http://dx.doi.org/10.21511/ppm.23(4).2025.45

adaptive administrative capacity and centralized coordination played a critical role in sustaining cyber operations under severe security pressure (Mamediieva & Moynihan, 2023; Fyshchuk et al., 2025). The observed negative association of CERT/CSIRT indicators further supports a reactive institutional dynamic, in which cybersecurity institutions tend to expand in response to heightened threat exposure rather than serving as purely preventive instruments (Aldasoro et al., 2020).

In line with the institutional findings, the technological dimension reveals a similarly conditional pattern. Although digital government development is often treated as a direct driver of cyber resilience, the results indicate that its effectiveness depends on institutional continuity. In conflict and post-conflict environments, digital capacity alone does not compensate for institutional disruption, reinforcing findings that technological systems amplify existing governance structures rather than operate independently (European Commission, 2022; Sanders et al., 2022). This helps explain why cyber resilience trajectories diverge sharply during periods of security shock, despite sustained investment in digital infrastructure (Song et al., 2024).

Financial determinants exhibit a more limited and contextually constrained role in shaping cyber resilience. In conflict-affected environments, financial indicators appear secondary to institutional and technological capacities, as policy priorities shift toward immediate security and operational continuity. Under relative stability, some financial variables become statistically significant, often with negative signs, suggesting that increased financial complexity and market integration may heighten cyber exposure rather than mitigate it. This interpretation aligns with broader evidence that economic turbulence and war-related shocks reshape financial vulnerabilities and risk transmission channels (Rogoff, 2022; Bampinas & Panagiotidis, 2024).

Taken together, the findings indicate that national cyber resilience is not a static attribute derived from institutional or technological endowments alone, but a dynamic outcome shaped by how these capacities interact with changing security conditions. By explicitly accounting for security regimes, the study helps reconcile heterogeneous empirical results reported in the literature and underscores the importance of regime-sensitive frameworks for assessing cyber resilience.

At the same time, the paper has certain limitations. The analysis relies on a restricted sample of countries with comparable data on cyber resilience and institutional indicators over the period 2010–2024, which limits the generalizability of the findings beyond European economies with medium to high levels of digital development. In addition, the absence of harmonized international data on cyber incidents constrains the direct measurement of cyber risk exposure. Future research could address these limitations by employing more flexible modeling approaches, such as Multivariate Adaptive Regression Splines (MARS) or Generalized Additive Models for Location, Scale, and Shape (GAMLSS), to identify nonlinear and threshold effects in the relationship between digital transformation and cyber resilience across security regimes.

CONCLUSION

This study aimed to analyze the impact of technological, institutional, and financial factors on national cyber resilience under conditions of armed conflict and post-conflict recovery. The results show that cyber resilience is fundamentally scenario-dependent: the same determinants operate through different mechanisms as countries transition between armed conflict, post-conflict recovery, and relative stability. Institutional digital capacity is most critical during armed conflict, when coordination and adaptive governance become essential for managing cyber risks. Although government effectiveness does not display a stable direct effect across all specifications, its relevance increases under conflict conditions, while operational cybersecurity institutions tend to follow a reactive rather than preventive logic. Macroeconomic factors exert more systematic effects across regimes. Higher unemployment is consistently associated with lower cyber resilience, whereas inflation shows a positive association that

may reflect crisis-driven fiscal mobilization. Financial variables play an ambivalent role: under relative stability, greater financial depth is often linked to higher cyber exposure rather than stronger resilience.

Overall, the findings suggest that cyber resilience is a dynamic, regime-sensitive outcome shaped by the interaction of institutional capacity, digital governance, and macroeconomic conditions. Effective cybersecurity policy, therefore, requires context-aware and regime-sensitive approaches rather than uniform policy solutions.

AUTHOR CONTRIBUTIONS

Conceptualization: Inna Shkolnyk, Inna Tiutiunyk, Andrii Semenog.
Data curation: Inna Shkolnyk, Inna Tiutiunyk, Andrii Semenog, Yuliia Kovalenko, Liudmyla Pavlenko.
Formal analysis: Inna Tiutiunyk, Yuliia Kovalenko, Liudmyla Pavlenko.
Funding acquisition: Inna Tiutiunyk, Andrii Semenog.
Investigation: Inna Shkolnyk, Inna Tiutiunyk, Andrii Semenog.
Methodology: Inna Shkolnyk, Inna Tiutiunyk.
Project administration: Inna Tiutiunyk.
Resources: Andrii Semenog, Yuliia Kovalenko, Liudmyla Pavlenko.
Software: Inna Shkolnyk, Inna Tiutiunyk.
Supervision: Inna Shkolnyk, Inna Tiutiunyk.
Validation: Inna Shkolnyk, Inna Tiutiunyk, Andrii Semenog, Yuliia Kovalenko, Liudmyla Pavlenko.
Visualization: Andrii Semenog, Yuliia Kovalenko, Liudmyla Pavlenko.
Writing – original draft: Inna Shkolnyk, Inna Tiutiunyk, Andrii Semenog, Yuliia Kovalenko, Liudmyla Pavlenko.
Writing – review & editing: Inna Shkolnyk, Andrii Semenog, Yuliia Kovalenko, Liudmyla Pavlenko.

