HYBRID THREATS AND ECONOMIC DEVELOPMENT: CHALLENGES AND RESPONSES IN THE CONTEXT OF DIGITAL TRANSFORMATION

Iryna Mazur[1]

[1]*Doctor of Science (Economics), PhD, Assistant Professor, Lecturer, School of Accounting, Economics and Finance, Technological University Dublin, Dublin, Ireland, ORCID: https://orcid.org/0000-0002-9492-6458*

Citation:
Mazur, I. (2025). *Hybrid Threats and Economic Development: Challenges and Responses in the Context of Digital Transformation. Economics, Finance and Management Review*, (3(23), 13–25. https://doi.org/10.36690/2674-5208-2025-3-13-25

Received: August 16, 2025
Approved: September 27, 2025
Published: September 30, 2025

Abstract. *Hybrid threats have become a defining challenge for economic development, representing a complex combination of cyberattacks, disinformation, economic pressure, energy dependence, and political manipulation. Their strength lies in the synergy between instruments of influence, amplified by digital transformation, which increases exposure to manipulation, data breaches, and disruptions of critical infrastructure. The article aims to determine how hybrid threats shape economic development within a digital environment and to outline strategic responses that strengthen resilience and sustain growth. The study characterizes hybrid threats as multidimensional and cross-sectoral; analyzes mechanisms that link micro-level disruptions to macro-level outcomes (investment, markets, innovation, trust); identifies highly exposed sectors (finance, energy, telecommunications, critical infrastructure); and systematizes countermeasures by integrating technological safeguards, institutional arrangements, and policy instruments. It further contributes a framework mapping threat vectors to economic transmission channels and resilience levers, an operational indicator set combining digital signals with traditional statistics, and a sector-sensitive template for risk and resilience scoring with a forward research agenda. The analysis indicates diversified hybrid-campaign pressure across regions and a pronounced escalation in Ukraine, translating into measurable pressures on investment attractiveness, market stability, and digital-infrastructure reliability. The evidence supports integrated detection, attribution, and mitigation that spans technical, informational, and policy layers. The article underscores the need for whole-of-society responses that align international cooperation, governance mechanisms, and technological innovation. Strengthening cross-border resilience and hardening digital infrastructure operate as pro-growth measures, while the proposed framework and indicator set provide practical guidance for building resilient, adaptive, and secure economic systems in an interconnected world.*

Keywords: *hybrid threats; economic development; digital transformation; cybersecurity; resilience; economic security; disinformation; financial stability; critical infrastructure; international cooperation.*

JEL Classification: O 21, H56, G 38, F 52

Formulas: 0; fig.: 0; table: 4; bibl.: 14

Introduction. The phenomenon of hybrid threats has become one of the defining challenges for economic development in the twenty-first century. Unlike traditional risks, hybrid threats represent a complex combination of cyberattacks, disinformation campaigns, economic pressure, energy dependence, and political manipulation. Their strength lies in the synergy between different instruments of influence, which makes them difficult to predict and counteract. For states and enterprises alike, these threats undermine stability by targeting vulnerabilities not only in the security system but also in the economy, financial sector, and societal trust.

The relevance of studying hybrid threats is particularly pronounced in the context of digital transformation. The rapid spread of digital technologies, while creating new opportunities for innovation, productivity, and global connectivity, simultaneously increases exposure to manipulation, data breaches, and disruptions of critical infrastructure. Modern economies rely heavily on digital platforms for trade, communication, governance, and finance, which makes them both more dynamic and more fragile. The speed and scale of digital interactions amplify the effects of hybrid attacks, allowing them to spread across borders and sectors almost instantaneously.

From an economic perspective, hybrid threats can slow down growth, reduce investment attractiveness, destabilize financial markets, and erode institutional trust. At the same time, the digital environment offers new tools for resilience, ranging from advanced cybersecurity systems to real-time monitoring and big data analytics that can detect and neutralize risks before they escalate. This duality creates a central research problem: how does digital transformation simultaneously enhance the vulnerability and the resilience of modern economies?

The article seeks to analyze the multifaceted influence of hybrid threats on economic development in the digital era. It highlights how these threats manifest across different sectors, evaluates their implications for long-term economic security, and outlines strategies for effective response. By focusing on the intersection of hybrid threats and digitalization, the study aims to provide both a conceptual framework and practical guidance for building resilient, adaptive, and secure economic systems in an increasingly interconnected world.

