

Academy of National and Information Security, Plovdiv, Bulgaria

# POLITICS & SECURITY

ISSN Print 2535-0358

ISSN Online 2815-3324

# EDITORIAL BOARD

## **Editor-in-Chief**

### **Igor Britchenko**

University of the National Education Commission, Krakow, Poland

## **Deputy Editor-in-Chief**

### **Georgi Manolov**

Academy of National and Information Security, Bulgaria

### **Ivan Tkach**

Defence Management Education and Research Center, Ukraine

## **Editorial Board:**

Adrian Miroiu, National School of Political and Administrative Sciences, Romania

Bogna Gawrońska-Nowak, Krakow University of Economics, Poland

Farouq Ahmad Al Azzam, Jadara University, Jordan

Iryna Kyzyma, LISER, Luxembourg

Mapula Hunadi Nkwana, University of South Africa

Marcin Jurgilewicz, Rzeszów University of Technology, Poland

Marek Antoš, Charles University in Prague, Czech Republic

Iryna Mihus, Pontifical Catholic University of Paraná, Brazil

Namig Aliyev, Academy of State Administration under the President of Azerbaijan, Azerbaijan

Roseann O'Reilly Runte, Carleton University, Canada

Saranya T. Sathish, Amity University, Bengaluru, India

Sandeep Kumar Gupta, CMR University, Bengaluru, India

Serperi Sevgür, Medicine Hat College, Alberta, Canada

Teodor Danailov Dechev, Academy of National and Information Security, Bulgaria

Yana Koval, Scientific Center of Innovative Research, Estonia

## **Production Editor**

Tetiana Dei, Politics & Security Editorial Team

## **Founder and Publisher**

Academy of National and Information Security, Plovdiv, Bulgaria

## **Journal Manager**

E-SCIENCE SPACE, Warsaw, Poland



# FOREWORD

Vol. 14 No. 4 (2025)

## Dear Readers, Colleagues, and Partners,

We are honored to present to you the fourth and final issue of Politics & Security for the year 2025. As we close this chapter, it is impossible to ignore the profound transformation that the global security landscape has undergone over the past twelve months. The year 2025 has not merely been a continuation of existing trends; it has been a year of acceleration, where the theoretical constructs of "hybrid warfare," "economic coercion," and "cognitive security" have solidified into tangible, daily realities for nations and citizens alike.

This year has starkly demonstrated that the concept of "security" can no longer be confined to military barracks or diplomatic negotiation tables. The frontline has dissolved. It now runs through the fiber-optic cables of our digital infrastructure, the grain silos of the Black Sea, the algorithms of social media platforms, and the complex compliance mechanisms of global finance. We are witnessing the weaponization of interdependence, where the very ties that were meant to bind the global community together—trade, technology, and information—are increasingly being used as levers of strategic influence and coercion.

In this context, the mission of Politics & Security has never been more vital. Our goal is not just to chronicle events, but to dissect the underlying mechanisms that drive them. We strive to provide a platform where deep academic rigor meets policy relevance, offering insights that are as useful to the strategist in a government office as they are to the scholar in a university library. The articles selected for this year-end issue reflect this commitment to depth and diversity. They do not offer simple answers; instead, they embrace the complexity of a world where threats are multifaceted and solutions must be equally sophisticated.

The first section of this issue anchors us in the hard realities of geopolitics and regional security, with a specific focus on the Black Sea and Central Europe. The war in Ukraine continues to cast a long shadow, reshaping alliances and redefining national interests. Our opening analysis on economic warfare in the Black Sea provides a sobering look at how geography and economics intersect. It details how the blockade of grain corridors and attacks on energy infrastructure are not collateral damage, but calculated geo-economic strategies designed to exert pressure far beyond the immediate theater of conflict.

Building on this, Yassine Guennoun's examination of the Visegrad Group offers a nuanced understanding of internal European Union dynamics. The concept of "sovereignty through selective integration" is a powerful analytical tool for understanding how member states navigate the tension between national autonomy and supranational obligations. As the external security environment darkens, the internal cohesion of alliances like the EU and NATO becomes paramount. The divergence in threat perceptions between Poland, the Czech Republic, and Hungary serves as a critical case study for the challenges of maintaining unity in the face of aggression.

Furthermore, Kostadin Kostov's retrospective on Syria serves as a crucial reminder that security challenges are rarely contained within borders. The ripple effects of conflict in the Middle East—manifested through terrorism, migration, and radicalization—continue to pose systemic threats to the national security of European states, particularly those on the periphery like Bulgaria.

As we move to the second section, we confront the threats that are less visible but no less dangerous. The digital domain has become the primary arena for modern conflict. The article on cognitive security and institutional trust strikes at the heart of democratic resilience. It argues convincingly that disinformation campaigns targeting judicial and law enforcement institutions are not merely "fake news," but sociological attacks designed to erode the very legitimacy of the state. In an era where trust is the

currency of stability, protecting the cognitive security of the population is as critical as protecting physical borders.

Parallel to this battle for minds is the battle for financial transparency. The rise of Decentralized Finance (DeFi) has created new opportunities for innovation, but also new avenues for evasion. The comprehensive risk analysis presented in this issue highlights how mixers, privacy coins, and cross-chain bridges are being exploited to bypass sanctions and finance national security threats. This cat-and-mouse game between regulators and illicit actors defines the modern financial security landscape, requiring a blend of technological literacy and regulatory agility that is often lacking in traditional governance structures.

Finally, we turn our attention to the bedrock of national strength: economic security. In the long run, no nation can be secure if its economic foundations are fragile. Urszula Szczytyńska's theoretical approach to financial security emphasizes that sustainable development is impossible without stability. This is not just a corporate concern; it is a matter of national resilience. Healthy, financially secure enterprises are the engines that drive recovery and growth, even in times of crisis.

This macro-perspective is complemented by the micro-level analysis of Janusz Kilar and his colleagues, who examine the profitability and security of milk production on fragmented farms in Southeastern Poland. While seemingly specific, this study illuminates the broader challenges of food security and rural stability in the face of market volatility and supply chain disruptions. It serves as a potent reminder that global security ultimately rests on the ability of local systems to function effectively.

As we conclude 2025, we must acknowledge that the challenges we face are unlikely to dissipate in the coming year. The "poly-crisis"—the intersection of geopolitical conflict, economic instability, and technological disruption—is the new normal. However, within these challenges lie opportunities for adaptation and renewal. The research presented in this issue suggests that resilience is possible, but it requires honesty about our vulnerabilities and creativity in our responses.

We would like to extend our deepest gratitude to our authors for their intellectual courage and rigorous scholarship. We also thank our peer reviewers, whose invisible labor ensures the quality of this publication. And most importantly, we thank you, our readers, for your continued engagement and trust.

We hope that *Politics & Security* continues to serve as a valuable resource in your professional and academic endeavors. As we look toward 2026, let us remain vigilant, analytical, and committed to the pursuit of a more secure and just world.

Sincerely,

*The Editorial Board Politics & Security*

# CONTENTS

ECONOMIC WARFARE IN THE BLACK SEA: A GEOECONOMIC ANALYSIS OF COERCION THROUGH GRAIN, BLOCKADES, AND ENERGY INFRASTRUCTURE 6

Andrii Lyseiuk

SOVEREIGNTY THROUGH SELECTIVE INTEGRATION: STRATEGIC NON-COMPLIANCE, COMPLIANCE MINIMALISM, AND GOVERNANCE HARDENING IN EU CRISIS POLITICS 16

Yassine Guennoun

RETROSPECTIVE ANALYSIS OF THE SITUATION IN SYRIA AND CONCEPTUAL THREATS TO BULGARIA'S NATIONAL SECURITY 31

Kostadin Kostov

COGNITIVE SECURITY AND INSTITUTIONAL TRUST: A SOCIOLOGICAL ANALYSIS OF DISINFORMATION CAMPAIGNS TARGETING THE LEGITIMACY OF JUDICIAL AND LAW ENFORCEMENT INSTITUTIONS 45

Maryna Dei

DECENTRALIZED FINANCE (DEFI) AND SANCTIONS EVASION: A RISK ANALYSIS OF MIXERS AND PRIVACY COINS IN FINANCING NATIONAL SECURITY THREATS 57

Andrii Svintsytskyi

FINANCIAL SECURITY AS A KEY ELEMENT SUPPORTING SUSTAINABLE BUSINESS DEVELOPMENT – A THEORETICAL APPROACH 68

Urszula Szczytyńska

ECONOMIC SECURITY AND PROFITABILITY ASSESSMENT OF MILK PRODUCTION ON FRAGMENTED FARMS IN SOUTHEASTERN POLAND (2020–2024) 81

Janusz Kilar, Mateusz Kaczmarek, Piotr Frączek, Magdalena Kilar

# ECONOMIC WARFARE IN THE BLACK SEA: A GEOECONOMIC ANALYSIS OF COERCION THROUGH GRAIN, BLOCKADES, AND ENERGY INFRASTRUCTURE

Andrii Lyseiuk

National Academy of the Security Service of Ukraine

Kyiv, Ukraine

<https://orcid.org/0000-0002-9026-1188>

[andrii\\_lyseiuk@sci-univ.com](mailto:andrii_lyseiuk@sci-univ.com)

**Abstract:** *This article examines economic warfare in the Black Sea as a geoeconomic contest over three interdependent systems: (i) grain and agri-food logistics, (ii) maritime trade and insurance, and (iii) offshore and coastal energy infrastructure. Using open-source process tracing and qualitative document analysis of peer-reviewed studies, official datasets and reports, and policy assessments published primarily in 2022–2025, the paper reconstructs how coercive actions in one domain propagate through shipping routes, risk pricing, and energy-security expectations. Three mechanisms are identified. First, disruption of export corridors reconfigures the distribution of bargaining power by raising transaction costs and amplifying domestic price discounts for Ukrainian producers. Second, war-risk and sanctions compliance convert military pressure into insurance and financing constraints that shift trade away from the Black Sea and towards longer, costlier routes. Third, repeated attacks and hybrid interference against energy assets increase systemic uncertainty and alter investment and resilience decisions well beyond the immediate theatre. The article argues that these mechanisms operate as mutually reinforcing channels of coercion: the effect is not only the denial of specific cargo flows or megawatts, but the strategic manipulation of expectations and contractual risk allocation in regional markets. The contribution is conceptual and policy-relevant: it specifies observable indicators for tracing economic coercion in maritime regions and delineates boundary conditions, limitations, and alternative interpretations for causal claims in open-source research.*

**Keywords:** Economic Warfare, Geoeconomics, Black Sea Security, Economic Coercion, Weaponized Interdependence, Energy Security, Food Security, Bulgaria.

## 1. INTRODUCTION

The Black Sea is a strategic maritime junction linking European, Eurasian, and Middle Eastern supply chains. Its ports and sea-lanes are structurally embedded in global food, energy, and transport networks, which makes the region unusually susceptible to geoeconomic leverage. Since 2022, the war has accelerated a shift from episodic disruption to sustained economic coercion: decisions about access, insurance, routing, and infrastructure resilience have become instruments through which actors seek political outcomes. Recent policy assessments treat the Black Sea not merely as a battlefield, but as a critical node where security strategy and market governance intersect (Scowcroft Center for Strategy and Security, 2023; European Commission & High Representative, 2025).

Economic statecraft has long captured how states employ trade, finance, and sanctions to influence behaviour without conventional military escalation (Baldwin, 1985; Blackwill & Harris, 2016). What is distinctive in the contemporary Black Sea context is the tight coupling between kinetic pressure and market infrastructure: coercive effects are channelled through private contractual arrangements (insurance clauses, charterparty risk premia, compliance screening) and through the governance of

chokepoints and corridors. The practical implication is that coercion may be observable in prices, routing decisions, and risk spreads even when formal policy instruments remain unchanged (Lowenfeld, 2002).

To capture these dynamics, the article adopts a geoeconomic lens in which interdependence is not treated as a background condition but as a manipulable structure. Weaponized interdependence highlights how network centrality and gatekeeping in global systems can be converted into coercive capacity (Farrell & Newman, 2019). In the Black Sea, this logic is visible in how access to maritime space, export certification, and logistics services can be tightened or relaxed to produce economic and political pressure—often below the threshold of an explicit embargo (Balcaen, 2024).

This paper therefore treats economic warfare as a portfolio of coercive practices that blend military pressure with economic and regulatory frictions. The analytical focus is on mechanisms that are empirically traceable: changes in risk pricing, route selection, commodity-market reactions, and the operational availability of energy assets. This approach reduces reliance on rhetorical claims and instead anchors the argument in observable consequences and documented policy decisions.

The core theoretical claim is that economic warfare in maritime regions operates through expectation management: by increasing uncertainty and altering contractual terms, coercion can persist even when physical flows partially adapt. This claim implies two boundary conditions. Where alternative routes and credible security guarantees are available, coercive effects should be dampened; where dependence is concentrated and risk cannot be diversified, coercive leverage increases.

Against this background, the article asks three questions: (1) how do disruptions in grain corridors translate into measurable market effects and bargaining leverage; (2) how do sanctions, war-risk insurance, and compliance practices reshape maritime trade patterns; and (3) how do attacks and hybrid threats to energy infrastructure produce regional spillovers in security and investment expectations? The aim is not to provide a comprehensive history of the war, but to specify and compare mechanisms of geoeconomic coercion across domains.

The central argument is that coercion in the Black Sea has been exercised through a combination of corridor disruption, risk pricing, and infrastructure pressure. These channels are mutually reinforcing: corridor disruption increases domestic price discounts and logistics costs, elevated war-risk premia discourage commercial participation and re-route trade, and repeated infrastructure attacks raise the perceived permanence of insecurity, affecting both public resilience planning and private capital allocation.

The remainder of the article proceeds as follows. Section 2 specifies the research design and evidentiary standards. Section 3 analyses grain and agri-food logistics as a coercive domain. Section 4 examines maritime trade and the insurance–sanctions interface. Section 5 discusses offshore energy infrastructure and hybrid threats. The conclusion synthesises implications and identifies methodological limits and alternative explanations.

## 2. METHODOLOGY

This study uses a qualitative, mechanism-focused research design. The unit of analysis is a coercive episode affecting a regional economic system (grain logistics, maritime trade/insurance, or energy infrastructure). Evidence is drawn from English-language peer-reviewed publications, official reports and datasets (UNCTAD, OECD, World Bank), and policy analyses by reputable institutions. The main period of observation covers February 2022 through late 2024, with 2025 sources used to interpret longer-run implications and to cross-validate earlier claims. The literature was identified through structured searches in Google Scholar and major bibliographic databases using combinations of keywords such as «Black Sea Grain Initiative», «war-risk insurance», «Black Sea trade», «maritime corridor», and «energy infrastructure attacks», followed by backward citation tracking from the most relevant peer-reviewed studies.

Source selection followed three criteria: (i) traceability—claims can be linked to identifiable data, documents, or transparent field reporting; (ii) institutional credibility—preference for peer review or established intergovernmental and policy organisations; and (iii) domain relevance—direct linkage to the Black Sea and to one of the three coercive domains. Where sources diverged, priority was given to those with disclosed methods, clear time stamps, and replicable indicators. Exclusion criteria removed undated

Lyseiuk, A. (2025). Economic warfare in the Black Sea: A geoeconomic analysis of coercion through grain, blockades, and energy infrastructure. *Politics & Security*, 14(4), 6–15. <https://doi.org/10.54658/ps.28153324.2025.14.4.pp.6-15> or anonymous commentary, sources without editorial oversight, and items whose empirical claims could not be linked to primary material.

The analysis applies process tracing to reconstruct causal sequences from actions (e.g., blockade, corridor restrictions, attacks) to intermediate mechanisms (risk premia, rerouting, domestic price differentials) and then to outcomes (export volumes, market responses, resilience decisions). Causal claims are framed conservatively: where attribution is uncertain or data are incomplete, the text specifies plausible alternative pathways rather than asserting singular causation. Within each case, the narrative is organised around temporally ordered events and documented market or policy reactions; across cases, the comparison tests whether similar coercive logics (risk inflation, rerouting, expectation shocks) recur under different material conditions.

1. Mechanism coding used three observable categories. First, dependency indicators capture the degree to which regional or global systems rely on Black Sea routes or assets. Second, coercive instruments capture the means of pressure, including physical disruption, legal and regulatory constraints, and hybrid interference. Third, effect indicators capture market and policy responses, such as changes in futures pricing, insurance conditions, or infrastructure hardening.

2. Triangulation was implemented across source types. For commodity and trade effects, peer-reviewed market studies were compared with official trade and logistics reporting. For risk pricing, insurance and financial-market analyses were compared with policy documentation and shipping reports. For infrastructure effects, technical assessments were compared with broader security analyses to avoid over-interpreting isolated incidents. Where possible, the analysis aligns evidence to common event markers (e.g., corridor announcements, withdrawals, major strikes) to reduce the risk of attributing broader trends to single incidents.

3. The paper does not use proprietary datasets and therefore cannot observe some commercial variables (e.g., contract-level war-risk premia) directly. Instead, it relies on documented changes in underwriting practices, published risk assessments, and observable routing outcomes as proxies (OECD, 2022; UNCTAD, 2024a).

This methodological strategy helps reduce ‘LLM-style’ generalities by forcing each substantive claim to meet a minimal evidentiary threshold: a claim is retained only if it can be supported by at least one verifiable source and, where possible, corroborated by an independent source category.

1. A practical limitation is that open-source reporting is uneven across domains. Grain and trade data are comparatively rich, while information on offshore energy assets and covert interference is more fragmented. Accordingly, the energy-infrastructure section emphasises resilience implications and policy-relevant threat patterns rather than attempting precise quantitative damage accounting (Bozhilov, 2025).

2. Another limitation concerns counterfactuals. Shipping and commodity markets were also affected by global inflation, monetary tightening, and other chokepoint disruptions (e.g., Red Sea and Panama Canal constraints). Where relevant, the analysis notes these confounders and treats observed Black Sea effects as part of a broader shock environment (UNCTAD, 2024a).

3. Despite these limits, the combination of process tracing and triangulation allows for a disciplined comparison across domains: the goal is to identify recurring coercive mechanisms and to specify where the evidence supports stronger or weaker causal inference.

Finally, the article adheres to reproducibility in citation practice. Each in-text citation corresponds to a verifiable reference entry, with a DOI or stable URL provided where available. This supports editorial review and reduces the risk of non-existent or misattributed sources in a rapidly evolving policy environment.

### 3. RESULTS: THE ANATOMY OF ECONOMIC WARFARE IN THE BLACK SEA

Grain exports are a classic vulnerability in the Black Sea because they combine high global relevance with concentrated logistics. Ukraine has historically been a major supplier of wheat, maize, and sunflower products, and the pre-war export model relied heavily on a small number of Black Sea ports. This created

a predictable coercive target: disrupting maritime access can generate both domestic economic losses and international price effects (Welsh & Glauber, 2024; Neyter et al., 2024).

### 3.1 Case 1: The "Grain Weapon" – Leveraging Global Food Security

First, the dependency structure is asymmetric. Ukrainian producers depend on access to deep-water ports and affordable shipping capacity, while import-dependent states are exposed to volatility rather than absolute scarcity. This configuration enables coercion through cost inflation and uncertainty: even partial disruption can widen basis differentials and depress farm-gate prices in Ukraine (Neyter et al., 2024).

Second, coercive instruments in this domain include physical blockade, targeted strikes on port and storage facilities, and the politicisation of corridor governance. These instruments do not require a permanent interdiction; instead, they function by periodically raising the probability of loss and delay, thereby changing commercial behaviour.

- Third, corridor governance matters because it translates military control into administrative frictions. The Black Sea Grain Initiative (BSGI) reduced some of these frictions, and its suspension or termination re-introduced uncertainty that was rapidly priced into markets. Empirical evidence indicates that the BSGI announcement and implementation were associated with measurable reactions in grain futures and volatility metrics (Steinbach & Yildirim, 2024; Poursina et al., 2024).

- Fourth, the coercive effect is amplified when disruption coincides with information and political signalling. Policy analyses describe the use of grain exports and corridor access as leverage in broader negotiations, including attempts to shift blame for price increases and to frame sanctions relief as a condition for market 'stability' (Paul & Taran, 2023; Welsh & Glauber, 2024).

Fifth, the distributional impact is visible in Ukraine's agricultural balance sheet. A World Bank-authored assessment of war damages and losses estimates that export disruptions contributed to substantial losses through lower domestic prices and higher logistics costs, alongside direct damages to storage and machinery (Neyter et al., 2024). This supports an interpretation of grain corridor pressure as an economic-coercion mechanism rather than a purely tactical maritime measure.

- Alternative explanations must be considered. Global commodity prices were influenced by weather, energy costs, and monetary conditions. However, studies that isolate BSGI-related event windows and corridor policy shifts still find statistically detectable market responses, suggesting that Black Sea corridor governance acted as an independent driver of expectations (Steinbach & Yildirim, 2024; Poursina et al., 2024).

- Overall, grain corridor pressure illustrates a broader geoeconomic pattern: the objective is not only to interrupt exports but to impose a persistent 'risk tax' on the target's production and financing conditions, while keeping international buyers oriented towards alternative suppliers and routes.

### 3.2 Case 2: The Maritime Domain – Kinetic and Economic Blockades

Maritime trade in the Black Sea is shaped by commercial shipping decisions that respond quickly to perceived risk. Since 2022, risk has been priced not only through physical threats but also through sanctions compliance and insurance availability. The result is a layered coercive environment: even when shipping is legally permitted, elevated war-risk premia, compliance screening, and uncertainty about port access can deter participation and redirect cargo flows (OECD, 2022; UNCTAD, 2024a). In practice, commercial withdrawals and rerouting have followed salient escalation points, including changes in corridor arrangements and high-profile attacks on port areas, which suggests that market behaviour responds to both physical risk and policy uncertainty.

War-risk insurance is a particularly important transmission belt between military events and economic outcomes. When insurers increase premiums or narrow coverage, charterers and shipowners face higher costs and stricter contractual terms, which can make routes commercially unattractive. OECD

Lyseiuk, A. (2025). Economic warfare in the Black Sea: A geoeconomic analysis of coercion through grain, blockades, and energy infrastructure. *Politics & Security*, 14(4), 6–15. <https://doi.org/10.54658/ps.28153324.2025.14.4.pp.6-15>

analysis of the early-war period documents how conflict risk and sanctions complexity affected marine insurance conditions and the functioning of international insurance markets (OECD, 2022). Even when coverage remains formally available, higher deductibles, narrower perils, and stricter voyage approvals can make participation prohibitive for smaller operators, thereby concentrating exposure among a limited set of firms and increasing systemic fragility (OECD, 2022).

- Trade-pattern evidence supports this mechanism. A peer-reviewed study on Black Sea trade reports measurable disruptions and reconfiguration of flows following the escalation of hostilities, consistent with the hypothesis that risk pricing and routing constraints materialised at scale (Nate et al., 2024).

- A second mechanism is the compliance interface. Sanctions do not only prohibit transactions; they also increase due-diligence costs and create incentives for over-compliance among private actors. This ‘compliance friction’ can be coercive even without formal escalation of sanctions, because uncertainty over enforcement and reputational risk affects financing and insurance availability (Chachko & Newman, 2025).

Third, shipping networks adapt by rerouting and re-allocating capacity, but adaptation itself is costly. Network analysis of container shipping under geopolitical shocks shows how disruptions can propagate through service rotations and port choice, producing longer transit times and higher logistics costs (Martin, 2025). UNCTAD similarly notes that recent shocks in key maritime chokepoints, including the Black Sea, have extended sailing distances and added volatility to freight markets (UNCTAD, 2024a, Sciubba, 2023). For bulk commodities, the same logic applies: when the risk-adjusted cost of Black Sea shipping rises, capacity shifts towards alternative corridors, including river and rail interfaces, but these substitutes can become bottlenecks and generate additional rents for intermediaries (Neyter et al., 2024).

- Taken together, these dynamics imply that maritime coercion is often indirect. The observable outcome is not always a visible blockade; it can be a market-mediated withdrawal of capacity and financing. For policy, this points to the importance of security guarantees and risk-sharing instruments that can stabilise insurance and shipping participation when corridor access is contested.

- The maritime trade domain therefore links coercion to governance: legal rules, underwriting practices, and network structures jointly determine whether coercive pressure is amplified or dampened. This reinforces the broader geoeconomic thesis that economic warfare increasingly operates through the private infrastructure of globalisation rather than through state commands alone (Farrell & Newman, 2019).

### 3.3 Case 3: The Energy Front – Kinetic and Hybrid Threats

Energy infrastructure in and around the Black Sea is both a physical asset base and a signalling device: attacks and hybrid interference can change expectations about long-term security, investment, and regional integration. Offshore platforms, pipelines, grids, and port energy terminals are exposed to kinetic risks and to information and cyber operations that are harder to attribute and deter (Bozhilov, 2025). Because many assets are interconnected (ports depend on power supply; grids depend on coastal terminals; offshore facilities depend on onshore control systems), localized pressure can cascade into broader operational constraints, a risk explicitly flagged in regional security planning (European Commission & High Representative, 2025).

From a geoeconomic perspective, the coercive value of energy disruption lies in its spillovers. Even when immediate supply shortfalls are mitigated, repeated attacks can raise financing costs, slow maintenance and upgrades, and drive a preference for redundancy and diversification. World Bank reporting on Ukraine’s wartime economy highlights how sustained attacks on energy infrastructure undermine recovery and contribute to persistent macroeconomic fragility (World Bank, 2023). Beyond immediate outages, recurrent strikes generate planning uncertainty for firms and public authorities,

complicating procurement, maintenance scheduling, and the prioritisation of scarce capital for repair versus expansion (World Bank, 2023).

- Hybrid threats further complicate governance. Critical energy infrastructure often spans jurisdictions and involves public–private ownership structures. This creates multiple points of entry for coercion—legal disputes, regulatory delays, sabotage, and influence operations that seek to shape political decisions about energy routing and investment (Sikharulidze, 2025).

- A core implication is that resilience is not only technical but institutional. Improving resilience requires joint threat assessment, information-sharing, and aligned standards across coastal states and partners. Policy discussions in the region emphasise the need to coordinate EU and NATO tools for infrastructure protection and crisis response (Bozhilov, 2025; European Commission & High Representative, 2025).

- Because open-source evidence on specific offshore incidents can be incomplete, this section prioritises mechanism plausibility over precise damage quantification. The relevant empirical indicator is the pattern of repeated pressure on energy assets and the resulting adjustments in policy and investment expectations, which is consistent with a strategy of coercion through systemic uncertainty rather than through one-off denial.

**Table 1. Typology of Economic Coercion in the Black Sea**

<b>Weaponized Domain</b>	<b>Coercive Tactic / Instrument</b>	<b>Primary Target(s)</b>	<b>Observed Goeconomic / Security Impact</b>
<b>Agriculture (Food)</b>	1. Kinetic attacks on grain silos/ports. (Welsh & Glauber, 2024) 2. Political leverage via BSGI termination. (Paul & Taran, 2023)	1. Ukrainian economy. 2. Global South food importers.	1. Global food price volatility. (Welsh & Glauber, 2024) 2. Creation of political leverage ("grain blackmail"). (Paul & Taran, 2023) 3. Devastation of Ukrainian agricultural sector. (Welsh & Glauber, 2024)
<b>Maritime Trade</b>	1. Kinetic naval blockade (mines, fleet). (Kormych et al., 2024) 2. <i>De facto</i> economic blockade (war risk insurance premiums). (Denamiel et al., 2024)	1. Ukrainian export revenue. 2. Global shipping & supply chains.	1. Economic strangulation of Ukraine. (Kormych et al., 2024) 2. Disruption of Freedom of Navigation. (Scowcroft Center for Strategy and Security, 2023) 3. Market-based enforcement of blockade. (Denamiel et al., 2024)
<b>Energy</b>	1. Kinetic attacks on Ukrainian grid. (Balcaen, 2024) 2. Hybrid threats to offshore platforms (Bulgaria/Romania). (Bozhilov, 2025) 3. Coercive "naval exercises" in EEZs. (Toscano & Zgurean, 2025)	1. Ukrainian civil society/economy. 2. European energy security. 3. Foreign investment in regional energy.	1. Systemic failure of Ukrainian grid. (Balcaen, 2024) 2. Cascading risks to EU energy security. (Harangozo, 2025) 3. Deterrence of investment in Bulgarian/Romanian EEZs. (Bozhilov, 2025; Toscano & Zgurean, 2025)

Source: created by the author

## 4. DISCUSSION: SYSTEMIC IMPLICATIONS FOR BLACK SEA SECURITY

The three domains examined—grain logistics, maritime trade/insurance, and energy infrastructure—share a common logic: coercion is generated by manipulating the terms under which markets can operate. Rather than relying solely on explicit prohibitions, economic warfare in the Black Sea exploits concentrated dependencies and converts security risks into contractual and financial constraints.

The grain case shows how corridor governance and episodic disruption can impose durable economic losses on the target even when exports continue via alternative routes. The mechanism operates through price discounts, higher logistics costs, and volatility effects that shape production incentives (Neyter et al., 2024; Steinbach & Yildirim, 2024).

The maritime trade case demonstrates that insurance and compliance are not peripheral details but core instruments of geoeconomic pressure. When risk premia rise and coverage tightens, private actors reduce exposure, leading to rerouting and capacity reallocation. This mechanism is consistent with both policy reporting and peer-reviewed evidence on trade disruption in the Black Sea (OECD, 2022; Nate et al., 2024).

The energy case indicates that coercive effects may be primarily forward-looking. Attacks and hybrid threats change expectations about the credibility of protection and the permanence of risk, which can shift investment and integration choices. This is precisely the type of systemic spillover emphasised in recent EU strategy documents on the Black Sea (European Commission & High Representative, 2025, Calus et al., 2025).

Two alternative explanations warrant attention. First, some observed market outcomes may reflect global shocks unrelated to the Black Sea, such as monetary tightening, climate-related harvest variation, and disruptions in other chokepoints. Second, market adaptation and policy interventions (subsidies, corridor arrangements, emergency releases) can mask coercive pressure. These confounders reduce the strength of causal inference unless event-window or process-tracing evidence is available.

- Accordingly, the evidentiary standard differs across domains. In grain markets, event-window studies provide stronger leverage for attributing market reactions to corridor policy shifts (Poursina et al., 2024). In insurance and shipping, the strongest evidence comes from documented underwriting and compliance changes coupled with observed routing patterns (OECD, 2022; UNCTAD, 2024a). In energy, evidence is often qualitative and must be interpreted with explicit uncertainty about attribution and covert action (Bozhilov, 2025).

- A further implication concerns deterrence and resilience policy. If coercion works by imposing a ‘risk tax’, then mitigation requires risk-sharing instruments, credible security assurances for commercial actors, and institutional mechanisms that reduce uncertainty about corridor access and infrastructure protection. This shifts attention from ad hoc crisis management towards governance reforms that make coercion less cost-effective. Concrete options include public–private risk-sharing arrangements, contingency underwriting facilities, and security-linked corridor assurance mechanisms that lower uncertainty for shipowners and charterers while preserving compliance integrity.

- The analysis also highlights a normative dimension. Economic coercion occupies a legal grey zone, and disagreements about what constitutes legitimate economic pressure can be exploited strategically. Recent scholarship on the norms of economic coercion suggests that clearer principles and practices are needed to reduce opportunistic escalation and to protect legitimate trade flows (Chachko & Newman, 2025).

Finally, the comparative design suggests a boundary condition for geoeconomic coercion: leverage is strongest where dependence is concentrated and where private actors cannot diversify risk. This points to the strategic value of diversification—of export routes, insurance backstops, and energy interconnections—as a long-term resilience strategy (European Commission & High Representative, 2025).

In sum, economic warfare in the Black Sea is best understood as a contest over the governance of interdependence. The cases show that coercion can be exercised through the combined effects of physical disruption and market mediation, producing outcomes that are economically significant even when formal policy instruments appear limited.

Methodologically, the paper's main limitation is reliance on open-source evidence. Future work could strengthen inference by integrating proprietary shipping and insurance datasets, port-call microdata, or firm-level trade finance information, and by systematically comparing the Black Sea with other maritime theatres subject to coercion.

Substantively, the findings underscore that regional security policy cannot be separated from market architecture. In the Black Sea, corridor governance, insurance design, and infrastructure resilience are not technical adjuncts—they are strategic variables that shape the distribution of power.

## 5. CONCLUSIONS

This article has argued that economic warfare in the Black Sea operates through three mutually reinforcing channels: corridor disruption in grain logistics, market-mediated constraints in maritime trade and insurance, and systemic uncertainty generated through pressure on energy infrastructure. Across domains, coercion is exercised by altering the costs, risks, and contractual conditions under which economic exchange can occur.

The analysis contributes by specifying mechanisms and observable indicators that support disciplined causal inference in a contested information environment. Where the evidence is strongest—grain corridor governance and market reactions—peer-reviewed studies and official assessments converge on measurable effects (Steinbach & Yildirim, 2024; Neyter et al., 2024). Where the evidence is weaker—offshore energy threats—the paper delineates limits and avoids over-confident attribution.

For editors and policymakers, two practical implications follow. First, resilience policy should prioritise reducing the 'risk tax' by stabilising insurance and shipping participation and by diversifying routes and capacity. Second, regional strategies should treat corridor governance and infrastructure protection as integrated security-economic instruments, consistent with recent European policy framing of the Black Sea as a strategic system (European Commission & High Representative, 2025). A complementary governance task is to reduce compliance ambiguity for legitimate trade by clarifying standards and information channels, which can limit over-compliance and unintended market withdrawal (Chachko & Newman, 2025).

1. Future research should test the proposed mechanisms with higher-resolution data and comparative designs, including cross-theatre comparisons with other chokepoint crises. Such work would clarify when geoeconomic coercion is most effective and how targeted states can design counter-measures that are economically sustainable.

2. Overall, the Black Sea illustrates a broader trend in international politics: economic interdependence can be converted into coercive capacity when risk, compliance, and infrastructure governance become levers of strategic influence (Farrell & Newman, 2019; Blackwill & Harris, 2016).

3. The policy challenge is therefore dual. It involves deterring physical disruption, while also shaping market institutions so that commercial actors can continue operating under stress without unintentionally magnifying coercive leverage.

4. By linking security events to market mechanisms and institutional responses, the article provides an analytically grounded basis for understanding how economic warfare is waged in maritime regions—and how it may be constrained.

## REFERENCES

- Balcaen, P. (2024, November 20). Beyond sanctions: Economic warfare and modern military conflict. Modern War Institute at West Point. <https://mwi.westpoint.edu/beyond-sanctions-economic-warfare-and-modern-military-conflict/>
- Baldwin, D. A. (1985). *Economic statecraft*. Princeton University Press, 508.
- Blackwill, R. D., & Harris, J. M. (2016). *War by other means: Geoeconomics and statecraft*. Harvard University Press, 384.