ACKNOWLEDGMENT

The authors acknowledge with gratitude the financial support provided by the Ministry of Education and Science of Ukraine for the research project "Modeling mechanisms for countering organized and transnational cybercrime in wartime and post-war times" (state registration number 0124U000550).

REFERENCES

1. Adams, J. N. (Ed.). (2016). Letter of Claudia Severa from Vindolanda (Tab. Vindol. 291), of the Early Second Century. In *An Anthology of Informal Latin, 200 BC–AD 900: Fifty Texts with Translations and Linguistic Commentary*. Cambridge: Cambridge University Press, 256-264. https://doi.org/10.1017/9781139626446.023
2. Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity, 4*(1), tyy006. https://doi.org/10.1093/cybsec/tyy006
3. Aldasoro, I., Gambacorta, L., Giudici, P., & Whyte, K. (2020). *The drivers of cyber risk* (BIS Working Papers No. 865). Retrieved from https://www.bis.org/publ/work865.htm
4. Arroyabe, M. F., Arranz, C. F.A., De Arroyabe, I. F., & De Arroyabe, J. C. F. (2024). Revealing the realities of cybercrime in small and medium enterprises: Understanding fear and taxonomic perspectives. *Computers & Security, 141,* 103826. https://doi.org/10.1016/j.cose.2024.103826
5. Atkins, S., & Chappell, L. (2021). An Improvised Patchwork: Success and Failure in Cybersecurity Policy for Critical Infrastructure. *Public Administration Review, 81*(5), 847-861. https://doi.org/10.1111/puar.13322
6. Bampinas, G., & Panagiotidis, T. (2024). How would the war and the pandemic affect the stock and cryptocurrency cross-market linkages? *Research in International Business and Finance, 70,* 102272. https://doi.org/10.1016/j.ribaf.2024.102272
7. Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2021). Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. *European Societies, 23*(S1), S47-S59. https://doi.org/10.1080/14616696.2020.1804973
8. Carlo, A., & Obergfaell, K. (2024). Cyber attacks on critical infrastructures and satellite communications. *International Journal of Critical Infrastructure Protection, 46,* 100701. https://doi.org/10.1016/j.ijcip.2024.100701

http://dx.doi.org/10.21511/ppm.23(4).2025.45

9. Carr, M. (2016). Public-private partnerships in national cyber-security strategies. *International Affairs, 92*(1), 43-62. https://doi.org/10.1111/1468-2346.12504

10. CERT-UA. (2025). *Cyber incidents overview*. Retrieved from https://cert.gov.ua/articles

11. Cook, S., Giommoni, L., Trajtenberg Pareja, N., Levi, M., & Williams, M. L. (2023). Fear of Economic Cybercrime Across Europe: A Multilevel Application of Routine Activity Theory. *The British Journal of Criminology, 63*(2), 384-406. https://doi.org/10.1093/bjc/azac021

12. Dodel, M., & Mesch, G. (2019). An Integrated Model for Assessing Cyber-safety Behaviors: How Cognitive, Socioeconomic and Digital Determinants Affect Diverse Safety Practices. *Computers & Security, 86,* 75-91. https://doi.org/10.1016/j.cose.2019.05.023

13. European Commission. (2022). *Digital Public Administration factsheet 2022.* Retrieved from https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/digital-public-administration-factsheets-2022

14. European Parliament. (2022). *Russia's War on Ukraine: Timeline of Cyber-Attacks.* Retrieved from https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733549

15. European Union Agency for Cybersecurity (ENISA). (2023). *ENISA Threat Landscape 2023*. Retrieved from https://data.europa.eu/doi/10.2824/782573

16. Frandell, F., & Feeney, M. (2022). Cybersecurity Threats in Local Government: A Sociotechnical Perspective. *The American Review of Public Administration, 52*(8), 558-572. https://doi.org/10.1177/02750740221125432