Literature Review. Economic security has been progressively reframed to reconcile the protection of core national values—sovereignty, prosperity, and resilience – with novel threats arising from deep globalization and technological interdependence. Recent scholarship synthesizes this as safeguarding "essential values such as national survival, sovereign independence, and economic prosperity" against risks including supply disruptions, technology leakage, and excessive external dependence, emphasizing an inherently relational logic that links a state's vulnerabilities to the instruments available for mitigation and defense (Yuzue & Sekiyama, 2025). In digital contexts, classical notions must expand to address new forms of fragility – data integrity, identity security, and network resilience – introduced by pervasive technologies and platformized economic activity (Saeed, Shah, Hassan, Raza, & Ahmed, 2023).

Hybrid threats blend military, informational, cyber, economic, and political tactics into synchronized campaigns that exploit institutional seams and social trust deficits.

Contemporary analyses detail how non-kinetic operations – disinformation, infrastructure disruption, and psychological influence – have become central tools in hybrid arsenals, underscoring the need for context-specific, intersectoral responses (Kaczmarek, 2025). In parallel, intelligence and security research highlights the composite and adaptive nature of hybrid risks and argues for whole-of-society frameworks that integrate political science, cybersecurity, economics, and strategic communications (Nilsson, 2025).

Digital transformation accelerates productivity and connectivity but simultaneously expands attack surfaces and systemic dependencies. A systematic review shows that digitalization raises the stakes for cybersecurity, data integrity, and organizational resilience, making risk governance a first-order condition for sustainable performance (Saeed et al., 2023). Sector-specific studies in energy further classify threats to the economic security of "digital enterprises" – from system intrusions and supply-chain disruptions to compromised control systems – demonstrating how domain exposure translates into macro-level vulnerability (Khusainova, Zemskii, & Khramova, 2021). Emerging quantitative work links cybersecurity risk evaluation to digital and sustainable business models, reinforcing the case for integrated, data-driven assessment (Erdem & Özdemir, 2025).

Across regions, hybrid campaigns commonly combine energy coercion, information operations, and cyber disruption targeting critical infrastructure. European practice increasingly organizes countermeasures around resilience ecosystems that span civilian and defense domains, reflecting interdependencies across sectors (Hybrid CoE/JRC, 2023). In Ukraine – a salient case given ongoing conflict and high digital dependency – evidence points to coordinated cyberattacks, propaganda, and economic coercion that blur boundaries between war and peace and between state and non-state actors, prompting calls for integrated countermeasures (Kovalchuk, 2025).

Despite the expanding literature, several substantive gaps remain at the intersection of hybrid threats, economic security, and digitalization. First, there is no widely accepted integrated measurement framework that links discrete hybrid-threat vectors (cyber incidents, disinformation shocks, energy coercion) to macro-economic outcomes (growth, investment, trade, market volatility) in a way that is comparable across countries and over time; existing studies tend to be siloed by threat type or sector (Yuzue & Sekiyama, 2025; Saeed, Shah, Hassan, Raza, & Ahmed, 2023). Second, empirical work rarely combines event-study designs for market-based effects with panel econometrics for real-economy impacts, limiting causal inference on how hybrid campaigns propagate from information systems to financial and production systems (Erdem & Özdemir, 2025). Third, sectoral analyses often emphasize energy and ICT but under-specify cross-sector spillovers – for example, how targeted infrastructure disruptions cascade into payment systems, logistics, and consumer confidence (Khusainova, Zemskii, & Khramova, 2021; Hybrid CoE/JRC, 2023). Fourth, while policy papers stress "whole-of-society" approaches, there is little operationalization of resilience metrics (redundancy, recoverability, adaptability) that allow benchmarking across jurisdictions and tracking improvement over time (Nilsson, 2025).

Fifth, the literature underexplores the interaction between disinformation dynamics and capital markets – specifically, whether coordinated information operations measurably alter risk premia, liquidity, or sector rotations beyond short-lived anomalies; this constrains the design of early-warning indicators for economic coercion. Sixth, ESG integration remains conceptually thin: studies seldom test whether governance and social-trust variables mediate the relationship between hybrid threats and economic outcomes, or whether ESG-aligned firms demonstrate differential vulnerability and recovery trajectories. Seventh, case evidence is geographically concentrated; comparative designs beyond headline cases (e.g., Ukraine) are needed to disentangle threat composition, institutional capacity, and digital maturity as drivers of heterogeneous impacts (Kovalchuk, 2025). Eighth, advances in real-time analytics (nowcasting using digital traces, anomaly detection on telemetry) are rarely validated against audited incident datasets, raising external-validity questions for decision support (Saeed et al., 2023).