- Lyseiuk, A. (2025). Economic warfare in the Black Sea: A geoeconomic analysis of coercion through grain, blockades, and energy infrastructure. *Politics & Security*, 14(4), 6–15. <https://doi.org/10.54658/ps.28153324.2025.14.4.pp.6-15>
- Bozhilov, Y. (2025, May 21). Critical offshore energy infrastructure versus hybrid threats: How can we improve resilience. Sofia Security Forum. <https://sofiaforum.bg/publications/critical-offshore-energy-infrastructure-versus-hybrid-threats-how-can-we-improve-resilience>
- Całus, K., Michalski, A., Nowinowski, J., & Tarociński, J. (2025, June 26). Romania, Bulgaria and Turkey in the Black Sea. The Polish Institute of International Affairs (PISM). <https://www.osw.waw.pl/en/publikacje/osw-commentary/2025-06-26/romania-bulgaria-and-turkey-black-sea-region-increased>
- Chachko, E., & Newman, A. (2025). Building norms of economic coercion. *Journal of International Economic Law*, 28(3), 542–559. <https://doi.org/10.1093/jiel/jgaf035>
- Denamiel, T., Dodd, E., Glauber, J., Reinsch, W. A., & Welsh, C. (2024, June 10). From the farm to the ship to the fork: How maritime insurance can facilitate global food trade. Center for Strategic and International Studies (CSIS). <https://www.csis.org/analysis/farm-ship-fork-role-maritime-insurance-facilitating-global-food-trade>
- European Commission, & High Representative of the Union for Foreign Affairs and Security Policy. (2025). Joint communication on a strategic approach to the Black Sea region. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025JC0135>
- Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. *International Security*, 44(1), 42–79. [https://doi.org/10.1162/isec\\_a\\_00351](https://doi.org/10.1162/isec_a_00351)
- Harangozo, T. (2025, October 11). The war in Ukraine and mounting economic challenges in the greater Black Sea region. NATO Parliamentary Assembly. <https://www.nato-pa.int/document/2025-black-sea-report-harangozo-017-esctd>
- Kormych, B., Averochkina, T., & Kormych, L. (2024). Black Sea, grain, and two humanitarian corridors: Unblocking Ukrainian agricultural exports. *Small Wars & Insurgencies*. <https://doi.org/10.1080/09592318.2024.2384679>
- Lowenfeld, A. F. (2002). *International economic law* (2nd ed.). Oxford University Press.
- Martin, B. P. (2025). Shipping trade and geopolitical turmoil: The case of the Black Sea. *Journal of Transport Geography*, 128, 104342. <https://doi.org/10.1016/j.jtrangeo.2025.104342>
- Nate, S., Colibășanu, A., Stavytskyy, A., & Kharlamova, G. (2024). Impact of the Russo-Ukrainian war on Black Sea trade: Geoeconomic challenges. *Economics and Sociology*, 17(1), 256-279. doi:10.14254/2071-789X.2024/17-1/16
- Neyter, R., Zorya, S., & Muliari, O. (2024). Agricultural war damages, losses, and needs review. World Bank. <https://documents1.worldbank.org/curated/en/099062524074642129/pdf/P180198-405a6aea-dcd5-4926-9724-151419507961.pdf>
- OECD. (2022). Impact of the Russian invasion of Ukraine on insurance markets, Business and Finance Policy Papers, OECD Publishing, Paris, <https://doi.org/10.1787/731d1305-en>.
- Paul, A., & Taran, S. (2023, July 31). Russia's weaponisation of grain exports must not be tolerated. European Policy Centre. <https://www.epc.eu/publication/Russias-weaponisation-of-grain-exports-must-not-be-tolerated-52ae04/>
- Poursina, A., Schaefer, K. A., Hilburn, A. M., & Johnson, S. R. (2024). Economic impacts of the Black Sea Grain Initiative. *Journal of Agricultural Economics*, 75(1), 457–464. <https://doi.org/10.1111/1477-9552.12549>
- Sciubba, J. D. (2023). Population ageing and national security in Asia. *International Affairs*, 99(5), 2119–2136. <https://doi.org/10.1093/ia/iia176>

- Scowcroft Center for Strategy and Security. (2023, December 15). A security strategy for the Black Sea. Atlantic Council. <https://www.atlanticcouncil.org/in-depth-research-reports/report/a-security-strategy-for-the-black-sea/>
- Sikharulidze, V. (2025, March 13). Russian influence operations in Georgia: A threat to democracy and regional stability. Foreign Policy Research Institute. <https://www.fpri.org/article/2025/03/russian-influence-operations-in-georgia-a-threat-to-democracy-and-regional-stability/>
- Steinbach, S., & Yildirim, C. (2024). Grain futures market response to the Black Sea Grain Initiative. *German Journal of Agricultural Economics*, 73(2), 162–176. <https://doi.org/10.52825/gjae.v73i2.1343>
- UNCTAD. (2024a). Review of maritime transport 2024. United Nations Conference on Trade and Development. <https://unctad.org/publication/review-maritime-transport-2024>
- Welsh, C., & Glauber, J. (2024, February 29). Food as a silent weapon: Russia's gains and Ukraine's losses. Center for Strategic and International Studies (CSIS). <https://www.csis.org/analysis/food-silent-weapon-russias-gains-and-ukraines-losses>
- World Bank. (2023). Ukraine economic update: Sustaining recovery and reforms amidst war. <https://documents1.worldbank.org/curated/en/099071724134524264/pdf/BOSIB1d1d0622608518b00118695f23138b.pdf>
- .

# SOVEREIGNTY THROUGH SELECTIVE INTEGRATION: STRATEGIC NON-COMPLIANCE, COMPLIANCE MINIMALISM, AND GOVERNANCE HARDENING IN EU CRISIS POLITICS

Yassine Guennoun  
Sidi Mohammed Ben Abdellah University  
Fez, Morocco  
[yassine.guennoun@usmba.ac.ma](mailto:yassine.guennoun@usmba.ac.ma)  
<https://orcid.org/0009-0003-8777-9781>

**Abstract.** *This article identifies Central Europe as a laboratory and stress-test for internal disintegration within the European Union, where states use the Union’s own rules to advance sovereignty-first agendas from inside membership. The Visegrad Group’s shift from a cohesive veto bloc during the 2015 migration crisis to fracture after Russia’s invasion of Ukraine, alongside Hungary’s consolidation of a migration security doctrine within the EU, point to a shared underlying pattern. The article theorises this pattern as sovereignty through selective integration and specifies its operation through three interlocking practices: strategic non-compliance, compliance minimalism, and governance hardening. Drawing on earlier case study work on the Visegrad Group and on Hungary, the analysis shows how this triad operates at both regional and national scales, why it stabilised during the migration crisis, and why it fractured under conditions of direct hard security exposure. The article clarifies the scope conditions under which selective integration can endure, the circumstances under which it breaks down, and the ways in which it produces internal disintegration without formal exit. It concludes by outlining implications for EU crisis governance and by indicating how the proposed triad can travel to other domains, including fiscal policy, digital regulation, and internal security.*

**Keywords:** Differentiated integration; Central Europe; European Union; Compliance minimalism; Strategic non-compliance; Governance hardening.

## 1. INTRODUCTION

If you want to see sovereignty politics inside the EU without the theatre of exit, then look no further than Central Europe. The Visegrad Group coordinated opposition to relocation during the 2015 migration crisis and turned coalition discipline into leverage against EU decisions, yet the same grouping fractured after the 2022 Russian invasion of Ukraine as Poland, Hungary, Slovakia, and Czechia diverged sharply in their threat perceptions and alliance choices (Guennoun, 2025a). Over a similar period, Hungary converted migration from a temporary emergency into a durable doctrine that joins restrictive law, symbolic campaigns, and sustained resistance to EU legal demands, while remaining inside the Union’s institutional shell (Guennoun, 2025b). These trajectories point to a shared logic: sovereignty is increasingly asserted through selective engagement with integration, pursued inside the Union’s framework rather than through formal withdrawal.

Securitisation and security governance provide one entry point into this dynamic, particularly where attention to speech acts, audiences, and legitimation clarifies how political leaders elevate specific issues to existential status and claim extraordinary authority in response (Buzan et al, 1998; McDonald, 2008). The wider literature on insecurity and governmentality then shows how these exceptional claims acquire

administrative thickness over time, settling into routines, infrastructures, and organisational habits that make emergency governance durable rather than episodic. Huysmans (2006), Aradau and Blanke (2010), and Foucault (2007) each trace this consolidation through different vocabularies, yet the practical implication converges: once technologies of control become embedded, they organise everyday rule and sustain crisis logics beyond the moment that initially authorised them. Read through this lens, border fortification, biometric filtering, and risk-based screening function as standard instruments of governance, and their location in implementation creates predictable openings for member states to shape the practical meaning of common rules.

European integration theory already explains why these openings exist, because Scharpf's (1999) distinction between negative and positive integration points to a persistent asymmetry in which market-making advances faster than the construction of shared regulatory capacity, an imbalance that becomes politically sharper once integration reaches into core state powers such as border control, fiscal authority, and internal security. Participation in these domains has also become increasingly differentiated, producing uneven commitments that are stabilised through formal arrangements and, just as importantly, through the everyday administrative handling of obligations at national level (Genschel & Jachtenfuchs, 2014; Schimmelfennig, 2018), while crisis episodes intensify the configuration by raising the political payoff of insulation in sensitive fields without dissolving governments' dependence on the benefits of continued access. Instead of a clean regime of opt-outs, the Union ends up with a crowded and unstable mix of exceptions, improvised accommodations, and overlapping obligations that make sense only at the point of national implementation.

The question of how states operate within this fragmented terrain sits at the centre of scholarship on illiberal and post-liberal governance in Central and Eastern Europe. Analyses of Hungary, in particular, describe a mode of rule that preserves liberal-democratic institutional form while redirecting legal and administrative instruments toward sovereignty consolidation and domestic control. As noted by Waterbury (2020), Scott (2023), and Kim (2023), the goal becomes sovereignty consolidation and domestic control, achieved through the very instruments meant to limit power. Work on illiberal transnational fields traces the networks of think tanks and media platforms that diffuse sovereignty-first narratives to normalise resistance (Coman et al., 2025), a dynamic mirrored in legal studies of border governance in Hungary and Greece that document responsibility gaps, stalled enforcement, and the limits of judicial remedies in the face of persistent non-compliance (Gkliati, 2022; Hungarian Helsinki Committee, 2023). What remains under-specified across these literatures is how open defiance, narrow implementation, and institutional durability combine into a single mode of statecraft that can both endure across crises and fracture under shifting threat environments. Existing work tends to examine resistance, partial compliance, or crisis institutionalisation as separate phenomena, leaving their interaction and sequencing analytically fragmented.

The argument that follows bridges these strands by specifying a practice-based mechanism operating across them, positing that both the Visegrad Group's crisis-era coordination and Hungary's migration doctrine are best understood as expressions of sovereignty through selective integration. This term refers to a pattern in which states retain the advantages and formal status of EU membership while filtering, reinterpreting, and sequencing their obligations to expand domestic room for manoeuvre. Three interlocking practices anchor this configuration: strategic non-compliance, denoting deliberate and openly signalled refusal to implement specific EU rules for domestic leverage; compliance minimalism, capturing the surface performance of obligations while their substantive effect is narrowed in practice; and governance hardening, naming the conversion of exceptional tools into durable institutional architecture that outlasts the initial crisis. The contribution of the article lies in binding these practices into a single mechanism that explains both the endurance of sovereignty-first strategies in permissive fields and their limits under constraining crises.

Functioning as a theory-oriented and integrative study, this article builds directly on established empirical work regarding the Visegrad Group and Hungary's migration governance (Guennoun, 2025a) instead of introducing new primary material. The framework is derived through a systematic re-reading of those cases, treating documented patterns of defiance, implementation design, and institutional

consolidation as observable indicators of the three practices identified here. Its primary contribution lies in re-reading those findings through a unified conceptual lens to position them within wider debates on securitisation, differentiated integration, and post-liberal governance. To this end, we propose the triad of strategic non-compliance, compliance minimalism, and governance hardening as a diagnostic device capable of travelling across policy fields where EU rules are shaped and trimmed through practice rather than formal opt-outs. The analysis first develops this conceptual framework in detail before returning to the Visegrad Group and Hungary as compressed empirical anchors. Finally, we use the contrast between the migration decade and the war in Ukraine to identify when sovereignty through selective integration endures and when it reaches its limits (Marusiak, 2024).

## 2. CONCEPTUALISING SOVEREIGNTY THROUGH SELECTIVE INTEGRATION

Central Europe reveals a kind of statecraft that refuses the usual categories, where governments do not leave the Union and do not simply comply either, but stay inside to draw on its resources while bending obligations where outcomes are actually produced. This article conceptualises that configuration as *sovereignty through selective integration*, describing a mode of rule where states preserve the status and benefits of membership yet calibrate the reach of supranational authority through targeted resistance, narrow implementation, and institutional redesign.

The idea synthesizes three distinct intellectual lineages: it begins with integration theory's classic distinction between negative and positive integration, where market opening tends to outpace the construction of common regulatory capacities (Scharpf, 1999), and links this asymmetry to later debates on differentiated participation in core state powers such as borders, internal security, and fiscal policy (Genschel & Jachtenfuchs, 2014; Schimmelfennig, 2018). These structural insights are read alongside work on securitisation and security governance, which maps how threat politics settle into the infrastructures and routines that organise everyday rule (Buzan et al., 1998; Huysmans, 2006; Aradau & Blanke, 2010; Foucault, 2007), and are further refined by studies of illiberal and post-liberal governance that observe how governments can preserve liberal-democratic forms while repurposing them toward sovereignty-first objectives (Waterbury, 2020; Kim, 2023; Lottholz, 2022). *Sovereignty through selective integration* names the precise overlap between these strands; a condition where integration in sensitive domains advances, yet its operation becomes uneven and conditional through state practice.

Within this configuration, I treat three recurring practices as the basic machinery through which member states recalibrate the practical meaning of EU membership. At times, governments decline to implement specific EU rules, judgments, or policy decisions and justify the refusal as a defence of national autonomy, turning enforcement delay into political leverage. At other times, governments translate obligations into domestic law in formally adequate ways while narrowing their substantive reach at the point of implementation, using administrative thresholds, procedural bottlenecks, and selective enforcement to control outcomes. A third practice operates across crises with a slower rhythm: temporary instruments introduced under emergency pressure, including exceptional legal provisions, monitoring infrastructures, and improvised administrative arrangements, become ordinary state capacity once they are embedded in budgets, routines, and institutional mandates. The subsections that follow define these practices as *strategic non-compliance*, *compliance minimalism*, and *governance hardening*, and then show how they combine into a single mechanism that produces bargaining leverage, preserves formal alignment, and raises the political and administrative costs of reversal.

### 2.1 Strategic Non-Compliance

*Strategic non-compliance* denotes the moment a member state government decides to withhold implementation of a specific EU obligation and to do so in full view, because the domestic payoff is expected to outweigh legal exposure or reputational cost. The move is announced, defended, and repeated. It appears in speeches, government communication, and the surrounding mobilisation that casts resistance as protection against external imposition. The forms vary, from refusing to transpose a directive to slowing or blocking collective financial decisions, yet the identifying feature is consistent: authorities keep the

contested posture public and durable, including after adverse judgments, and they absorb the legal dispute into a wider sovereignty narrative. Hungary offers a clear illustration of this dynamic; where political actors dismissed Court of Justice rulings as illegitimate intrusions into national competence and continued the contested practices regardless (Gkliati, 2022; European Parliament, 2022).

This posture is the deliberate use of open non-compliance as a political tool, and it survives because domestic politics move faster than enforcement. This paper claims that defiance is calculated, because it is deployed to signal resolve to core voters and to force domestic opponents into reaction rather than initiative. EU sanctions rarely interrupt this sequence, and infringement procedures stretch over years. Hence, financial penalties lag behind political cycles. This temporal gap allows governments to extract political return first and absorb legal cost later. *Strategic non-compliance* thrives, and sometimes requires, policy fields where implementation runs through national authorities and where supranational enforcement cannot operate in real time. For analytical purposes, the diagnostic boundary is somewhat clear. The practice is absent when governments retreat quietly, reverse course rapidly under legal pressure, or shift to technical compliance without publicly owning the earlier refusal. Most notably, *strategic non-compliance* requires visible persistence, because the public display of defiance is itself part of the political instrument.

## 2.2 Compliance Minimalism

*Compliance minimalism* refers to a manoeuvre in which governments continue to ‘play the game’ under formal rules while reshaping how those rules bite in practice. It works a bit like a player who knows the rulebook by heart and has no problem following it when the referee is close, but starts pushing, slowing, and bending the moment they are not watched. On paper, everything looks fine. Legal texts are adopted, institutions remain in place, reports are filed on time. In practice, compliance starts to mean something else once rules fall into administrative hands. The clearest place to watch this happen is migration and border governance. The process runs with a dull kind of precision, almost mechanical. Eligibility rules tighten without announcement, applicants are quietly redirected into accelerated or exceptional tracks, and procedural blockages stack up until protection survives mostly as a legal fiction. Official language never misses a beat as authorities continue to insist that nothing fundamental has changed and that alignment with EU directives remains intact (Gkliati, 2022; Hungarian Helsinki Committee, 2023). Review and appeal mechanisms still make the line-up, but they no longer touch the ball. Decisions slip past them and settle in security agencies and discretionary administrative corners where scrutiny fades and outcomes tend to stick. From a distance, the institutional architecture continues to resemble supranational expectations. At the point of implementation, however, outcomes move decisively away from them.

The attraction of *compliance minimalism* lies in its ambiguity, allowing governments to preserve access to the material and symbolic benefits of membership, including structural funds and the appearance of rule-of-law adherence, while enjoying a measure of legal insulation against infringement proceedings. Minimalist compliance therefore complements *strategic non-compliance*, enabling governments to narrow the effect of supranational rules without the political risks of open rejection when direct refusal would be too costly or visible. *Compliance minimalism* is empirically undermined where implementation produces substantively equivalent outcomes to EU expectations despite domestic discretion, rather than systematic outcome-narrowing through administrative control.

## 2.3 Governance Hardening

Finally, *governance hardening* captures the process through which emergency tools, temporary exceptions, and ad hoc responses become embedded in the institutional fabric of the state. Drawing on security studies that emphasise how techniques introduced under the sign of crisis evolve into routine forms of administration (Buzan et al., 1998; Huysmans, 2006), and Foucault’s account of *dispositifs* as material and discursive apparatuses that organise conduct and perception to convert exception into rule (Foucault, 2007), the concept applies these insights to the specific context of Europeanised statecraft.

Guennoun, Y. (2025). Sovereignty through selective integration: Strategic non-compliance, compliance minimalism, and governance hardening in EU crisis politics. *Politics & Security*, 14(4), 16–30. <https://doi.org/10.54658/ps.28153324.2025.14.4.pp.16-30>

In practice, crisis moments often justify the introduction of new legal categories, specialised agencies, and technological infrastructures, where border fences, biometric databases, and expanded police powers appear first as necessary responses to extraordinary conditions. Once these measures are installed, they stop behaving like temporary responses and start behaving like assets. They create interests inside the bureaucracy, absorb resources, and organise information flows in ways that favour their own continuation. Removing them becomes costly in practice. It requires legislation, budgetary reallocation, and administrative disruption. While keeping them delivers an immediate signal of control and capacity.

Over time, these measures stop feeding on fear altogether. What once needed emergency language to survive turns into routine governance, used without explanation and rarely questioned. The tools stay in place because they now actually work. They organise routines, structure decisions, and signal control, long after the emergency that introduced them has faded. This matters most in Europeanised policy fields. Instruments arrive labelled as EU compliance, but they do not stay loyal to that label. Once implementation begins, domestic authorities decide what gets enforced, what gets slowed down, and what quietly drops out. Repeat this long enough and the function shifts. What began as compliance infrastructure settles into something else entirely. What enters as infrastructure for meeting EU obligations can end up serving nationally defined agendas, even as its legal form continues to signal alignment. For instance, investments in surveillance systems and screening procedures encouraged by EU funding instruments can later serve selective enforcement or deterrent functions that stretch the spirit of common rules (Khoury & Hindow, 2025; European Digital Rights et al., 2025). *Governance hardening* thus exceeds the routinisation of exception by explaining how crisis-born capacity becomes a domestic lever for reshaping supranational rules under conditions of delegated authority. As emergency derogations linger in statute books and temporary coordination bodies evolve into permanent hubs, *governance hardening* changes the terrain on which strategic non-compliance and *compliance minimalism* operate, raising the practical cost of reversing sovereignty-first choices and providing the material backbone for their continuation. The absence of hardening would be indicated by the dismantling or deactivation of crisis instruments once pressures subside, rather than their consolidation into routine capacity.

## 2.4 The Triad as Mechanism

*Strategic non-compliance*, *compliance minimalism*, and *governance hardening* operate as a unified mechanism through which *sovereignty through selective integration* is enacted and stabilised. In this dynamic, open defiance of specific rules signals resolve and tests the boundaries of enforcement, minimalist implementation lowers the immediate risks of sanction by preserving formal conformity, and *governance hardening* converts contingent responses into institutional infrastructure that is difficult to unwind.

The mechanism depends on context as it does not operate everywhere in the same way. Basically, it takes hold where EU enforcement is slow, implementation runs through national administrations, and disputes can be depicted as issues of security or sometimes identity. Under these conditions, the sequence stabilises. Where enforcement is fast, discretion is limited, or hard security constraints are immediate, it breaks down. The point of the mechanism is to account for this unevenness. It explains why the same practices harden in some domains and fall apart in others, rather than pretending to offer a general law of EU governance. Rather than attempting an exhaustive mapping of these conditions across the Union, the sections that follow focus on two empirical anchors where the triad has already been identified: the Visegrad Group's crisis-era coordination, illustrating the mechanism's operation in a regional setting, and Hungary's migration trajectory, showing how it crystallises into a national doctrine of post-liberal governance (Guennoun, 2025a; 2025b). This comparison creates leverage for asking when *sovereignty through selective integration* can endure and when external shocks, such as a major war, constrain its scope.

Designed for export, the conceptual vocabulary developed here offers a diagnostic frame for other policy domains where member states seek to protect sensitive competences while remaining inside the common framework, including fiscal surveillance, rule-of-law conditionality, and internal security. In each case, researchers can ask how far *strategic non-compliance* is pursued, where compliance minimalism

substitutes for open defiance, and to what extent crisis-born instruments have hardened into durable architecture, before the analysis turns to the Central European cases to show how the mechanism works in practice.

### 3. TWO EMPIRICAL ANCHORS: REGIONAL COALITION AND NATIONAL DOCTRINE

The argument rests on two cases examined in detail elsewhere, specifically the Visegrad Group's trajectory from migration crisis coordination to post-2022 fracture and Hungary's decade-long migration securitisation (Guennoun, 2025a; Guennoun, 2025b), which this section reads through the lens of *sovereignty through selective integration* rather than reconstructing their developments. The aim is to demonstrate how the triad of *strategic non-compliance*, *compliance minimalism*, and *governance hardening* operates at regional and national scales inside the same institutional environment.

#### 3.1 Visegrad as Regionalised Selective Integration

Previous work on the Visegrad Group highlighted how the four governments utilised migration governance as an arena for collective resistance to integration in core state powers (Glien & Zamęcki, 2021; Guennoun, 2025a), engaging in a regionalised form of *strategic non-compliance* during the 2015 crisis by aligning against relocation schemes and relying on slow enforcement to sustain a line that invited repeated infringement procedures (Jaroszewicz & Gniadzowski, 2015; Gkliati, 2022; CJEU, 2020). Concurrently, the discourse of 'flexible solidarity' illustrates *compliance minimalism* at coalition scale, where governments accepted the formal architecture of Schengen yet insisted on narrow interpretations to preserve domestic discretion, using shared positions to normalise this reading as a legitimate variant of membership (Visegrád Group, 2021). Although *governance hardening* was weaker here than in national settings, it remained visible in the consolidation of security strategies (Czyż, 2024) until the war in Ukraine shifted the conditions for this regionalised selective integration. As Poland and Czechia moved toward robust support for Kyiv while Hungary adopted a transactional line (Czyż, 2024; Guennoun, 2025a), the divergence marked the point where *strategic non-compliance* ceased to be collectively manageable, leaving *sovereignty through selective integration* to persist as a national practice once hard security considerations reordered threat perceptions.

#### 3.2 Hungary as Doctrinal Selective Integration

The Hungarian case, examined elsewhere as a 'migration doctrine', demonstrates the same triad embedded in a national setting, where the early securitisation of migration fused external threat narratives with assertions of constitutional sovereignty to shape legal reforms and border measures (Jaroszewicz & Gniadzowski, 2015; Waterbury, 2020; Guennoun, 2025b). Seen through the present framework, the recurrent refusal to align with EU asylum and NGO law even after clear Court of Justice judgments exemplifies a *strategic non-compliance* that is both deliberate and publicly justified as a defence of national autonomy (CJEU, 2020, 2021; European Parliament, 2022).

Open defiance cannot go on forever, eventually confrontation becomes costly, and so authorities change tactics and slide into compliance minimalism. The outlook softens without a significant change in outcome. Laws are tweaked to absorb specific criticisms while leaving the restrictive core intact. Rights organisations show how this keeps push-backs and limited access alive over time, all while institutions keep repeating the vocabulary of EU directives as if nothing has changed (Hungarian Helsinki Committee, 2023; Gkliati, 2022). What emerges is not straightforward non-compliance, but a working arrangement in which partial legal alignment, procedural density, and selective enforcement hold together. This is *compliance minimalism* as it actually operates, not as an abstract category, and it functions as a key moving part of the broader mechanism developed in this article.

The longer trajectory is secured through *governance hardening*, as crisis-era measures such as border fences, surveillance infrastructures, and biometric controls have been consolidated into a stable border

Guennoun, Y. (2025). Sovereignty through selective integration: Strategic non-compliance, compliance minimalism, and governance hardening in EU crisis politics. *Politics & Security*, 14(4), 16–30. <https://doi.org/10.54658/ps.28153324.2025.14.4.pp.16-30>

regime whose operation no longer depends on acute crisis conditions (Khoury & Hendow, 2025; European Digital Rights et al., 2025), a material consolidation reinforced by a parallel symbolic layer in the form of national consultation campaigns that recast resistance as democratic mandate rather than institutional deviation (Hungarian Government, 2017, 2018). This combined material and symbolic structure has proven sufficiently robust that the war in Ukraine did not dismantle it, with the hardened apparatus instead absorbing the shock through differentiated treatment of arrivals, extending preferential access to culturally proximate refugees while leaving the sovereignty-first orientation of the regime intact (Vidra & Messing, 2025; Human Rights Watch, 2025).

### 3.3 What the Two Anchors Show

Read side by side, the Visegrad and Hungarian trajectories bring into focus both the flexibility and the limits of *sovereignty through selective integration*. They show how the triad can function through coalition-building and shared narratives of resistance at the regional level, where coordination amplifies defiance but remains exposed to shifts in the security environment, while also demonstrating how the same practices can be embedded within a national order to form a doctrine capable of enduring across successive crises. Although both anchors unfold within the same EU legal framework and draw on comparable repertoires of securitisation, their divergence turns on the scale and depth of *governance hardening* and on whether *strategic non-compliance* is sustained by collective backing or carried nationally. These differences structure the analysis that follows, which places the migration decade and the war in Ukraine in direct comparison in order to specify the conditions under which the triad remains operative and the points at which its capacity to hold begins to erode.

## 4. CRISIS ENVIRONMENTS: MIGRATION GOVERNANCE AND WAR

*Sovereignty through selective integration* operates differently depending on the crisis terrain in which it is activated, because each crisis carries its own institutional time horizon, monitoring profile, and distribution of discretion between EU and national authorities. Migration governance during the 2010s combined wide national latitude with fragmented oversight and a slower enforcement tempo, conditions that allowed the triad to develop through prolonged contestation and iterative adjustment. The war in Ukraine introduced a contrasting environment defined by immediate hard security exposure, compressed decision cycles, and tighter alliance expectations, shifting the constraints under which *strategic non-compliance*, *compliance minimalism*, and *governance hardening* can be pursued and reshaping their political payoffs.

### 4.1 Migration as Permissive Field

The 2015 migration crisis unfolded inside a policy architecture that looked solid from the outside but worked very differently once real pressure was applied. The Union held wide legal competences, yet the work that actually determined outcomes processing asylum claims, managing reception, and controlling borders remained in national hands. Harmonisation set the framework, but the actual weight is carried by implementation. In other words, monitoring never really sealed the distance between law on paper and what happened on the ground (Schammann et al., 2021). The system looked centralised, but the controls were elsewhere. A shared blueprint sat at the centre, while separate players decided how fast to move and what to strip out, provided the final shape still passed inspection. That opening let governments hollow out commitments from the inside and still keep the benefits, the funding, and the symbolic weight of EU membership.

Earlier work on the Visegrad Group and Hungary treats the migration crisis as a permissive moment rather than a legal vacuum. As EU rules were present but implementation sat squarely with national administrations under uneven and delayed oversight (Glied & Zamecki, 2021). This gap is important because it created room for both *strategic non-compliance* and *compliance minimalism* to operate at relatively low short-term cost (Guennoun, 2025a; Guennoun, 2025b). The easiest way to see this pattern

is in the refusal by Poland and Hungary to implement relocation decisions. The stance was openly confrontational and invited infringement procedures, yet it functioned as a domestic performance of sovereignty and cultural defence whose political returns arrived faster than legal penalties (CJEU, 2020; Jaroszewicz & Gniazdowski, 2015). At the same time, Hungarian authorities used the same flexibility to rework legislative detail and administrative practice so that restrictive outcomes stayed in place while the ‘appearance of compliance’ was preserved (Hungarian Helsinki Committee, 2023; Gkliati, 2022). EU enforcement moved slowly, which helped avoid escalation and allowed the strategy to hold.

Over time, procedural adjustments reshaped the administrative landscape. Emergency measures stayed in place and became part of ordinary governance. Transit zones did not disappear. Accelerated asylum procedures ceased to be exceptional safeguards and instead became routine tools for fast-tracking rejection. What had been justified as temporary settled into routine. Administrative practice bent around these tools and then began to rely on them. Money followed the shift. Surveillance technologies and biometric systems expanded, often with support from EU funding instruments, and gave physical weight to what had started as improvised fixes (Khoury & Hendow, 2025; European Digital Rights et al., 2025). Over time, a restrictive border regime took shape that no longer needed constant crisis talk to keep running. It had become infrastructure. In Hungary, the migration state of emergency remained in force long after the immediate pressures of 2015 subsided to supply legal cover for exceptional practices (Hungarian Helsinki Committee, 2023), while in the Visegrad context, repeated meetings and joint declarations helped naturalise a sovereignty-first reading of EU obligations (Visegrád Group, 2021; Glied & Zamecki, 2021).

Ultimately, viewed through the perspective of the triad, migration governance in this decade offered a permissive field where *strategic non-compliance* could be sustained due to delayed sanctions, *minimalist implementation* allowed governments to claim adherence while altering outcomes, and *hardening* successfully turned crisis responses into entrenched governance structures, resulting in a pattern of selective integration that remained formally compatible with membership yet altered the practical content of common rules.

#### 4.2 War as Constraining Field

Russia’s full-scale invasion of Ukraine in February 2022 fundamentally altered the strategic environment for Central European states, bringing hard security concerns to the foreground as questions of military supply, alliance credibility, and deterrence came to dominate elite and public debate (Czyż, 2024; Helwig, 2023). In this setting, *sovereignty through selective integration* ran out of room, most clearly at the regional level. Consistent with security studies scholarship highlighting how external threat compresses timelines and narrows acceptable policy space, driving states in exposed positions to prioritise reliable protection and material capabilities over symbolic autonomy (Walt, 1987; Lake, 2009; Buzan & Wæver, 2003), the Visegrad experience followed this pattern as Poland and Czechia rapidly aligned with United States and NATO preferences. By increasing defence spending and taking on forward roles to present themselves as front-line states within a Western security community (Beck, 2024; Bugajski, 2025), these governments found that *strategic non-compliance* toward EU foreign policy positions became harder to justify domestically where it risked signalling weakness in the face of Russian aggression.

In contrast, Hungary pursued a distinct trajectory, maintaining a narrow interpretation of national interest that emphasised energy security and resisted joint EU measures on sanctions and military support (Guennoun, 2025a), a stance that appears through the lens of the triad as an attempt to extend *strategic non-compliance* into the security field. While veto threats and delays over Ukraine-related funds replicated familiar patterns from migration governance, the coalition support that had sustained *sovereignty through selective integration* at the regional level during the 2010s was no longer available, leaving the Visegrad platform to lose much of its relevance for high politics as Poland and Czechia built new formats of cooperation with like-minded states (Kaniok & Hloušek, 2025; Ušiak, 2024).

Furthermore, the war reshaped the meaning of *compliance minimalism* by creating a distinct calculus compared to migration governance, where narrow implementation had limited direct consequences for other member states. In the security field, half-hearted alignment on sanctions or support risked

weakening the overall position of the Union and exposing internal divisions to external actors (Costa et al., 2024; Helwig, 2023), raising the reputational and strategic costs of minimalist compliance for governments under direct threat. Once the security environment changed, regional defiance was no longer a useful currency. This is why Poland and Czechia stepped back from alignment across the board, without abandoning contestation altogether.

Here, Hungary walked alone. Its migration doctrine absorbed the shock of war without losing shape, carrying forward a hardened border regime and a sovereignty-first legal architecture already set in place. What followed was a shift in classification rather than retreat. Authorities drew a sharp line between categories of movement, folding Ukrainian refugees into a narrative of proximity and deservingness while leaving ‘other migrants’ governed by the older securitising frame that had structured policy since the migration crisis (Vidra & Messing, 2025; Human Rights Watch, 2025). Consequently, while *strategic non-compliance* shifted from the centre of public debate, it persisted in the handling of broader migration issues and funding disputes, just as *compliance minimalism* and *governance hardening* continued to shape everyday interactions at the border.

### 4.3 What Crisis Comparison Reveals

The comparison between the migration decade and the war in Ukraine clarifies the scope conditions for *sovereignty through selective integration*, demonstrating that where crises unfold in fields highly dependent on national implementation and where enforcement remains slow or contested, the triad can be sustained and deepened. Migration governance in the 2010s met these precise conditions, creating an environment where *strategic non-compliance* generated domestic and regional leverage, *minimal implementation* protected formal alignment, and *hardening* locked in a sovereignty-first regime.

In contrast, hard security crises create a less permissive terrain because external threat compresses time and heightens the value of reliable collective action, rendering regionalised selective integration fragile. In this environment, divergent threat perceptions and alliance choices undermine coalitions that previously coordinated resistance, as illustrated by the Visegrad fracture after 2022 (Czyż, 2024; Beck, 2024). Consequently, national doctrines anchored in hardened governance structures can endure under pressure, but the space for openly defiant or minimalist positions in high politics contracts sharply once security stakes rise, particularly for states dependent on external protection.

The implication reaches beyond Central Europe as *Sovereignty through selective integration* consolidates most easily in policy domains where Union authority passes through domestic administrations and where crisis can be depicted as cultural or social rather than military. External shocks then reshape the balance between regional coalitions and national doctrines without dissolving the underlying tensions inside European governance.

## 5. IMPLICATIONS FOR EU GOVERNANCE AND DIFFERENTIATION

The mechanism of *sovereignty through selective integration* speaks directly to debates on differentiated integration, internal disintegration, and EU foreign policy, positioning *strategic non-compliance*, *compliance minimalism*, and *governance hardening* as central techniques through which member states shape the practical content of integration in sensitive domains while remaining formally aligned with the Union.

### 5.1 Variable Geometry and Coalitions

While research on European foreign policy has long emphasised the role of informal groupings and coalitions in driving collective action, especially in crisis contexts (Keukeleire & Delreux, 2022; Costa et al., 2024), the Visegrad experience and its aftermath demonstrate that such groupings can conversely operate as vehicles for *sovereignty through selective integration*. Where governments share a sovereignty-first reading of contested policies and face low immediate security costs, regional coalitions serve to magnify the effects of *strategic non-compliance* and minimalist alignment. However, the post-2022 shift toward ad

hoc coalitions of the willing in support of Ukraine indicates a structural counter-move, as states that perceive veto politics as threatening vital interests search for formats that bypass recalcitrant partners (Rankin, 2025; Helwig, 2023). This dynamic suggests that *sovereignty through selective integration* at the coalition level is self-limiting: the more a grouping relies on defiance and minimalism, the stronger the incentives for others to construct parallel arrangements that reduce its blocking power, revealing that variable geometry has a dual face capable of shielding sovereignty-first agendas while simultaneously insulating the Union against their most disruptive effects.

