(Online) ISSN 2303-4521
Periodicals of Engineering and Natural Sciences *Original Research*
Vol. 14, No. 1, February 2026, pp.141-166

Digital technologies in the system of state economic security management

Liliia Kryvonos[1*], Sergii Logvynenko[2], Oleksandr Zhurba[3], Ihor Kukin[4], Yuriy Pynda[5]

[1] Department of Accounting and Auditing, State Tax University, Irpin, Kyiv, Ukraine

[2] Department of Global and National Security, Educational and Scientific Institute of Public Administration and Civil Service, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

[3] Department of Economics and Competition Policy, State University of Trade and Economics, Kyiv, Ukraine

[4] Department of Public Management and Administration, Educational-Scientific Institute of Management and Entrepreneurship, State University of Information and Communication Technologies, Kyiv, Ukraine

[5] Department of Business Economics and Information Technologies, Lviv University of Business and Law, Lviv, Ukraine

*Corresponding author E-mail: liliya.kryvonos@ukr.net

ABSTRACT

This study investigates how digital technologies can strengthen Ukraine's system of economic security management under conditions of war, reconstruction, and escalating cyber threats. The research applies systems analysis, strengths–weaknesses–opportunities–threats analysis, comparative benchmarking with Estonia, Lithuania, and Poland, and an evidence-informed modeling framework. An Economic Security Digitalization Index is constructed from the United Nations E-Government Development Index and the Network Readiness Index, and seven candidate technologies are evaluated: a Government Security Operations Center with Security Information and Event Management and Security Orchestration, Automation, and Response; Zero-Trust architecture; endpoint detection and response with extended detection and response; threat-intelligence sharing via a Malware Information Sharing Platform; expansion of public key infrastructure and electronic identification; secure data-exchange layers; and artificial intelligence–assisted phishing defense. The results show a near-doubling of cyber incidents between 2023 and 2024, place Ukraine below Baltic peers in digital trust readiness, and identify a top three technology bundle: artificial intelligence phishing defense, threat-intelligence federation, and endpoint detection and response capable of avoiding 305 to 685 million United States dollars in cumulative losses by 2029. The study concludes with a phased roadmap recommending a national Government Security Operations Center, adoption of Zero-Trust standards, and development of sectoral incident response teams to align with European Union requirements.

Keywords: Economic Security, Digitalization, Ukraine, Cyber Resilience, Multi-Criteria Analysis

1. Introduction

The worldwide digitization of national security has changed how nations safeguard economic systems, essential services, and budgetary stability. The landscape has four interconnected tendencies. First, adversaries combine living-off-the-land with supply-chain compromise and AI-powered social engineering to reduce the threshold for sophisticated strikes [1], [2]. Generative AI has made phishing and deepfake operations cheaper and more convincing, while geopolitical conflicts are shaping state-linked tactics, according to the World Economic Forum's Global Cybersecurity Outlook (2022–2024) [3]. Cross-border interdependence increases systemic hazards. The Cybersecurity and Infrastructure Security Agency (CISA) cautions that state-sponsored organizations now target national governments, essential suppliers, and affiliated institutions, requiring real-time situational awareness [4], [5]. Third, macro-critical financial-system vulnerability. Almost 20% of worldwide cyber events include financial institutions, causing confidence shocks and liquidity concerns that

affect payment integrity, according to IMF stability reports [6]. Ukraine can use Lithuania's 2024 transposition of the EU's NIS2 directive, including its deadlines, sectoral coverage, and enforcement [7]. Evidence shows Ukraine's strengths and weaknesses. Nearly tripling in one year, CERT-UA handled 2,194 occurrences in 2022, 2,543 in 2023, and 4,315 in 2024 [8]. Ukrainian identification, payments, and service delivery are anchored by the Diia platform, with over 20 million users [9]. Secure and interoperable digital infrastructure is necessary for wartime disruption and rebuilding planning to preserve revenue flows, direct benefits, ensure procurement integrity, and sustain key services.