Anchored in these gaps, the article contributes a structured framework that maps hybrid-threat vectors to economic transmission channels and resilience levers; an operational indicator set that fuses digital signals (incident logs, sentiment indices, network metrics) with traditional statistics (FDI, market depth, production indices); a sector-sensitive template for risk and resilience scoring usable by policymakers and firms; and a research agenda specifying data standards and identification strategies to strengthen causal claims. Together, these advances aim to move the field from descriptive taxonomy toward comparative, measurable, and actionable economic-security analysis in the context of digital transformation.

Table 1. Research Gaps at the Intersection of Hybrid Threats, Economic Development, and Digital Transformation

	Research gap (short)	Why it matters	Proposed contribution / response
1	No integrated framework linking hybrid-threat vectors to macroeconomic outcomes	Current studies are siloed; results aren't comparable across countries/time	Unified mapping from threat vectors → transmission channels → macro indicators
2	Limited causal designs (event-study + panel)	Hard to infer how shocks propagate from info/cyber to real economy	Combine event studies (market effects) with panel econometrics (growth, FDI, trade)
3	Under-specified cross-sector spillovers	Disruptions cascade across finance, logistics, energy	Sector-to-sector spillover template and network view of critical interdependencies
4	Vague resilience metrics	Can't benchmark redundancy, recoverability, adaptability	Operational resilience scorecard with measurable KPIs and thresholds
5	Disinfo–capital markets link underexplored	Lacks early-warning signals for coercion via narratives	Tests for effects on risk premia/liquidity; narrative-to-market early-warning indicators
6	Thin ESG integration	Missed mediators/moderators of impact and recovery	Model ESG/governance and social trust as mediators; heterogeneity of firm responses
7	Case concentration, low comparability	Findings don't generalize beyond a few high-profile cases	Comparative, multi-country design with harmonized indicators and context controls
8	Weak validation of real-time analytics	Nowcasts/anomaly detection may lack external validity	Pair digital traces with audited incident datasets; rolling revalidation protocols

Source: systematized by the author

The synthesized gaps reveal fragmentation in concepts, methods, and validation practices, which obscures causal pathways from hybrid-threat vectors to macroeconomic outcomes. By offering an integrated mapping framework, sector-sensitive spillover analysis, operational resilience metrics, and validated real-time indicators fused with traditional statistics, the article advances the field from descriptive taxonomies toward comparable, decision-useful measurement and evidence-based policy design.

Aims. The article aims to determine how hybrid threats shape economic development within a digital environment and to outline strategic responses that strengthen resilience and sustain growth.

To achieve this purpose, the study first characterizes hybrid threats as multidimensional, cross-sectoral phenomena whose form and intensity have evolved in the digital era, combining cyberattacks, disinformation, economic coercion, and other non-kinetic instruments into integrated campaigns. It then analyzes the mechanisms through which such threats propagate across economic systems – distorting investment flows, destabilizing financial markets, constraining innovation capacity, and eroding institutional trust – thereby linking micro-level disruptions to macro-level development outcomes. Building on this analysis, the article identifies the sectors most exposed to hybrid risks, with particular attention to finance, energy, telecommunications, and other elements of critical infrastructure where digital interdependence creates systemic vulnerabilities. Finally, it systematizes countermeasures and formulates strategies to enhance economic resilience by integrating technological safeguards (cybersecurity and data-integrity controls), institutional arrangements (governance and risk-management frameworks), and policy instruments (regulatory coordination and international cooperation), thus providing a coherent roadmap from diagnosis to actionable response.