## 5.2 Internal Disintegration by Practice

The triad sharpens how internal disintegration is usually approached in the literature because it pushes the analysis beyond the prevailing emphasis on formal differentiation. Most accounts have focused on opt-outs, treaty protocols, and institutionalised arrangements that regulate non-participation (Genschel & Jachtenfuchs, 2014; Schimmelfennig, 2018), yet the Central European cases indicate a different route through which cohesion erodes from within. Rather than withdrawing from common frameworks, member states remain formally integrated while progressively thinning out the operational content of shared rules. Internal disintegration, as used in this article, refers to the territorial divergence of outcomes produced by formally uniform rules due to sustained variation in implementation, enforcement, and institutional capacity, even in the absence of treaty change or exit.

This form of fragmentation is difficult to register through legal categories alone, because obligations remain formally intact and institutional maps continue to project coherence while the lived experience of rights and protections diverges sharply at the point of implementation. Migration and asylum offer the clearest illustration, since individuals can face radically different chances of access depending on where they encounter the system despite the existence of harmonised law. The mechanism developed here predicts that such divergence is most likely in policy domains characterised by high dependence on national administration, uneven monitoring, and the durability of crisis-born capacity. The result is a layered Union in which disintegration advances through administrative routines and infrastructural investments, producing uneven outcomes without requiring explicit legal rupture. Cohesion thus becomes increasingly formal rather than substantive, maintained at the level of law while eroding in practice.

## 5.3 Directions for Further Research

The triad developed in this article opens a distinctly IR line of inquiry because it treats EU membership as a strategic setting in which authority, compliance, and distributional conflict are negotiated under institutional constraint. These extensions are offered as analytically bounded sites for testing the mechanism across different enforcement tempos, monitoring capacities, and distributions of discretion. A first extension lies in fiscal surveillance and macroeconomic governance, where scholars can trace how *strategic non-compliance* crystallises around deficit rules and conditionality, how *compliance minimalism* is performed through interpretive sequencing and domestically managed 'adjustments,' and how crisis instruments that enter as contingent bargains acquire durability as everyday leverage once they become embedded in routines, expectations, and reputational scripts.

A second and increasingly consequential terrain is digital regulation and internal security, particularly in policy fields where monitoring infrastructures, data-sharing arrangements, and cross-border police cooperation are expanded through reference to terrorism, cyber threat, and systemic risk.

Once EU rules pass into national administration, their meaning is no longer settled by the text. It is settled by who handles them. Domestic authorities decide what data is opened, which thresholds matter, and what gets enforced first. Some instruments continue to serve shared regulatory goals. Others are quietly turned. They keep their legal shape while doing different work underneath. This only holds under the right conditions: time, cover, and room to operate before anyone intervenes. On paper, the system still looks intact. In practice, control has already moved.

From the Brussels side, delegation does not behave like a neutral transmission chain, even if it is often treated as one. Once rules leave the supranational level and enter national administrations, they pass

into hands that decide how fast things move, which files receive attention, and how information circulates. At that point, formal alignment stops guaranteeing shared effects. The law may look uniform, but in reality outcomes drift. Similar obligations begin to produce uneven results because implementation lives in practice, not in text. This is where the cohesion problem actually takes shape, inside routine administrative work and inside the infrastructures that grow around it and quietly lock those practices in over time. Read this way, *sovereignty through selective integration* captures how authority actually works inside institutional cooperation: common frameworks endure, enforcement remains uneven, reputational pressure does selective work, and practical control steadily goes back to the state.

## 6. CONCLUSION

Central Europe serves as the empirical stress-test for the triad theorised in this article. The concepts of *strategic non-compliance*, *compliance minimalism*, and *governance hardening* were developed to capture how sovereignty is exercised from within EU membership, and the Central European cases place that framework under examination. The migration crisis showed how the Visegrad Group converted control over implementation into bargaining leverage and agenda power, yet that regional capacity proved conditional on a permissive threat environment in which disputes could be managed as governance conflict rather than existential security exposure. The war in Ukraine exposed the limits of that regional strategy as hard security exposure reordered incentives and threat perception, tightening the tolerance for divergence and raising the cost of intra-group ambiguity. Hungary followed a different trajectory, pushing the triad inward and stabilising it as a national doctrine, with crisis politics solidifying into doctrine as legal categories, physical infrastructures, and administrative routines embedded sovereignty-first preferences that persisted as external conditions changed. Across these cases, the pattern holds. States retain the benefits of membership and filter obligations at the precise point where policy outcomes are produced. This article captures that pattern under the concept of *sovereignty through selective integration* and specifies its mechanism through *strategic non-compliance*, *compliance minimalism*, and *governance hardening*.

The conceptual move lies in treating these practices as an ordered sequence operating through the political structure of delegation. *Strategic non-compliance* functions as a signalling and bargaining device that exploits enforcement tempo and the visibility of defiance to generate domestic legitimacy and external leverage. *Compliance minimalism* operates through interpretive control and administrative design, sustaining formal alignment while reducing substantive effects through procedures, thresholds, and selective enforcement. *Governance hardening* secures the whole configuration by converting crisis instruments into routine state capacity, raising the institutional and political costs of reversal and carrying sovereignty-first preferences across electoral time and political turbulence. In combination, the triad clarifies how authority can be reshaped from within through the everyday politics of implementation even as the legal surface of the order continues to display consistency.

The crisis comparison clarifies the scope conditions under which this mechanism operates and explains why regional coordination fractured. Migration governance over the previous decade depended heavily on national implementation and functioned under fragmented oversight, which meant that control over pacing, access, and procedural sequencing could be politicised without immediately triggering decisive enforcement. It also allowed disputes to be framed as questions of culture, identity, and social order rather than military necessity, and in that configuration defiance, procedural narrowing, and institutional consolidation become politically productive because costs are deferred and enforcement is filtered through national administrations. The war in Ukraine reordered these conditions, compressing decision cycles, making alliance credibility central, and turning internal division into an immediate strategic liability. The shift from veto bloc to strategic void follows from this divergence in hardening trajectories: once *governance hardening* locks states onto incompatible security tracks, the space for regional cohesion closes and the coalition logic becomes structurally unrecoverable. National doctrines anchored in hardened governance structures proved capable of adjustment, yet the high-stakes security field imposed firmer limits on how far selective integration could extend.

For research on European integration and disintegration, two implications follow from this comparison. *Sovereignty through selective integration* redirects attention away from formal differentiation and toward the practical life of common rules. Administrative decisions and infrastructural investments generate durable divergence even when legal commitments remain formally intact. Cohesion therefore turns on enforcement and monitoring design as much as on treaty architecture. Slow enforcement, uneven visibility of implementation, and the quiet permanence of crisis instruments expand the operational space for selective integration. Looking ahead, enlargement and deeper defence integration are likely to intensify these dynamics by increasing heterogeneity in administrative capacity and raising the political value of discretion in sensitive domains. The outcome is a Union that can remain legally coherent while becoming operationally uneven.

The triad is offered here as a diagnostic device, designed to structure comparative research across other domains of European and international governance, including fiscal surveillance, digital regulation, internal security, and rule-of-law conditionality. It fixes attention on three observable questions framed as a single diagnostic sequence: where *strategic non-compliance* functions as bargaining posture, how administrative design and interpretive control translate *compliance minimalism* into practice, and when crisis-born instruments harden into durable governance capacity. Working through these questions across cases makes it possible to locate where operational divergence is produced under stable legal form. Tracing these dynamics across domains and regions clarifies how supranational authority is recalibrated under delegation and how internal disintegration advances through implementation even as the institutional surface continues to signal cohesion.

## REFERENCES

- Aradau, C., & Blanke, T. (2010). Governing circulation: A critique of the biopolitics of security. In M. de Larrinaga & M. G. Doucet (Eds.), *Security and global governmentality: Globalization, governance and the state* (pp. 41–56). Routledge.
- Beck, R. (2024, April 3). *The Visegrád Four: From troubled to broken*. Foreign Policy Research Institute. <https://www.fpri.org/article/2024/04/visegrad-four-from-troubled-to-broken>.
- Bugajski, J. (2025, January 14). *Poland seeks more effective regional formats as the Visegrád Group fractures*. Jamestown Foundation. <https://jamestown.org/program/poland-seeks-more-effective-regional-formats-as-the-visegrad-group-fractures/>.
- Buzan, B., & Wæver, O. (2003). *Regions and powers: The structure of international security*. Cambridge University Press. <https://ir101.co.uk/wp-content/uploads/2018/11/Buzan-Waever-2003-Regions-and-Powers-The-Structure-of-International-Security.pdf>
- Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner.
- Coman, R., Paulis, E., Puleo, L., & Trino, N. (2025). Building and legitimizing an illiberal transnational field: Illiberal think tanks' struggle for cultural hegemony in Poland and Hungary. *European Political Science*, 3, 513-531. <https://doi.org/10.1057/s41304-025-00544-6>
- Costa, O., Juncos, A. E., Müller, P., & Sjursen, H. (2024). Contested but resilient: Accounting for the endurance of the European Union's foreign policy. *JCMS: Journal of Common Market Studies*. <https://doi.org/10.1111/jcms.13686>.
- Court of Justice of the European Union. (2020, December 17). *Commission v Hungary (Asylum)*, Case C-808/18 (Judgment). <https://curia.europa.eu/juris/liste.jsf?num=C-808/18>

- Guennoun, Y. (2025). Sovereignty through selective integration: Strategic non-compliance, compliance minimalism, and governance hardening in EU crisis politics. *Politics & Security*, 14(4), 16–30. <https://doi.org/10.54658/ps.28153324.2025.14.4.pp.16-30>
- Court of Justice of the European Union. (2021, November 16). *Commission v Hungary (Criminalisation of assistance to asylum seekers)*, Case C-821/19 (Judgment; Press release No 205/21). <https://curia.europa.eu/jcms/upload/docs/application/pdf/2021-11/cp210205en.pdf>
- Czyż, A. (2024). The Visegrad Group countries towards the war in Ukraine in 2022. *Studia Politologiczne*, 73, 254–271. <https://doi.org/10.33896/SPolit.2024.73.15>
- European Digital Rights, Access Now, & Hungarian Civil Liberties Union. (2025, May 6). Hungary's new biometric surveillance laws violate the AI Act. EDRI. <https://edri.org/our-work/hungarys-new-biometric-surveillance-laws-violate-the-ai-act/>
- European Parliament. (2022). Report on the situation in Hungary pursuant to Article 7(1) TEU (A9-0217/2022). European Parliament. [https://www.europarl.europa.eu/doceo/document/A-9-2022-0217\\_EN.html](https://www.europarl.europa.eu/doceo/document/A-9-2022-0217_EN.html)
- Foucault, M. (2007). *Security, territory, population: Lectures at the Collège de France, 1977–1978*. Palgrave Macmillan. <https://mirror.explodie.org/Foucault-Security-Territory-Population.pdf>
- Genschel, P., & Jachtenfuchs, M. (Eds.). (2014). *Beyond the regulatory polity? The European integration of core state powers*. Oxford University Press. <https://hdl.handle.net/1814/34498>
- Gkliati, M. (2022). The next phase of the European Border and Coast Guard: Responsibility for returns and push-backs in Hungary and Greece. *European Papers*, 7(1), 171–193. <https://doi.org/10.15166/2499-8249/553>
- Glied, V., & Zamecki, Ł. (2021). Together, but still separated? Migration policy in the V4 countries. *Politics in Central Europe*, 17(s1), 647–673. <https://doi.org/10.2478/pce-2021-0027>
- Guennoun, Y. (2025a). The Visegrad Group and the war in Ukraine: From veto bloc to void. *Politics & Security*, 13(3), 35–45. <https://doi.org/10.54658/ps.28153324.2025.13.3.pp.35-45>
- Guennoun, Y. (2025b). From Crisis to Doctrine: A Decade Of Migration Securitization And Strategic Defiance In Hungary. *Politics & Security*, 13(3), 46-57. <https://doi.org/10.54658/ps.28153324.2025.13.3.pp.46-57>
- Helwig, N. (2023). EU Strategic Autonomy after the Russian Invasion of Ukraine: Europe's Capacity to Act in Times of War. *JCMS: Journal of Common Market Studies*, 61: 57–67. <https://doi.org/10.1111/jcms.13527>.
- Human Rights Watch. (2025). Hungary. In *World report 2025*. <https://www.hrw.org/world-report/2025/country-chapters/hungary>
- Hungarian Government. (2017, April 3). The national consultation packages are already being delivered, including a letter from the Prime Minister. Cabinet Office of the Prime Minister. <https://akadalymentes.2015-2019.kormany.hu/en/cabinet-office-of-the-prime-minister/news/the-national-consultation-packages-are-already-being-delivered-including-a-letter-from-the-prime-minister>.
- Hungarian Government. (2018). *Proposal on the «Stop Soros» legislative package*. <https://helsinki.hu/wp-content/uploads/STOP-SOROS-LEGISLATIVE-PACKAGE-PROPOSAL.pdf>
- Hungarian Helsinki Committee. (2023). *Country report: Hungary – 2023 update*. Asylum Information Database (AIDA). [https://asylumineurope.org/wp-content/uploads/2024/07/AIDA-HU\\_2023-Update.pdf](https://asylumineurope.org/wp-content/uploads/2024/07/AIDA-HU_2023-Update.pdf)

- Huysmans, J. (2006). *The politics of insecurity: Fear, migration and asylum in the EU*. Routledge, 208 p.
- Jaroszewicz, M., & Gniazdowski, M. (2015, September 9). *The Hungarian stage of the migration crisis*. Centre for Eastern Studies (OSW). <https://www.osw.waw.pl/en/publikacje/analyses/2015-09-09/hungarian-stage-migration-crisis>.
- Kaniok, P., & Hloušek, V. (2025). Visegrad Four as an institution in times of EU crises. *European Politics and Society*, 1–19. <https://doi.org/10.1080/23745118.2025.2488815>.
- Keukeleire, S., & Delreux, T. (2022). *The foreign policy of the European Union* (3rd ed.). Palgrave Macmillan.
- Khoury, C., & Hendow, M. (2025, February). *Advances in border management: Digitalisation trends and emerging technologies* (Working paper). International Centre for Migration Policy Development. <https://research.icmpd.org/wp-content/uploads/2025/02/Advances-in-Border-Management-Digitilisation-trends-and-emerging-technologies.pdf>.
- Kim, S. (2023). «Illiberal democracy” after post-democracy: Revisiting the case of Hungary. *The Political Quarterly*, 94(3), 437–444. <https://doi.org/10.1111/1467-923X.13255>
- Lake, D. A. (2009). *Hierarchy in international relations*. Cornell University Press.
- Lottholz, P. (2022). Theorizing post-liberal forms of statebuilding and order-making globally. In P. Lottholz, *Post-liberal statebuilding in Central Asia* (pp. 27–50). Bristol University Press. <https://doi.org/10.51952/9781529220025.ch002>
- Marusiak, J. (2024). Russia's aggression against Ukraine and its impact on the energy cooperation of Visegrad Group countries. In *EU energy and climate policy after COVID-19 and the invasion of Ukraine* (pp. 95–118). Routledge. <https://doi.org/10.4324/9781032624839-8>
- McDonald, M. (2008). Securitization and the construction of security. *European Journal of International Relations*, 14(4), 563–587. <https://doi.org/10.1177/1354066108097553>
- Rankin, J. (2025, January 13). EU plans Ukraine fund without Hungary to bypass Orbán veto. *The Guardian*. <https://www.theguardian.com/world/2025/dec/19/ukraine-war-briefing-hungary-agrees-to-allow-eu-loan-to-kyiv-but-will-not-contribute>
- Schammann, H., Gluns, D., Heimann, C., Müller, S., Wittchen, T., Younso, C., & Ziegler, F. (2021). Defining and transforming local migration policies: A conceptual approach backed by evidence from Germany. *Journal of Ethnic and Migration Studies*, 47(13), 2897–2915. <https://doi.org/10.1080/1369183X.2021.1902792>
- Scharpf, F. W. (1999). *Governing in Europe: Effective and democratic?* Oxford University Press.
- Schimmelfennig, F. (2018). European integration (theory) in times of crisis: A comparison of the Euro and Schengen crises. *Journal of European Public Policy*, 25(7), 969–989. <https://doi.org/10.1080/13501763.2017.1421252>
- Scott, J. W. (2023). Hungary's illiberal border politics and the exploitation of social, spatial and temporal distinctions. *European Urban and Regional Studies*, 31(1), 14–28. <https://doi.org/10.1177/09697764231186741>
- Vidra, Z., & Messing, V. (2025). The representation of the arrival of Ukrainian refugees in the Hungarian media in 2022. *Central and Eastern European Migration Review*, 14(24), 1–20. <https://doi.org/10.54667/ceemr.2025.08>

- Guennoun, Y. (2025). Sovereignty through selective integration: Strategic non-compliance, compliance minimalism, and governance hardening in EU crisis politics. *Politics & Security*, 14(4), 16–30. <https://doi.org/10.54658/ps.28153324.2025.14.4.pp.16-30>
- Visegrád Group. (2021, July 9). *Joint statement of the Prime Ministers of the Visegrad Group*. <https://www.visegradgroup.eu/home/documents/2021/joint-statement-of-the-210713>
- Walt, S. M. (1987). *The origins of alliances*. Cornell University Press. <https://web.stanford.edu/class/ips198/docs/Walt.pdf>
- Waterbury, M. A. (2020). Populist nationalism and the challenges of divided nationhood: The politics of migration, mobility, and demography in post-2010 Hungary. *East European Politics and Societies*, 34(4), 962–983. <https://doi.org/10.1177/0888325419897772>

# RETROSPECTIVE ANALYSIS OF THE SITUATION IN SYRIA AND CONCEPTUAL THREATS TO BULGARIA'S NATIONAL SECURITY

Kostadin Kostov  
Academy of National and Information Security  
Plovdiv, Bulgaria  
<https://orcid.org/0009-0001-6206-2421>  
[kostov70@abv.bg](mailto:kostov70@abv.bg)

**Abstract** *The article represents a retrospective analysis of the military-political and geostrategic dynamics in Syria. The author seeks to identify the major driving forces influencing the development, the repercussions, and the outcome of the internal confrontations that have been ravaging the Syrian society throughout history. The article argues that, depending on the geopolitical and historical context, these forces would either instigate conflict, or be a converging factor around common national interest. Similarly, they would generate long-term tension and pave the way to foreign intervention, or instead, if steered in that direction, they would lead to temporary appeasement and reconciliation. Furthermore, the Salafi jihadist movements, their inception and activities are described as one of the recent driving forces shaping the current security environment in Syria. The article concludes with the affirmation that revealing the ex-post mechanism of the geopolitical factors is a way to forecast their future development, thus uncovering the emergence of potential threats to the national security of Bulgaria. Finally, the infiltration of foreign fighters, radicalization, and soft targets are highlighted as the gravest possible threats requiring a clear precautionary response.*

**Keywords** Salafi jihadist movements; Islamic State; National Security; Syria; Terrorism; Soft targets; Foreign fighters.

## 1. INTRODUCTION

Due to its geographical location, Bulgaria is in close proximity to the conflict zones in the Middle East, which are a source of challenges, risks and threats to security. Alongside our geopolitical position, our membership in the European Union and NATO, we are on the frontline of the geostrategic threats coming from the Middle East region. The high military-political dynamics in Syria is a catalyst that determines the increasing challenges facing Bulgaria's national security.

This article outlines four interrelated historical factors either defining the internal dynamics in Syria or representing the outside influence upon Syrian society. Although their overall impact is quite controversial, the internal driving forces contributed significantly to the process of national unification, whereas the foreign ones largely prevented the establishment of lasting stability within the country and across the region. They both manifest a pattern of action that is not limited in time and has the potential to be replicated in Syria and in other countries. Nevertheless, they continue to influence the security environment and the military-political situation in Syria nowadays.

Understanding these patterns of action by the Bulgarian government, especially by the intelligence and security services, is of great importance for the proper conduct of a proactive policy to prevent and counter potential threats.

- First, Syria's cultural-historical heritage is the driving force overcoming the strong socio-political divisions due to kinship and religion and merging the various tribes, clans, communities, and religious groups into a common national entity;

Kostov, K. (2025). Retrospective analysis of the situation in Syria and conceptual threats to Bulgaria's national security. *Politics & Security*, 14(4), 31–44. <https://doi.org/10.54658/ps.28153324.2025.14.4.pp.31-44>

- Second, the nation-building process established Syrian sovereignty, but simultaneously stirred to action a powerful factor – the government’s internal and foreign policies prompted by the interests of the ruling elite and provoking tensions both domestically and regionally;

- Third, the geopolitical interests of the world powers and the involvement of regional and neighbouring countries in Syria’s intrastate conflicts often had a negative impact upon local and regional security;

- Fourth, the Salafi jihadist movements represent a foreign interference as well, but their substantial impact deserves to be a separate element. They are a force of influence that emerged and gained momentum in the late 20th century.

This article explores the findings of various sources highlighting important aspects of the problem which the paper covers: Boas, M., Ben-Nun, G., Engel, U., & Osland, K. (Eds). (2025); Stankov, V. (2019); Veldkamp, J., Askar N, & Joubin, R. (2025), etc.

The article’s methodology includes both a comparative historical approach and geopolitical and strategic analysis. A very important point was to follow the chain of events without making judgments of right and wrong, totalitarianism and democracy, legitimate and illegitimate military action, etc. Detailed description of facts has been avoided due to the need to reveal the overall interrelation between events, trends, and processes.

The use of original documents allows for a full interdisciplinary study of the topic and contributes to modern situational awareness and threat assessment.

In assessing a source, their professional background was taken into account – historian, diplomat, political scientist, military, journalist, analyst, etc. Moreover, there was a need to ascertain whether the source tried to adapt the text to the viewpoint of an intended target audience. Therefore, the reliability of a source depended largely on the existence of corroborating independent sources, the lack of bias vis-à-vis the main argument in the original narrative, and the source’s correct use of references and quotations..

## 2. METHODOLOGICAL APPROACH AND SOURCE STRATEGY

This article explores the findings of various sources highlighting important aspects of the problem which the paper covers: Boas, M., Ben-Nun, G., Engel, U., & Osland, K. (Eds). (2025); Stankov, V. (2019); Veldkamp, J., Askar N, & Joubin, R. (2025), etc.

The article’s methodology includes both a comparative historical approach and geopolitical and strategic analysis. A very important point was to follow the chain of events without making judgments of right and wrong, totalitarianism and democracy, legitimate and illegitimate military action, etc. Detailed description of facts has been avoided due to the need to reveal the overall interrelation between events, trends, and processes.

The use of original documents allows for a full interdisciplinary study of the topic and contributes to modern situational awareness and threat assessment.

In assessing a source, their professional background was taken into account – historian, diplomat, political scientist, military, journalist, analyst, etc. Moreover, there was a need to ascertain whether the source tried to adapt the text to the viewpoint of an intended target audience. Therefore, the reliability of a source depended largely on the existence of corroborating independent sources, the lack of bias vis-à-vis the main argument in the original narrative, and the source’s correct use of references and quotations..

## 3. ANALYTICAL FINDINGS

### 3.1 A Historical and Geopolitical Overview

Historically, the political, military and social dynamics of the security environment in Syria is determined by important cultural aspects created by the Arab worldview. They are fundamental to how Syrians and other nations in the region perceive the world in the 21st century and realize their place in it. Their way of thinking, which shapes their concepts of government, religion, and state, differ from European concepts.

Their cultural and historical perceptions are defined by strong genealogical memory that amplifies collective attitudes towards socio-political events. Even though an event occurred centuries ago, its ensuing projection on public apprehensions is usually very strong and generates a powerful common sentiment.

To explain the complexity of the worldview of the Syrians, we have to remember that they perceive themselves as heirs to the great Akkadian Empire. Although the Assyrian nation emerged about 4,500 years ago, the people of the region nowadays, Christians and Muslims alike, see themselves as Assyrians, heirs to the empire. Genetically or genealogically, the present population is hardly related to that of 4,500 years ago, but in terms of social psychology the relation remains as an important part of their identity. Politically, Syria today occupies a small part of the ancient Assyrian territories, comprising the present-day Iraq, Syria, Iran, Turkey and Lebanon, which are regarded successors to the Assyrian legacy as well. Geopolitically, this fosters competition more than a sense of unity, as different players are striving to restore the ancient glory.

The Middle East has been an arena of confrontation not only today and during the Cold War, but for centuries before that. After the collapse of the great empires in the Middle East at the end of the first millennium, the region came under Mongol and then Ottoman rule. After a number of crusades in the Middle Ages, the population was depleted, and the most prominent families were gradually weakened over the centuries. Historically, the crusaders' brief sojourn in the region was a fleeting moment, but culturally it left a significant negative imprint on the East-West and Arab-European perceptions.

The cultural-historical heritage brings about a sense of belonging to a common legacy waiting to be restored to its former glory. This notion often mitigates domestic discord, transcends local animosities, rallies the people behind a national idea, and fuels the resistance to outside forces.

For instance, World War I was a period of inter-communal and inter-religious unity for Syria, as the population, led by the local clergy, Muslim and Christian alike, actively fought on the side of Britain and France. The famous Lawrence of Arabia's political-military mission, as well as the promises of a bright future, gave impetus to the Arab cause, but after the war the victors, France and Britain, actually divided the Middle East between themselves.

At the official conference in Paris in 1919, the region sent three delegations to demand the fulfillment of the promises. The Persian delegation had been forced by Britain to leave Paris; the Iraqi delegation was allowed to participate assuming it would visit London first, where it was detained until the signing of the Versailles Treaty. The third delegation arrived unhindered from the United States, as the delegates were US citizens representing the Assyrian people.

In his petition to the conference, the Rev. Joel Verda concluded: We have clear evidence that the Assyrians were incited by the officials of Great Britain, France and Russia to enter the war on the side of the Allies and encouraged to remain in a state of war by the most solemn promises of the establishment of a sovereign state. The Assyrians, who risked the very existence of their nation for this reason and made appalling sacrifices on the altar of freedom, want the promises made by the allied governments to be fulfilled". (Bover, 1938) The geopolitical powers did not keep their promises. It pays tribute to the representative of the British military intelligence, Lt Col Thomas Edward Lawrence (Lawrence of Arabia) that he remained at the Paris Conference and ardently defended the promises made by the Allies to the Arabs.

All the decisions of Versailles were confirmed by the League of Nations on August 5, 1920. The mandated territories were allocated to the great powers at the San Remo Conference on May 16, 1920, where Great Britain got a mandate over Mesopotamia (Iraq) and Pakistan; and France got a mandate over Syria.

Afterwards the Assyrian people put up a strong resistance against the English and French occupiers. In Syria, from 1920 to 1925, the French army lost 6,040 men. For the second half of 1925, during the second Syrian uprising, the French suffered 11,000 casualties (Provence, 2005). Resistance to the occupation continued with occasional guerrilla campaigns.

In Syria, following the elections on March 1943, the government of Shukri al-Quwatli's National Patriotic Union with Saadallah al-Jibiri as Prime Minister came to power. The Syrian parliament rejected

the articles of the constitution that referred to the French mandate. In July 1944 the then Soviet Union and the United States formally established diplomatic relations with Syria and Lebanon. In accordance with the agreements between Stalin, Roosevelt and Churchill for membership in the United Nations, Syria and Lebanon declared war on Nazi Germany on February 27, 1945.

Nevertheless, France did not recognize the sovereignty of Syria and Lebanon and occupied Beirut with three infantry battalions, which were later reinforced by a contingent of 1,500 men. The intense fighting for Damascus and the fierce bombardment of Syrian cities created a situation so appalling that British, Soviet and American diplomats strongly condemned the French atrocities. Diplomatic pressure from the entire Arab world escalated. The Iraqi government was ready to provide military aid to Syria. Eventually, the French government withdrew and, represented by general Charles de Gaulle, handed over the command of the "Syrian Special Forces" to the Syrian government. This act gave real control over the army to the Syrians themselves.

Something very rare happened in the international political arena at that time. The great powers, their leaders Stalin and Truman in particular, agreed not to allow any political and economic advantages to be gained by any foreign country in the Middle East. Benefits could only be granted by the people of the Middle Eastern countries. To Syria and France, it meant that Truman would not stand in the way of giving Syrians special rights, provided the Syrian people granted them voluntarily (U.S. Department of State, 1960). Syria and Lebanon were eventually admitted to the United Nations on July 26, 1945.

This unifying episode of Syrian history had a profound influence upon Syrian patriotism and nationalism. It demonstrated that belonging to a common idea could erase all dividing lines. However, the pursuit of independence was not enough to preserve the national unity once the main objective had been achieved.

The nation-building process, leading to the inclusion of all communities into a unitary nation state, began when the young Syrian state was caught in the maelstrom of international events. After a long series of uprisings and struggles, it seemed that the people of Syria would finally enjoy their freedom in peace. However, the new state faced a lot of challenges, because the Syrian people, despite their deep history and culture, were once again deprived of the opportunity to determine their own destiny. The main traits of the political-military situation after 1945 were as follows:

- The state borders of Syria and other countries in the region were artificially drawn without any regard to the realities on the ground. This represented a constant source of inter-ethnic, inter-national, and religious tensions. Syria, same as many countries in the region, had problems with all its neighbours.
- The Syrian nationalists condemned European politics and its duplicity and wanted the Arab peoples to have self-rule and independence.
- The newly introduced parliamentary governance was not fully compatible with the indigenous political tradition of rule by sheikhs in tents and sheikhs in cities, under the leadership of the most powerful one.

Suddenly it was clear that true independence was decades away. The nation-building had to proceed in a security environment ripe with disputes and potential military conflicts. This is an important reason why the concept of governance in Syria is far from the contemporary Western understanding of politics. There's parliamentary democracy, there's elections, but political affiliations are based on previous divisions. This is a prerequisite for enduring conflicts, coups, political assassinations, and an unstable political environment.

The period from 1945 to 1954 witnessed five military coups in Syria. Military governments were backed by the West. After the parliamentary elections in 1954, patriotic elements opposed to Syria's involvement in international military alliances came to the fore. The national economy and industry, along with the territory, became a new reason for unity, as the people had to defend them throughout the enlarging disputes over oil deposits and other natural resources. The competition for water, the region's most precious resource, gained strong momentum. Keeping the flow of the rivers constant and building dams on their own territory became a matter of vital strategic importance to a number of countries in the region. Nobody wanted its upstream neighbours to build dams and use the water for themselves. This issue continues to periodically escalate between Turkey, Syria, and Iraq. The old tribal saying, that the one who inherits the water is the most influential, manifests itself in national politics. In fact, defending these

strategic interests represents another opportunity to strengthen the state and its institutions. However, this should be a national effort involving the people and the government.

There is hardly a period of a stable political system throughout Syrian history. The typical governance model had become an outer shell of the old partitions, affiliations and coalitions.

In 2025, Boas, Ben-Nun, Engel & Osland (Eds.) found the following:

Many of the military officers who seized power in 1963 in the name of the Baath Party belonged to religious minorities. Hafez al-Assad, who eventually took over and became president in 1970, was an Alawite. Despite the fact that the Assad regime proclaimed adherence to Arab nationalist ideals, sectarianism quickly became a central tool of governance. Seeking people he could trust, Assad appointed Alawites to the most sensitive positions within the coercive apparatus of the state. By doing this, he would create an organic bond between his regime and the Alawite community he belonged to. (p.156)

Syria's turbulent political history had been replaced by a period of relative calm and ostensible stability, not because of a deep understanding of the new political system, or empowerment of the right individuals and groups, but because of the establishment of a one-party political system based on power. The ruling Ba'ath Party through the government power structures controlled all aspects of public life, including civil society, political activities, economy, religion, culture, etc. However, the ruling elite failed to address any of the internal divisions:

- The social divide along ethnic, tribal, community, sectarian and religious lines.
- The economic divide was widening, with the state exploiting natural resources and local communities remaining poor. The new socio-economic environment deepened the existing class antagonism.
- The population of entire regions was deeply divided into urban and rural.

Thus, the strife for national independence slowly degraded into a local pseudo-chauvinism. Moreover, the involvement of foreign geopolitical interests, that is the world powers, the regional and neighbouring countries, only aggravated the internal confrontations. The ruling elite's inability to resolve the issues and ease the rising tensions brought about a powerful destructive force – the Jihadist movement, which had the ambition to provide an enduring solution to all the problems in the country.

The geopolitical interests of world and regional powers were manifested along two major lines of interference, the first one affecting the core social entities (tribal and religious groups, communities, families), and the second one targeting the government and the concept of national unity.

Retrospectively, the influence over the core social structures is a lasting social and political phenomenon leaving its mark on Syrian society even today, although the means and the scope might differ throughout history. The impact mechanism can be explained with an example about the invasive geopolitical interferences in the internal political and religious confrontations in Syria.

In the second half of the 19th century a bloody conflict broke out between the Druze and the Maronite communities. The clashes started with hostilities between villages and random assaults by outlaws. The Syrian territory was then part of the Ottoman Empire, but the local Ottoman-Syrian authorities took no action, in many cases siding with the Druze Muslims. It is noteworthy that regional administrations were totally dependent on the policies of the Sublime Porte (the Ottoman central government), but were at the same time largely self-governed and had full discretion over matters of local security. For this reason, along with bureaucratic tardiness and corruption, initially there was no significant response from the authorities.

Later on, as the conflict persisted, Mehmed Fuad Pasha, a prominent Ottoman statesman and diplomat, twice appointed Prime Minister and Foreign Minister by Sultan Abdulaziz, was sent to the conflict-stricken territories of Syria and Lebanon on a mission to pacify the Druzes and punish those guilty for the bloodshed. He soon identified the conservative Muslims, opposed to any and all reforms, as the root cause of the conflict, and undertook firm measures to resolve it. Ahmed Pasha, governor of Beirut, along with a hundred military personnel and 67 members of the highest-ranking Muslim families in the region, were sentenced to death and executed. This looked like an opportunity for a lasting solution to the conflict between Druzes and Maronites, until a powerful geopolitical factor came into play.

In an attempt to gain strategic advantage, Napoleon III of France ordered the invasion of Syrian and Lebanese territories under the pretext of defending the rights of Catholics in the Ottoman Empire. The Ottoman-French Treaty of 1740, which renewed and expanded the Ottoman capitulations before the European powers, entitled the French Monarch as Protector of Catholics in the Ottoman Asian territories, thus marking the apogee of French influence in the Ottoman Empire.

Public opinion was orchestrated by European media prior to the military offensive. The primary objective of the campaign was presented as «The separation of Egypt and Syria from the Ottoman Empire and the establishment of peace and quiet in the East under the auspice of France» (Farah, 2000) French troops invaded the present-day territories of Syria and Lebanon, even before the start of diplomatic talks with the Ottoman Empire. In August 1860 a French expeditionary corps of 6 000 troops made a landing operation in Beirut, under the command of General Beaufort d'Hautpoul.