17. Fyshchuk, I., Mette Strange N., & Jeppe Agger N. (2025). Managing Cyberattacks in Wartime: The Case of Ukraine. *Public Administration Review, 85*(3), 619-627. https://doi.org/10.1111/puar.13895

18. Guitton, M. J., & Frechette, J. (2023). Facing cyberthreats in a crisis and post-crisis era: Rethinking security services response strategy. *Computers in Human Behavior Reports, 10,* 100282. https://doi.org/10.1016/j.chbr.2023.100282

19. Hui, K. L., Seung, H. K., & Qui-Hong, W. (2017). Cybercrime Deterrence and International Legislation: Evidence from distributed denial of service attacks. *MIS Quarterly, 41*(2), 497-524. Retrieved from https://ink.library.smu.edu.sg/sis_research/3420

20. Lynch, III, T. F. (2024). Cyberspace: Great Power competition in a fragmenting domain. *Orbis, 68*(4), 607-623. https://doi.org/10.1016/j.orbis.2024.09.007

21. Mamediieva, G., & Moynihan, D. (2023). Digital Resilience in Wartime: The Case of Ukraine. *Public Administration Review, 83*(6), 1512-1516. https://doi.org/10.1111/puar.13742

22. Miadzvetskaya, Y. (2024). EU sanctions in response to cyber-attacks as crime-based emergency measures. *Computer Law & Security Review, 54,* 106010. https://doi.org/10.1016/j.clsr.2024.106010

23. Moore, T. (2010). The economics of cybersecurity: Principles and policy options. *International Journal of Critical Infrastructure Protection, 3*(3), 103-117. https://doi.org/10.1016/j.ijcip.2010.10.002

24. Nobles, C. (2024). The Weaponization of Artificial Intelligence in Cybersecurity: A Systematic Review. *Procedia Computer Science, 239,* 547-555. https://doi.org/10.1016/j.procs.2024.06.206

25. Norris, D. F., Mateczun, L., Hatcher, W., Meares, W., & Heslen, J. (2023). Local Government Cyber Insecurity: Causes and Recommendations for Improvement. *Public Administration Review, 84*(4), 651-59. https://doi.org/10.1111/puar.13743

26. Rogoff, K. (2022). *The Long-Lasting Economic Shock of War*. International Monetary Fund. Retrieved from https://formatresearch.com/wp-content/uploads/2022/05/The-Long-lasting-Economic-Shock-of-War.pdf

27. Sanders, P., Bronk, C., & Bazilian, M. D. (2022). Critical energy infrastructure and the evolution of cybersecurity. *The Electricity Journal, 35*(10), 107224. https://doi.org/10.1016/j.tej.2022.107224

28. Smith, B. (2022). *Defending Ukraine: Early lessons from the cyber war*. Microsoft Digital Threat Analysis Center. Retrieved from https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/

29. Song, U., Hur, G., Lee, S., & Park, J. (2024). Unraveling the dynamics of the cyber threat landscape: Major shifts examined through the recent societal events. *Sustainable Cities and Society, 103,* 105265. https://doi.org/10.1016/j.scs.2024.105265

30. Streltsov, L. (2017). The System of Cybersecurity in Ukraine: Principles, Actors, Challenges, Accomplishments. *European Journal for Security Research,* 2(2), 147-184. Retrieved from https://link.springer.com/article/10.1007/s41125-017-0020-x

31. Tiutiunyk, I. (2025). *Cyber Resilience Determinants in Wartime and Post-Conflict Conditions: Evidence from a Six-Country Panel Dataset* [Data set]. Zenodo. https://doi.org/10.5281/zenodo.18043321

32. Ubowska, A., & Królikowski, T. (2022). Building a cybersecurity culture of public administration system in Poland. *Procedia Computer Science, 207,* 1242-1250. https://doi.org/10.1016/j.procs.2022.09.180

33. United Nations. (2025). Global Programme on Cybercrime. Retrieved from https://www.unodc.org/unodc/en/cybercrime/home.html

34. Virtanen, S. M. (2017). Fear of Cybercrime in Europe: Examining the Effects of Victimization and Vulnerabilities. *Psychiatry, Psychology and Law, 24,* 323-38. Retrieved from https://pmc.ncbi.nlm.nih.gov/articles/PMC6818400/

35. Yilma, K. M. (2014). Developments in cybercrime law and practice in Ethiopia. *Computer Law & Security Review, 30*(6), 720-735. https://doi.org/10.1016/j.clsr.2014.09.010