Methodology. The study proceeds by characterizing hybrid threats as multidimensional, cross-sectoral phenomena that combine cyberattacks, disinformation, economic coercion, energy dependence, and political manipulation into integrated campaigns. It analyzes the mechanisms through which such threats propagate across economic systems – distorting investment flows, destabilizing financial markets, constraining innovation capacity, and eroding institutional trust – thereby linking micro-level disruptions to macro-level development outcomes. Building on this analysis, the article identifies sectors most exposed to hybrid risks (finance, energy, telecommunications, and other elements of critical infrastructure), and systematizes countermeasures by integrating technological safeguards (cybersecurity and data-integrity controls), institutional arrangements (governance and risk-management frameworks), and policy instruments (regulatory coordination and international cooperation). Anchored in identified research gaps, the contribution includes a structured framework that maps threat vectors to economic transmission channels and resilience levers, an operational indicator set fusing digital signals with traditional statistics, and a sector-sensitive template for risk and resilience scoring accompanied by a research agenda for data standards and identification strategies.

Results. In the digital environment, hybrid threats manifest as a confluence of cyberattacks, disinformation campaigns, economic coercion, and data manipulation. These tactics exacerbate one another, forming a layered risk profile that undermines institutional legitimacy, distorts markets, and constrains strategic autonomy.

In the digital sphere, hybrid threats manifest as mutually reinforcing vectors – coordinated cyberattacks, disinformation, economic coercion, and data manipulation – that erode institutional trust, unsettle markets, and constrain strategic autonomy. Empirically, Ukraine illustrates the acceleration in intensity: according to the State Service of Special Communications and Information Protection (CERT-UA), cyber incidents rose from 2,541 in 2023 to 4,315 in 2024, a 69.8% increase, with recurrent targeting of public authorities, energy, and defense-adjacent entities (State Service of Special Communications and Information Protection of Ukraine, 2025; Institute of Mass Information, 2025). Independent trackers corroborate the surge and emphasize concentration against critical infrastructure (Center for Strategic and International Studies, 2025). Across the European Union, the European Union Agency for Cybersecurity (ENISA) reports a persistently diversified threat landscape for July 2023 – June 2024, with public administration (19%), transport (11%), and finance (9%) among the most targeted sectors; availability attacks (e.g., DDoS), ransomware, and data compromise feature prominently (ENISA, 2024). A finance-specific assessment covering January 2023 – June 2024 highlights cross-border interdependence and modality patterns affecting EU financial entities and neighboring countries, including Ukraine (ENISA, 2025).

These dynamics translate into measurable pressures on economic development. Intensified cyber operations and information manipulation dampen investment attractiveness, erode trust in institutions, distort price discovery and liquidity in financial markets, and threaten the reliability of digital infrastructure – collectively raising risk premia and complicating long-term growth planning. Recent EU statements formally recognize that "hybrid campaigns," comprising cyber operations and disinformation, are aimed at undermining security, resilience, and democratic foundations across Member States and partners, reinforcing the need for integrated, whole-of-society responses (Council of the European Union, 2025).

Sectoral exposure is uneven. Finance, energy, and telecommunications – together with other critical-infrastructure domains – exhibit heightened vulnerability due to dense digital interdependencies, complex supply chains, and the potential for cascading effects. Correspondingly, effective counter-strategies must combine international cooperation (intelligence sharing, joint exercises, harmonized sanctions), robust institutional mechanisms (risk governance, regulatory coordination, resilience metrics), and technological innovation (modernized cybersecurity, OT/IT segmentation, real-time detection and response). The evidence base – rising incident volumes in Ukraine, sustained pressure on EU priority sectors, and official acknowledgement of coordinated hybrid campaigns - supports an integrated approach to detection, attribution, and mitigation that spans technical, informational, and policy layers (Council of the European Union, 2025; ENISA, 2024, 2025; State Service of Special Communications and Information Protection of Ukraine, 2025).

Table 2. Systematization of Hybrid-Threat Manifestations and Indicative Metrics (EU vs. Ukraine)

Vector	Illustrative metrics (from text)	EU (2023–2024)	Ukraine (2023–2024)	Notes for analysis
Cyberattacks	Incident counts; attack types; sectoral targeting	≈10,000 incidents (Jul 2023–Jun 2024); DoS/DDoS 41.1%; malware 25.7%; personal-data breaches 19%; sectors most targeted: public admin 19%, transport 11%, finance 9%	Incidents up from 2,541 (2023) to 4,315 (2024) (≈+69.8%); recurrent targeting of government, energy, defense-adjacent entities	Use as baseline for trend lines (YoY growth; sectoral heat map)
Disinformation / data manipulation	Volume; reach; automation share	— (structure noted as EU-wide hybrid campaigns accompanying cyber ops)	Large-scale social-media corpus during 2022 war: 349,455 messages; ~14.4M reach via retweets; ~20.28% of spreaders bots	Link narrative spikes to cyber events (lead/lag correlation)
Economic coercion & infrastructure sabotage	Qualitative identification of hybrid campaigns against CI; escalation risk windows	EU statements on persistent hybrid campaigns targeting CI; risk projected to escalate around major political/summit events	>650 cyberattacks documented since 2022 aligned with kinetic and narrative tactics	Code binary indicators for "campaign periods" for event-study windows
Interlocking effects	Co-occurrence of vectors (cyber + info + economic)	Recognized in EU hybrid doctrine as confidence-eroding and attribution-complicating	Observed synchronization of DDoS/intrusions with narrative pushes	Model multi-vector episodes as compounded shocks (interaction terms)