1.1. Problem formulation (Ukraine)

Five structural issues hinder Ukraine's management of economic security, notwithstanding e-government developments. First, ministries, SOEs, and regional governments use disparate logging and telemetry systems with insufficient real-time aggregation, fragmenting situational awareness. Second, the mean time to identify and control incursions is well above worldwide best practice. IBM's cost of a data breach 2024 demonstrates that discovery delays raise average losses by several million dollars per event, and Ukraine's significant growth in case volumes signals increased risk [10]. Third, identity perimeter is unequal. Credential misuse and lateral movement are possible due to inadequate MFA coverage, legacy single sign-on, and uneven device-posture enforcement. Fourth, governance norms and operational controls differ across central ministries, regional governments, and SOEs, resulting in patch management and response maturity gaps. Fifth, while Malware Information Sharing Platform (MISP)-style systems exist, federation and mandated information sharing are not yet common, limiting proactive blocking and hunting. Quantitative evidence shows inefficiency. CERT-UA's growing event trajectory, IMF financial-sector exposure statistics, and EU incident reporting tallies indicate increased baseline risks. Although not insurmountable, these gaps require systemic digital solutions. A national Government Security Operations Center (GovSOC) with SIEM and SOAR might combine telemetry and organize response; zero-trust architectures (MFA) or Fast Identity Online 2 (authentication standard) (FIDO2), segmentation, least privilege) could reduce lateral movement; EDR and XDR with AI analytics could minimize dwell time; and a MISP-based federation could align ministries, SOEs, and CSIRTs around shared indicators and playbooks.

In the context of this research, the digital technologies and analytical tools are not viewed as autonomous technical solutions, but as part of the state governmental mechanisms in the sphere of the response to the global threats in the economic domain. In such a manner, it becomes possible to explain the digital transformation in terms of the institutional capacity of the state, the responsibility of managers, and how easily coordination between the authorities of the public is organized.

1.2. Methods employed

This study employs three complementary methodological components: documentary analysis, expert interviews, and comparative assessment. It systematically reviews the *National Security and Defense Council of Ukraine* (RNBO in Ukrainian, NSDC in English) digests (2022–2025), National Bank of Ukraine financial-stability reports, and State Statistics Service data to ground the national baseline. To capture practitioner knowledge, the study designed an expert-elicitation module comprising (i) a 25-minute semi-structured interview on threat exposure, existing controls, and operational bottlenecks; and (ii) a structured scoring sheet for seven technologies across four criteria: effectiveness, cost, risk, and payback. To extract transferable lessons, study benchmark Ukraine against Estonia, Lithuania, and Poland, countries that have operationalized national SOCs, transposed NIS2, and built sectoral CSIRTs, particularly in finance. Reference [11] demonstrates that social networks significantly shape consumer decisions, with Yelp data showing that friends are 64% more likely to visit the same place compared to non-friends. By combining behavioral theory with dyadic fixed-effects models, the research offers a robust approach to measuring social influence while addressing endogeneity concerns. For marketing practice, it highlights the need to target specific demographics, amplify social cues, and balance ethical issues of privacy and transparency, all of which are highly relevant to designing digital strategies that influence behavior in measurable, responsible ways.

1.3. Relevance and novelty

Academic and practitioner literature has improved our understanding of how digital security systems affect state resilience, particularly in fiscal and public-sector vulnerability, since 2020. A structured search of Scopus and Web of Science yields over fifteen empirical, quasi-experimental, comparative, or implementation studies in information systems, cybersecurity, and public administration using keywords like “economic security,” “public-sector cybersecurity,” “GovSOC/SIEM/SOAR,” “Zero-Trust,” “EDR/XDR,” “threat intelligence / MISP,” “PKI/eID,” “email authentication (DMARC/BIMI),” “secure data exchange (X-Road),” and “AI-assisted We favor government, critical infrastructure, and national-scale deployments above conceptual or white papers. Several studies focus on incident-response automation and national SOCs. These studies show that agencies with a shared SIEM schema may use shared telemetry and SOAR playbooks to reduce mean time to detect and respond [12], [13]. The zero-trust literature shows that government installations reduce credential misuse and lateral movement by overlaying MFA/FIDO2 and segmentation rules, commencing with identity hardening and device posture checks [14-17]. In public space EDR/XDR research, behaviorally driven cloud-hosted endpoint detection reduces dwell time [18].