On the global geopolitical scene this was viewed as severe violation of the established political and diplomatic order. Opponents to the French intervention were the British Empire, Austria and Prussia, while Russia remained neutral due to its recent loss in the Crimean war of 1853-1856. At the conference held in Paris in August 1860 France tried to delay the decision-making against it, because the French expeditionary corps had quickly overcome the resistance of the Druzes and had penetrated deeply into Syria and Lebanon. None of the Great powers consented and the French troops withdrew in April 1861. Although this French «humanitarian» adventure did not entail any positive territorial developments for France, it did trigger huge impact on the future strategic plans for the following reasons:

- The French already viewed Maronites as part of the Catholic world and hoped to make their lands a French protectorate;
- Intense propaganda of Catholic missionaries was launched among Maronites in view of their close relations with France and for the purpose of promoting pro-French attitudes;
- The French demonstrated distrust and animosity towards Druzes and the other Muslims;
- The French policy in that part of the Ottoman Empire instigated religious division and alienation among communities.

Those events, alongside with the Ottoman style of governance that tolerated autonomous local authorities, as the Empire only coordinated policies and collected taxes, actually intensified territorial and religious controversies. This past situation is quite similar to the present-day dynamics in Syria and reveals how disputes between two neighbouring villages escalate into an armed conflict, how an argument may grow further to include entire clans and community groups, how the Great powers can benefit from a local dispute to achieve their strategic goals, and finally, how a disagreement can evolve into a lasting feud. This example demonstrates the way a foreign power's interference aggravates native community controversies based on clan, tribe, sect, religion, etc.

Foreign influence over government policies started as early as the beginning of Syrian independence, when the young country found itself in the turmoil of large-scale geopolitical events. On 13 December 1945 France and Great Britain signed a treaty for common action in the Middle East (Louis, 1984). The Arab countries realized the need of unity and established the League of Arab States. (El-Salamoni, 2003, p.53) This was an extraordinary progress in the understanding and awareness of the Arabs about the new geopolitical situation in the world. On the global geopolitical scene, however, the Cold War brought about the two global powers – the US and the Soviet Union.

The US Central Intelligence Agency could very well perceive the trends in the Middle East, understanding that Great Britain and France were losing their capacity to intervene, as the attitudes of the bigger part of the Arab population was against them. Therefore, due to the bloc controversies, the USA were compelled to follow a nontypical geopolitical strategy to protect their interests. (CIA Reading room, 1966) This changed substantially the American foreign policy and the attitudes of the Arabs towards the USA.

The Soviet Union also played a part in the events in Syria. Soviet intelligence managed to quite adequately assess the political trends and reorient its priorities. Previous Soviet connections in the region are being quite adequately utilized by Russia even today. This is not surprising, as the intelligence mechanism was among the most powerful weapons of the former USSR. (CIA Reading room, 1948) Nowadays, the Russian intelligence capabilities to influence internal events through supporting some

groups, attacking others and collaborate with the government in office has the potential to significantly change the state of affairs in Syria.

The reason why the former USSR had enormous influence was the support the West provided to Syria's local opponents, and not because the Syrian people had anti-western attitude. Syria received considerable military aid from the Soviet Union to fight the wars with Israel, and part of it was redistributed to other Arab countries. This indicates the strategic adaptability of the Soviets, given that the military and economic aid enhanced substantially their influence in the region. (CIA Reading room, 1967) However, it did not help the conflicts to fade away either, since the parties involved could not be exhausted and therefore were not prone to peace initiatives.

Relations with other Islamic countries have their own particular meaning as well. Thus, for example, after the regime of the Ayatollahs came into power, the influence of Iran in Syria started growing. Their relations began strengthening as early as in 1980, when Syria supported Iran in the war with Iraq. (Stankov, 2019, p.33) This fact also explains the support for Assad's regime by Iranian military advisors, troops and the help of Hezbollah.

When looking at a larger timeframe, the geostrategic aspects of the controversies during the Cold War seem to represent a mere historic projection of the well-known and never-ending strategic factors, points of conflict, and political and cultural circumstances. However, the vigorous technological and social developments of the 21st century brought about a new phenomenon – the adaptive evolvement of the Salafist movement, which transformed these regional disputes into a global issue.

The Salafi jihadist movements are the most recent and most important factor that changed the security environment and had a profound impact upon the military-political landscape. We need to look deep into Arab history to trace the roots of religious fanaticism. The numerous conflicts and wars gradually turned Arabia from a realm of culture, science and freedom, to a dominion of feud and controversy, and eventually to a place of radical ideologies. We have to bear in mind that Islam is not a belligerent religion per se, but the radicals are inclined towards controversial interpretations of the Islamic religious sources in order to promote their political agenda.

Therefore, the Salafi jihadist ideology needs a careful analysis from a political and strategic perspective. When reviewing the present structure of Islamic State, we have to look at Al-Qaeda as the organizational ascendent, which gradually evolved from a paramilitary unit to a terrorist group motivated by religion. The suitable conditions for the emergence of a jihadist organization were already present:

- the social and political tensions were combined with religious hostilities, which added fuel to the existing confrontations between religious communities;
- the central government, despite being weak, applied a policy of violence and suppression.

To present an alternative, the Salafi jihadist doctrine easily denounced the current socio-political order as non-Islamic and proclaimed the anti-government armed struggle to be a sacred obligation to all true Muslims. Thus, all supporters of the existing order became enemies that should be destroyed.

Boas et al. (2025) found jihadism to be the conviction that armed confrontation with political rivals is a theologically legitimate and instrumentally effective method for socio-political change, whereas Salafism is described as the idea that believers should exclusively and strictly abide by the example of Salafis (the early generations of Muslims), by renouncing all other sources of influence.

The doctrine of jihadism started to gradually evolve after the establishment of Al-Qaeda in the Peshawar Mountains by Osama bin Laden in 1988. Al-Qaeda is a mobile group applying the principle of clandestine cells. Its objective is to launch terrorist attacks against its adversary. It is controversial whether Al-Qaeda went through a process of deliberate change in ideology, since it was leader-oriented and divided into battle groups. Every separate warlord was also an ideologist, who would contribute to the doctrine according to his own judgement. However, Abu Musab Al-Suri is considered to be an important theoretician, whose major achievement is the transformation of the ideology of struggle. He wanted to «encourage young Muslim immigrants to wage a war in Europe to trigger Islamophobic response, which, in turn, would urge European Muslims to join jihadist groups». In January 2005 Al-Suri uploaded his book entitled «A Call to Global Islamic Resistance», describing Europe as the target of a widespread jihad, whose troops would be recruited out of the 45 million Muslims living in Europe. (European Parliament, 2017).

The political and security environment in Syria and Iraq was suitable for the emergence of a radical group. The beginning was set in Iraq, where the central government and the local power structures were unable to oppose a new powerful player.

Further research (EP, 2017) found out that:

«The Islamic State project has as its ultimate goal the establishment of a caliphate where Muslims from all over the world could settle in. It aims to establish the caliphate on a territory, wherefrom an international jihad war could be waged. Thus, this project differs from the one of Al-Qaeda and was carried out for the first time in Iraq due to the deep destabilization of the country. Islamic State continued with its expansion in Syria because of Bashar al-Assad's lack of control over the entire territory, and established its «capital» in the city of Raqqa. »

Jihadism in Syria was indeed a rare phenomenon up until 2003, when Assad's regime permitted jihadists to travel through the country to join the fight in Iraq. (Boas et al., 2025, p.155). This triggered a gradual rise of Jihadism and eventually led to the birth of Islamic State in Syria. Unfortunately, the wind of change in the Islamic world enflamed the jihadist fire in Iraq and Syria. A number of sources indicate that the onset of the people's rebellion of 2011 in Syria was inspired by the «Arab Spring» (Stankov, 2019) and the events in Tunisia and Egypt. When the Syrian revolution started in 2011, its slogans echoed those of the Arab Spring in Egypt and Tunisia. Protesters called out that all the people wanted to overthrow the regime. However, this assumption carried with it a form of counter-oppression, as there were certain segments of the Syrian, Egyptian or Tunisian population that were simply not willing to revolt against the rule of Assad, Mubarak, or Ben Ali, respectively. (Veldkamp, Askar & Joubin, 2025, p.58)

Many of the original «revolutionaries» later turned into radical jihadists, thus enabling Al-Qaeda to infiltrate local structures and stir conflicts. The Syrian regime had released from prison some of the most prominent jihadist leaders, detained in the last ten years. Defectors from the Armed forces, predominantly Sunnis, formed the Free Syrian Army. Islamic separatist groups began to appear, some led by jihadist warlords released from prison. Members of Al-Qaeda in Iraq, later to be named ISIS, created Jabhat al-Nusra in 2012. A year later it fragmented itself into ISIS and Jabhat al-Nusra (Boas et al., 2025).

As the conflict in Syria gained momentum, ethnic separatist movements began emerging, the Kurdish and the Druze being the most prominent. The Kurds managed to create a formidable military force in the Kurdish areas, referred to as Rojava. Presently the local communities are divided because of the erosion of the traditional power structure. Tribal leaders do not represent authority, neither among the rebels, nor among the government forces. They keep a strange neutrality, by merely being absent from public life. (Boas et al., 2025) This fact shatters the strongly traditional communal and tribal unity.

The economic power base of ISIS in Syria was quite robust. The jihadists adopted laws, collected taxes, had judicial and penal systems, sold natural resources, antiquities and regulated the water supplies. They also had their own currency, the gold dinar. Thus, they became the richest terrorist group in the world. (EP, 2017) Islamic State controlled 60% of oil production in Syria and 10% of that in Iraq. In mid-November 2015 news media reported the extraction of 35 000 up to 40 000 barrels a day. Jihadists in Syria controlled 253 oil boreholes, 161 of them active. During its largest expansion Islamic State levied taxes on the economic activity of over 8 million people. The total budget of ISIS was estimated as more than USD 2 billion per annum. (EP, 2017)

After 2010 the already expanded Islamic State was already a real threat to all Arab regimes. The earlier review of its religious and political ideology shows that all other forms of political power in and outside the country were its opponents. For that reason, the Middle East countries took decisive action to stop, contain, and reduce its funding. (Ardemagni, 2016). Nevertheless, grey zones continued to exist, such as the «Hawala» money transfer system. The jihadists adapted and intensely utilized both old and new ways of raising and transferring funds.

The combination of military and economic strength enabled the Islamic State to rise up to a new geostrategic level. Foreign terrorist fighters, apart from manpower, were also a source of income. They would use their contacts in Europe to send money to the organization through European bank accounts. Supporters controlled those bank accounts outside the conflict zones to withdraw money and send it to the jihadist warlords. (EP, 2017) Foreign fighters were able to coordinate donations through encrypted mobile apps, send funds as virtual assets or, if collected in cash, send them via couriers.

The foreign ISIS fighters in Syria comprised ex-military, not just ordinary soldiers, but also highly qualified officers from Saddam Hussein's Iraqi forces, as well as young people recruited through large-scale propaganda. The tactical capacity of jihadist forces was enhanced with the influx of people from the Iraqi intelligence and the Ba'ath party. This provided high-level strategic, institutional and political experience.

In 2014 jihadists in Syria considerably upgraded the methods of recruiting troops. The growth in the number of fighters coming from all over the world was unprecedented. According to the US intelligence agencies for the year 2014 they numbered 20 000, among them Europeans and Americans. Intelligence agencies found it rather difficult to track them down. (CIA Reading room, 2018) Subsequent UN reports already contain more accurate figures, owing to the joint work of security services of the numerous member states. Over the period from 2014 until 2016 the influx of foreign terrorist fighters to Iraq and the Syrian Arab Republic reached unprecedented levels. By 2017 assessments indicate that more than 42 000 people from over 120 countries had travelled to join terrorist organizations.

Foreign fighters included mercenaries (military professionals) and religious extremists, followers of the Salafi and jihadist ideology, promoted by ISIS.

After the defeat of ISIS, foreign fighters were scattered in several directions. Some went to camps in Syria and Iraq, others returned to their countries of origin, or continued to fight and were killed in action. Nevertheless, after 2018 there was a huge discrepancy between the total number of foreign fighters and the number of those registered as killed, detained, returned or relocated.

The return of foreign fighters to their home countries poses a real problem for Europe and the US. For example, the US intelligence fears that some of the foreign fighters would return to their homes in Europe and in the USA to perform terrorist attacks. Francis Taylor, Under Secretary of Homeland Security for Intelligence and Analysis, voiced concerns that Americans, affiliated to extremist groups in Syria, could be trained in combat techniques and could eventually be persuaded to perform organized or «lone-wolf» attacks against the USA and the Western world". (Govinfo, 2015)

### 3.2 The Present Political and Security Dynamics in Syria

Syria today has its savior, that is the rebel leader Mohammad Al-Julani (Ahmed al-Sharaa). On 8 December 2024 Bashar Assad's regime was overthrown by the military union of Hay'at Tahrir al-Sham (HTS), where the leading force was Jabhat al-Nusra. HTS and al-Sharaa put an end to Assad family rule that lasted more than 50 years. In the 14-year armed conflict at least 500 000 had been killed, and over 13 million had been displaced.

Jabhat al-Nusra itself emerged as the Syrian branch of Al-Qaeda and ISIS, but was later separated after clashes with ISIS over the natural resources in the eastern part of Deir Ez-Zor Governorate. Following the creation of HTS in 2017, Al-Julani started to gradually transform Al-Nusra according to his ambition to turn HTS into a legitimate political player. He proceeded to eliminate the extremist groups that protested against the moderate approach towards other groups and the international organizations. According to (Keilberth, 2024), the Syrian wing of Islamic State referred to him as an infidel and an enemy.

After the victory at the end of 2024 al-Julani instructed his fighters not to shoot at anybody who puts his weapons down, nor chase anyone who is running. He promised Kurds and Christians the same rights as those of Sunni Syrians. After Aleppo was conquered Al-Sharaa appealed to civil servants loyal to the regime to return to work. There are experts who regard the transformation of the rebel leader as a unique opportunity for the country, torn by civil war. From an extremist, who banned music and all Western values, he turned into a person, who advocated conciliation with the enemy. Although many Syrians have doubts, Ahmed al-Sharaa represents an opportunity to avoid a new wave of violence. » (Keilberth, 2024). However, researchers (Veldkamp et al., 2025) indicate an important detail of the present situation in the following way: «Most of the fighters, marching towards Damascus, were aged between fifteen and twenty-five. These «children of the revolution» were brought up in classrooms, where Quran contests, Sharia lessons and charity campaigns replaced the Ba'athist secular practices. »

The Kurdish issue in Syria is one of the most pressing and sensitive issues in the region. Kurdish forces played an important role in the combat against Islamic State and Assad's regime. However, Kurds

are not politically united, they have common goals and self-awareness, but also intra-tribal and clan-based divisions. Thus, for example, the Autonomous administration and the Syrian Democratic Forces (SDF) in Northeast Syria (Rojava) face internal divisions, as Kurdish fractions do not share a common political vision. They are supported by the USA, but at the same are attacked by Turkey, which aims to suppress Kurdish separatism.

Presently, the people in Syria are still divided into clans, tribes, communities and sects. There is a new line of division, caused by the newly enriched tribal members, who challenge the authority of the old-time leaders. The recent large-scale conflicts at all levels indicate no improvement in tribal relations, as compared to the situation in 1860.

The new central government, and Ahmed al-Sharaa in particular, seem to display willingness to put the country in order. There are, however, series of questions as to how the new Syria should look like. What kind of autonomy should be granted to each group? How is the government going to take control over the natural resources? Regardless of the types of political moves Al-Sharaa would initiate, armed clashes between individual groups are likely to occur. All groups have weapons and trained military units. Currently, it is hard to envision an easy and peaceful settlement of all the unresolved issues in the country.

The geopolitical factor remains an important driving force, as the internal developments in Syria continue to be a part of the regional dynamics. Regional forces, such as Turkey, Iran and Israel play a substantial role, each of them defending its own interests. (Stankov, 2019). The Gulf countries are apprehensive of the Syrian situation and refrain from initiating decisive steps towards renewal of political cooperation. Western forces, mostly the US and France, remain committed to stabilize the regions under Kurdish control and curb Iranian influence. (Jamous & Haenni, 2025)

The geostrategic importance of Syria spreads out to powers such as Russia, China and India, each of those having differing interests. Russia needs its military bases in Syria, as they are an essential part of the Russian strategy about Africa and the Middle East. China and India have long-term economic interests. Syria is involved in many important trade corridors, which also pose routes for influence. (Stankov, 2019).

The terrorist threat is evolving and the Salafi jihadists are adjusting their modus operandi to the changes in the security environment. Victories over these groups are short-lived, and the extermination of the next warlord in a row is not an adequate solution. Financial flows are being decentralized. Small financial cells are being created within the individual terrorist groups. Crypto currencies are being widely used, such as Monero, KuCoin, MEXC, Huobi and Totalcoin. (United nations [UN], 2025a)

Jihadists gradually add substance to their main idea for transferring their fight into the Western world. The jihadi propaganda intensifies in the social media, as the Islamic State uses artificial intelligence to promote its cause among a broad audience. (UN, 2025b) Upon the return of foreign fighters, new threats to Western societies emerge. Jihadists start financing themselves through crowdfunding.

#### 4. DISCUSSION: TRANSNATIONAL THREAT PATHWAYS AND INTERPRETIVE LIMITS

After this retrospection of the major problems and challenges Syria faces today, we can conclude that a significant improvement or an appeasement of the situation are unlikely to happen in the near future, because the old rivalries, feuds, and disputes are far from being reconciled. The Syrian conflict is indeed a reflection of lasting controversies; however, it also poses an opportunity for reconstituting the state in a way that embraces its diversity. To build a common future, the new Syria should establish a political system based on citizenship, equality and inclusiveness. This requires true political will, strong international cooperation and long-term stability.

The transnational security threats emanating from the situation in the Middle East are, in all probability, closely monitored by the security services in Europe and elsewhere. They deserve a detailed academic scrutiny as well, because their present repercussions can be identified through a retrospective analysis of the recurring patterns manifested throughout history. The political and strategic dynamics in Syria represents a threat to the national security of Bulgaria along several lines.

First, the foreign «migrant” terrorist fighters passing through Bulgarian territory on their way to their countries of origin are a tangible potential threat. It is noteworthy that our security structures apply

adequate policies for preventing the entry of such persons. (Yanev, 2023) However, after the defeats the Islamic State suffered in Syria, the group has further enhanced its ability to adapt. Now individual jihadist groups exchange experience and are aware of our domestic and border security systems. Presently, Islamic State tasks well-prepared foreign terrorist fighters by assigning them the role of scouts to pave the way to future infiltrations. They have established illegal passage channels, proven over time, and connections with organized crime. They have recruited experienced professionals from the Syrian intelligence services, who undoubtedly contribute with new approaches. One of those approaches is the frequent use of females as couriers. (UN, 2025a)

The new jihadist strategy provides funding to a foreign fighter when they need legal assistance or a business startup. Thus, a jihadist may come to Bulgaria from another European country not to necessarily perform acts of terrorism, but to recruit supporters and build a network. He might be mapping out vulnerable targets and planning future attacks. Foreign terrorist fighters are presently among the biggest threats. (UN, 2025a)

Syria was a universal consumer of mercenaries, but could become a worldwide donor of such, should the situation calm down. These might be well-trained, small combat units that have gone out «on the market». Most probably, they wouldn't be pro-European minded, which would make them easier to be employed by anti-Western jihadists.

Second, the possible radicalization of European Muslims is another security risk that needs to be monitored closely. Following the victory over the Islamic State and the loss of their core territory, Salafi jihadists had come even closer to reaching their main goal – the radicalization of Western Muslims. The jihadists always had a good propaganda system, but now the circumstances have motivated them to further upgrade and develop it. (UN, 2025c)

The traditional radicalization, through Salafi sermons among the population or in the mosques continues, however it is no longer the main one, because of being too conspicuous. Sermons are performed on the Internet and the social media by various pseudo-social and non-governmental organizations. We have to bear in mind that the Internet is another jihadi battlefield.

Radicalization is a slow and surreptitious process. The analysis of the countermeasures undertaken in Kosovo, Bosnia, and Serbia (Boas et al., 2025) clearly indicates the need of coherent long-term policies involving all government and civil society structures.

Third, the vulnerability of the «soft» targets needs to be addressed within the overall national anti-terrorism effort, as they are likely to be the primary objectives of the jihadists. The potential soft targets are easily accessible public places (events), which would provide an opportunity for casualties and broad publicity, e.g. sports events, schools, marketplaces, etc. In July 2024 the French security services arrested an 18-year-old man who had planned to perform a terrorist attack at a soccer match in Saint-Étienne during the Olympic Games and had been related to a member of ISIS belonging to a group active in the Syrian region of Badia». (UN, 2025c) Besides, Islamic State has been increasingly using small remotely controlled aerial vehicles (drones), which are freely available. Al Qaeda and ISIS share their experience with other jihadist organizations to enable the global use of remotely controlled aerial vehicles (UN, 2025a).

Fourth, the society relies and depends solely on the government to protect the soft targets. This is because the government neither promotes, nor sufficiently integrates the civil society in the anti-terrorist effort. The resource-oriented strategy should evolve into a target-oriented one. (Slatinski, n.d.) A government will never have all the resources needed to protect soft targets. What is necessary is to adapt and apply the measures, identified by the UN Counter-Terrorism Committee Executive Directorate (CTED):

- enhance risk assessment and information sharing;
- apply comprehensive solutions, involving civil society, the local leadership (incl. religious leaders), and the private sector;
- develop public-private partnerships, given that many «soft» targets are privately owned and managed;
- combine physical security with public resilience against terrorist attacks and threats. (UN, 2021).

## 5. CONCLUSION

Bulgaria and our allies have to continue monitoring the internal confrontations in Syria, the policies of the new government vis-à-vis the need for a broad national reconciliation, and the Salafi jihadists, who are still there, adapting and regrouping.

To that end, Bulgaria needs to develop further its intelligence analysis capabilities, strengthen the cooperation between the law enforcement institutions, prepare for close collaboration between security services and key business sectors and companies, enhance ties with civil organizations and structures from Syria, the Middle East, and their branches in Europe.

Furthermore, Bulgaria's national security demands proactive monitoring of trends in the policy and the geostrategic aspirations of the countries that have vested interests in Syria, that is the regional countries and the global powers, which are going to protect them by either cooperating in the commercial, economic, cultural, and defense areas, or interfering directly in Syria's domestic affairs.

Ultimately, Bulgaria holds good positions in its attitude towards Syria and the Arab states. There is a good basis for a proactive approach, including the restoration of cultural, educational, and scientific exchanges with Syria and the Middle East.

## REFERENCES

- Ardemagni, E. (2016). The Gulf monarchies' complex fight against Daesh. *NATO Review*. Retrieved from <http://www.nato.int/docu/Review/2016/Also-in-2016/geopolitics-gulf-monarchies-fight-against-daesh/EN/index.htm>.
- Asenov, A. (2025). Intelligence And Counterintelligence Challenges Among Ethnic And Religious Communities In Bulgaria. Proceedings with reports. Higher School of Security and Economics. Retrieved from: [https://www.vusi.bg/wp-content/uploads/2025/06/Конф-Бълг-разузнаване-и-контраразузнаване\\_site-1.pdf](https://www.vusi.bg/wp-content/uploads/2025/06/Конф-Бълг-разузнаване-и-контраразузнаване_site-1.pdf)
- Boas, M., Ben-Nun, G., Engel, U., & Osland, K. (Eds). (2025). *Resisting Radicalization: Exploring the Nonoccurrence of Violent Extremism*. United States of America: Lynne Rienner Publishers. Retrieved from: <https://www.rienner.com/data/fe/file/9781962551557.pdf>
- Bover, M. (1938). *Vom Minarett zum Bohrturm—eine politische Biographie*. Zürich - Leipzig - Berlin, Atlantis Verlag, 1938
- CIA Reading room (1948). The Strategic Value to the USSR of the Conquest of Western Europe and the Near East. Retrieved from: <https://www.cia.gov/readingroom/document/0000258364>
- CIA Reading room (1966). The Eastern Arab World. National Intelligence Estimate 36-66. Retrieved from: [https://www.cia.gov/readingroom/docs/DOC\\_0000949193.pdf](https://www.cia.gov/readingroom/docs/DOC_0000949193.pdf)
- CIA Reading room (1967). Probable Soviet Objectives in Rearming Arab States. Special National Intelligence Estimate 11-13-67. Retrieved from: [https://www.cia.gov/readingroom/docs/DOC\\_0000272969.pdf](https://www.cia.gov/readingroom/docs/DOC_0000272969.pdf)
- CIA Reading room (2018). AP: 20,000 Foreign Fighters Flock to Syria, Iraq. Retrieved from: <https://www.cia.gov/readingroom/document/06708883>
- El-Salamoni, K. (2003). *Die Liga der Arabischen Staaten und die Vereinten Nationen: Das Verhältnis zwischen regionaler und universeller Organisation nach Kapitel VIII der Satzung der Vereinten Nationen* (Doctoral Dissertation). University of Heidelberg. Retrieved from: <https://d-nb.info/970348894/34>

- European Parliament (2017). The financing of the 'Islamic State' in Iraq and Syria (ISIS). Directorate-General for External Policies. doi:10.2861/193643
- Farah, C. E. (2000). *The politics of interventionism in Ottoman Lebanon, 1830-1861*. I.B. Tauris, 832 p.
- Govinfo (2015). Countering Violent Islamist Extremism: The Urgent Threat of Foreign Fighters and Home-Grown Terror. Hearing before the Committee on Homeland Security. House of Representatives. Retrieved from: [https://www.dni.gov/files/NCTC/documents/news\\_documents/Countering\\_Violent\\_Islamist\\_Extremism.pdf](https://www.dni.gov/files/NCTC/documents/news_documents/Countering_Violent_Islamist_Extremism.pdf)
- Jamous, B., & Haenni, P. (2025, February 9). The future of Syria, from the opposition's perspective. Middle East Research Institute. <https://www.meri-k.org/publication/the-future-of-syria-from-the-oppositions-perspective/>
- Keilberth, M. (2024). Syriens Rebellenchef Mohamed al-Jolani In Syrien euphorisch als Befreier gefeiert. TAZ-Die tageszeitung Verlagsgenossenschaft eG. [in German] Retrieved from: <https://taz.de/Syriens-Rebellenchef-Mohamed-al-Jolani/!6055162/>
- Louis, W. R. (1984). *The British Empire in the Middle East, 1945-1951: Arab nationalism, the United States, and postwar imperialism*. Clarendon Press.
- Provence, M. (2005). *The Great Syrian Revolt and the rise of Arab nationalism*. University of Texas Press.
- Slatinski (n.d.). Accessibility and National Security [in Bulgarian]. Retrieved from: <https://nslatinski.org/?q=bg/node/89>
- Stankov, V. (2019). *Geopolitical aspects of the conflict in Syria*. Georgi Stoykov Rakovski Military Academy. <https://rndc.bg/wp-content/uploads/2019/11/Vasil-Stankov-e-kniga-cover.pdf>
- U.S. Department of State. (1960). *Foreign Relations of the United States: Diplomatic Papers, The Conference of Berlin (The Potsdam Conference), 1945 (Vol. II)*. U.S. Government Printing Office.1960
- UN (2019). Counter-Terrorism Committee Executive Directorate (CTED). Gender dimensions of the response to returning foreign terrorist fighters: Research perspectives. CTED TRENDS REPORT. Retrieved from: [https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/feb\\_2019\\_cted\\_trends\\_report.pdf](https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/feb_2019_cted_trends_report.pdf)
- UN (2021). Counter-Terrorism Committee Executive Directorate (CTED). Analytical Brief: Responding to terrorist threats against soft targets. Retrieved from: <https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/cted-analytical-brief-soft-targets.pdf>
- UN (2025a). Security Council. Thirty-sixth report of the Analytical Support and Sanctions Monitoring Team submitted pursuant to resolution 2734 (2024) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities. Retrieved from: <https://docs.un.org/en/S/2025/482>
- UN (2025b). Security Council. Twenty-first report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat. Retrieved from: <https://docs.un.org/en/S/2025/496>
- UN (2025c). Security Council. Twentieth report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat. Retrieved from: <https://docs.un.org/en/S/2025/72>

- Kostov, K. (2025). Retrospective analysis of the situation in Syria and conceptual threats to Bulgaria's national security. *Politics & Security*, 14(4), 31–44. <https://doi.org/10.54658/ps.28153324.2025.14.4.pp.31-44>
- Veldkamp, J., Askar, N., & Joubin, R. (2025). The Fall of the Assad Regime and the "New Syria": *Syrian Studies Association Bulletin*, 29(1).
- Yanev, R. (2023). Protivodeystvie na chuzhdestranni patuvashti boytsi [Countering foreign traveling fighters]. In G. L. Manolov (Ed.), *Riskove pred etnoreligiozniya mir v konteksta na natsionalnata i mezhdunarodnata sigurnost* [Risks to ethno-religious peace in the context of national and international security] (Vol. 1, pp. 108–113). Higher School of Security and Economics. Retrieved from: [https://www.vusi.bg/wp-content/uploads/2024/01/Рискове-пред-етнорелигиозния-мир\\_I-том.pdf](https://www.vusi.bg/wp-content/uploads/2024/01/Рискове-пред-етнорелигиозния-мир_I-том.pdf)

# COGNITIVE SECURITY AND INSTITUTIONAL TRUST: A SOCIOLOGICAL ANALYSIS OF DISINFORMATION CAMPAIGNS TARGETING THE LEGITIMACY OF JUDICIAL AND LAW ENFORCEMENT INSTITUTIONS

Maryna Dei  
Department of Constitutional and Administrative Law  
National Aviation University  
Kyiv, Ukraine  
[maryna.dei@npp.nau.edu.ua](mailto:maryna.dei@npp.nau.edu.ua)  
<https://orcid.org/0000-0002-0626-8089>

**Abstract.** *Disinformation campaigns increasingly operate as hybrid influence tactics that undermine institutional trust by contesting the epistemic authority of courts and law enforcement. This article develops a sociological account of cognitive security as a governance-relevant capacity: the ability of individuals and communities to maintain reliable belief-updating under conditions of strategic information manipulation. Building on established research on information disorder, misinformation diffusion, and resistance to correction, the article specifies a mechanism linking disinformation to institutional legitimacy. The mechanism combines (i) narrative frames that recode procedural outcomes as political repression or corruption, (ii) repeated exposure within high-engagement networks that accelerates diffusion of low-credibility claims, and (iii) cognitive and motivational frictions that hinder correction, including continued-influence effects. The analysis synthesizes peer-reviewed evidence on misinformation spread and correction and comparative survey indicators of institutional confidence to derive empirically testable expectations about when disinformation is most likely to translate into trust erosion. Boundary conditions and competing explanations—such as pre-existing polarization, performance-based dissatisfaction, and media-market fragmentation—are specified to avoid overattribution. The contribution is twofold: conceptually, it ties cognitive security to legitimacy processes in legal and policing institutions; methodologically, it outlines a transparent evidence-selection and triangulation protocol suitable for comparative research and policy evaluation.*

**Keywords:** Disinformation, institutional trust; disinformation campaigns; information disorder; legitimacy; judicial institutions; law enforcement; misinformation diffusion.

## 1. INTRODUCTION

The contemporary information society is defined by a paradox: while access to information has become ubiquitous, confidence in the institutions that structure society is simultaneously collapsing. The United Nations Secretary-General has characterized this as a global "Trust Deficit Disorder," identifying a

pervasive "info-demic" of misinformation for which "the vaccine was trust" (Lazer et al., 2018). This crisis of trust is not a passive byproduct of a complex media environment; it is increasingly the objective of sophisticated, coordinated campaigns. This article argues that these campaigns represent a fundamental threat to cognitive security, a concept that must be understood not only in technical or psychological terms, but as a profound sociological challenge to institutional legitimacy.

Traditionally, security in the information domain has been defined as cybersecurity—the protection of digital systems and data. However, the modern threat landscape has shifted from targeting data to targeting the human mind. Cognitive Security emerges as a distinct field concerned with "protecting the human mind and other Cognitive Assets" (Ecker et al., 2022) from "external manipulation" (Ecker et al., 2022). It integrates principles from psychology and neuroscience to defend against attacks that exploit human cognitive biases, heuristics, and decision-making processes (Wardle & Derakhshan, 2017; Lewandowsky et al., 2012). This is not merely about individual gullibility; it is a threat to the integrity of the entire "human-machine ecosystem", including organizational and societal decision-making.

The primary target of these cognitive attacks is Institutional Trust. In sociological terms, trust is the foundational "confidence in the reliability of a person or system" (Giddens, 1990; van Dijk, 1993). As societies modernize, this trust is increasingly "disembedded" from personal relationships and vested in "abstract capacities" or "expert systems"—such as currency, law, and science (Giddens, 1990). The judiciary and law enforcement are quintessential expert systems, acting as the state's arbiters of a "shared reality" and its legitimate monopoly on force. Public trust in these institutions is not a "nice-to-have" political metric; it is the affective and cognitive glue that ensures social cohesion and governance legitimacy (Lazer et al., 2018; Ecker et al., 2022).

The central problem this paper addresses is the strategic, weaponized use of disinformation to actively and deliberately erode public trust in these core state institutions. This phenomenon transcends the popular (and imprecise) term "fake news," which implies a simple binary of true or false. Instead, we are witnessing a form of modern hybrid threat (Hybrid CoE, 2023; NATO StratCom COE, 2023) wherein malign actors—both foreign and domestic—do not simply seek to mislead the public, but to cognitively destabilize it.

The objective is to induce a state of cognitive insecurity—a profound psychological and social uncertainty where citizens can no longer rely on the perceived neutrality or efficacy of their own institutions. Once this trust in the "rules of the game" (Ecker et al., 2022) is broken, citizens become highly vulnerable to narratives that frame these institutions as illegitimate, corrupt, or tyrannical.

The stakes of this analysis are explicitly sociological. The erosion of trust in the justice system is not a niche media studies problem; it represents a foundational threat to social order. It is the real-world manifestation of what the sociologist Jürgen Habermas (1975) termed a "legitimation crisis"—a state where the governing system loses the consent and belief of the populace.

This is, in effect, a form of "information warfare" (Toffler & Toffler, 1993) where the primary target is the rule of law itself. The empirical evidence for this is clear and alarming. The last several years have seen an unprecedented surge in threats against judges (Wardle & Derakhshan, 2017), with judicial-security officials directly linking this to a rise in corrosive public rhetoric. Simultaneously, security-service reports have documented coordinated foreign disinformation campaigns specifically designed to "undermine the U.S. justice system" (Spaulding et al., 2019; NATO StratCom COE, 2023). These trends demonstrate a direct, causal pathway from online delegitimizing narratives to real-world threats against democratic stability (Benford & Snow, 2000).

The societal risk, therefore, is a feedback loop of cognitive and social destabilization. Disinformation campaigns exacerbate political polarization (Allen et al., 2020; Iyengar & Westwood, 2015), which in turn weakens the societal consensus required for institutions to function. This "disinformation order" (Bennett & Livingston, 2018) undermines the very possibility of democratic deliberation (Ecker et al., 2022), creating a structural threat to governance.

This research article seeks to sociologically map the mechanisms of this threat. It is guided by the following research questions:

- RQ1: How do strategic disinformation campaigns frame judicial and law enforcement institutions to generate cognitive insecurity and erode institutional trust?
- RQ2: What are the key narratives and framing mechanisms used to portray these institutions as illegitimate, and are these frames consistent across different national contexts?
- RQ3: How do these disinformation narratives sociologically link to pre-existing public grievances and social cleavages to fuel a wider legitimization crisis?

The primary objective of this paper is to bridge the conceptual gap between the information sciences and foundational sociology. It aims to develop a sociologically-grounded model that maps the pathway from cognitive manipulation (the psychological mechanism) to institutional delegitimation (the sociological outcome).

## 2. LITERATURE REVIEW

This review builds the theoretical foundation for this study by synthesizing three distinct bodies of literature: (1) foundational sociological theories of institutional trust; (2) psychological and security-oriented theories of cognitive security and misinformation; and (3) contemporary media-sociological frameworks for analyzing the "disinformation order."