Source: systematized by the author

Hybrid operations reduce investment attractiveness, erode institutional trust, distort the functioning of financial markets, and compromise digital infrastructure – effects that are now visible in macro- and meso-level indicators across the EU and Ukraine.

Investment and growth dynamics. In the EU, investment intensity (gross fixed capital formation) stood at 21.2% of GDP in 2024 (21.1% in the euro area), with higher ratios in Czechia (26.2%), Estonia (26.1%) and Romania (25.7%), reflecting divergent post-crisis growth paths and uneven exposure to security shocks (Eurostat, 2025). Ukraine's growth profile shows a war-shock contraction followed by a slowing recovery: −28.8% GDP in 2022, a +5.3% rebound in 2023, and ~2.9% in 2024, with forecasts pointing to ~2%–3% for 2025 as energy damage, labor shortages, and security risks weigh on expectations (European Parliament, 2024; Reuters, 2024; World Bank, 2025a; CES, 2025; NBU, 2025a). These trajectories are consistent with heightened country-risk premia and precautionary behavior among investors under hybrid pressure.

Financial-market functioning and risk. EU authorities increasingly treat cyber and hybrid vectors as systemic. The European Systemic Risk Board highlights financial-stability risks from cyber incidents and calls for macroprudential responses; sectoral guidance has been reinforced by resilience regulation (e.g., NIS2/DORA) and supervisory attention (ESRB, 2024). For Ukraine, the Financial Stability Index in 2025

was driven by volatility in government-debt spreads, while FX-related factors remained the largest contributors—an environment typical of elevated geopolitical risk and intermittent energy shocks (NBU, 2025b). Such market signals align with the broader European tightening of investment-screening regimes amidst security concerns (European Commission, 2024).

Digital-infrastructure stress and incident trends. The European Union Agency for Cybersecurity's latest Threat Landscape synthesizes over 11,000 publicly reported incidents across 2023–2024, with availability attacks (e.g., DDoS), ransomware, and threats against data among the prime vectors; finance, public administration, and transport feature prominently among targeted sectors (ENISA, 2024a, 2024b). A finance-specific cut for Jan 2023 – Jun 2024documents 488 publicly reported incidents affecting the European financial sector and neighboring countries, including Ukraine – evidence of cross-border risk transmission into payment, market, and customer-data functions (ENISA, 2025a, 2025b). EU officials also reported that disruptive attacks doubled into early 2024, with geopolitically motivated activity linked to Russia (Associated Press, 2024).

Ukraine's hybrid exposure and macro linkages. In parallel, Ukraine's cyber-incident count rose from 2,541 (2023) to 4,315 (2024) (+69.8%), with recurrent targeting of public authorities, energy assets, and defense-adjacent entities (SSSCIP/CERT-UA, 2025). Physical-digital spillovers are salient: the Kyiv School of Economics estimates $170 billionin infrastructure damage as of Nov 2024, a stock that constrains productive capacity, raises reconstruction needs, and complicates investor risk assessments (KSE Institute, 2025). These conditions feed through to financing costs and investment timing, dampening the pace of recovery even amid external support and policy efforts.

Across the EU and Ukraine, hybrid-threat dynamics are visible in investment ratios, growth slowdowns, market-risk indicators, and escalating incident statistics. The economic channel runs from digital disruptions and narrative shocks to higher risk premia, delayed capital formation, and productivity headwinds, especially where critical infrastructure and finance are repeatedly targeted. Strengthening cross-border resilience (regulatory, supervisory, and operational) and hardening digital infrastructure are therefore not only security imperatives but also pro-growthmeasures that stabilize expectations and lower the cost of capital.