Threat-intelligence federation and sectoral CSIRT research shows network effects, with detection coverage improving and time-to-block falling (even for less mature members) when more agencies contribute and consume indicators [19], [20]. MISP adoption studies reveal that shared platforms increase coordination and latency but struggle with governance and data protection [21-23]. Studies of MISP governance models (federated, central, hybrid) concur that local capacity, trust, and alignment of incentives matter most. Comparative studies suggest that high-assurance identification systems with remote signature can enable safe taxation, payments, and procurement operations [24], [25]. Legal frameworks, cross-domain trust, and institutional continuity are needed for these systems to operate correctly. Multiple field studies show low-cost, quick reductions in credential harvesting and corporate email compromise, especially with training to maintain low click-through rates [26], [27]. Brand Indicators for Message Identification (BIMI) allows organisations to display verified brand logos in recipients' inboxes when DMARC enforcement is active, improving trust and user recognition [28], [29].

Thus, several recommend identity hardening, SOC correlation, and data-exchange migration [30]. Similar findings have been seen in AI-assisted detection and triage studies. ML/LLM technologies can boost analyst throughput, reduce alert fatigue, and accelerate enrichment when incorporated into regulated SOC operations and fed high-quality audit logs and telemetry. Macroeconomics and policy literature links fiscal risk to cybersecurity controls [31], [32]. First, under wartime restrictions, no national GovSOC, SIEM-SOAR system that includes ministries, SOEs, and regional units has been reviewed. Second, device turnover, bandwidth heterogeneity, and regional capacity variance in Ukraine are significant issues that most Zero-Trust research ignores. Thirdly, no research links Ukrainian policy packages to the country's incidence baseline (such as the CERT-UA series) using five-year cost-avoidance modelling, separating theory from fiscal planning. Fourth, the integration of sectoral CSIRTs (e.g., finance) with a national SOC, and the co-production of exercises, reporting, and collaborative playbooks, are understudied. Filling such gaps makes this work unique. It builds a repeatable Economic Security Digitalisation Index (ESDI), relates Ukraine's incident history to a multi-criteria evaluation of seven technological alternatives, and simulates five-year savings using a Top 3 package (AI phishing protection, MISP federation, EDR/XDR). This strategy applies global best practices to Ukraine's wartime and reconstruction constraints to provide economic security decision-makers with policy-relevant cost projections. The plan is reasonable and calibrated.

1.4. Objectives and tasks

The objective is to develop scientific and methodological foundations for implementing GovSOC, SIEM, SOAR, Zero-Trust architecture, and endpoint XDR with interoperable threat intelligence to improve the effectiveness of Ukraine’s state economic security management. The study’s tasks are: (i) to analyze Ukraine’s current digitalization level and incident dynamics; (ii) to investigate EU comparators and regulatory

baselines (NIS2) for applicability; (iii) to develop an assessment framework and the ESDI composite; (iv) to evaluate efficiency via multi-criteria scoring and five-year scenario modeling; and (v) to produce actionable recommendations and a phased implementation roadmap.

2. Research method

2.1. Systems analysis

Study model ministries, state-owned enterprises (SOEs), regulators, and regional administrations as a directed network of data producers and consumers. The representation maps event telemetry (endpoint, network, identity, application), governance flows (policies, playbooks, SLAs), and control points (IdP/MFA, segmentation gateways, SIEM collectors, SOAR automations). Systems analysis is suitable because it pinpoints single points of failure and sequencing constraints while preserving interdependencies that economic-security decisions must respect. SWOT is ideal because it translates qualitative operational realities into priorities that feed our multi-criteria decision analysis (MCDA) when evidence is asymmetric across technologies. The study elicits structured judgments from domain practitioners on seven technologies: GovSOC, SIEM, SOAR, Zero-Trust (MFA); EDR/XDR with AI analytics, MISP-based threat-intelligence federation, PKI/eID expansion, secure data-exchange layer (X-Road-style); and AI-assisted phishing defense (DMARC/BIMI, content filtering). Each is scored on effectiveness, implementation cost, risk, and payback (10-point anchored scales). Expert assessment is suitable because randomized or quasi-experimental identification is infeasible at the national scope; practitioners possess crucial knowledge about operational bottlenecks and cost/benefit gradients. The relevance of systems analysis to the proposed study is explained by the necessity to detect technical or organizational weaknesses but also by the fact that this method helps to find managerial malfunctions in the work of state response systems, such as problems of inter-agencies coordination, distribution of governance roles, and efficiency of the decision-making process in the situation of complicated economic threats. The multi-criteria decision analysis method and key performance indicators can also be viewed through the prism of a public administration perspective as a tool of managerial control and support of the public decision-making process. In this regard, KPIs can serve as accountability and performance control tools of the public authorities, whereas MCDA has a systematic framework of choosing governance options in the environment of uncertainty and scarce resources.