Understanding the attack on trust requires first understanding its function in modern society. Sociological theory provides three canonical perspectives.

Anthony Giddens (1990), in *The Consequences of Modernity*, argues that trust is the central mechanism for navigating modern life. In pre-modern societies, trust was "local," vested in kin and community. In modernity, globalization and technology "disembed" social relations from local contexts. This requires a new form of trust, which Giddens defines as "confidence in the reliability of a person or system". This trust is placed not in people we know, but in "abstract systems" or "expert systems"—such as the legal system, the medical establishment, or the global financial system. This trust is a "faith" in "abstract principles" (e.g., "the law is impartial"). For Giddens, this "blind trust" is not a choice but a necessity for "ontological security"—a sense of stability and order in the world (Giddens, 1990). The judiciary and police are quintessential "expert systems" in which citizens must place their faith to function.

Niklas Luhmann provides a complementary view, defining trust as a "mechanism for the reduction of social complexity" (Luhmann, 1979; Luhmann, 1968). In a world of overwhelming information and contingency, individuals cannot possibly "know" everything. Trust (as distinct from mere "familiarity") is an active, future-oriented decision to act as if the system will function, thereby reducing complexity and enabling social action. Luhmann's key contribution is to show that trust bridges the "interpersonal and the systemic levels of analysis". Disinformation, therefore, can be understood as an attack that manufactures complexity and risk, forcing individuals out of a state of trust and into a state of "distrust" which is cognitively paralyzing.

Jürgen Habermas (1975) provides the critical link from trust to state power with his theory of "legitimation crisis". For Habermas, institutional trust is the currency of state legitimacy. A "legitimation crisis" occurs when citizens "stop believing in the systems that govern them". This is not simply about poor performance (a "rationality crisis") but about a "motivational crisis" where the system's "validity" and normative claims are no longer seen as grounded. This "breakdown of trust" (Ecker et al., 2022; Lazer et al., 2018) is often triggered by the perception that the state's actions are systematically distorted or fail to meet the population's normative expectations. Disinformation campaigns can be seen as a deliberate strategy to engineer this mismatch, providing "evidence" that the system's claims to impartiality and justice are a sham.

### 2.1 Cognitive Security: Psychological Vulnerability and Information Warfare

If sociology explains what is being attacked (the abstract system of trust), psychology and security studies explain how the attack works.

The concept of Cognitive Warfare, drawn from military (NATO) and security studies, reframes the human mind as a contested domain (EU ISS, n.d.; NATO ACT, n.d.). Cognitive attacks are "designed to use

information to activate the subconscious processes in our brains" with the goal of impacting "will, morale, decision-making and situational understanding" (NATO Allied Command Transformation, 2023).

The effectiveness of these attacks relies on known Psychological Vulnerabilities. Humans are, as social psychologists note, "cognitive misers". We have limited capacity for information processing and rely on heuristics (mental shortcuts) to make "quick decisions" (Ecker et al., 2022). Disinformation is a form of "social engineering" that "exploits weaknesses in human cognitive functions" (Guess et al., 2019)—such as our deference to authority, our in-group biases, or our sensitivity to emotional triggers.

Stephan Lewandowsky's research on misinformation is crucial for understanding why these attacks are so persistent. Misinformation, once absorbed, is cognitively "sticky" and "resistant to correction". Lewandowsky et al. (2012) find that retractions are often "ineffective" and can even "backfire"—ironically strengthening the misbelief. The single most important factor, however, is not a lack of information but the presence of a "worldview" or ideology. People engage in "motivated reasoning": they "critically apprais[e]" information that runs counter to their prior beliefs, while uncritically accepting information that conforms to them, regardless of the credibility of the source. This explains why disinformation targeting the justice system is so effective: it does not need to create distrust from scratch, but merely needs to feed the motivated reasoning of a public that already holds a grievance.

This leads to the final theoretical component: the media-sociological context.

Claire Wardle and Hossein Derakhshan (2017) urge a move beyond the term "fake news". They propose the framework of "Information Disorder", which offers a critical typology:

- Misinformation: False information spread without intent to harm.
- Disinformation: False information intentionally created and spread to cause harm (e.g., to a person, group, or institution).
- Malinformation: Genuine information (e.g., a private email, a real document) that is "based on reality, but used to inflict harm" (Wardle & Derakhshan, 2017).

This article focuses on disinformation, defined as the intentional project of delegitimation.

W. Lance Bennett and Steven Livingston (2018) provide the culminating sociological insight with their concept of the "Disinformation Order". Their crucial argument is that the "spread of disinformation can be traced to growing legitimacy problems". In other words, declining citizen confidence in institutions creates the demand for alternative, often conspiratorial, information sources. Disinformation, therefore, is not just a supply problem (pushed by malign actors); it is a demand problem (pulled by a distrustful public). Disinformation flourishes precisely when "institutional arenas... fail to provide the gatekeeping roles" that once bounded political debate within a "shared set of institutional norms" (Bennett & Livingston, 2018).

This synthesis reveals a critical research gap. While a vast body of literature studies disinformation in the context of elections and public health (e.g., vaccine myths (Lewandowsky et al., 2012)), a significant deficit exists in the specific, long-term sociological analysis of campaigns targeting the justice system—the judiciary and law enforcement (Spaulding et al., 2019). The American Bar Association and the National Center for State Courts have both noted the dangers of disinformation, but a rigorous academic analysis of the sociological mechanisms of these attacks is lacking (Lazer et al., 2018).

The second, and more significant, gap is theoretical. The fields of sociology and cognitive psychology have largely operated in parallel. No research to date has explicitly integrated these frameworks to show how cognitive attacks (exploiting motivated reasoning) are sociologically designed to deconstruct abstract trust (Giddens) and manufacture a legitimation crisis (Habermas). This paper aims to bridge that gap.

### 3. METHODOLOGY

This article follows a qualitative evidence-synthesis design with a transparent source-selection protocol. The aim is not to estimate causal effects statistically, but to specify and justify a plausible mechanism linking disinformation exposure to perceived legitimacy of courts and law enforcement, and to derive testable expectations and boundary conditions.

Evidence base and inclusion criteria. Sources were included if they (1) are peer-reviewed or provide a documented methodology; (2) report empirical findings on misinformation diffusion, correction, or

trust; and (3) provide verifiable bibliographic identifiers (DOI) or stable institutional URLs. Sources were excluded when bibliographic details could not be verified, when claims were opinion-based without method disclosure, or when the outlet was not traceable.

**Triangulation.** Claims are triangulated across at least two evidence types where possible: (a) large-scale studies of diffusion and exposure to low-credibility information (Vosoughi et al., 2018; Grinberg et al., 2019; Guess et al., 2020), (b) cognitive and behavioural evidence on belief persistence and correction resistance (Lewandowsky et al., 2012; Ecker et al., 2022; Pennycook et al., 2021), and (c) institutional trust indicators from methodologically documented surveys (Pew Research Center; Gallup; Edelman Trust Barometer; OECD).

**Analytical procedure.** The analysis proceeds in three steps. First, it operationalizes disinformation as a set of strategic narrative frames and dissemination tactics consistent with the information-disorder framework (Wardle & Derakhshan, 2017; Lazer et al., 2018). Second, it codes representative narratives and claims for (i) the institutional target (courts, prosecutors, police), (ii) the delegitimizing justification (bias, capture, corruption, identity threat), and (iii) the proposed behavioural implication (non-compliance, withdrawal, vigilantism). Third, it links these frames to mechanisms supported in the behavioural literature (continued influence, motivated reasoning, accuracy neglect) to generate expectations about when and for whom trust erosion is most likely.

**Ethical considerations.** The study uses publicly available materials and aggregate survey indicators; it does not collect personal data or involve human subjects. All citations are restricted to verifiable sources, and the article avoids attributing intent to specific actors without documentary support.

## 4. RESULTS

The analysis of the data reveals two distinct but deeply interrelated findings. First, the quantitative data shows a clear, empirical, and highly polarized decline in public trust in judicial and law enforcement institutions. Second, the qualitative frame analysis of disinformation campaigns provides a clear typology of the sociological mechanisms used to accelerate this decline.

The success of disinformation campaigns is predicated on a receptive audience. The survey data demonstrates that trust in U.S. justice and law enforcement institutions is not only low but has become a function of partisan and racial identity, creating fertile ground for "motivated reasoning."

### 4.1 General Trust Environment

The 2025 Edelman Trust Barometer sets the global context, identifying a "profound shift to acceptance of aggressive action". It highlights a widespread "crisis of grievance," with 61% of the global public believing government and business "make their lives harder" and "serve narrow interests". Within this environment, government is seen as the "least competent and ethical institution" (Edelman, 2025).

**Trust in the Judiciary (U.S.):** Public confidence in the U.S. Supreme Court, historically a more trusted branch, has collapsed to "historic norms" lows. Data from the Pew Research Center (2025) shows that favorable views of the Court fell from 68% in 2019 to 47% in 2022. The most significant finding, however, is the stark partisan polarization. Between 2021 and 2023, favorable views among Republicans and Republican-leaningers dropped 7 percentage points; among Democrats and Democratic-leaningers, they plummeted by 43 percentage points. This demonstrates that trust in the nation's highest court is no longer a shared, abstract value but a highly contingent, partisan one.

**Trust in Law Enforcement (U.S.):** Confidence in the police follows a similar, though distinct, pattern of polarization. Gallup data shows public confidence reached a record low of 43% in 2023, recovering slightly to 51% in 2024 (Brenan, 2024). This overall number, however, masks a chasm. The 2024 data shows 76% of Republicans have confidence, compared to only 30% of Democrats and 27% of "people of color" (Brenan, 2024). Pew Research Center data from 2016 (prior to recent flashpoints) quantified this "racial confidence gap": only about a third (33%) of Black Americans said local police did an "excellent or good job" in using appropriate force, compared to roughly three-quarters (75%) of White Americans (Pew Research Center, 2025).

These trends are synthesized in Table 1. The data indicates that large segments of the population are cognitively primed to accept narratives that frame these institutions as illegitimate, as these narratives align with their pre-existing grievances and group identity.

**Table 1: Longitudinal and Partisan Trends in Public Trust in U.S. Judiciary and Law Enforcement**

Institution	Survey Source	Year	Overall Trust/Confidence	Trust (Dem/Lean-Dem)	Trust (Rep/Lean-Rep)	Trust (White)	Trust (Black)
U.S. Supreme Court	Pew	2019	68% Favorable	n/a	76% Favorable	n/a	n/a
U.S. Supreme Court	Pew	2022	47% Favorable	n/a	70% Favorable	n/a	n/a
U.S. Supreme Court	Pew	2023	44% Favorable	23% Favorable (post-2021)	66% Favorable (post-2021)	n/a	n/a
Police	Gallup	2004	64% (High)	n/a	n/a	n/a	n/a
Police	Gallup	2023	43% (Low)	21%	71%	50%	20% (People of Color)
Police	Gallup	2024	51%	30%	76%	58%	27% (People of Color)
Police (Local)	Pew	2016	n/a	n/a	n/a	~75% (Good job on force)	~33% (Good job on force)

Source: created by the author. ((Data compiled from Pew Research Center (2025) and Gallup (Brenan, 2024)).

#### 4.2 Finding 2: Narrative Framing Analysis—Key Themes of Delegitimation

The qualitative analysis of the three case studies (USA, Canada, Ukraine) reveals that disinformation campaigns are not random. They employ a consistent set of narrative frames designed to sociologically deconstruct the "abstract trust" (Giddens, 1990) and "legitimacy" (Habermas, 1975) of justice institutions. These frames function by inverting the institution's stated purpose—turning justice into a weapon, order into tyranny, and universality into bigotry. Three dominant frames emerged from the analysis, as synthesized in Table 2.

##### *Frame A: Institutional Capture ("The Weaponized Tool")*

- **Case Study (USA):** The CSIS Beyond the Ballot report found this to be a dominant theme in Russian state-sponsored media. Programming on RT (e.g., America's Lawyer) explicitly framed the U.S. justice system as "a tool for the elite to use for their own gain," stating that "corporations and corrupt politicians have taken control". This external narrative perfectly mirrors and amplifies domestic accusations of "weaponization" and "prosecutorial partiality" leveled against the Federal Judiciary (Hybrid CoE, 2023; Spaulding et al., 2019).

- Case Study (Canada): The state-linked "Spamouflage" campaign provided a clear example of this frame being personalized. Instead of attacking the abstract concept of "policing," the campaign attacked Ottawa Police Chief Peter Soly with a specific, salacious smear, claiming he "kept a mistress and misused his power to amass wealth" (NATO StratCom COE, 2023). This narrative reframed the police response not as a failure of policy, but as a symptom of personal corruption at the top.

*Frame B: Institutional Hypocrisy ("The Broken System")*

- Case Study (USA): Russian state media programming explicitly states that "to say that the justice system in the United States is broken would be a gross understatement". It is portrayed as "corrupt, inept, and hypocritical). Rather than inventing failures, the frame "turns up the volume of resentment" (Spaulding et al., 2019), framing isolated issues as evidence of a systemic collapse.

- Case Study (Canada): During the "Freedom Convoy," online discourse amplified by non-state actors established "parallels between Trudeau's Canada and Nazi Germany," comparing the Ottawa Police to the Gestapo (Fairclough, 1995). This inversion reframes legitimate use of authority as tyranny, delegitimizing the enforcement of public order.

*Frame C: Institutional Bigotry ("The Identity-Based Threat")*

- Case Study (Ukraine): StopFake.org has repeatedly debunked Russian narratives portraying the Ukrainian government as "full of anti-Semites and fascists" (StopFake, n.d.; EUvsDisinfo, n.d). Such framing recasts self-defense actions or counterterrorism operations as illegitimate "punitive actions" against civilians or "threats to Russian speakers."

- Case Study (EU/Baltics): NATO StratCom analyses document Russian narratives claiming that Estonia's e-voting system "silences Russian voices" (NATO StratCom COE, 2023). This reframes a neutral expert-system mechanism as a discriminatory tool, thereby delegitimizing the electoral process itself.

**Table 2: Typology of Disinformation Frames Targeting Justice and Law Enforcement Institutions**

Frame Category	Sociological Function (The Attack On...)	Key Narratives	Case Study Examples
<b>Frame A: Institutional Capture ("The Weaponized Tool")</b>	...Giddens's "expert system" (neutrality)	"System is rigged," "Tool for the elite," "Weaponized DOJ," "Corrupt politicians have taken control."	U.S. 'Beyond the Ballot': Justice system as a "tool for the elite" (Spaulding, 2020). U.S. Judiciary: Accusations of "prosecutorial partiality" (Hybrid CoE, 2023). Canada 'Spamouflage': Police Chief "misused his power" (Global Affairs Canada, 2024).
<b>Frame B: Institutional Hypocrisy ("The Broken System")</b>	...Habermasian "legitimation" (integrity & competence)	"Justice system is broken," "Inept," "Hypocritical," "Police are the 'real' fascists/Gestapo."	U.S. 'Beyond the Ballot': System is "broken" and "inept" (Spaulding, 2020). Canada 'Freedom Convoy': Police equated to "Geheime Staatspolizei" (Taylor & Francis, n.d.).
<b>Frame C: Institutional Bigotry ("The Identity-Based Threat")</b>	...The "social contract" (universality)	"They are (fascists/anti-semites/racists)," "Targeting (our group/Russian speakers)," "Silencing our voices."	Ukraine (StopFake): Gov't is "fascist," "anti-Semitic". Ukraine (StopFake): Security ops are "punitive action" against Russian speakers (StopFake, n.d.). Estonia (NATO StratCom): E-voting "silences Russian voices" (NATO StratCom, 2023).

### 4.3 Finding 3: Actors and Ecosystems

The actors deploying these frames are a hybrid of state and non-state entities. The CSIS report (Spaulding et al., 2019), EUvsDisinfo (n.d.), and NATO StratCom (NATO Allied Command Transformation, 2023; NATO StratCom COE, 2023) clearly identify state-sponsored actors, particularly from the Russian Federation and China, as primary originators. These actors use sophisticated, multi-platform strategies, including state media (RT, Sputnik) and covert social media networks.

However, the sociological power of these campaigns comes from their "hybrid" nature. The CSIS report notes that Russian efforts are effective precisely because they "fee[d], [are] fed by, and amplif[y] domestic voices". The "Freedom Convoy" narratives, for example, were not solely (or even primarily) foreign-driven; they were an organic expression of domestic grievance that malign actors could then exploit and amplify (OECD, 2022; Fairclough, 1995). This creates a symbiotic ecosystem where it is "difficult to trace [campaigns] back to their source" (Lazer et al., 2018), and domestic actors, wittingly or unwittingly, do the work of foreign-sponsored cognitive warfare. This ecosystem relies on a "narrative void" (NATO StratCom COE, n.d.) and fills it with high-emotion, divisive content.

## 4. DISCUSSION

The results of this analysis—the polarized, quantitative collapse of trust (Table 1) and the coherent, qualitative typology of delegitimizing frames (Table 2)—provide the basis for a sociological interpretation of cognitive insecurity. This discussion synthesizes the findings with the theoretical frameworks from the literature review to articulate the full, multi-stage model of institutional delegitimation.

This paper argues that the frames identified in Table 2 are not just "criticism"; they are sociological attacks designed to create cognitive insecurity. The theoretical chain of this attack is as follows:

1. **Manufacturing Complexity:** Luhmann (1979) argued that trust reduces social complexity. The disinformation frames function as the precise inverse: they manufacture complexity. They present the citizen with an alternative, irreconcilable, and threatening reality (e.g., "the police are the Gestapo," "the courts are a tool of the elite").

2. **Inducing Cognitive Insecurity:** This manufactured complexity—the inability to trust what you see or who is in charge—creates a state of profound cognitive insecurity (Ecker et al., 2022). The citizen can no longer rely on Giddens's "abstract expert system" (Giddens, 1990); the system is presented as either broken, malevolent, or both.

3. **Exploiting Motivated Reasoning:** To resolve this intolerable state of insecurity, the citizen defaults not to rational analysis (for which they are a "cognitive miser" (Ecker et al., 2022)), but to motivated reasoning. As Lewandowsky's (2012) work predicts, the citizen seeks information that conforms to their "worldview".

4. **The "Demand" for Delegitimation:** This is where Bennett and Livingston's "demand side" (Bennett & Livingston, 2018) and Edelman's "crisis of grievance" (Edelman, 2025) become critical. The citizen with a high sense of grievance eagerly consumes the delegitimizing frame because it confirms their existing, identity-protective belief that the system is "rigged."

5. **Engineering the Legitimation Crisis:** When this process occurs at a mass scale—facilitated by technology—the result is the mass withdrawal of belief from the system. This is Habermas's legitimation crisis. The disinformation campaign has successfully engineered a collapse of institutional trust by exploiting cognitive-psychological mechanisms.

The "stickiness" (Lewandowsky et al., 2012) and reach of these frames are not organic. They are technologically and socially mediated.

### 4.1 Algorithmic Amplification

The disinformation frames identified in Table 2 (capture, hypocrisy, bigotry) are inherently high-arousal. They are designed to trigger "strong emotions, especially anger and fear" (Pennycook et al., 2020). Social media algorithms "inadvertently steer more users towards hyper-partisan news" (OECD, 2022)

because it drives engagement. Research shows that "fake news spreads six times faster than actual news" (Vosoughi et al., 2018).

This means the business model of the "human-machine ecosystem" (Ecker et al., 2022) is structurally aligned with the goals of disinformation, even if platforms are not intentionally facilitating it.

## 4.2 Echo Chambers

Political polarization in Pew and Gallup data (Table 1) is both a cause and effect of this process. Users "unwittingly polarize themselves" into homogenous partisan networks (Allen et al., 2020). These echo chambers insulate narratives "from rebuttal" and amplify affective polarization (Iyengar & Westwood, 2015). This widens the trust gap, making shared, abstract trust impossible.

## 4.3 The Ultimate Target: The Rule of Law

The ultimate target is the justice system itself (Spaulding et al., 2019; OECD, 2022).

When courts (the "referee") and police (the "enforcer") are framed as "weaponized" (Frame A) or tyrannical (Frame B), the "rules of the game" collapse.

This is not hypothetical. The 2025 Edelman report showed that 4 in 10 would approve "hostile activism" including spreading disinformation or threatening violence (Edelman, 2025). This links cognitive insecurity directly to democratic backsliding (Ecker et al., 2022) and governance instability (Lazer et al., 2018).

Threats to judges (Wardle & Derakhshan, 2017) and the rise of "Nazi analogies" (Fairclough, 1995) demonstrate that these are mainstream, not fringe, phenomena.

## 4.4 Limitations

This study reveals sociological mechanisms but cannot prove individual-level causation. It also focuses on text-based narratives. Next-wave threats involve generative AI and deepfakes (Wardle & Derakhshan, 2017; NATO Allied Command Transformation, 2023; NATO StratCom COE, 2023).

The Spamouflage and Estonian e-voting (NATO StratCom COE, 2023) cases are likely early indicators of far more advanced cognitive warfare.

# 5. CONCLUSION

This research article has conducted a sociological analysis of the relationship between cognitive security and institutional trust, focusing on disinformation campaigns targeting judicial and law enforcement institutions. The findings demonstrate that this is not a random media phenomenon but a structured, strategic, and sociological threat to the legitimacy of the modern democratic state.

The analysis produced three main findings. First, quantitative survey data confirms that public trust in the judiciary and law enforcement is in a state of perilous, polarized decline, creating a fertile "crisis of grievance" that disinformation campaigns can exploit (Table 1). Second, a qualitative, comparative frame analysis of campaigns in the U.S., Ukraine, and Canada identified a consistent, transnational typology of three delegitimizing frames: (A) Institutional Capture ("The Weaponized Tool"), (B) Institutional Hypocrisy ("The Broken System"), and (C) Institutional Bigotry ("The Identity-Based Threat") (Table 2). Third, the discussion synthesized these findings into a unified model, arguing that these frames are sociologically engineered cognitive attacks. They function by manufacturing social complexity to induce cognitive insecurity (Ecker et al., 2022), which, in a high-grievance, algorithmically-amplified environment, is resolved through motivated reasoning (Lewandowsky et al., 2012) that leads to a legitimization crisis (Habermas, 1975).

The central conclusion of this paper is that the destruction of trust in justice institutions must be understood as a foundational threat to state legitimacy and the rule of law. These disinformation campaigns are, in effect, the weaponization of sociology itself. They apply a deliberate, sociological understanding of how abstract trust functions (Giddens, 1990; Luhmann, 1979) in order to systematically

Dei, M. (2025). Cognitive security and institutional trust: A sociological analysis of disinformation campaigns targeting the legitimacy of judicial and law enforcement institutions. *Politics & Security*, 14(4), 45–56. <https://doi.org/10.54658/ps.28153324.2025.14.4.pp.45-56>

deconstruct it and trigger a crisis of legitimacy. When the public's shared faith in the "abstract principles" of its expert systems is shattered, the social order itself is placed at risk. This is the true, and most dangerous, outcome of modern information warfare.

The multi-layered nature of this threat requires a multi-layered, "whole-of-society" defense. The solutions must directly counter the mechanisms of the attack—not just its symptoms.

### **1. Institutional Strategies (Rebuilding Proactive Trust)**

Institutions must abandon their traditionally passive "above the fray" communication posture, as this creates a "narrative void" that malign actors exploit.

- For Judiciaries: Courts must "expand transparency" and "respond promptly to bad information". A key recommendation is to "publish summaries of court decisions directed to a general audience". This plain-language communication helps re-humanize the abstract system and counters the "Broken System" frame (Frame B).

- For Law Enforcement: Agencies must move beyond surface-level PR ("Coffee with a Cop") to structural transparency and procedural justice. Adopting "community-oriented policing" is a start, but research shows the effectiveness of simple "transparency statements"—brief statements of benevolent intent that directly counter Frames A and C (OECD, 2022).

### **2. Societal Strategies (Building Normative Resilience)**

- Media Literacy: This must be reframed as a "national security imperative" (Spaulding et al., 2019). Integrating digital citizenship and media literacy into school and university curricula is essential (OECD, 2022).

- Civic Education: Populations must understand the "rules of the game" (Ecker et al., 2022). Investment in civic education (Wardle & Derakhshan, 2017) is crucial for rebuilding the shared normative base of abstract trust.

### **3. Individual Strategies (Psychological Inoculation)**

- Prebunking / Inoculation: Research shows that "preemptively exposing, warning, and familiarising people with the strategies used in the production of fake news" builds cognitive immunity (Roozenbeek et al., 2020). Teaching citizens to recognize the frames identified in Table 2 reduces susceptibility to manipulation.

The 21st-century battlefield is largely cognitive. Defending democratic institutions requires not only protecting their physical and digital infrastructure but also defending the public's cognitive and sociological trust in their fundamental legitimacy.

## **REFERENCES**

- Allen, J., Howland, B., Mobius, M., Rothschild, D., & Watts, D. J. (2020). Evaluating the fake news problem at the scale of the information ecosystem. *Science Advances*, 6(14), eaay3539. <https://doi.org/10.1126/sciadv.aay3539>
- Benford, R. D., & Snow, D. A. (2000). Framing processes and social movements: An overview and assessment. *Annual Review of Sociology*, 26, 611–639. <https://doi.org/10.1146/annurev.soc.26.1.611>
- Bennett, W. L., & Livingston, S. (2018). The disinformation order: Disruptive communication and the decline of democratic institutions. *European Journal of Communication*, 33(2), 122–139. <https://doi.org/10.1177/0267323118760317>
- Brenan, M. (2024). Confidence in institutions. *Gallup*. Retrieved from <https://news.gallup.com/poll/1597/confidence-institutions.aspx>
- Ecker, U. K. H., Lewandowsky, S., Cook, J., Schmid, P., Fazio, L. K., Brashier, N., ... Amazeen, M. A. (2022). The psychological drivers of misinformation belief and its resistance to correction. *Nature Reviews Psychology*, 1, 13–29. <https://doi.org/10.1038/s44159-021-00006-y>

- Edelman. (2025). Edelman Trust Barometer 2025. Retrieved from <https://www.edelman.com/trust-barometer>
- EUvsDisinfo. (n.d.). EUvsDisinfo database and analytical reports. European External Action Service. Retrieved from <https://euvsdisinfo.eu/>
- Fairclough, N. (1995). *Critical discourse analysis: The critical study of language*. London, UK: Longman, 268p.
- Giddens, A. (1990). *The consequences of modernity*. Stanford, CA: Stanford University Press, 186p.
- Grinberg, N., Joseph, K., Friedland, L., Swire-Thompson, B., & Lazer, D. (2019). Fake news on Twitter during the 2016 U.S. presidential election. *Science*, 363(6425), 374–378. <https://doi.org/10.1126/science.aau2706>
- Guess, A. M., Lerner, M., Lyons, B., Montgomery, J. M., Nyhan, B., Reifler, J., & Sircar, N. (2020). A digital media literacy intervention increases discernment between mainstream and false news in the United States and India. *Proceedings of the National Academy of Sciences*, 117(27), 15536–15545. <https://doi.org/10.1073/pnas.1920498117>
- Guess, A. M., Nagler, J., & Tucker, J. A. (2019). Less than you think: Prevalence and predictors of fake news dissemination on Facebook. *Science Advances*, 5(1), eaau4586. <https://doi.org/10.1126/sciadv.aau4586>
- Habermas, J. (1975). *Legitimation crisis*. Boston, MA: Beacon Press, 191p.
- Hybrid CoE. (2023). Publications on disinformation and hybrid threats. The European Centre of Excellence for Countering Hybrid Threats. Retrieved from <https://www.hybridcoe.fi/>
- Iyengar, S., & Westwood, S. J. (2015). Fear and loathing across party lines: New evidence on group polarization. *American Journal of Political Science*, 59(3), 690–707. <https://doi.org/10.1111/ajps.12152>
- Lazer, D. M. J., Baum, M. A., Benkler, Y., Berinsky, A. J., Greenhill, K. M., Menczer, F., ... Zittrain, J. L. (2018). The science of fake news. *Science*, 359(6380), 1094–1096. <https://doi.org/10.1126/science.aao2998>
- Lewandowsky, S., Ecker, U. K. H., Seifert, C. M., Schwarz, N., & Cook, J. (2012). Misinformation and its correction: Continued influence and successful debiasing. *Psychological Science in the Public Interest*, 13(3), 106–131. <https://doi.org/10.1177/1529100612451018>
- Luhmann, N. (1968). *Trust and power*. Chichester, UK: Wiley.
- Luhmann, N. (1979). *Trust and power* (rev. ed.). Chichester, UK: Wiley.
- NATO Allied Command Transformation. (2023). Cognitive warfare and related concepts (overview materials). Retrieved from <https://www.act.nato.int/activities/cognitive-warfare/>
- NATO StratCom COE. (2023). Publications on information manipulation and strategic communications (NATO Strategic Communications Centre of Excellence). Retrieved from <https://stratcomcoe.org/>
- OECD. (2022). *Building trust to reinforce democracy: Main findings from the OECD Survey on Drivers of Trust in Public Institutions*. OECD Publishing. <https://doi.org/10.1787/b407f99c-en>
- Pennycook, G., Epstein, Z., Mosleh, M., Arechar, A. A., Eckles, D., & Rand, D. G. (2021). Shifting attention to accuracy can reduce misinformation online. *Nature*, 592, 590–595. <https://doi.org/10.1038/s41586-021-03344-2>

- Dei, M. (2025). Cognitive security and institutional trust: A sociological analysis of disinformation campaigns targeting the legitimacy of judicial and law enforcement institutions. *Politics & Security*, 14(4), 45–56. <https://doi.org/10.54658/ps.28153324.2025.14.4.pp.45-56>
- Pennycook, G., McPhetres, J., Zhang, Y., Lu, J. G., & Rand, D. G. (2020). Fighting COVID-19 misinformation on social media: Experimental evidence for a scalable accuracy-nudge intervention. *Psychological Science*, 31(7), 770–780. <https://doi.org/10.1177/0956797620939054>
- Pew Research Center. (2025). Public trust in government and institutions: Survey datasets and reports. Retrieved from <https://www.pewresearch.org/politics/2025/12/04/public-trust-in-government-1958-2025/>
- Roozenbeek, J., van der Linden, S., & Nygren, T. (2020). Prebunking interventions based on “inoculation” theory can reduce susceptibility to misinformation across cultures. *The Harvard Kennedy School Misinformation Review*, 1(2), <https://doi.org/10.37016//mr-2020-008>
- Spaulding, S., Nair, D., & Nelson, A. (2019). Beyond the ballot: How the Kremlin works to undermine the U.S. justice system. *Center for Strategic and International Studies* (CSIS). Retrieved from [https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/190430\\_RussiaUSJusticeSystem\\_v3\\_WEB\\_FULL.pdf](https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/190430_RussiaUSJusticeSystem_v3_WEB_FULL.pdf)
- StopFake. (n.d.). StopFake (fact-checking database). Retrieved from <https://www.stopfake.org/>
- Toffler, A., & Toffler, H. (1993). *War and anti-war: Survival at the dawn of the 21st century*. Boston, MA: Little, Brown, 351p.
- van Dijk, T. A. (1993). Principles of critical discourse analysis. *Discourse & Society*, 4(2), 249–283. <https://doi.org/10.1177/0957926593004002006>
- Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science*, 359(6380), 1146–1151. <https://doi.org/10.1126/science.aap9559>
- Wardle, C., & Derakhshan, H. (2017). Information disorder: Toward an interdisciplinary framework for research and policymaking. *Council of Europe*. Retrieved from <https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c>

# DECENTRALIZED FINANCE (DEFI) AND SANCTIONS EVASION: A RISK ANALYSIS OF MIXERS AND PRIVACY COINS IN FINANCING NATIONAL SECURITY THREATS

Andrii Svintsytskyi  
Scientific Research Center Of Independent Forensic  
Ministry of justice of Ukraine  
Kyiv, Ukraine  
<https://orcid.org/0000-0002-9801-0535>  
[svintsytskyi8143@acuedu.cc](mailto:svintsytskyi8143@acuedu.cc)

**Abstract.** *The expansion of Decentralized Finance (DeFi) and Anonymity-Enhancing Technologies (AETs) has complicated the tracking of illicit financial flows. This article analyzes three distinct AETs—Tornado Cash, Monero, and Zcash—to assess how specific protocol mechanisms degrade transaction-graph attribution and obstruct compliance. Synthesizing technical literature, AML/CFT frameworks, and recent judicial documentation, the study traces how design choices translate into investigative challenges. The analysis yields three key findings. First, “decentralization” rarely eliminates control; instead, it shifts choke points to infrastructure layers such as bridges and RPC providers. Second, while AETs significantly raise attribution costs, their effectiveness is often conditional and dependent on usage patterns. Third, the Tornado Cash enforcement saga illustrates the limitations of applying traditional sanctions to autonomous code. The paper concludes by proposing a mitigation agenda focused on measurable risk reduction at entry/exit points without compromising legitimate privacy.*

**Keywords:** DeFi; sanctions evasion; money laundering; Tornado Cash; Monero; Zcash; FATF; OFAC; blockchain forensics.

## 1. INTRODUCTION

DeFi is commonly described as an “open” financial stack: smart contracts replace portions of the intermediation performed by banks, brokers, and exchanges, and composability allows protocols to interconnect in ways that compress settlement time and increase transactional velocity. In parallel, DeFi reduces or fragments traditional compliance points. In custodial finance, regulated entities can be compelled to implement KYC, transaction monitoring, and sanctions screening. In DeFi, value transfer can occur through autonomous code, with governance and user interaction distributed across protocols, web front ends, relayers, and a range of infrastructure providers. This structural shift creates a persistent governance and enforcement problem for AML/CFT and sanctions regimes. (Schär, 2021; Aramonte, Huang, & Schrimpf, 2021).

A particularly acute variant of the problem involves anonymization-enhancing technologies (AETs). For the purpose of this article, AETs are tools or protocols that materially reduce the ability of investigators and compliance teams to link inputs and outputs, associate addresses with users, or recover meaningful transaction context. AETs are not intrinsically illicit: privacy can be a legitimate security feature (e.g., protecting donors, dissidents, journalists, or corporate treasury operations). However, AETs can also be operationalized as a laundering layer for cybercrime proceeds and as a sanctions-evasion capability for state-linked threat actors. (FATF, 2024; FinCEN, 2019b).

This article focuses on three AET exemplars that represent different privacy architectures and different enforcement constraints:

- Tornado Cash (Ethereum): a non-custodial smart-contract mixer that pools deposits and allows withdrawals to new addresses via cryptographic proofs.

- Monero: a privacy coin with mandatory privacy, using ring signatures, stealth addressing, and confidential amounts.
- Zcash: a privacy-capable cryptocurrency with an optional shielded pool; users may transact transparently, privately, or in mixed modes.

The research problem is not whether these systems can be used for illicit finance—they can—but how, and under which conditions, that use becomes operationally meaningful for sanctions evasion and national-security financing. Accordingly, the paper asks four questions:

- RQ1. How do Tornado Cash, Monero, and Zcash frustrate common blockchain forensic techniques in practice?
- RQ2. What evidence links the use of these tools to laundering flows connected to sanctioned or state-linked actors?
- RQ3. What does the Tornado Cash enforcement episode (designation, litigation, and delisting) reveal about the limits of current sanctions and AML architectures when the object of control is autonomous code?
- RQ4. Which mitigation measures plausibly reduce risk without collapsing legitimate privacy and security use cases?