Hybrid threats in the digital environment – spanning cyberattacks on operational technologies, disinformation, data manipulation, economic coercion, and supply-chain compromise – represent multi-layered risks to both national economies and enterprise stability. The policy matrix operationalizes a comprehensive approach by linking each vector of threat with a specific objective, high-impact actions, economic buffers, and measurable indicators. By doing so, it transforms a complex risk landscape into a practical tool for policymakers, regulators, and firms alike (Table 4).

Table 3. Key Economic and Cyber Indicators Linked to Hybrid-Threat Dynamics (EU vs. Ukraine, 2022–2025)

Domain	Indicator (period)	EU (or selected MS)	Ukraine	Notes / trend interpretation
Investment	Gross fixed capital formation share of GDP (2024)	21.2% EU-27; 21.1% euro area; higher in Czechia 26.2%, Estonia 26.1%, Romania 25.7%	—	Divergent investment intensity reflects uneven exposure to shocks and post-crisis paths.
Growth	Real GDP dynamics	—	−28.8% (2022) → +5.3% (2023) → ~2.9% (2024) → ~2–3% (2025f)	War-shock contraction followed by slower recovery; security risks and energy damage weigh on outlook.
Financial stability	Market/FS indicators (2025)	Systemic cyber/hybrid risk recognized; resilience rules (NIS2/DORA) emphasized	FSI driven by gov't-debt spread volatility; FX factors largest contributors	Heightened risk premia and precautionary behavior under hybrid pressure.
Cyber incidents (total)	Reported incidents (2023–2024 window)	>11,000 publicly reported incidents across 2023–2024; key vectors: availability (DDoS), ransomware, threats against data	2,541 (2023) → 4,315 (2024) (+69.8%)	EU pattern diversified across sectors; Ukraine shows sharp YoY escalation targeting gov't/energy/defense.
Cyber incidents (finance)	Sector cut (Jan 2023–Jun 2024)	488 publicly reported incidents affecting European financial sector (incl. spillovers)	Included within cross-border set	Evidence of transmission into payments, markets, and customer-data functions.
Disruptive activity	Year-over-year change (early 2024)	Disruptive attacks doubled; geopolitically linked	—	Signals intensification of hybrid vectors around geopolitical events.
Physical–digital spillover	Infrastructure damage stock (as of Nov 2024)	—	~$170 billioncumulative damage	Capital stock losses constrain capacity, raise reconstruction needs, and lift financing costs.

Source: systematized by the author

The matrix demonstrates that technical hardening alone is insufficient without institutional and macroeconomic complements. For example, cyber-segmentation and zero-trust architectures must be supported by continuity-of-service buffers in financial markets, while rapid detection and response must be reinforced by disclosure safe-harbors and coordinated international attribution. In this sense, the matrix provides a multi-scalar framework, balancing micro-level operational resilience with macro-level stability.

Table 4. Policy Matrix to Minimize the Economic Impact of Hybrid Threats in the Digital Environment