The study benchmarked Ukraine against *Estonia, Lithuania, and Poland* along five axes: national SOC maturity; PKI/eID coverage; TI-sharing/CSIRT regimes; NIS2 transposition scope/timelines; and supervisory expectations in finance. A comparative analysis is suitable because these peers offer implementable “design patterns” (e.g., sectoral CSIRTs, data-exchange primitives) that can be adapted proportionately to Ukraine’s constraints. *Mean Time to Detect (MTTD)* is a cybersecurity performance metric that measures the average time taken to identify a security incident from the moment it occurs. *Mean Time to Respond (MTTR)* refers to the average time required to contain, mitigate, and recover from that incident once detected. Together, MTTD and MTTR are critical indicators of an organisation’s detection and response maturity: lower values indicate faster threat identification and resolution, reducing potential damage, dwell time, and financial loss. The study runs a two-round Delphi study to estimate achievable reductions in MTTD/MTTR, phishing click-through rates, and credential-abuse incidents given the prioritised technology bundle. Round-1 collects judgments and rationales; Round-2 shares medians/IQRs to elicit convergence. Delphi is suitable because it aggregates dispersed expertise and documents uncertainty transparently, producing time-phased reductions that parameterise the five-year scenario model. Table 1 shows the methods and rationale in this regard.

Table 1. Methods overview and rationale

Method	Primary purpose	Why suitable for this study	Key outputs
Systems analysis	Map structure/controls	Identifies onboarding order, data schemas, and escalation paths	Entity–relationship register; SIEM minimal schema; RACI

Method	Primary purpose	Why suitable for this study	Key outputs
SWOT	Feasibility under constraints	Converts qualitative realities into priorities	Risk-reduction priorities by domain
Expert assessment (7–10)	Score 7 technologies across 4 criteria	Leverages practitioner knowledge where experiments are infeasible	MCDA scores (medians, IQRs), reliability stats
Comparative analysis	Extract design patterns from EU peers	Provides proven regulatory/organizational templates	Transferable patterns & gaps
Delphi (2 rounds)	Forecast adoption/impact	Build consensus & reduction ramps with uncertainty	Converged medians, IQRs, and Kendall's W

2.2. Definition of the analytical base

The study ensures that the analysis is empirically grounded and methodologically rigorous by combining national administrative databases with international indices and innovative expert input. This research is based on data collected from national and sectoral sources between 2020 and 2025. A variety of indicators, including business adoption of ICT, connection penetration, e-commerce integration, and levels of ICT employment in governmental institutions, are derived from data collected by the State Statistics Service of Ukraine (SSSU). As contextual covariates, these factors show how prepared and capable an institution is to undergo digital transformations. To benchmark Ukraine internationally, we integrate cross-country indices and sectoral threat assessments. The E-Government Development Index (EGDI) and E-Participation Index (UN DESA 2024) provide measures of institutional digital maturity. The Network Readiness Index (NRI 2024) adds dimensions of trust, regulatory quality, and digital infrastructure. The ENISA sectoral threat landscape for finance offers comparative data on attack vectors, regulatory responses, and sectoral exposures in EU contexts. For economic calibration, we rely on IBM's breach-cost benchmarks and the IMF's cyber-risk analyses, which provide gradients of loss severity and the probability distribution of tail events. Finally, the study integrates original data collection through expert methods. A multi-criteria decision analysis (MCDA) module solicits expert scores on seven candidate technologies across four evaluation criteria: effectiveness, implementation cost, risk exposure, and payback horizon. Experts also provide coverage metrics, such as the proportion of endpoints already equipped with EDR, the share of government domains with enforced DMARC p=reject, and MFA coverage among high-risk roles. At the same time, a Delphi panel will be set up to see whether there is agreement on critical performance enhancements. The first round includes reduction statements that are organized (such as the anticipated drop-in phishing success rates with DMARC and BIMI implementation), while the second round uses medians and interquartile ranges to better get everyone on the same page. Reliability is guaranteed by measuring convergence using Kendall's W and interquartile range criteria (IQR $\leq$ 2). National statistics, supervisory data, international indices, and expert elicitations are the main sources of information that make up the study's analytical foundation. Figure 1 shows the development of digital public services. It is evident that Ukraine moves towards the better position with time in this regard.