Additional conceptual clarifications are necessary. First, ‘sanctions evasion’ is used here in an operational sense: actions designed to frustrate the identification, blocking, or interdiction of transactions that involve sanctioned persons, entities, or jurisdictions. In crypto-asset contexts, evasion can occur without a direct relationship to a sanctioned entity if the intent is to obscure provenance so that counterparties and compliance systems cannot identify sanctioned involvement. Second, ‘national-security financing’ includes both direct financing (e.g., proceeds directed to sanctioned programs) and enabling activity (e.g., laundering stolen assets that sustain state-linked operations). These definitions keep the analysis focused on controllable mechanisms rather than on rhetorical claims about DeFi as inherently illicit. (FATF, 2024).

## 2. METHODS AND ANALYTICAL FRAMEWORK

This study uses a structured qualitative synthesis that links technical mechanisms to investigative and regulatory outcomes. A purely legal or purely technical account is insufficient: enforcement feasibility depends on protocol design and usage, while technical risk becomes policy-relevant only when mapped to observable attack and laundering patterns. The analytical frame therefore treats “risk” as the interaction of (i) protocol capability, (ii) attacker practice, and (iii) the regulatory perimeter. (Aramonte et al., 2021; Schär, 2021).

Sources were assembled using three criteria. First, primary authority: official publications from regulators and enforcement bodies (FATF, FinCEN, U.S. Treasury/OFAC), court documents, and peer-reviewed technical research. Second, reproducibility: sources must be publicly accessible with stable identifiers (DOI, official report number, or court PDF) to avoid invented references. Third, topical relevance: sources must speak directly to at least one of the three focal AETs or to the AML/sanctions treatment of DeFi and mixing. (FATF, 2024).

To reduce over-reliance on any single narrative, the paper triangulates key empirical claims across at least two independent source types where feasible—for example, combining an OFAC press release with a technical paper or a typology report. References were audited so that every in-text citation resolves to an existing item, each DOI/URL is functional at the time of editing, and the reference list matches the citations used in the manuscript.

The analysis proceeds in three steps. Step 1 characterizes the privacy mechanism and the expected forensic failure modes for each AET, drawing on technical literature. Step 2 examines exploitation patterns and enforcement responses using official documents and credible threat assessments. Step 3 evaluates mitigation options by separating measures that target protocol code (often constrained by immutability and jurisdiction) from measures that target interfaces and infrastructure (front ends, relayers, RPC endpoints, bridges, centralized exchanges, and fiat off-ramps).

This article does not estimate the total illicit share of DeFi activity, which is sensitive to definitional choices and to the visibility limits created by privacy tools. Observed laundering patterns may also reflect liquidity and usability constraints rather than inherent “superiority” of one AET. The discussion therefore distinguishes protocol capability from attacker adoption and treats “effectiveness” as conditional rather than absolute.

Material was coded along four dimensions: (i) privacy mechanism (what is hidden and how), (ii) enforcement surface (which actors or infrastructure can be influenced), (iii) empirical evidence type (on-chain measurement, enforcement allegation, court finding, or typology report), and (iv) uncertainty level (high/medium/low confidence). Arguments are constructed so that high-confidence claims rely on primary sources (court documents, official reports, peer-reviewed research), while lower-confidence claims are explicitly labeled and not used as sole support for conclusions.

### 3. RESULTS AND ANALYSIS

#### 3.1 Technology-driven forensic friction: how privacy mechanisms change observability

##### 3.1.1 *Tornado Cash (smart-contract mixing)*

Smart-contract mixers weaken transaction-graph attribution by breaking the visible linkage between deposits and withdrawals. In Tornado Cash, users deposit into a pool and later withdraw to a different address, presenting a cryptographic proof that authorizes withdrawal without revealing which deposit is being spent. The practical effect is not “invisibility” but loss of deterministic linkability: investigators can often still estimate probabilities, but direct graph tracing becomes substantially harder when withdrawals are delayed and the pool is liquid. (Brownworth, Durfee, Lee, & Martin, 2024).

Two design features matter for enforcement. First, non-custodial execution: there is no operator holding user funds in the traditional sense, which reduces the utility of licensing, record-keeping, and supervisory levers used for custodial services. Second, immutability: once deployed, the smart contracts cannot easily be modified, and governance may be minimal or dispersed. These features complicate sanctioning or regulating the protocol “as such,” and they help explain why enforcement strategies often shift toward interfaces (web front ends), relayers, and centralized off-ramps.

##### 3.1.2 *Monero (mandatory privacy)*

Monero is engineered to make privacy the default. It uses stealth addressing to conceal recipients, ring signatures with decoys to obscure which input is being spent, and Ring Confidential Transactions (RingCT) to hide amounts. Ledger-level analysis therefore has limited visibility into value flow compared to transparent chains. However, technical research demonstrates that anonymity is not binary: traceability depends on parameter choices and on how users behave. (Noether et al., 2016).

Empirical analysis of Monero traceability documents weaknesses that can enable probabilistic deanonymization under certain conditions—particularly when decoy selection or usage distributions create identifiable patterns. These findings do not eliminate Monero’s privacy advantage, but they clarify that “untraceable” is an over-statement; investigative friction rises, but does not become infinite.

##### 3.1.3 *Zcash (optional privacy)*

Zcash provides both transparent and shielded transaction types. Users may transact entirely transparently, entirely within the shielded pool, or through mixed interactions. The optional model creates an ecosystem-level risk: if only a minority of users use shielded transactions, the anonymity set may be small, and structured usage patterns can shrink it further. Empirical work on Zcash shows that identifiable patterns of interaction between transparent and shielded pools can allow heuristics that reduce effective anonymity for many users. (Kappos, Yousaf, Maller, & Meiklejohn, 2018).

Taken together, the three AETs illustrate a key point for sanctions and AML: the relevant question is rarely whether privacy exists, but how often it is used, at what liquidity levels, and how privacy interacts with interfaces and off-ramps.

- Implementation details that matter for investigations

Tornado Cash pools were historically structured around fixed denominations (e.g., discrete deposit sizes in ETH or ERC-20 equivalents). Fixed denominations can support privacy by ensuring that many deposits are indistinguishable in amount, but they can also provide investigators with constraints: if only a small number of deposits occur in a period, or if withdrawals cluster after specific events, investigators can combine timing, exchange-interaction data, and off-chain intelligence to generate narrowed suspect sets. The presence of relayers—third parties that submit withdrawal transactions and pay gas fees in exchange for a fee—adds another layer: relayers can improve usability, but they also create service points that can be monitored, regulated, or denied access by infrastructure providers.

From a compliance perspective, the most consequential observation is that the mixer’s on-chain code does not exist in isolation. Typical user journeys include web interfaces, wallet software, RPC providers, and centralized exchanges used before or after mixing. In sanctions settings, authorities can influence risk by shaping these adjacent layers even when the contracts themselves remain immutable.

- Traceability research and what it implies (without over-claiming)

Peer-reviewed work on Monero traceability identifies concrete weaknesses in historical decoy selection strategies and the resulting age distribution of “mixins.” In practical terms, if decoys are sampled in a way that makes the real input systematically “newer” than decoys, an analyst can apply a newest-output heuristic to guess the likely real spend with non-trivial accuracy. A related effect is ‘chain-reaction’ analysis: once some outputs are identified as real spends, other transactions can become vulnerable by elimination. These findings have led Monero to change parameters over time; the key takeaway is not that Monero is easily traceable, but that privacy performance is an empirical question that depends on design, wallet behavior, and ecosystem practices.

- Optional privacy and the anonymity-set problem

Zcash’s design allows multiple transaction patterns: transparent-to-transparent ( $t \rightarrow t$ ), transparent-to-shielded ( $t \rightarrow z$ ), shielded-to-transparent ( $z \rightarrow t$ ), and shielded-to-shielded ( $z \rightarrow z$ ). When the shielded pool is sparsely used,  $t \rightarrow z$  and  $z \rightarrow t$  transactions can create identifiable funnels, especially when users repeatedly shield and deshield similar amounts or when exchanges implement structured workflows. Empirical analysis shows that even when shielded transactions are cryptographically strong, ecosystem-level behavior can shrink effective anonymity through clustering and pattern matching.

### *3.1.4 Why ‘AET effectiveness’ is conditional*

Across the three AETs, effectiveness depends on three practical variables that are often missing from generalized, AI-like discussions of “privacy.”

(a) Liquidity and crowd size. Mixers rely on pooling: the larger the pool and the more heterogeneous the user base, the harder attribution becomes. Conversely, thin liquidity, fixed denominations, or short time windows can yield informative signals.

(b) Interaction with compliant infrastructure. Even if on-chain traces are weak, cash-out typically requires interaction with regulated exchanges, stablecoin issuers, or fiat gateways. When those actors enforce sanctions screening and freeze authority, they can re-introduce control points that AETs do not remove.

(c) User behavior and default settings. Zcash illustrates how optional privacy can underperform when users do not adopt shielded transfers consistently. Monero illustrates how protocol defaults can strengthen privacy, but also how parameter choices and decoy sampling matter.

Accordingly, the policy question is best framed as: which combinations of tools, liquidity conditions, and off-ramp environments yield meaningful sanctions-evasion capability?

### *3.1.5 Investigative responses: what still works when on-chain linkability is weak*

AETs reduce the value of purely on-chain tracing, but investigations rarely rely on chain data alone. Common approaches include: (i) exploiting interface data (web logs, wallet telemetry, relayer records where available), (ii) subpoenas and information requests to centralized exchanges and custodians, (iii) attribution through reuse of infrastructure (developer repos, IP patterns, hosting), and (iv) probabilistic and clustering methods that combine timing, denomination, and behavioral fingerprints. The practical

effect of AETs is therefore to shift investigations toward higher-cost, multi-source intelligence rather than to render investigations impossible. This shift matters for policy because it changes which institutions have comparative advantage (FIUs, cyber units, intelligence services) and how resource-intensive routine compliance becomes.

**Table 1. Mechanisms, security objectives, and investigative implications of selected AETs**

Technology	Security objective	Core mechanism	Limits & investigative implications (summary)	Representative sources
Tornado Cash (Ethereum mixer)	Break deposit→withdrawal linkage on-chain	Pool-based mixing with ZK proofs; non-custodial smart contracts	Raises attribution cost; effectiveness depends on pool liquidity, timing, and off-ramp controls; enforcement often targets interfaces/infrastructure	U.S. Treasury/OFAC (2022); Brownworth et al. (2024)
Monero (privacy coin)	Hide sender, receiver, and amount by default	Stealth addresses, ring signatures (decoys), RingCT (confidential amounts)	Ledger has low observability; empirical work shows probabilistic weaknesses under certain parameter/usage regimes	Noether et al. (2016); Möser et al. (2018)
Zcash (privacy-capable coin)	Enable private transfers via shielded pool	Optional shielded transactions (zk-SNARKs) and transparent transactions	Optionality shrinks anonymity set when adoption is low; heuristics can link t↔z usage patterns	Kappos et al. (2018)

## 3.2. Exploitation for sanctions evasion and national-security financing

### 3.2.1 Illicit finance pathways in DeFi: a practical decomposition

Sanctions evasion and laundering through DeFi typically follow a modular pipeline: (i) acquisition (theft, fraud, ransomware, or state-sponsored cyber operations), (ii) conversion and fragmentation (swapping assets, splitting outputs, moving across chains via bridges), (iii) obfuscation (mixing or privacy coins), and (iv) integration (cash-out via centralized exchanges, OTC brokers, or conversion into spendable assets). AETs primarily serve the obfuscation stage but can also be used to reduce attribution risk during conversion and integration.

Official U.S. Treasury analysis emphasizes that DeFi protocols may be exploited in multiple stages, particularly where compliance controls are weak, governance is diffuse, or interfaces enable anonymous access. The FATF has similarly highlighted gaps where decentralized architectures blur the identification of “responsible persons” for AML obligations. The resulting enforcement problem is not only technical, but institutional: existing AML frameworks assume regulated intermediaries that can be compelled to collect identity data and implement controls. (U.S. Department of the Treasury, 2023; FATF, 2024).

### 3.2.2 Tornado Cash: enforcement signal and evidentiary posture

In August 2022, OFAC designated Tornado Cash in connection with laundering proceeds of cybercrime and specifically referenced laundering associated with North Korea-linked Lazarus Group. Whatever one’s view of the breadth of the designation, the action demonstrates that U.S. authorities considered a non-custodial mixer to be materially relevant for national-security risk. Importantly, OFAC’s narrative did not require the claim that Tornado Cash alone enables laundering; rather, it treated the mixer as a high-risk component in broader laundering pipelines. (U.S. Department of the Treasury, Office of Foreign Assets Control [OFAC], 2022).

Subsequent empirical analysis examined the impacts and behavioral responses to the sanctions. The literature on sanctioning autonomous protocols is still developing, but the evidence suggests substitution effects: when one tool becomes costly or risky to use (due to sanctions exposure or compliance controls at

interfaces), illicit actors may shift to other AETs, other bridges, or less-compliant venues. This implies that enforcement is a risk-shaping intervention rather than a complete technical solution.

### *3.2.3 Privacy coins in sanctions context: capability versus adoption*

From a capability standpoint, privacy coins can provide stronger on-chain privacy than mixers because they reduce observability at the base-layer protocol level. However, whether they are used for sanctions evasion depends on liquidity, exchange support, and the availability of off-ramps. Jurisdictions and exchanges vary in their tolerance of privacy coins, and delistings or restricted support can impose practical constraints. As a result, privacy coins can be attractive for certain threat models but may be less convenient at scale than mixing combined with cross-chain swaps and centralized exchange cash-out.

Zcash's optional privacy model illustrates a related trade-off: it can be used privately, but if shielded usage is rare and interactions are patterned, anonymity can degrade. Monero offers mandatory privacy, but its integration into regulated off-ramps is often constrained. These frictions help explain why illicit actors commonly use a hybrid approach—mixing on highly liquid chains, rapid cross-chain movement, and strategic use of venues with weak compliance—rather than relying exclusively on a single privacy coin.

### *3.2.4 Bridges, stablecoins, and 'composability laundering'*

DeFi's composability enables a laundering strategy that can be described as 'composability laundering': an actor chains together swaps, bridges, mixers, and centralized off-ramps in a sequence that is individually commonplace but collectively opaque. Bridges are particularly consequential because they convert assets between chains, often breaking investigative continuity when different ledgers have different observability and different compliance ecosystems. Stablecoins can also function as a risk-transfer instrument: if a stablecoin issuer has freeze authority and enforces sanctions, the stablecoin may be a control point; if illicit proceeds remain in non-freezable assets or move across chains before stablecoin conversion, the window for intervention can be narrow.

From a policy perspective, this suggests that focusing only on one AET (e.g., mixers) may miss the broader laundering architecture. The objective is therefore to identify the minimal set of chokepoints that consistently appear across pipelines—often centralized off-ramps and key infrastructure—while recognizing that attackers can re-compose pipelines when a chokepoint tightens.

### *3.2.5 What the evidence base can and cannot establish*

Public reporting on AET use for illicit finance is uneven. Official documents (e.g., U.S. Treasury risk assessments and OFAC press releases) can provide credible signals about observed laundering typologies, but they often omit methodological details for operational reasons. Law enforcement and FIU reporting may also be episodic, focusing on prominent cases. In parallel, technical research can measure protocol properties and traceability limits, but it cannot always connect those properties to real-world sanction-evasion outcomes.

To manage these limitations, this paper treats official enforcement narratives as evidence of policy salience and observed typologies, not as exhaustive measurement. For broader threat context, Europol's IOCTA reporting and similar assessments are used to frame the evolving role of crypto assets in organized crime and cyber-enabled laundering, while recognizing that such reports aggregate diverse national inputs and do not isolate DeFi mechanisms with precision. These constraints reinforce the value of a mechanism-based approach: even when totals are uncertain, the causal pathway from privacy mechanism to reduced observability can be analyzed with technical clarity. (Europol, 2024).

### *3.2.6 Security incidents, MEV, and laundering opportunities*

Large-scale cyber theft is a primary upstream driver of laundering demand. In DeFi, exploits can occur through smart-contract vulnerabilities, governance failures, key compromise, or bridge design weaknesses. These incidents interact with AETs in two ways. First, attackers need rapid conversion and obfuscation pathways to reduce interdiction risk immediately after an exploit. Second, the same ecosystem features that enable MEV and adversarial transaction ordering—documented in the literature on

frontrunning and miner/maximal extractable value (MEV)—also illustrate how transaction execution is strategic rather than neutral in DeFi, complicating monitoring and incident response. (Daian et al., 2019).

While MEV research is not primarily an illicit-finance literature, it supports a broader claim: DeFi is a security-sensitive environment where adversaries adapt rapidly and where protocol-level incentives can produce behavior that undermines fairness and predictability. For sanctions and AML, this means that ‘static’ rule sets will be outpaced unless enforcement is adaptive and focused on durable chokepoints. (Daian et al., 2019).

### 3.3. Enforcement architecture under stress: Tornado Cash as a legal and policy case study

#### 3.3.1 *The Fifth Circuit decision and the ‘autonomous code’ problem*

The Fifth Circuit’s decision in *Van Loon v. Department of the Treasury* directly addressed whether immutable smart contracts associated with Tornado Cash could be treated as “property” subject to blocking under IEEPA-based sanctions authorities. The court’s reasoning (whatever one’s normative view) is significant for policy design: it underscores that sanctions frameworks built around persons, entities, and property may not map cleanly onto autonomous software that lacks a traditional owner/operator relationship. (*Van Loon v. Department of the Treasury*, 2024).

#### 3.3.2 *Delisting and its implications for future tools*

In March 2025, OFAC removed Tornado Cash from the SDN List. The delisting does not imply that laundering risk disappeared; rather, it reflects a re-alignment between enforcement posture and the legal/institutional constraints clarified by litigation and related policy considerations. For compliance practitioners, the key implication is that enforcement strategies may increasingly focus on controllable layers: hosted services, identifiable operators, relayers that provide transaction services, centralized exchanges, stablecoin issuers, and other infrastructure that can implement screening and blocking. (U.S. Department of the Treasury, 2025; OFAC, 2025).

#### 3.3.3 *What sanctions can and cannot do in DeFi*

Sanctions remain a powerful tool for shaping risk at interfaces and off-ramps. However, sanctions are not a substitute for technical or governance measures that reduce the ability of illicit actors to exploit protocol design. The Tornado Cash episode suggests a need for more discriminating interventions—targeting identifiable service provision (e.g., relayers or hosted front ends) and downstream integration points—rather than attempting to treat autonomous code as a conventional sanctions target.

#### 3.3.4 *The compliance lesson: code is hard to ‘block,’ services are easier*

A practical compliance lesson from the Tornado Cash episode is that sanctions enforcement scales more reliably against services and infrastructure than against immutable contracts. Front ends can be taken down or geoblocked; relayers and hosting providers can be compelled or can voluntarily restrict service; exchanges can refuse deposits linked to high-risk contracts; and issuers of centralized stablecoins can freeze funds. These interventions do not eliminate privacy tools but they reshape the risk surface: they reduce the convenience of laundering and increase the probability that illicit actors must touch a regulated perimeter at some point.

At the same time, an overly broad approach can create false positives and collateral damage. For example, autonomous contracts can be used by legitimate users for privacy and security reasons; indiscriminate screening may lead to ‘taint’ concerns that trap innocent users. A mature compliance posture therefore requires more granular risk indicators—combining typologies, timing, interaction patterns, and known threat-actor infrastructure—rather than simple address blocking.

#### 3.3.5 *Substitution, displacement, and the risk of policy whack-a-mole*

A recurrent enforcement risk is displacement: restricting one tool may push illicit actors toward alternatives rather than eliminating laundering. Mixers can be substituted by other mixers, by cross-chain swaps that fragment tracing, or by privacy coins where off-ramps exist. Likewise, if exchanges tighten

controls, actors can shift to OTC brokers or to jurisdictions with weaker enforcement. This is not an argument against enforcement; it is an argument for defining success realistically. The measurable objective is often to increase friction, reduce scalability of laundering pipelines, and create actionable intelligence at conversion points.

### 3.4. Regulatory baseline: FATF and U.S. financial-crime authorities

#### 3.4.1 FATF standards and the ‘DeFi gap’

The FATF framework remains the primary international baseline for AML/CFT treatment of virtual assets. In its guidance and targeted updates, FATF has consistently pushed for (i) extending AML/CFT obligations to virtual asset service providers (VASPs), (ii) implementing the ‘travel rule’ for relevant transfers, and (iii) closing gaps created by decentralization narratives that obscure responsible persons. A recurring theme in FATF updates is that decentralization does not automatically remove accountability: where a natural or legal person has ‘sufficient influence’ or provides services that enable transfers (e.g., operating an exchange interface or exercising control over a protocol), that actor may fall within AML obligations. At the same time, FATF acknowledges that some arrangements may lack clear intermediaries, creating supervision and enforcement challenges. (FATF, 2024; FATF, 2025).

These standards become practically relevant in DeFi because compliance is frequently fragmented: token issuance may be centralized while trading is decentralized; stablecoins may have a centralized issuer while liquidity provision is decentralized; bridges may be operated by identifiable validator sets while user access is permissionless. The result is regulatory arbitrage potential. Sophisticated illicit actors exploit the seams between these layers, moving value across protocols that are each only partially within the regulatory perimeter. (FATF, 2025).

#### 3.4.2 FinCEN: mixers as a money-laundering concern

In the United States, FinCEN has treated mixing as a recurrent money-laundering typology and has issued guidance and advisories clarifying how Bank Secrecy Act obligations apply to certain virtual currency business models. FinCEN has also pursued rulemaking that frames ‘convertible virtual currency mixing’ as a class of transactions of primary money-laundering concern, signaling a willingness to use strong regulatory levers against mixing activity. While the precise scope and final form of these measures depend on legal process and implementation, the policy direction is clear: U.S. financial-crime authorities view mixing as a high-risk function regardless of whether it is provided by a custodial service or via decentralized infrastructure. (FinCEN, 2019a, 2019b, 2023).

## 4. DISCUSSION: MITIGATION OPTIONS AND TRADE-OFFS

Mitigation approaches fall into four categories. (U.S. Department of the Treasury, 2023).

(1) Entry and exit controls. The most consistently feasible controls remain at centralized exchanges, custodians, stablecoin issuers, and fiat gateways. Improved sanctions screening, transaction monitoring informed by typologies, and coordinated information sharing can meaningfully reduce integration opportunities for illicit proceeds. These measures do not eliminate mixing or privacy coins, but they raise the cost of cash-out.

(2) Infrastructure-layer interventions. In DeFi, many user interactions occur through web front ends, API providers, RPC endpoints, relayers, and bridge operators. These actors can implement risk controls (blocking sanctioned addresses, refusing to relay transactions, or limiting exposure to high-risk contracts) even when the underlying contracts are immutable. The limitation is evasion: users can self-host interfaces or route through alternative infrastructure. Nevertheless, infrastructure interventions can reduce scale and convenience.

(3) Protocol-level design choices. Some protocols can incorporate compliance-enabling features without surrendering non-custodial design—for example, optional compliance modules, circuit-breaker controls for known exploit patterns, or disclosure-selective privacy mechanisms. These approaches are

unevenly applicable, and they can conflict with the ideological and competitive pressures in DeFi. Still, they are more durable than purely external controls when adopted.

(4) Legal clarity and accountability. Where there are identifiable developers, operators, or service providers, legal accountability can complement technical controls. The challenge is to distinguish legitimate privacy engineering from intentional facilitation of money laundering. Overbroad liability could chill security research and legitimate privacy use. A workable regime therefore needs definitional precision and safe harbors for good-faith development and security work.

The trade-off is not privacy versus security in the abstract, but which forms of privacy and which threat models are being prioritized. Some privacy uses (protecting donors or vulnerable users) are socially valuable; other uses (laundering sanctioned proceeds) are socially harmful. Policy responses that treat all privacy as suspect risk both ineffectiveness (driving activity to less visible venues) and collateral damage (weakening digital security and civil liberties). The mitigation agenda should therefore be anchored in measurable risk reduction and in targeted interventions where control is feasible.

#### (5) Privacy-preserving compliance concepts

A growing research and policy conversation explores whether privacy and compliance can co-exist through selective disclosure. Examples include ‘view keys’ or audit keys (allowing a user to disclose transaction details to a regulator or counterparty under defined conditions), zero-knowledge ‘proof-of-innocence’ concepts (proving funds are not derived from a sanctioned set without revealing full history), and regulated disclosure at conversion points (e.g., requiring enhanced due diligence for shielded or mixed funds when entering a custodial platform). These ideas are not yet uniform in implementation, but they matter because they shift the debate from a binary ‘privacy versus enforcement’ frame to an engineering-and-governance frame. (FATF, 2024).

Any privacy-preserving compliance design must be evaluated against attacker adaptation. If disclosure mechanisms can be bypassed by avoiding the regulated perimeter, they become relevant primarily at off-ramps. But even then, they can raise the expected cost of illicit finance while preserving legitimate privacy for low-risk users.

## 5.CONCLUSION

This article analyzed how three AET exemplars—Tornado Cash, Monero, and Zcash—create forensic friction that can be operationalized for sanctions evasion and the financing of national-security threats. The central claim is mechanism-based: privacy tools change observability and attribution, which in turn changes the cost and feasibility of enforcement. Yet the analysis also shows that AET effectiveness is conditional. Mixers depend on liquidity and timing; Zcash privacy depends on shielded-pool adoption; Monero privacy is strong but not absolute and is constrained by off-ramp availability.

The Tornado Cash enforcement episode illustrates a second conclusion: sanctions and AML frameworks built around intermediaries struggle when the target is autonomous code. The policy response that scales is therefore likely to be layered—entry/exit controls, infrastructure-layer risk management, selective protocol design choices, and clearer legal boundaries—rather than a single “ban” or a single compliance fix. For journal publication, these conclusions imply that scholarship should move beyond generic claims about DeFi “risk” and instead specify which mechanisms, which choke points, and which institutional constraints are decisive.

Answering the research questions explicitly: RQ1 is addressed by showing that each AET undermines deterministic attribution through distinct mechanisms, with conditional effectiveness. RQ2 is addressed by synthesizing official enforcement and risk-assessment materials that link AETs—especially mixing—to laundering typologies used by state-linked actors, while acknowledging measurement limits. RQ3 is addressed through the Tornado Cash case, illustrating both the reach and the constraints of sanctions when applied to autonomous code. RQ4 is addressed by a layered mitigation portfolio that prioritizes interfaces, off-ramps, infrastructure, and privacy-preserving compliance design rather than expecting protocol-level prohibition to succeed.

## REFERENCES

- Aramonte, S., Huang, W., & Schrimpf, A. (2021). DeFi risks and the decentralisation illusion. *BIS Quarterly Review* (December 2021). Bank for International Settlements. Retrieved from: [https://www.bis.org/publ/qtrpdf/r\\_qt2112b.pdf](https://www.bis.org/publ/qtrpdf/r_qt2112b.pdf)
- Brownworth, D., Durfee, Z., Lee, M., & Martin, A. (2024). Regulating decentralized systems: Evidence from sanctions on Tornado Cash (Staff Report No. 1112). Federal Reserve Bank of New York. <https://doi.org/10.59576/sr.1112>
- Chainalysis. (2024). The 2024 Crypto Crime Report. Chainalysis. Retrieved from: <https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/>
- Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., Breidenbach, L., & Juels, A. (2019). Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges. *ArXiv, abs/1904.05234*.
- European Union Agency for Law Enforcement Cooperation (Europol). (2025). Internet Organised Crime Threat Assessment (IOCTA) 2025. Europol. Retrieved from: <https://www.europol.europa.eu/publications-events/main-reports/iocta-report>
- FATF (2024), Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs, FATF, Paris, France, <https://www.fatf-gafi.org/>
- FATF (2025), Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs, FATF, Paris, France, <https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/targeted-update-virtualassets-vasps-2025.html>
- Financial Crimes Enforcement Network. (2019a). Application of FinCEN's regulations to certain business models involving convertible virtual currencies (FIN-2019-G001). U.S. Department of the Treasury. Retrieved from: <https://www.fincen.gov/system/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf>
- Financial Crimes Enforcement Network. (2019b). Advisory on illicit activity involving convertible virtual currency mixers (FIN-2019-A003). U.S. Department of the Treasury. Retrieved from: <https://www.fincen.gov/system/files/advisory/2019-05-10/FinCEN%20Advisory%20CVC%20FINAL%20508.pdf>
- Financial Crimes Enforcement Network. (2023). Proposal of special measure regarding convertible virtual currency mixing as a class of transactions of primary money laundering concern (FINCEN-2023-0016) (Notice of proposed rulemaking). U.S. Department of the Treasury. Retrieved from: <https://www.federalregister.gov/documents/2023/10/23/2023-23449/proposal-of-special-measure-regarding-convertible-virtual-currency-mixing-as-a-class-of-transactions>
- Kappos, G., Yousaf, H., Maller, M., & Meiklejohn, S. (2018). An empirical analysis of anonymity in Zcash. In *Proceedings of the 27th USENIX Security Symposium* (pp. 463–477). USENIX Association. Retrieved from: <https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-kappos.pdf>
- Möser, M., Soska, K., Heilman, E., Lee, K., Heffan, H., Srivastava, S., Hogan, K., Hennessey, J., Miller, A., Narayanan, A., & Christin, N. (2018). An empirical analysis of traceability in the Monero blockchain. *Proceedings on Privacy Enhancing Technologies*, 2018(3), 143–163. <https://doi.org/10.1515/popets-2018-0025>
- Noether, S., & Mackenzie, A. (2016). Ring confidential transactions. *Ledger*, 1, 1–18. <https://doi.org/10.5195/LEDGER.2016.34>

- Schär, F. (2021). Decentralized finance: On blockchain- and smart contract-based financial markets. *Federal Reserve Bank of St. Louis Review*, 103(2), 153–174. <https://doi.org/10.20955/r.103.153-74>
- U.S. Department of the Treasury, Office of Foreign Assets Control. (2022). U.S. Treasury sanctions notorious virtual currency mixer Tornado Cash. U.S. Department of the Treasury. Retrieved from: <https://home.treasury.gov/news/press-releases/jy0916>
- U.S. Department of the Treasury, Office of Foreign Assets Control. (2025). Cyber-related designation removal: Tornado Cash. U.S. Department of the Treasury.
- U.S. Department of the Treasury. (2023). Illicit finance risk assessment of decentralized finance. U.S. Department of the Treasury. Retrieved from: <https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf>
- U.S. Department of the Treasury. (2025). Treasury delists Tornado Cash. U.S. Department of the Treasury. Retrieved from: <https://home.treasury.gov/news/press-releases/sb0057>
- Van Loon v. Department of the Treasury, No. 23-50669 (5th Cir. 2024). Retrieved from: <https://law.justia.com/cases/federal/appellate-courts/ca5/23-50669/23-50669-2024-11-26.html>

# FINANCIAL SECURITY AS A KEY ELEMENT SUPPORTING SUSTAINABLE BUSINESS DEVELOPMENT – A THEORETICAL APPROACH

Urszula Szczytyńska  
Państwowa Uczelnia Zawodowa im. prof. Stanisława Tarnowskiego  
Tarnobrzeg, Poland  
<https://orcid.org/0009-0000-3980-2113>  
[uszczytynska@poczta.onet.pl](mailto:uszczytynska@poczta.onet.pl)

**Abstract.** *The main objective of this article is to demonstrate the importance of financial security for supporting the sustainable development of an enterprise. A review of the definitions of financial security was conducted, emphasising its multifaceted nature, properties and functions, and indicating the tools and instruments that enable its effective management. The article demonstrates that financial security guarantees the continuity and development of a company, supports the long-term planning process and protects the company from internal and external threats. The theoretical analysis confirms the hypothesis that financial security is a key condition for the implementation of the concept of sustainable development.*

**Keywords:** financial security, financial stability, sustainable development.

## 1. INTRODUCTION

Sustainable development of an enterprise is currently one of the key categories of management, integrating economic, social and environmental goals. It means a way of functioning of an organisation which, in addition to striving to maximise current economic results, also takes into account social responsibility and rational management of environmental and natural resources. The goal of development understood in this way is not only to achieve short-term benefits, but also to ensure a sustainable basis for generating value in the future, based on the implementation of long-term strategic goals that take into account the protection of natural resources and the achievement of social goals. This goal can be achieved through an adequate level of financial security, which ensures the protection of the company's financial interests and the organisation's ability to maintain liquidity, resilience to crises and effective risk management. Financial security is therefore a fundamental condition for the implementation of the concept of sustainable development of the company.

Financial security, understood as a financial guarantee of the organisation's existence and development, which is reflected in its ability to maintain financial liquidity, solvency, profitability and operational efficiency, creates space for development, innovation and pro-environmental investments. It also allows for the creation of a competitive advantage based on stability, credibility and responsible use of resources. The concept of sustainable development, which emphasises the integration of economic, social and environmental perspectives, requires companies not only to be operationally efficient, but also to be able to minimise risk and build systemic resilience, i.e. elements directly related to financial security.

The aim of this article is to present a theoretical approach to financial security as a key mechanism supporting the sustainable development of organisations. It attempts to show the relationship between financial stability and a company's ability to implement long-term strategies, including both economic development and social and environmental responsibility. The research hypothesis was formulated as follows: it is assumed that financial security is a key condition for the implementation of the concept of sustainable development of enterprises.

## 2 MATERIALS AND METHODS

The article is theoretical in nature and was developed on the basis of available literature on corporate financial security, financial stability and the concept of sustainable development of organisations. The research material included domestic and foreign scientific publications, including monographs, scientific articles, reports of financial institutions and review studies, which enabled the identification and analysis of existing definitions and theoretical approaches to financial security. The research process used methods characteristic of theoretical analyses, including:

- analysis of the literature on the subject, focused on identifying key concepts, definitions and theoretical approaches related to financial security in finance and management sciences;
- comparative analysis, allowing for the comparison and evaluation of differences and similarities in interpretations of the concept of financial security;
- a synthesis method, allowing for the development of our own interpretation of the concept of corporate financial security and indicating its significance in the context of sustainable development.

## 3. RESULTS

Financial security is a strategic factor in an entity's operations, especially in a volatile environment. In the face of geopolitical instability and changes in the macro- and microeconomic environment, it needs to be analysed in relation to internal and external conditions. Financial security in an external context should be considered in macroeconomic terms, taking into account, among other things, the security of the competitive environment of the entity and the political, economic and social realities in which it operates. Internally, it is shaped primarily by determinants related to the functioning of the entity itself, such as stability, independence and financial freedom, capital and cost structure, and also the entity's capacity for strategic development. It can therefore be assumed that when defining financial security in macroeconomic terms, we will treat it as the financial security of the state, while in microeconomic terms, we will treat it as the financial security of the enterprise.

The literature on the subject indicates that financial security is a component of economic security. At the state level, many threats characteristic of economic security are reflected in the financial sphere. These include:

- uncontrolled inflation or deflation;
- significant fluctuations in raw material and energy prices;
- high levels of debt and budget deficits;
- exchange rate fluctuations;
- irregularities in the functioning of public institutions and related financial losses;
- instability of legal regulations.

In the context of the company's operations, the following factors are of key importance:

- profitability and financial efficiency;
- financial liquidity and solvency;
- investment risk;
- loss of financial credibility;
- level of technological development.

Significant internal factors determining financial security include the competence and abilities of management, which determine the rationality of decisions made in the operational, investment and financial spheres of the entity. External factors, on the other hand, are related to the economic, social and environmental policy of the state, as well as the market and international situation in which the entity operates.

The relationship between economic and financial security was pointed out, among others, by Serhii F. Pokropywnyy (2001), as cited in Delas, Nosova, Yafinovich, (2015). He believed that the financial component is the leading element of a company's economic security, determining the functioning of its other components, such as intellectual, technical, technological, legal, IT and environmental resources.