	Threat vector	Objective	High-impact actions (technical, org, policy)	Economic buffers	KPIs / Indicators
1	Cyberattacks on critical infrastructure (IT/OT)	Preserve continuity of essential services and market plumbing	Zero-trust + strict IT/OT segmentation; asset inventory & SBOM; MFA everywhere; immutable/offline backups; EDR/XDR + threat hunting; red/blue/purple teaming; sectoral cross-border drills	Continuity-of-service plans; pre-arranged central-bank/clearing liquidity; offline payments modes	MTTD/MTTR; patch latency; backup restore time; % crown-jewel assets with compensating controls
2	Ransomware & DDoS (availability)	Reduce downtime, revenue loss, and confidence shocks	Anycast/DDoS scrubbing; geo-fencing in surge windows; JIT hardening before elections/summits; quarterly ransomware tabletop + clean-room restores	Cyber insurance with IR panels; tax incentives for resilience CapEx	Downtime hours/quarter; % systems restorable from clean backup; loss-given-incident
3	Data manipulation & integrity attacks	Protect price discovery, reporting, and operations	Cryptographic signing of critical data; append-only logs; dual control for updates; integrity analytics on oracles/master data	Safe-harbor for prompt disclosure of integrity incidents	% critical datasets with integrity checks; integrity alerts resolved <24h
4	Disinformation / influence ops	Limit demand shocks, bank-runs, and investor panic	Narrative nowcasting (rumor velocity, botnets, cross-platform checks); pre-authorized crisis messaging; media-literacy toolkits for high-impact groups	Temporary disclosure relief during proven manipulation	Time-to-debunk; rumor half-life; spread vs baseline; CDS/spread moves during events
5	Supply-chain / third-party compromise	Prevent cascades from a vendor breach	Tiered due-diligence; continuous posture scoring; SBOM + patch SLAs; tenant isolation; JIT credentials; coordinated disclosure & patch sprints	Diversification mandates for critical SaaS/cloud; strategic redundancy	% critical vendors under continuous monitoring; median time to remediate 3rd-party CVEs
6	Economic coercion (energy, logistics, finance)	Blunt macro shocks to growth, trade, inflation	Hybrid stress tests (OT compromise + info ops + FX pressure); strategic reserves & alternate routes; joint procurement; market safeguards (collateral flex, short-selling curbs, emergency liquidity)	Reserve adequacy; standing swap/credit lines	Stress-loss under hybrid scenarios; reserve sufficiency; settlement fails
7	Event-driven surges (elections, summits)	Reduce risk premia around sensitive windows	Time-boxed elevated posture (access tightening, patch freeze, surge SOC staffing, DDoS uplift); targeted public advisories	Stabilization communications to markets/SMEs	Incident rate vs baseline; recovery times; volatility deltas around event
8	SME & municipal weak-links	Lift the floor to protect the macro system	Subsidized MSSP bundles; one-click baseline hardening (MFA, backups, EDR); ISAC membership & auto-IOC sharing	Grants/vouchers; pooled procurement	SME controls adoption; incidents per 1,000 SMEs; average CIS/ISO control score
9	Measurement, early warning & disclosure	Make risks priced and managed, not hidden	National hybrid-threat dashboards (weekly vector/sector metrics, narrative heatmaps); event-study + panel models linking incidents to markets/output; rapid, standardized disclosure	Legal safe-harbor for fast disclosure	Metric timeliness; statistical significance of incident→market links; disclosure latency

	Threat vector	Objective	High-impact actions (technical, org, policy)	Economic buffers	KPIs / Indicators
10	Governance, ESG & international coordination	Turn security into a growth enabler	Board-level cyber committees; exec pay tied to resilience KPIs; integrate resilience into ESG "G"; harmonize NIS2/DORA-style rules; joint attribution/sanctions	Cross-border MoUs; shared playbooks	Board cyber competence; audit pass rates; number of joint actions; ESG-G score with resilience metrics

Source: systematized by the author

Discussion. The comparative analysis of approaches to assessing and responding to hybrid threats demonstrates both the diversity of methodologies and the need for integration. Quantitative frameworks – such as indices, incident counts, or econometric models – offer standardized benchmarks but may overlook narrative dynamics or institutional trust erosion. Conversely, qualitative and mixed-method approaches capture perceptions, social trust, and sectoral spillovers but often lack comparability across time and jurisdictions. Thus, hybridized approaches – combining structured indicators with context-sensitive insights – provide the strongest foundation for policy and resilience design.

A persistent tension exists between the speed of digitalization and the slower evolution of security governance. Rapid deployment of AI, cloud, and interdependent infrastructures drives productivity but widens the attack surface, outpacing the development of regulatory safeguards and organizational resilience. This imbalance is particularly pronounced among small and medium-sized enterprises and municipal institutions, where resource limitations constrain the implementation of advanced security measures.

In addition, systemic challenges complicate response strategies. Legal regulation remains fragmented, with the European Union advancing harmonization through instruments such as NIS2 and DORA, but global coordination still hampered by divergent interests. International alignment is further challenged by geopolitical rivalries, even though hybrid campaigns are inherently transnational. Resource constraints – including financial capacity, skilled cybersecurity professionals, and technological sovereignty – exacerbate these difficulties, leaving many economies exposed to persistent vulnerabilities.

Yet forward-looking perspectives offer new pathways. The economy of trust framework positions transparency, rapid disclosure, and resilience as sources of competitive advantage rather than compliance burdens. Cyberdiplomacy is gaining traction as a mechanism for joint attribution, norm-building, and coordinated sanctioning of hybrid aggressors. Meanwhile, digital sovereignty emphasizes the strategic importance of secure infrastructure, indigenous innovation, and reduced dependency on foreign providers. Together, these emerging models suggest that economic development and security are converging into a single agenda: sustainable growth requires resilient digital ecosystems, and resilient digital ecosystems strengthen economic competitiveness.

Conclusion. Hybrid threats in the digital era undermine stability by eroding institutional trust, reducing investment attractiveness, distorting financial-market functioning, and stressing digital infrastructure. The evidence of diversified pressure across the European Union and the sharp escalation of incidents in Ukraine underscores uneven sectoral exposure and the need for integrated, whole-of-society responses. Effective strategies combine international cooperation, robust institutional mechanisms, and technological innovation, while strengthening cross-border resilience and hardening digital infrastructure as pro-growth measures that stabilize expectations and reduce risk premia. By providing a conceptual framework and practical guidance, the article supports the design of resilient, adaptive, and secure economic systems in an increasingly interconnected world.

Funding. The author declare that no financial support was received for the research, authorship, and/or publication of this article.

Conflict of interest. The author declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement. The author declare that no Generative AI was used in the creation of this manuscript.

Publisher's note. All claims expressed in this article are solely those of the author and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References:

1. Gatopoulos, D. (2024, May 7). Europe's cybersecurity chief says disruptive attacks have doubled in 2024, sees Russia behind many *AP News*. https://shorturl.at/ulVwK
2. Center for Strategic and International Studies. (2025, May). *Significant cyber incidents since 2006* (tracker report) [PDF]. https://shorturl.at/E130b
3. Council of the European Union. (2025, July 18). *Hybrid threats / Russia: Statement by the High Representative on behalf of the EU condemning Russia's persistent hybrid campaigns against the EU, its Member States and partners*. https://shorturl.at/Zq8E7
4. Erdem, M., & Özdemir, A. (2025). Evaluation of cyber security risk pillars for a digital, innovative, and sustainable model utilizing a novel fuzzy hybrid optimization. *Computers & Security, 153*, 104394. https://doi.org/10.1016/j.cose.2025.104394
5. ENISA. (2024, September 19). *ENISA Threat Landscape 2024* (ETL 2024) [PDF]. European Union Agency for Cybersecurity. https://shorturl.at/EqL9t
6. ENISA. (2025, February 21). *Threat landscape: Finance sector (reporting period Jan 2023–Jun 2024)* [PDF]. European Union Agency for Cybersecurity. https://shorturl.at/tR9GO
7. Jungwirth, R., Smith, H., Willkomm, E., Savolainen, J., Alonso Villota, M., Lebrun, M., Aho, A. and Giannopoulos, G., Hybrid Threats: A Comprehensive Resilience Ecosystem, EUR 31104 EN, Publications Office of the European Union, Luxembourg, 2023, ISBN 978-92-76-53292-7 (main), doi:10.2760/37899 (main), JRC129019. https://publications.jrc.ec.europa.eu/repository/handle/JRC129019
8. Kaczmarek, K. (2025). Security and hybrid threats. *Defence Science Review*. https://doi.org/10.37055/pno/208458
9. Khusainova, E., Zemskii, V., & Khramova, M. (2021). Threats to the economic security of a digital enterprise in the energy industry. *E3S Web of Conferences, 288*, 01018. https://doi.org/10.1051/e3sconf/202128801018
10. Kovalchuk, M. (2025). Hybrid Threats and Economic Coercion: Contemporary Challenges to Economic Security in the Digital Environment. *Bulletin of the Academy of Labor, Social Relations and Tourism. Series: Economics, Psychology and Management*, *5*. https://doi.org/10.54929/3041-2390-2025-05-01-04
11. State Service of Special Communications and Information Protection of Ukraine / SSSCIP (CERT-UA). (2025, January 8). *CERT-UA processed 4,315 cyber incidents in 2024* [News release]. https://cip.gov.ua/en/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv

12. Nilsson, N., Weissmann, M., & Palmertz, B. (2025). Hybrid Threats and the Intelligence Community: Priming for a Volatile Age. *International Journal of Intelligence and CounterIntelligence*, 1–23. https://doi.org/10.1080/08850607.2024.2435265
13. Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. *Sensors*, *23*(15), 6666. https://doi.org/10.3390/s23156666
14. Yuzue, N., & Sekiyama, T. (2025). Defining economic security through literature review. *Frontiers in Political Science, 7*. https://doi.org/10.3389/fpos.2025.1501986