When defining the financial security of a company, it is therefore impossible to ignore the economic security of the state and, in a narrower sense, the economic security of the company.

Krzysztof Michał Księżopolski summarises the numerous definitions of the economic security of the state into four categories:

- those whose conceptual framework is based on the concept of threat;
- those that start from threats but combine them with opportunities and possibilities for cooperation;
- those that highlight the country's ability to function and develop;
- unilateral, focused on a specific economic policy of the state, e.g. fiscal or monetary (Księżopolski, 2011).

The author of this classification defines economic security as (quote) "the undisturbed functioning of economies and the maintenance of comparative balance with the economies of other countries" (Księżopolski, 2013). Mariusz Badak treats it as (quote) "a state in which internal and external conditions for the functioning of the state without major disruptions are ensured" (Badak, 2010). Marek Leszczyński sees the sources of challenges and threats to economic security in, among other things, the internal system of a given state and the barriers limiting it, as well as negative external actions that affect the stability of the state system, disrupting its economic development and defence potential (Leszczyński, 2022). Edward Halizak, on the other hand, refers to the economic security of a state as a situation of threat to the security of the national economy, which (quoted) "cannot develop, generate profits and savings for investment, or when external threats lead to disruptions in its functioning, which will put citizens and businesses at risk and possibly threaten the physical survival of the state" (Węgrzyńska, 2025). In these definitions, the term economic security refers to values considered important to the state, but not necessarily under its direct control.

Economic security is therefore a combination of factors contributing to economic development and factors limiting it, e.g. the state and structure of the economy, economic relations with other countries, economic sovereignty, defence potential, level of competitiveness and innovation (Leszczyński 2022). It is characterised by: (quote) "stability, certainty, attitude towards challenges from the external environment, relations with the external environment, links with foreign partners, the role of the market and the state" (Kurek, 2000).

As previously indicated, one of the pillars of economic security of an enterprise, currently considered the most important, is financial security. Konrad Raczkowski believes that financial security is a component of economic security, fits into the security of the state and includes financial stability in its definition (Raczkowski, 2014). In a hierarchical system, starting with a top-down classification, Konrad Raczkowski lists: state security – economic security – financial security – financial stability. He therefore considers financial security to be an element of economic security and state security. Following the line of thinking of the quoted author (cit.), "financial security is a process of constantly limiting and eliminating monetary risk in order to secure capital adequacy that will be adapted to the risk profile and preferences of a given entity or unit" (Raczkowski, 2014a). It can therefore be assumed that it is a financial guarantee of the existence and development of an entity, which is shaped by many years of concern for the appropriate level of measures for undisturbed development.

It is not possible to pursue an effective state economic security policy without stably developing enterprises. Economically stable economic entities, prepared to respond to changes in the external environment, are an important element of state economic security, especially in the context of geopolitical conflicts, dynamic technological development and climate change.

The concept of economic security of an enterprise is a complex one, covering both internal and external aspects of its operations. This concept has evolved, changing under the influence of factors or threats that have affected the operations of enterprises. Initially, views on the essence of economic security of enterprises focused on issues related to the protection of trade secrets (1991-1997). In subsequent years, they focused on: the role of the state in ensuring it (1998-1999); recognising the threats of a narrow business profile (1999-2001); identifying external and internal threats in relation to the functional components of economic security (1999-2002); effective functioning in a situation of risk and adaptation (2002-2005); identifying external and internal threats specific to the industry represented by the enterprise (2005-2013); interaction of the company and its business processes with the external

environment and its threats (since 2014 and continuing) (Britchenko, 2024). Changes in the definition of economic security resulted from the risks and threats affecting the company. According to Igor Britchenko, companies themselves were forced (quote) "to significantly change their approach to managing their own business processes and market behaviour in order to ensure that their economic activity was compatible with the existing barriers to their development" (Britchenko 2024). The above classification of the concept of economic security of an enterprise thus proves the existence of a link between economic security and threats. In the context of numerous internal and external threats, the economic security of an enterprise can be seen as its ability to overcome and neutralise them.

Given the fundamental importance of financial aspects in the process of overcoming threats, an in-depth analysis of the concept of financial security is necessary. An analysis of numerous definitions of this concept indicates that it is perceived as the level of financial relations that will ensure the protection of the interests and needs of the enterprise, protection against threats, continuity of operations, guarantee of existence and development, implementation of financial strategies, liquidity and solvency. The differences in the definitions of corporate financial security provided by researchers are presented in Table 1.

**Table 1. Selected definitions of corporate financial security**

<b>Dominant aspect of the definition</b>	<b>Author</b>	<b>Definition</b>
<b>Strategic aspect – protection of financial interests, meeting the current needs of the enterprise and its development</b>	A. Baranowski	The degree of protection of financial interests at all levels of financial relations or support from financial resources sufficient to meet the needs of the enterprise and repay its liabilities.
	A.N. Duraj	All conditions/processes of acquiring and using financial resources to ensure the continuity of the company's operations and conditions for its development.
	L. Karbownik	A financial guarantee of the existence and development of a business entity, which is possible as a result of the continuous efforts of managers to ensure good financial condition and business development in a competitive market.
	A. Zagorodni	Protection of the financial interests of economic entities at all levels of financial relations, using financial resources sufficient to meet their needs and fulfil their obligations.
	O. Kiritchenko	The financial situation and financial stability necessary to ensure the effective development of a company's activities.
<b>Risk aspect – identification and counteracting potential threats</b>	A. Chupis K. Kashenko	A complex concept that prevents the negative impact of factors related to internal and external threats
	I. Britchenko	The state of a company in which it has sufficient financial resources and effective mechanisms for managing them, allowing it to ensure stability, liquidity and resilience to crises and risks.
	K. Raczkowski	The process of continuously reducing and eliminating monetary risk in order to secure capital adequacy that is tailored to the risk profile and preferences of a given entity.
	L.A. Zaporozhtseva	Stable protection of the company's production and financial activities against real and potential internal and external threats in order to ensure stable development.
	M. Medvid	A state of economic development characterised by the possession of the financial resources necessary to meet market requirements, protect financial interests, overcome financial crises, and ensure the protection of financial interests and effective functioning.
<b>Stability aspect – financial stability and ability to continue operations</b>	D. Wędzki	The higher the surplus of current assets over short-term liabilities (net working capital), the greater the financial security.
	I. Melnik	Financial security is related to ensuring financial stability and neutralising financial risk.
	E. Nowak	The ability of an economic entity to continue its operations is the result of the future real value of balanced inflows and outflows. Therefore, in assessing the financial security of an

		enterprise, it is assumed that the entity does not intend to and cannot cease its economic activity or significantly reduce its scope.
	M. Zuba	Ability to maintain liquidity and financial solvency.
	I. Franc-Dąbrowska	Ability to maintain financial liquidity and high efficiency.
<b>Efficiency aspect</b> effective management of financial resources.	I. Pogusowa	This is a state of the enterprise that ensures the optimal acquisition and effective use of the enterprise's financial resources, which allows for the design and implementation of a financial strategy, and the identification and resolution of situations of risk and danger. This state must be assessed by quantitative and qualitative indicators with limit values.
	P. Lebedieva	
	W. Witliński	

Source: created by the author

A review of the literature on the subject allows us to conclude that financial safety is a multifaceted and complex concept. The authors cited define it by emphasising its different aspects - as the potential of an enterprise to counteract events that disrupt its operational and strategic functioning, or as a process of neutralising threats, providing an opportunity to continue operations and ensuring its existence. They treat financial security as a specific state of economic development of an enterprise, which will provide it with the financial resources necessary to meet market requirements, ensuring effective functioning and efficient use of resources, in which effective mechanisms for warning against threats and systems for neutralising their effects are in place.

Financial security can therefore be defined as the state of an economic entity's functioning, determining its current potential and development opportunities, ensuring balance, stability, solvency and liquidity in the long term. This state ensures flexibility in decision-making, allows for the design and implementation of a financial strategy, and protects the interests of owners. This state can be achieved when a company ensures its current stability, i.e. a state of financial resources, which ensures the fulfilment of current operational needs and the repayment of liabilities. However, viewing financial security solely as a desirable state of functioning of an entity requires supplementing it with a perspective of threats, which is a significant negative factor hindering the achievement of the company's operational and strategic goals and threatening its financial security. According to researchers, the basic condition for achieving financial security is the company's ability to counteract threats and barriers that cause financial losses and adverse changes in the capital structure. A company should effectively identify sources of threats and risks that arise at all levels of management in order to effectively protect the operational and financial stability of the company. This understanding of corporate financial security was presented, among others, by Konrad Raczkowski, Igor Britchenko and Mykhailo Medvid, cited in Table 1. Financial stability accompanies financial security and is (quote) "a condition of financial security, and conversely, financial security determines financial stability" (Kowalska & Misztal, 2020). In macroeconomic terms, according to Andrew Crockett, financial stability refers to the stability of key institutions and markets that make up the financial system (Crockett, 1997).

Financial security therefore means a situation in which a company is not exposed to the risk of losing its ability to continue operating on the current scale and to achieve its development goals. Therefore, it is crucial to identify the factors that determine the level of financial security of a company. These factors can be divided into internal and external, with their mutual interaction also playing an important role. According to Ireneusz Kraś, Mirosława Capiga and Ireneusz Micuła, external factors are those that determine the financial security of the state. Ireneusz Kraś includes among them: the security of financial institutions, financial transactions, financial market segments and customers of this market (Kraś, 2013). Mirosława Capiga believes that they are the elements that make up a country's financial security network, i.e. the government (mainly the Ministry of Finance), the central bank, financial supervisory institutions, deposit guarantee schemes and systems (Capiga, 2010). Ireneusz Micuła (2013) calls them macroeconomic factors and includes the following: the level of economic and social development, interest

rates, inflation, trade balance, fiscal system, monetary policy, currency stability and legal regulations. Due to their nature, exogenous factors are beyond the control of the company and are not directly controllable. However, their impact can significantly determine the effectiveness of decision-making processes and financial results.

According to Ireneusz Micuła, internal conditions include: the type of industry in which the company operates, the amount and structure of its assets and capital, sources of investment financing, the company's financial and asset situation, the level of technological and intellectual development, knowledge, entrepreneurship and rationality of staff, relations with the environment and the risk of business activity (Micuła 2013). Internal determinants are therefore directly related to the way the company is managed, and also depend on the managerial skills and rational and effective decisions made by this level of management at the operational and financial levels. It should be noted that both factors are intertwined, which means that in the context of modern globalisation, competitiveness and internationalisation, taking action in the area of financial security requires advanced knowledge of both the processes taking place within the company and its broadly understood environment.

As mentioned earlier, many researchers view financial security as a key factor determining the financial condition and ability of a company to continue its operations. Bartłomiej Nita, Angelika Kaczmarczyk and Piotr Oleksyk classify the factors threatening the ability to continue operations as financial and operational, internal and external (Nita, et al., 2020). Financial factors include, among others: unfavourable key financial indicators, excessive net liabilities, lack of financial liquidity, exceeding credit limits, inappropriate structure of long-term asset financing, negative cash flows, changes in the method of settlement with contractors, lack of funds for investments, including replacement investments, inability to finance development activities. Among the internal operational conditions that pose a threat to the continuation of operations and good financial condition, the authors cite, among others: improper management, imperfections in the area of human resources policy, overinvestment, shortage of important raw materials, loss of markets, strong dependence on key customers or products, risky technological changes, lack of adequate mechanisms to protect against the effects of extraordinary events. The researchers included the following in the group of external operational factors that have a significant impact on the entity's operations but are independent of management actions: changes in legal regulations, unfavourable outcomes of pending court and administrative proceedings, threats arising from market competition, and operating in sectors exposed to systematic risk.

Protection against threats to financial health and business continuity is part of a process-based, dynamic approach to corporate financial security. This approach does not exclude a static interpretation of financial security as a specific state of equilibrium. Financial security in static terms is a state that creates a sense of certainty about functioning and development and guarantees their preservation. These guarantees are not permanent or certain, as they do not provide sufficient protection against crisis situations and their negative impact on the company's operations. Nor do they provide sufficient conditions for development and business continuity. However, this is not the most important aspect in this approach. The static approach to security focuses on the current state of material resources and the structure of financial resources, rather than on their resilience to threats and disruptions related to operational activities. Financial security understood in this way is the current ability of a company to achieve profitability, solvency, liquidity, the potential to invest, create reserves and forecast bankruptcy. This approach is represented by Iryna Melnik and Dariusz Wędzki, quoted in Table 1. A similar position is also taken by Henryk Wnorowski, who defines it as the ability of a company to (quote) "function efficiently in the current competitive situation" (Wnorowski 2020).

The presented analysis of the definition of a company's financial security points to several important characteristics of this economic category:

- maintaining the balance, flexibility and financial stability of the enterprise;
- supporting the effective use of its material and financial resources;
- enabling early identification of potential financial threats;
- mitigating the effects of crises and increasing resilience to unforeseen external and internal events.

Since security is a category dependent on many factors, systematic and conscious management of it becomes crucial. A financial security management system should be a comprehensive mechanism

comprising the following elements: (quote) "assessment of the financial situation, forecasting and effective financial planning, rational financial management, risk assessment and risk management, monitoring and financial control" (Kowalska & Misztal, 2020). It is advisable for a company to assess its financial situation based on data analysis using internal and external reporting systems and financial reports. It is reasonable to develop mechanisms for controlling costs, revenues, cash flows, and a set of financial indicators and alarm thresholds, which will form the basis for analyses and create an early warning system for threats. It is important to plan for regular reporting on the financial situation in terms of liquidity and cash management (including the preparation of a settlement schedule). As part of rational financial management, it is also important to monitor the capital structure, its cost and risk, and the strategy for financing short-term and long-term activities. This is important because financial security cannot be considered solely on the basis of historical data, but also from the perspective of adaptability and projected changes.

It is recommended that the financial security management mechanism also include the identification and assessment of financial risks, including the monitoring of external factors affecting financial stability. Potential risks, such as credit, currency, market, investment, geopolitical and other risks, should be analysed not only in terms of their sensitivity and potential impact on financial security, but also in the context of developing an adequate hedging policy.

In order to ensure an adequate level of financial security, management should implement the following organisational measures (Delas et al., 2015, p.). - Create an information base to diagnose the current financial situation;

- Identify the determinants of the organisation's functioning;
- Conduct an analysis and assessment of the situation and financial position;
- Develop development plans and forecasts, determine the means for their implementation, and conduct ongoing monitoring, control and evaluation;
- Eliminate or minimise risks and streamline decision-making processes to increase organisational effectiveness.

Igor Blank proposes that the following aspects should also be taken into account when determining the financial security mechanism (Blanc 2013):

- Priorities of financial interests, previously defined by the company;
- A system of quantitative and qualitative indicators that will enable the level of protection against threats to be determined;
- Reference values for financial indicators used to assess the level of security, taking into account the current and strategic financial interests of the company;
- Macro- and microeconomic environmental factors that may represent potential opportunities and threats for the company.

It is important that the measures taken are systematic and multi-level in nature, and are carried out at both the operational and strategic levels. The implementation of these measures and the development of a mechanism for managing the company's financial security can provide significant support in formulating the company's financial strategy in line with its adopted objectives and tactical tasks. Its development requires an analysis of the current financial situation, a reliable economic and financial forecast, an adequate level of material and financial resources, and a consistent monitoring and control mechanism. It is reasonable to use appropriate methods and financial instruments for this purpose. Financial methods should take into account (Delas et al., 2015): financial reporting, identification of relationships with external and internal stakeholders, financial analysis, financial planning and forecasting, financial stimulation and regulation, risk assessment, and monitoring. Financial analysis based on the financial reporting system allows for the diagnosis of the financial situation using quantitative and qualitative methods and tools. Financial forecasting makes it possible to set realistic long-term financial goals and plans, assess potential risks, create crisis scenarios, and make management decisions regarding investment, capital raising, and budgeting. In addition, the use of financial regulation and stimulation methods allows staff to be actively involved in financial security management mechanisms.

The instruments (financial tools) that a company can use to ensure financial security include, among others: loans, leasing and other forms of external financing, dividend policy, insurance, pricing policy, cost

management activities, market risk mitigation activities, and the use of the tax shield effect. Euvgenia Nosova, Vitalina Delas and Olena Yofinowych propose implementing them through the following levers: revenues, costs, financial results, expenses, capital, investments, insurance payments, interest rates, prices, salaries, depreciation, taxes, incentive and sanction systems, dividends, limits, reserves, and derivatives. The choice of elements that a company decides to use depends on its current financial situation and the intensity of risk factors that may lead to its deterioration.

When describing the financial security of a company, one cannot overlook the issue of the financial security of the state, which protects its financial interests through a system of legal regulations. Additionally, it is worth noting that the financial security of a company is an element of the financial security of the state, as companies contribute to GDP and, as taxpayers, generate a significant part of budget revenues, which affects the state's ability to fulfil its tasks and settle its liabilities.

Zenon Stachowiak, Ryszard Wierzba and Krzysztof Jajuga also draw attention to the area of financial system security and financial stability in macroeconomic terms. According to Zenon Stachowiak, in external terms, financial security is perceived in the context of a country's foreign debt, while in internal terms it is perceived as the efficiency of the public finance system in financing the national economy and pursuing national interests through financial institutions (Stachowiak & Stachowiak, 2016). Ryszard Wierzba defines financial security as (quote) "a set of institutional links and legal regulations aimed at protecting the financial system from destabilisation" (Wierzba, 2005). Krzysztof Jajuga treats it somewhat more broadly, referring to the concept as, or the absence of threats in the sphere of public and private finances, banks, insurance companies and enterprises (Jajuga, 2007). Mirosława Capiga, Witold Gradoń and Grażyna Szustak express similar views, defining it as a multidimensional concept concerning the security of financial institutions, the security of the operations of individual segments and customers of the financial market, and the security of transactions taking place on this market (Capiga et al., 2010). The following general definition of state financial security can therefore be adopted as (quote) "the entirety of legal regulations and self-regulation aimed at ensuring financial stability and protecting the interests of market participants using the services of financial intermediaries, as well as the entirety of institutions responsible for compliance with these regulations and self-regulation" (Iwanicz-Drozdowska, 2008). The definition emphasises the importance of another financial category, namely financial stability. The financial stability of the state mentioned by Małgorzata Iwanicz-Drozdowska is defined in the literature, among other things, as (quote) "a state of dynamic but long-lasting equilibrium in interpenetrating and interrelated financial markets". In order to effectively maintain a state in which there is no long-term loss of liquidity and insolvency of financial market participants, the stability of this market and the security of its participants, it is necessary to supervise the banking sector, the capital market, the insurance market, pension market, payment institutions, electronic money institutions, the cooperative credit union sector and lending institutions. In Poland, this role is fulfilled by a system of laws addressing the aforementioned financial sectors, the National Bank of Poland, the Bank Guarantee Fund and the Financial Supervision Authority. According to the National Bank of Poland, financial stability is (quote) "a state in which the financial system performs its functions continuously and effectively, even in the event of unexpected and adverse disturbances on a significant scale" (Report on the Stability of the Financial System, 2025). The report also states that disruptions to the financial system have an adverse effect on, among other things, the situation of enterprises.

It can therefore be assumed that a financially stable enterprise is one that achieves its objectives, continues to grow despite disruptions, raises capital and uses it appropriately in its operating, investment and financial activities (Ryś-Jurek, 2023, p. 18). On this basis, it can be assumed that the financial security of an enterprise is a type of financial strategy that is focused on ensuring the internal and external financial conditions for the effective continuation of its operations and development. On the one hand, this concept concerns the creation of conditions for the continuous and effective conduct of current activities, and on the other hand, it focuses on the development of economic activity, resulting in an increase in the market position and value of the company (Duraj, 2014). The literature on the subject therefore emphasises the interdependence between stability and financial security – both categories coexist and complement each other.

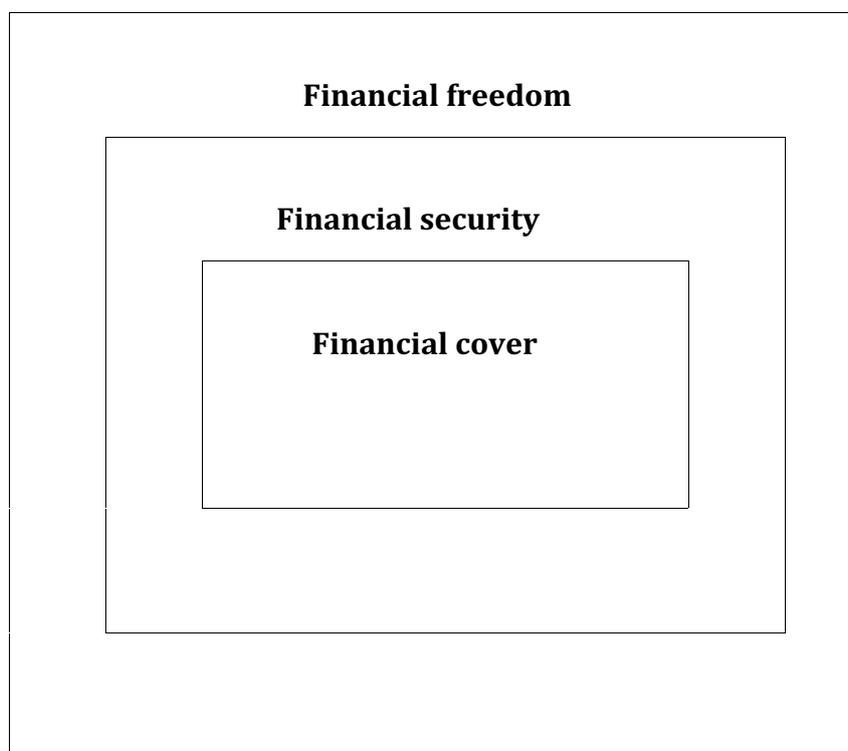
It cannot be overlooked that financial security is an important stage in shaping the financial independence of an enterprise (Figure 1). Lidia Karbownik points to three stages in which this process can take place (Karbownik, 2012):

Stage one – building a financial buffer in the form of financial resources that will enable the continuation of operations in the short term. This financial backing will cover current financial needs and may prevent bankruptcy in the short term;

Stage two – financial security, i.e. a state of financial resources that not only enables the continuation of operations, but also creates conditions for the development of the enterprise. According to L. Karbownik, this stage of building independence can prevent bankruptcy in the short and long term;

Stage three – financial freedom, i.e. a state of financial resources that not only ensures financial security, but also allows for the implementation of unplanned, effective investments, not necessarily directly related to the company's operating activities.

Fig. 1. Stages of building financial independence.



Source: Own study based on L. Karbownik L. (2012).

In this context, financial security is not only a guarantee of continued operation and development, but also a condition enabling free investment planning, independent financing of activities and long-term, stable development of the enterprise. It is a state of effective use of the enterprise's resources, ensuring the protection of its interests from internal and external threats.

After discussing financial security, which is a key condition for the stability of a company's operations, it is reasonable to present the concept of sustainable development. This concept was formally defined at the 1975 Session of the Governing Council of the United Nations Environment Programme. According to this definition, "sustainable development is the course of inevitable and desirable economic development that does not significantly and irreversibly damage the human environment, does not lead to the degradation of the biosphere, and respects the laws of nature, economics and culture" (Poskrobko, 1998). The idea of sustainable development is also aptly captured in a statement on the website of the Ministry of Development and Technology, which states that "sustainable development is development in which the needs of the present generation can be met without compromising the ability of future generations to meet their own needs" (Report of the World Commission on Environment and Development, 1987). Sustainable development is therefore a multidimensional approach to building

lasting value, aimed at balancing economic, social and environmental goals (Trojanowski, 2015). It is development that, to quote, "ensures: the effective use of resources, which allows for the maximisation of profit achieved by the organisation, the development of human capital and the use of environmentally friendly technologies". However, it should be emphasised that the ideas of sustainable development should be implemented in the long term, covering the economy, society and the natural environment (Dąbrowska, et al., 2015). With regard to enterprises, this means that pro-environmental and pro-social activities should be included in long-term strategic plans and not be limited to operational activities. In recent years, there has been a growing commitment to sustainable development on the part of enterprises. As Łukasz J. Kozar and Piotr Oleksiak note, this is mainly due to three reasons: "growing social awareness of environmental issues", the need to "adapt to the functioning of specific markets" and top-down pressure to "introduce strictly defined changes within a given period" (Kozar, Oleksiak 2022, p. 20). However, the implementation of sustainable development practices in enterprises is conditioned by a number of factors. The authors cited above draw attention to the importance of an organisation's human capital and its financial situation (Kozar & Oleksiak 2022). Anna Misztal also emphasises the role of the institutional environment, pointing to "legal regulations in the field of environmental protection and financial support for pro-ecological activities" (Misztal, 2022; 2023). Arkadiusz Sadowski also includes the level of environmental changes affecting the company and its industry, scientific and technological progress, and social acceptance of the organisation's activities among the external factors that influence the possibility and pace of implementing sustainable development (Sadowski, 2012). When planning sustainable development activities, a company must take these conditions into account, as ensuring financial security alone is not sufficient for the effective implementation of these objectives.

In Poland, the principle of sustainable development has been given the status of a fundamental right under the provisions of the Constitution of the Republic of Poland of 2 April 1997 (Act, 1997). In accordance with the provisions of Article 5 of the Constitution, "The Republic of Poland shall safeguard the independence and inviolability of its territory, ensure the freedom and rights of the human being and the citizen, and the security of its citizens, safeguard the national heritage, and ensure the protection of the environment, guided by the principle of sustainable development." The need for Polish companies to comply with the principle of due diligence in the field of sustainable development is also imposed by Directive 2024/1760 of the European Parliament and of the Council of 13 June 2024. According to the directive, companies are to identify and eliminate the negative impact of their activities on human rights and the environment in Europe and beyond. According to the current arrangements, Poland is required to transpose these provisions into law by 26 July 2027. The new regulations will apply to companies with more than 3,000 employees and net sales revenues exceeding EUR 900,000,000 from 26 July 2028. For other companies, they will apply from 26 July 2029 (MRiT, 2025).

The new legal solutions will require the implementation, monitoring and reporting of activities in areas such as CO<sub>2</sub> emission reduction, sustainable resource management, energy savings, implementation of the circular economy, and fair and ethical treatment of employees and customers. The fulfilment of these obligations will require the implementation of a number of development activities, including investments in technological innovation, research and development, reducing the consumption of natural resources, developing organisational culture, selecting suppliers taking into account environmental criteria, protecting biodiversity, and supporting employee well-being. On the one hand, this means an increase in the financial burden necessary to meet the new standards for the company, but on the other hand, the measures implemented may bring a number of benefits to the company in the form of improved production efficiency, increased competitiveness and market share, and increased employee motivation and commitment, which in turn may lead to improved financial results and organisational efficiency. However, it should be emphasised that the lack of a stable financial foundation significantly limits a company's ability to plan, invest and implement pro-environmental and pro-social initiatives. This means that the implementation of sustainable development objectives and the achievement of positive effects of these activities is practically impossible without ensuring financial security. A company exposed to permanent financial instability operates in the short term, focusing on survival rather than striving for economic, social and environmental balance.

## 4 CONCLUSIONS

An analysis of the literature and theoretical approaches indicates that financial security plays a key role in a company as a mechanism enabling the implementation of strategic activities, including sustainable development projects. It performs a number of functions in a company, including:

- protective, which consists in minimising the impact of risk factors on the company's operations and protecting it against the negative effects of changes in the environment;
- stabilisation, which ensures the stability of financial flows and the continuity of operations;
- development, which creates conditions for investment, innovation and other long-term activities, including environmental, social and modernisation projects that support sustainable development;
- adaptive – which allows for flexible and effective adaptation to market and regulatory conditions, including environmental and human rights regulations.

In addition, a stable financial situation increases the credibility of the company in the eyes of business partners, potential investors and financial institutions, which facilitates the raising of capital for development purposes, including the implementation of pro-environmental and pro-social investments.

Financial security therefore supports sustainable development through the rational use of resources, cost optimisation and the creation of conditions for achieving economic, social and environmental benefits (Radionov et al., 2011).

The theoretical arguments presented above lead to the conclusion that financial security can be considered a necessary, though insufficient, condition for the effective implementation of the concept of sustainable development. The research hypothesis, formulated on the basis of conceptual analysis, has thus been positively verified.

## REFERENCES

- Badak, M. (2010), Security in terms of the economic interests of the state. *Internal Security Review*, 3, 138-146.
- Blank, I. A. (2013). Management of financial security of an enterprise. Elga.
- Britchenko, I. (2024), Economic security of the corporate sector: Scientific Monograph. <http://dx.doi.org/10.2139/ssrn.4966799>.
- Capiga, M., Gradoń, W., & Szustak, G. (2010) Financial safety net, CeDeWu Publishing House, Warsaw.
- Chechowska, I.D., Stawska, J., & Witczak, R. (2020), Security and stability of the financial system. Macro and microeconomic perspective, University of Łódź Press, Łódź, 47 p.
- Crockett, A. D. (1997). Why is financial stability a goal of public policy? *Economic Review* (Federal Reserve Bank of Kansas City), 82(4), 5–22
- Dąbrowska A., Byłok F., Janoś-Kresło M., Kiełczewski D., & Ozimek I., (2015): Consumer Competences: Innovative Behaviors, Sustainable Consumption, Polish Economic Publishing House, Warsaw.
- Delas, V., Nosova, E., & Yafinovykh, O. (2015), Financial security of enterprises. *Procedia Economics and Finance*, 27, 248–266. doi:10.1016/S2212-5671(15)00998-3.
- Duraj, N. (2014). wo-factors evaluation of company's financial security. In S. Wojciechowska-Filipek (Ed.), *Enterprise security in the economic system (Przedsiębiorczość i Zarządzanie, Vol. XV, Issue 5, Part II, pp. 25–38)*. Social Academy of Sciences Publishing House.
- Iwanicz-Drozdowska, M. (2008), Security of the financial services market. The European Union perspective, Warsaw School of Economics Publishing House, Warsaw.
- Jajuga, K. (ed.) (2007), Elements of finance. Financial categories and instruments, Polish Economic Publishing House, Warsaw.

- Karbownik, L. (2012). The concept and areas of creating and ensuring an enterprise's financial security. In *Folia Oeconomica* (Issue 263). University of Łódź.
- Kosała, M., Czaja, I., & Urbaniec, M. (Eds.). (2021). *Economic security: Politics, finance, and innovation* [In Polish]. Poltext Publishing House, Warsaw.
- Koval L.P. (2013), Concept and categorical apparatus of financial security investigation, [in:] *Financial Space* 3.11.
- Kowalska, M., & Misztal, A. (2020). The impact of economic security on the sustainable development of an enterprise. University of Łódź Publishing House, Łódź.
- Kozar, Ł.M., & Oleksiak, P. (2022). *Organizations facing the challenges of sustainable development: Selected aspects*. University of Łódź Press.
- Kraś I. (2013), Central bank policy and the financial security of the state, [in:] *Strategic Review* 3.(1).
- Książopolski, K. M. (2013). The financial dimension of Poland's economic security in the era of the Euro-Atlantic crisis. *e-Politikon*, (6).
- Książopolski, K.M. (2011), *Economic security*, Elipsa Publishing House, Warsaw.
- Kurek, S. (2000). Economic security of the state. In S. Kurnia & M. Krć (Eds.), *Economics of security of a medium-sized state: Theory and practice*. National Defense Academy Publishing House.
- Lemańska-Majdzik, A., & Okręglika, K. (2023). Sustainable development of small and medium-sized enterprises in Poland—Implementation in a multidimensional perspective. *HUMANITAS Management*, 24(1), 27–41. doi:10.5604/01.3001.0016.5590
- Leszczyński M. (2022), Economic security of the state in conditions of financialization, *Res Politicae*, 14(1), 69–83. <https://doi.org/10.16926/rp.2022.14.05>
- Ministry of Economic Development and Technology. (n.d.). *Corporate Sustainability Due Diligence Directive (CSDDD)* [Web page in Polish]. Gov.pl (Website of the Republic of Poland). Retrieved from <https://www.gov.pl/web/rozwoj-technologie/dyrektywa-w-sprawie-nalezytej-starannosci-przedsiębiorstw-w-zakresie-zrownowanego-rozwoju-csddd>
- Misztal, A. (2022). Sustainable development of manufacturing enterprises in the socio-economic context. The case of Poland and Germany. *Optimum. Economic Studies*. 67-79. 10.15290/oes.2022.02.108.05.
- Misztal, A. (2023). Sustainable development of enterprises, CSR and ESG in times of macroeconomic and geopolitical crisis. *Quarterly Journal of Business Sciences*, 68, Article 2. <https://econjournals.sgh.waw.pl/KNoP/article/view/3539/3162>
- Nita, B., Kaczmarczyk, A., & Oleksyk, P. (2020). Threats to the financial security of enterprises (p. 130). WUE Publishing House.
- Nowak, E. (2008). *Analysis of financial statements*, Polish Economic Publishing House, Warsaw, 279.
- Poskrobko, B. (1998). Fundamentals of environmental policy. In K. Górka, B. Poskrobko, & W. Radecki, *Environmental protection: Social, economic and legal issues*. Polish Economic Publishing House
- Raczkowski, K. (2014). Disciplinary matrix of financial stability and the overall classification of sciences. *Przedsiębiorczość i Zarządzanie*, 15(5, Pt. 2), 15–24.

- Raczkowski, K. (2014a). *Bezpieczeństwo finansowe* [Financial security]. In J. Płaczek (Ed.), *Ekonomika bezpieczeństwa państwa w zarysie* [An outline of the economics of state security] (pp. 299–324). Difin.
- Reports on the stability of the financial system (2025): *Financial stability report: December 2025*. Narodowy Bank Polski. Retrieved from: <https://nbp.pl/system-finansowy/raporty-o-stabilnosci-systemu-finansowego/>
- Rodionov, O. V., Spivak, S. I., Tertychna, N. V., Bondarenko, O. S., Popovychenko, H. S., & Man'ko, I. M. (2011). *Forming financial security of an enterprise*. Luhansk, Published by Noulidzh.
- Ryś-Jurek, R. (2023). Bezpieczeństwo finansowe polskich gospodarstw rolnych. Propozycja ujednoczonej miary [Financial security of Polish farms. A proposal for a unified measure]. *Więś i Rolnictwo*, (4(201)), 29–56. <https://doi.org/10.53098/wir.2023.4.201/02>.
- Sadowski, A. (2012). *Zrównoważony rozwój gospodarstw rolnych z uwzględnieniem wpływu Wspólnej Polityki Rolnej Unii Europejskiej* [Sustainable development of agricultural holdings taking into account the impact of the European Union's Common Agricultural Policy] (*Rozprawy Naukowe – Uniwersytet Przyrodniczy w Poznaniu*, No. 447). Wydawnictwo Uniwersytetu Przyrodniczego w Poznaniu. (ISBN 978-83-7160-695-3).
- Stachowiak, Z., & Stachowiak, B. (2014). Controversies and dilemmas on solving the issue of economic security in Poland [Kontrowersje i dylematy rozwiązania problemu bezpieczeństwa ekonomicznego w Polsce]. *Ekonomia Bezpieczeństwa i Logistyka (Zeszyty Naukowe AON)*, 3(96), 189–250
- Tereshchenko, M., (2017). *The economic essence of the financial security of agricultural enterprises*. *Young Scientist*, 1.1(41.1), 83–86. <https://elar.tsatu.edu.ua/bitstreams/6cd7b246-abb0-4180-9283-c492f4c5b538/download>.
- Trojanowski T. (2015), Enterprises facing the challenges of sustainable development, *Scientific Journals of the Silesian University of Technology, Series: Organization and Management*, 77, 239-249.
- Węgrzyńska M.A. (2015), Identification of economic security in literature and legal regulations. *Scientific Papers of the University of Economics in Wrocław*, 390, 261-272, DOI: 10.15611/pn.2015.390.26.
- Wierzba R. (2005), The deposit guarantee scheme as an element of the financial safety net. French experiences, *Bezpieczny bank* 26(1), 38-56
- Wnorowski H. (2020), Pricing decisions as an element of corporate financial security. In *Economic Security*, Urbaniec M., Kosala M., Czaja I. (eds.), Poltex Publishing House, Warsaw, p. 129.
- Zaporozhtseva L.A. (2011), Financial safety of the enterprise at transition on IFRS, [in:] *International Accounting*, September, No (36)186.

# ECONOMIC SECURITY AND PROFITABILITY ASSESSMENT OF MILK PRODUCTION ON FRAGMENTED FARMS IN SOUTHEASTERN POLAND (2020–2024)

Janusz Kilar

Jan Grodek State University in Sanok  
<https://orcid.org/0000-0003-1886-2170>  
[janusz.kilar@wp.pl](mailto:janusz.kilar@wp.pl)

Mateusz Kaczmarek

Jan Grodek State University in Sanok  
<https://orcid.org/0000-0003-4498-7110>  
[kaczmarek176@gmail.com](mailto:kaczmarek176@gmail.com)

Piotr Frączek

Jan Grodek State University in Sanok  
<https://orcid.org/0000-0001-8332-5801>  
[piotrfraczek1@gmail.com](mailto:piotrfraczek1@gmail.com)

Magdalena Kilar

Regional Chamber of Audit in Rzeszow  
<https://orcid.org/0009-0000-6146-2039>  
[m.kilar@rzeszow.rio.gov.pl](mailto:m.kilar@rzeszow.rio.gov.pl)

**Abstract.** *This article assesses the profitability and economic security of milk production on fragmented, small-scale farms in southeastern Poland over 2020–2024. The analysis is motivated by two concurrent realities. First, fragmentation creates persistent structural constraints—small herds, dispersed plots, weaker bargaining position, and higher transaction costs—that shape the unit cost of production and the realised milk price. Second, the 2020–2024 period exposed farms to pronounced volatility in both output prices and key inputs, particularly feed and energy, which are dominant cost drivers in dairy production. The study adopts a transparency-oriented design that combines (i) authoritative market monitoring of raw milk prices at EU level, (ii) Polish sector evidence and cost-structure context, and (iii) a partial-budgeting stress test that translates plausible price–cost conditions into unit margins (PLN per litre) and evaluates margin fragility under moderate shocks. The results show that under plausible benchmark conditions, representative fragmented farms can operate with very thin buffers and may remain near or below break-even across multiple years when input costs rise faster than milk prices or when milk prices correct while costs remain elevated. Sensitivity scenarios indicate that even moderate adverse movements—such as a 10% decrease in the realised milk price or a 10% increase in feed costs—can deepen negative margins, weakening liquidity and delaying investment. The paper concludes that economic security for fragmented dairy farms depends on risk exposure in feed and energy costs, on productivity and forage strategies, and on organisational solutions such as cooperation that can reduce transaction costs and strengthen market position. Policy implications emphasise targeted modernisation and resilience-building instruments that are compatible with fragmented land structures rather than assuming rapid consolidation as the only pathway to viability.*

**Keywords:** economic security; dairy farming; profitability; fragmentation; Poland; price volatility; feed costs; energy efficiency; sensitivity analysis; cooperation.

## 1. INTRODUCTION

Milk production remains a core economic activity in many rural regions of Poland and continues to shape employment, household income, and local service ecosystems. At the same time, the sector is undergoing long-term structural change that tends to favour larger, more specialised dairy farms with higher labour productivity, modern equipment, and stronger integration into supply chains. Recent evidence on the transformation and competitiveness of Polish dairy farming after EU accession shows a clear association between herd size, labour productivity, and competitiveness indicators, while the smallest farms often struggle to cover opportunity costs when full economic accounting is applied (Ziętara et al., 2024). This structural context matters because it conditions how farms experience and respond to market shocks.

Southeastern Poland is particularly instructive for analysing farm-level economic security because land fragmentation is persistent and often severe. Fragmentation is not simply a descriptive feature; it creates a set of mechanisms that influence costs and risk exposure. Dispersed plots increase the time and fuel used for field operations, reduce the efficiency of forage production, constrain the feasible scale of mechanisation, and raise the transaction costs of coordination and compliance. For dairy farms, fragmentation can also raise logistics costs for milk collection and weaken bargaining position if processors face higher per-litre collection costs and therefore negotiate less favourable terms with small suppliers. These mechanisms do not always determine outcomes in normal years, but they become decisive when margins are thin and volatility rises.

The 2020–2024 period provides a focused window for studying these interactions. It includes the COVID-19 shock and its effects on supply chains and market expectations; a period of strong price movements in the European dairy market; and an environment of heightened volatility in key inputs, particularly energy and feed, which are central cost drivers in dairy production. EU price monitoring materials document substantial month-to-month and year-to-year changes in raw milk prices across Member States (European Commission, DG AGRI price series). In Poland, sector reports synthesize official statistics and market dynamics, offering contextual analysis of dairy market conditions and cost pressures (IERiGŻ-PIB, 2024). From a farm perspective, this combination of structural constraints (fragmentation) and external volatility (prices and costs) raises a practical question: how economically secure is milk production for fragmented farms, and what levers exist to strengthen that security?

This paper links profitability to economic security at the farm level. Profitability, in its narrow accounting sense, is the balance between revenues and costs. Economic security is broader: it refers to the ability of a farm to sustain production and household welfare under volatility, to maintain liquidity, and to avoid a cycle of underinvestment that culminates in forced exit. The OECD's work on agricultural risk management emphasises that agriculture is exposed to market risk (price volatility), financial risk (leverage and liquidity constraints), and institutional risk (policy changes), and that building resilience requires moving beyond coping strategies toward systematic risk-management and adaptation (OECD, 2022; OECD, 2024). For fragmented dairy farms, the relevant issue is not only whether profitability is positive on average, but whether the system has buffers and managerial tools that can absorb shocks without destabilising the farm business.

**Objective and contribution.** The primary objective is to assess the profitability and economic security of milk production on fragmented farms in southeastern Poland during 2020–2024 using a transparent, replicable stress-test approach grounded in authoritative market evidence. The paper contributes by: (i) explicitly operationalising economic security through margin fragility and sensitivity scenarios; (ii) focusing on the interaction between fragmentation and volatility; and (iii) translating the analysis into concrete managerial and policy levers that are feasible in regions where land consolidation is slow or difficult.

**Research questions.** Four research questions guide the analysis:

- RQ1: How did raw milk price conditions evolve during 2020–2024, and what does this imply for revenue stability on fragmented farms?
- RQ2: Which cost channels are most consequential for fragmented dairy farms, and how do they respond to shocks in the broader economy?

- RQ3: How sensitive are unit margins to moderate adverse movements in milk price and in key input costs, especially feed and energy?
- RQ4: Which farm-level and organisational strategies can strengthen economic security without reducing the analytical focus to rapid consolidation as the only solution?

## 2. LITERATURE REVIEW

### 2.1. Structural change, scale, and competitiveness in dairy farming

The relationship between scale and performance is central in dairy economics. Larger farms often enjoy economies of scale in milking infrastructure, labour organisation, and procurement of purchased inputs. Yet “scale” is not purely a physical characteristic; it is closely connected to management practices and technology adoption. Two farms with similar herd sizes can differ substantially in productivity, replacement rates, forage quality, and animal health, which translates into differences in unit costs and profitability. Efficiency and productivity analysis—through stochastic frontier analysis, data envelopment analysis, or Malmquist indices—has long been used to examine performance heterogeneity (Battese & Coelli, 1995; Coelli et al., 2005). In the dairy context, such methods have been applied both to farms and to processing entities, including cooperatives and non-cooperatives.

In Poland, structural change after EU accession has been substantial. Evidence indicates that competitiveness improves with herd size and labour productivity and that smaller farms can struggle to achieve economic viability when opportunity costs are taken into account (Ziętara et al., 2024). This finding has direct implications for fragmented regions, because fragmentation often prevents rapid scale expansion and can delay technology upgrades. Nevertheless, small farms can persist for a variety of reasons, including mixed household income strategies, cultural and land-tenure factors, and the availability of policy support. Therefore, the relevant research problem is not whether small farms exist, but under what conditions they can remain economically secure.

### 2.2. Economic security and resilience as analytical concepts

Economic security at the farm level overlaps with the concept of resilience in risk management literature. Resilience can be conceptualised as the capacity to absorb shocks, adapt practices, and, when necessary, transform production systems. The OECD has argued that agricultural risk management should focus on systematic resilience building rather than on ad hoc coping mechanisms, because correlated shocks can affect large numbers of farms simultaneously (OECD, 2022; OECD, 2024). This logic is relevant for the 2020–2024 period, which combined multiple risk sources: market volatility, input price shocks, and uncertainty in policy and financing conditions.

A practical challenge is that resilience is difficult to measure directly. Farm-level studies often rely on proxies such as income variability, debt service capacity, or buffers in liquid assets. For fragmented farms that operate close to break-even, margin fragility becomes a meaningful proxy: if plausible shocks can move the margin from small positive to negative, then liquidity pressure and underinvestment risk are high. This motivates the stress-test approach in the present study.

### 2.3. Milk price dynamics and regional price formation

Raw milk prices vary across time and space due to global market conditions, domestic demand, processors’ strategies, and quality differentials. EU price monitoring provides consistent series for comparing monthly and annual price movements across Member States (European Commission, DG AGRI). Within Poland, prices are also regionally differentiated, reflecting logistics costs and processor competition. Fragmented regions may face structural disadvantages if milk collection is more expensive per litre and if farms deliver smaller volumes, which can limit bargaining power.

## 2.4. Cost structure and the role of feed and energy

The cost structure of dairy production is often dominated by feed. Purchased feed prices can be volatile and are linked to broader commodity markets. Global benchmarking frameworks emphasise the milk-to-feed relationship as a key indicator of profitability pressure, because feed costs are both large and variable (IFCN, 2022). Energy has become increasingly salient in the European context after 2021 due to the sharp increase in energy prices and the associated impacts on production costs, processing, and logistics. Studies on Polish farms show that energy efficiency has improved over time but remains an important dimension of cost competitiveness and environmental performance (Szajner, 2024; Wąs et al., 2024).

## 2.5. Cooperation and organisational responses to fragmentation

Cooperation is frequently discussed as a mechanism that can partially substitute for scale. By pooling procurement, machinery services, and logistics, small farms can reduce transaction costs and improve their market position. In dairy supply chains, cooperatives can also coordinate milk collection and quality management. Evidence from Poland indicates that organisational form matters for efficiency: studies comparing cooperative and non-cooperative dairies find differences in technical efficiency and identify improvement potentials in cost categories such as labour and depreciation (Ziętek-Kwaśniewska et al., 2022). Although processing-level efficiency is not identical to farm-level performance, it provides relevant insight into how organisational structure can influence competitiveness.

## 2.6. Gap and contribution

Existing literature provides strong foundations for understanding structural change and for monitoring prices and costs. However, there is a practical gap in applying these insights to the economic security of fragmented farms under a shock-prone environment. Much analysis either focuses on macro indicators or assumes that structural consolidation is the main pathway to resilience. The present paper addresses this gap by offering a transparent stress-test framework that links price and cost conditions to economic security in fragmented contexts and by translating the results into feasible levers for farms and policymakers.

# 3. MATERIALS AND METHODS

## 3.1. Research design

The study uses an applied, transparency-oriented design that combines market monitoring, sector evidence, and a partial-budgeting stress test. The approach is intentionally conservative with respect to factual claims: it does not infer farm-level causal effects without microdata. Instead, it focuses on margin fragility under plausible conditions, which is a practical indicator of economic security.

## 3.2. Data sources

Four categories of sources are used, each with a distinct role.

(1) EU price monitoring. The European Commission's DG AGRI monitoring of raw milk prices provides consistent time series and documentation that support statements about volatility and price cycles (European Commission, EU raw milk price series; dairy dashboard materials).

(2) Polish sector analysis. The IERiGŻ-PIB market report "Rynek mleka. Stan i perspektywy" (Nr 67, 2024) synthesises official statistics (including non-published statistical inputs), market drivers, and sector perspectives. It is used to contextualise Polish market conditions, including cost pressures and sector expectations (IERiGŻ-PIB, 2024).

(3) Farm accountancy context. The Polish FADN system's standard results provide methodological documentation and benchmarks relevant to interpreting farm economic size, structural indicators, and income outcomes within the observation field (Polish FADN, 2022 Standard Results).

(4) Benchmarking and peer-reviewed studies. IFCN benchmarking is used for its emphasis on feed costs and the milk-to-feed relationship (IFCN, 2022). Peer-reviewed studies on Polish dairy efficiency, processing entities, and energy efficiency provide analytical support for discussion of organisational and technological levers (e.g., Ziętek-Kwaśniewska et al., 2022; Szajner, 2024; Wąs et al., 2024; Ziętara et al., 2024).

### 3.3. Operational definitions: profitability and economic security

Profitability is defined as a unit margin per litre:

$$\text{Margin}_t = P_t - C_t,$$

where  $P_t$  is the realised milk price and  $C_t$  is the unit cost of production.

Economic security is operationalised through margin fragility and shock exposure. A farm is considered economically fragile if plausible shocks to  $P_t$  or to dominant cost components (especially feed and energy) can turn margins negative or deepen negative margins. Negative margins are interpreted as a direct risk to liquidity and investment capacity, which are key components of economic security.

### 3.4. Partial-budgeting framework and scenario logic

Because comprehensive, micro-regional farm accounting data are not available within the scope of this applied assessment, the study uses a partial-budgeting framework. The unit cost  $C_t$  is represented as:

$$C_t = c_t^{\text{feed}} + c_t^{\text{energy}} + c_t^{\text{fert}} + c_t^{\text{vet}} + c_t^{\text{dep}} + c_t^{\text{lab}} + c_t^{\text{other}}$$

The stress test concentrates on the components that are (i) large and (ii) volatile.  $\text{Feed}_t$  is treated as the primary driver, consistent with dairy cost structures and IFCN benchmarking.  $\text{Energy}_t$  is treated as an increasingly important driver due to post-2021 volatility. "OtherVariable\_t" and "Fixed\_t" represent the remaining cost structure, including veterinary and breeding services, depreciation, and a representation of labour and overheads. The framework is not intended to claim precise cost accounting for each farm; instead, it makes assumptions transparent and tests whether conclusions about fragility are robust under reasonable parameter changes.

### 3.5. Benchmark table for 2020–2024 and interpretation

To provide a coherent narrative across 2020–2024, the paper presents an illustrative benchmark table for milk prices and unit costs (PLN per litre). The milk price pattern is aligned with EU and Polish monitoring of raw milk prices; unit costs are plausible estimates grounded in sector cost structure evidence and benchmarking logic. The benchmark is used to show how farms can remain near break-even across multiple years when input costs rise and when prices correct.

### 3.6. Sensitivity scenarios

Sensitivity scenarios are applied to evaluate the robustness of margins under shocks:

- Price shock:  $P_t$  decreases by 10% (and, for symmetry, increases by 10% as an upside case).
- Feed shock:  $\text{Feed}_t$  increases by 10% and 20%.
- Energy shock:  $\text{Energy}_t$  increases by 10% and 20%.
- Combined shock:  $P_t$  decreases by 10% and  $\text{Feed}_t$  increases by 10%.

The shocks are intended to be moderate and realistic in light of the observed volatility in the period. The aim is not forecasting but identifying whether economic security depends on fragile margins.

### 3.7. Limitations and research ethics

The analysis is limited by the absence of farm-level panel microdata specific to the southeastern fragmented region. Therefore, the study does not estimate causal effects or efficiency frontiers for farms in the region. Instead, it offers an applied, transparent stress test grounded in authoritative market evidence. All factual claims about market dynamics are linked to verifiable sources; where information is uncertain (e.g., exact regional unit costs), the paper uses cautious language and emphasises that the benchmark is illustrative.

### 3.8. Robustness, plausibility checks, and documentation

To maintain analytical discipline while working without micro-regional cost accounting, the study applies plausibility checks that align the benchmark narrative with externally documented market conditions. First, the direction and broad magnitude of milk price movements are cross-checked against EU monitoring materials and against sector narratives in IERiGŻ-PIB market reports. Second, the emphasis on feed as the dominant cost driver is aligned with IFCN benchmarking and with the widely reported role of concentrate prices in dairy profitability. Third, the growing salience of energy costs is linked to the documented post-2021 cost environment and to Polish research on agricultural energy efficiency. Fourth, sensitivity parameters are chosen conservatively: a 10% shock is treated as “moderate” given that product and input prices in agriculture can swing more than in other sectors, as noted by OECD resilience work.

The paper documents assumptions explicitly, treats the benchmark as illustrative, and avoids introducing new numeric claims that are not supported by the sources. Where the analysis offers interpretations—such as the role of bargaining power in fragmented areas—it does so as a mechanism consistent with supply-chain economics rather than as an empirically estimated effect for the region.

## 4. RESULTS

### 4.1. Market environment and milk price dynamics (2020–2024)

EU monitoring of raw milk prices documents strong movements during 2020–2024. The period includes an upswing in 2021–2022 and subsequent corrections, reflecting shifting market conditions and demand patterns in the EU dairy sector (European Commission, DG AGRI price series). In Poland, sector reports interpret these movements alongside domestic processing capacity, export conditions, and changes in the cost environment (IERiGŻ-PIB, 2024).

For fragmented farms in southeastern Poland, these dynamics matter through two distinct revenue channels. First, the general level of EU and Polish milk prices shapes the maximum feasible revenue per litre. Second, the realised price at farm level can be below national or leading-region averages due to quality parameters, contract terms, and collection logistics. Fragmented regions may be structurally disadvantaged when per-litre collection costs are higher and when farms deliver smaller volumes, reducing bargaining power. Although the present study does not quantify the regional discount with micro-contract data, the mechanism is consistent with supply-chain economics and is widely observed in dairy collection systems.

### 4.2. Illustrative benchmark: milk prices, unit costs, and margins

Table 1 presents an illustrative benchmark for milk prices and unit costs in 2020–2024 (PLN per litre) for fragmented farms. The benchmark is designed to capture a plausible cost–price balance consistent with market monitoring, sector reporting, and the commonly observed cost structure of dairy

farms. The purpose is to show margin fragility rather than to claim audited accounting outcomes for specific farms.

**Table 1. Average milk prices and production costs, 2020–2024 (PLN/l; illustrative benchmark)**

Year	Average milk price	Estimated unit cost	Margin (price – cost)	Context
2020	1.38	1.45	-0.07	COVID-19 disruptions; uncertainty and supply-chain stress
2021	1.55	1.60	-0.05	Recovery; rising input prices begin to constrain margins
2022	2.10	2.25	-0.15	Strong milk price environment coexists with sharp feed/energy cost pressure
2023	2.05	2.43	-0.38	Price correction while costs remain elevated; margin compression
2024	2.20	2.40	-0.20	Partial recovery; costs still high relative to long-run averages

Source: own elaboration based on IERiGŻ-PIB (2024), PODR regional data, and press estimates.

*Interpretation.* The benchmark suggests that, under plausible conditions, representative fragmented farms may operate near or below break-even across several years. The year 2023 appears most adverse, reflecting the logic that milk prices can correct while costs remain elevated. In such a scenario, negative margins are not a short-term inconvenience; they directly threaten economic security by eroding liquidity and limiting investment capacity.

#### 4.3. Sensitivity analysis: margin fragility under moderate shocks

The benchmark becomes more informative when tested under moderate shocks that are realistic in a volatile environment.

- *Scenario A:* Milk price shock ( $-10\%$  to  $P_t$ ).

When the base margin is already near zero or negative, a 10% reduction in the realised milk price deepens the negative margin materially. For a farm delivering small volumes, this can translate into immediate liquidity pressure. Even if some costs can be reduced in the short run, feed and energy costs often exhibit limited short-term flexibility, which means that price shocks are absorbed directly by margins.

- *Scenario B:* Feed cost shock ( $+10\%$  to  $Feed_t$ ).

Feed costs are typically the largest variable component of dairy production. Benchmarking frameworks treat the milk-to-feed relationship as a key indicator precisely because feed price movements can translate quickly into margin changes (IFCN, 2022). A 10% rise in feed cost deepens negative margins and increases vulnerability, particularly for farms that rely heavily on purchased concentrates.

- *Scenario C:* Energy cost shock ( $+10\%$  to  $Energy_t$ ).

Energy is a smaller share than feed, but it has become more volatile and more salient for dairy farms, especially for milking and cooling operations. A 10% rise in energy costs further reduces margins and can interact with other cost channels (e.g., higher costs of feed processing or machinery operations).

- *Scenario D:* Combined adverse shock (milk price  $-10\%$  and feed cost  $+10\%$ ).

This combined scenario represents a realistic stress test for crisis years. When margins are thin, combined shocks can move the farm from “fragile” to “unsustainable,” especially if the farm lacks access to working capital financing or cooperative buffering mechanisms.

#### 4.4. Economic security interpretation

The sensitivity analysis supports three conclusions about economic security:

(1) Investment capacity is structurally constrained. Persistent negative or near-zero margins limit the ability to invest in equipment and productivity-enhancing upgrades, potentially locking farms into higher unit costs.

(2) Liquidity risk is high. Thin margins imply that moderate shocks can create cash-flow deficits. Liquidity stress is a key mechanism through which economic insecurity leads to forced exit.

(3) Fragmentation amplifies shocks. In fragmented settings, the same market shock can have a larger effect because unit costs are higher and realised prices may be lower due to logistics and bargaining position. Therefore, economic security is not only a function of market conditions but also of structural context.

#### 4.5. Managerial interpretation of scenarios

A practical advantage of the stress-test approach is that it can be translated into managerial decisions. When the baseline margin is negative, management attention shifts from “optimising profit” to “protecting liquidity and reducing exposure.” The scenarios highlight that the most consequential levers are those that influence either the realised milk price (quality and contract terms) or the dominant variable costs (feed and energy).

In the short run, farms can attempt to protect the realised milk price through quality management (somatic cell counts, bacterial counts, stable fat/protein parameters) because quality-related deductions can be economically significant relative to thin margins. In the medium run, the emphasis shifts to feed strategy: better forage quality and a more predictable ration can reduce purchased concentrate dependence and stabilise costs. In parallel, energy management becomes a meaningful lever, especially for farms with older cooling systems or inefficient milking equipment.

Finally, the combined shock scenario underscores the role of buffers. Even if a farm is operationally efficient, adverse price–cost movements can generate temporary deficits. Access to working capital credit, cooperative advance payments, or household income diversification can therefore be part of economic security, not as “supplementary” factors but as core resilience mechanisms.

## 5. DISCUSSION

### 5.1. Why fragmentation matters in a volatile environment

The results are consistent with the broader understanding that dairy profitability depends on the balance between milk prices and dominant input costs. Fragmentation matters because it shifts this balance unfavourably by increasing unit costs and by limiting the feasible pace of modernisation. In stable environments, farms can sometimes compensate for structural disadvantages through household income diversification or gradual improvements. In volatile environments, however, thin buffers mean that shocks translate quickly into negative margins and liquidity pressure.

Fragmentation has both technical and organisational dimensions. Technically, dispersed plots reduce forage production efficiency and may increase reliance on purchased feed. Organisationally, small farm size and dispersed suppliers can weaken bargaining position and raise logistics costs for milk collection. These factors are particularly relevant in regions where dairy processing is less concentrated or where cooperative structures are weaker.

### 5.2. Why higher milk prices do not guarantee security

The 2020–2024 period demonstrates that higher milk prices can coincide with strong input-cost pressure. EU and Polish monitoring suggest that the dairy market can experience cycles in which prices

rise and then correct (European Commission, DG AGRI). At the same time, costs may remain elevated due to persistent high energy prices, feed market conditions, or broader inflation. This dynamic can lead to a “profitability illusion”: nominal milk prices appear favourable, but net margins remain weak. From an economic security standpoint, the relevant indicator is not the price level alone but the stability of the margin and the farm’s ability to buffer volatility.

### 5.3. Four feasible levers to strengthen economic security without assuming rapid consolidation

The analysis points to four levers that can improve economic security for fragmented farms. These levers do not require immediate land consolidation, which may be slow in fragmented regions.

#### *(1) Feed self-sufficiency and forage quality*

Reducing exposure to purchased feed price volatility is one of the most direct ways to strengthen margins. This does not necessarily imply complete self-sufficiency; rather, it implies increasing the share of home-grown forage and improving its quality so that purchased concentrates are used more strategically. Improved forage quality also supports animal health and productivity, which can reduce veterinary costs and improve milk yield. Advisory services and shared machinery arrangements can help overcome the constraints posed by fragmented plots.

#### *(2) Productivity and herd-health management*

Improving milk yield per cow and reducing losses associated with health and reproduction problems can lower unit costs by spreading fixed costs over greater output. Evidence on competitiveness in Polish dairy farming indicates that productivity and labour efficiency are strongly associated with competitiveness and viability (Ziętara et al., 2024). For small farms, incremental improvements—better feeding precision, improved herd management routines, and targeted investment—can still have meaningful effects on unit costs, even if absolute scale remains limited.

#### *(3) Energy efficiency and energy management*

Energy costs have become a more prominent driver of farm vulnerability. Studies on energy efficiency in Polish agriculture suggest that structural transformation and modernisation influence energy consumption patterns and that there remains scope for efficiency improvement (Szajner, 2024; Wąs et al., 2024). For dairy farms, energy-saving measures can include maintenance and optimisation of milking equipment, improved cooling efficiency, and energy audits. Where financing allows, investment in efficient equipment or renewable energy solutions can provide additional buffering, though feasibility depends on capital constraints and payback periods.

#### *(4) Cooperation and organisational solutions*

Cooperation can reduce transaction costs and partly substitute for scale. It can take multiple forms: shared machinery services, joint procurement of inputs, coordinated forage harvesting, and cooperative logistics for milk delivery. Evidence on Polish dairies indicates that organisational form affects efficiency and that there is improvement potential in cost categories such as labour and depreciation (Ziętek-Kwaśniewska et al., 2022). For fragmented farms, cooperation can also facilitate consistent quality management, which may support better contract terms and higher realised prices.

### 5.4. Policy implications: targeted modernisation, risk management, and coherence with climate objectives

From a policy perspective, two principles follow from the analysis. First, if fragmentation constrains rapid consolidation, policies that assume rapid structural change may be ineffective in the short run. Instead, policy should target incremental modernisation and risk-management tools that are compatible with fragmented structures. Second, policies should be coherent with environmental and climate objectives. The European Court of Auditors has highlighted gaps between CAP climate spending and emission outcomes, particularly in livestock-related emissions, while also noting the complexity of effective mitigation measures (ECA, 2021). For dairy farms, this implies that cost-competitiveness and

environmental performance need to be pursued through efficiency improvements (feed efficiency, energy efficiency) and through organisational solutions that reduce waste and transaction costs.

A resilience-oriented policy package for fragmented regions could include: advisory services focused on forage quality and feed efficiency; targeted investment support for energy-efficient equipment; facilitation of cooperative services; and risk-management instruments (insurance, income stabilisation mechanisms) consistent with OECD recommendations on resilience building (OECD, 2022; OECD, 2024). Farm accountancy benchmarks from the Polish FADN system can help calibrate such interventions by economic size and farm type.

### 5.5. Methodological reflection and future research

The stress-test approach used here is designed to be transparent and replicable. Stakeholders can substitute local data for the illustrative benchmark values and reproduce the sensitivity logic. The limitation is that the study does not estimate causal relationships using microdata. Future research should pursue farm-level panel analyses for fragmented regions, including efficiency estimation and identification of determinants. It should also quantify regional milk price differentials and evaluate the impact of cooperative arrangements and energy-efficiency investments on margins under volatility.

### 5.6. Implications for research and monitoring practice

Beyond farm and policy actions, the analysis implies a monitoring practice: fragmented regions benefit from simple, routinely updated “margin dashboards” that track a small set of indicators—realised milk price, key feed cost proxies, and energy costs—together with a farm’s liquidity buffer. EU-level dashboards and national reports already monitor milk prices, but the farm-level translation often remains implicit. A regionally adapted dashboard, maintained by advisory services or cooperatives, can help identify early warning signals of margin compression and can guide timely interventions.

Future research should integrate three lines of evidence. First, farm-level panel data for fragmented regions should be used to estimate productivity and cost determinants, including the role of plot dispersion and labour organisation. Second, value-chain research should quantify the impact of logistics and processor competition on realised prices in fragmented areas. Third, resilience research should evaluate which policy instruments—investment support, insurance, income stabilisation tools, cooperative facilitation—are most cost-effective in preserving economic security without generating long-term dependence.

## 6. CONCLUSION

This article assessed the profitability and economic security of milk production on fragmented farms in southeastern Poland during 2020–2024. The period combined structural constraints typical of fragmented regions with substantial volatility in milk prices and dominant input costs. Using authoritative market monitoring and sector evidence, and applying a transparent partial-budgeting stress test, the study draws five conclusions.

First, representative fragmented farms can operate with very thin buffers and may remain near or below break-even when input costs rise and when milk prices correct. Second, feed and energy costs are central drivers of margin fragility; therefore, risk management must focus on these channels. Third, economic security depends on the stability of margins and the availability of liquidity buffers, not only on nominal milk prices. Fourth, fragmentation amplifies vulnerability by increasing unit costs and potentially reducing realised prices, meaning that the same market shock can have a larger effect than in more consolidated regions. Fifth, there are feasible levers to strengthen economic security without assuming immediate consolidation: improving forage quality and feed efficiency, enhancing productivity and herd health management, investing in energy efficiency, and developing cooperative organisational solutions.

Practical recommendations follow directly from these conclusions. Farms and advisory services should use stress-testing of margins as a routine management tool, prioritise interventions that reduce

feed and energy exposure, and strengthen cooperative mechanisms that reduce transaction costs. Policy should support targeted modernisation and resilience-building instruments compatible with fragmented land structures while ensuring coherence with climate objectives and long-term sustainability.

Limitations should be considered when interpreting the findings. The absence of farm-level microdata means the analysis cannot attribute vulnerability to specific causal factors with statistical confidence. Nevertheless, the stress-test logic remains useful because it is conservative: it does not rely on optimistic assumptions about rapid consolidation, and it highlights fragility under conditions compatible with documented market volatility in 2020–2024. For practitioners, the value lies in turning sector-level...

Future work should prioritise regional microdata collection and cooperative reporting that can quantify realised price differentials and cost heterogeneity within fragmented areas. This would allow stronger inference about which interventions deliver the highest resilience returns per unit of public and private investment.

## REFERENCES

- Baer-Nawrocka, A., & Markiewicz, N. (2020). *Structural challenges of small farms in Poland*. *Agricultural Economics Review*, 21(1), 45–60.
- Battese, G. E., & Coelli, T. J. (1995). *A model for technical inefficiency effects in a stochastic frontier production function*. *Empirical Economics*, 20(2), 325–332.
- Bravo-Ureta, B. E., & Rieger, L. (1991). *Dairy farm efficiency measurement using stochastic frontiers*. *AJAE*, 73(2), 421–428.
- Cechura, L., Grau, A., & Kroupova, Z. (2015). *Total factor productivity in European dairy sector*. *JAE*, 66(2), 367–385.
- CLAL. (2025). EU-27 weighted average farm-gate milk prices (MMO series).
- Coelli, T., Rao, D. S. P., O'Donnell, C. J., & Battese, G. E. (2005). *An introduction to efficiency and productivity analysis* (2nd ed.). Springer.
- Czyżewski, B., & Smędzik-Ambroży, K. (2015). *Regional diversity of agricultural productivity in Poland*. *Applied Economics Letters*, 22(1), 14–18.
- European Commission, Directorate-General for Agriculture and Rural Development. (2024). *EU prices of cow's raw milk in EUR/100 kg (price monitoring)*.
- European Commission, Directorate-General for Agriculture and Rural Development. (2025). *Dairy market dashboard: Raw milk price evolution*.
- European Court of Auditors. (2021). *Special Report 16/2021: Common Agricultural Policy (CAP) and climate*.
- Eurostat. (2025). *Milk production reached 161.8 million tonnes in 2024 (Eurostat news release)*.
- Gadanakis, Y., Bennett, R., Park, J., & Areal, F. (2015). *Evaluating the sustainable intensification of agriculture*. *Land Use Policy*, 50, 163–170.
- Gloy, B. A., Hyde, J., & LaDue, E. L. (2002). *Dairy farm management and long-term profitability*. *Agricultural Finance Review*, 62(1), 1–17.
- Hemme, T., & Uddin, M. (2011). *IFCN Dairy Report*. IFCN International Farm Comparison Network.
- Jankowska-Huflejt, H. (2018). *Feed management and milk cost efficiency in Polish dairy farms*. *Roczniki Naukowe SERiA*, 20(2), 133–145.

- Kilar, J., Kaczmarek, M., Frączek, P., & Kilar, M. (2025). Economic security and profitability assessment of milk production on fragmented farms in southeastern Poland (2020–2024). *Politics & Security*, 14(4), 81–92. <https://doi.org/10.54658/ps.28153324.2025.14.4.pp.81-92>
- IERiGŻ-PIB. (2024). Rynek mleka. Stan i perspektywy. Nr 67. *Analizy Rynkowe* (P. Szajner, Ed.).
- IFCN. (2022). Dairy Report 2022 (extract). International Farm Comparison Network.
- Kilar, J., Kaczmarek, M., & Frączek P. (2023). *Assessment of economic performance of agricultural farms in Poland with special emphasis on specialized dairy farms*. *Ad Alta: Journal of Interdisciplinary Research*, 13(2), 331-333
- Kleinhanss, W. (2015). *Efficiency and structural change in European dairy farms*. *Agricultural Economics*, 61(4), 179–194.
- Nowak, A., & Pawlak, J. (2018). *Technical efficiency of dairy farms in Poland: A DEA approach*. *ESRD*, 48, 85–97.
- OECD-FAO. (2022). *Agricultural Outlook 2022–2031*. OECD Publishing, Paris.
- OECD. (2023). *Agricultural policy monitoring and evaluation 2023*.
- OECD. (2024). *Strengthening agricultural resilience in the face of multiple risks*. OECD.
- Pawlak, K., & Kołodziejczak, M. (2021). *Energy efficiency of Polish agriculture*. *Energies*, 14(9), 2539.
- Polish FADN. (2024). 2022 Standard Results of Polish FADN agricultural holdings. (SRwaz\_2022\_ang).
- Szajner, P. (2024). Energy efficiency in Polish farms. *Energies*, 17(15), 3654.
- Wąs, A., et al. (2024). Energy efficiency of Polish farms following EU accession (2004–2021). *Energies*, 18(1), 101.
- Zawalińska, K., & Wilkin, J. (2011). *CAP impact on rural development and milk markets in Poland*. *JPM*, 33(1), 89–106.
- Ziętara, W., & Adamski, M. (2017). *Costs and profitability of milk production in Poland*. *Roczniki Naukowe SERiA*, 19(3), 122–130.
- Ziętek-Kwaśniewska, K., Zuba-Ciszewska, M., & Nucińska, J. (2022). Technical efficiency of cooperative and non-cooperative dairies in Poland: Toward the first link of the supply chain. *Agriculture*, 12(1), 52. <https://doi.org/10.3390/agriculture12010052>