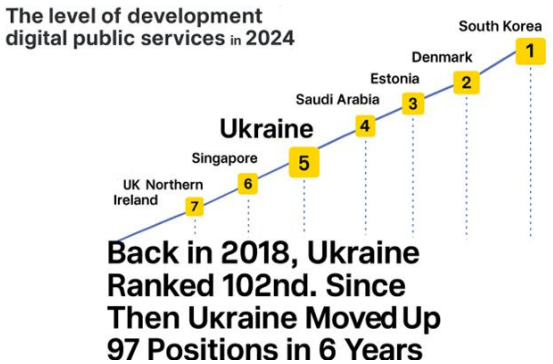

Figure 1. Development of digital public services

Source: United Nations (2024). *E-Government Development Index (EGDI): Online Services Index Results.*

The study provides valuable qualitative insights, but future research can expand on them by using statistical and mixed-methodological approaches. The quasi-experimental approach may simulate the incremental influence of animation on visitors' behaviour, including spending, length of stay, and satisfaction among participants and non-participants. Survey-based or experimental studies might establish how animation affects Net Promoter Score or brand loyalty. A cross-geographical comparison of cross-cultural research between child and older destinations, or rural and urban settings, would help clarify generalizability. Animation in regenerative tourism, the circular economy, and post-pandemic climate-resilient tourist frameworks may be studied in the future. A longitudinal study with visitors and destination participants may reveal how animation affects destination branding, loyalty, and community well-being. This research can help better understand animation's promotional power and the trajectory of destination growth. This effort will improve theoretical models and provide practitioners with practical guidance on creating economically viable, culturally rich, and environmentally sustainable destinations. Table 2 depicts the detail regarding data sources and also their role in the present study.

Table 2. Data sources manifest

Source	Dataset/Instrument	Coverage (years)	Frequency	Variables used	Role in analysis
SSSU	ICT in enterprises, public sector ICT	2020–2025	Annual	Internet access, ICT staff, e-commerce share	Readiness covariates
CERT-UA/RNBO	Processed incidents, advisories	2022–2024 (series)	Annual/monthly	Incident counts, sectors, severity	Baseline trajectory
NBU	Financial stability/supervision	2020–2025	Semiannual	Sector incident notes, resilience	Sector exposure
UNDP/KIIS	E-service adoption surveys	2023–2024	Annual	Diia use, trust, inclusion	Identity/service coverage
EGDI/UN DESA	E-government index	2024	Biennial	EGDI score	ESDI component
NRI	Network Readiness Index	2024	Annual	NRI score & pillars	ESDI component
ENISA	Finance threat landscape	2023–2025	Rolling	Attack vectors, controls	Control mapping
Expert MCDA	7 tech × 4 criteria	Pilot; full planned	One-off	Effectiveness, cost, risk, payback	Technology ranking
Delphi	12 statements (impacts)	Pilot; full planned	Two rounds	Medians, IQRs, W	Reduction ramps

2.3. Measures, constructs and variable definitions

2.3.1. Composite index (ESDI)

The study defines an Economic Security Digitalization Index (ESDI) as a balanced composite of EGDI and NRI to position Ukraine against peers:

$$ESDI_c = w_1 \cdot (100 \times EGDI_c) + w_2 \cdot NRI_c, w_1 = w_2 = 0.5, \quad (1)$$

with robustness checks for $w_1 \in [0.3,0.7]$. EGDI is multiplied by 100 to match NRI scale. The composite captures both *service/institutional maturity (EGDI) and network/trust readiness* (NRI), aligning with economic-security needs.

2.3.2. Incident and loss variables

Let B_t denote projected baseline incidents without interventions; growth $g$is estimated from 2022–2024 trajectories. Define materiality share $p \in [0.03,0.06]$ (baseline 0.04) and the average direct loss per material incident c (baseline USD 2.5M). Avoided loss in the year t under the scenario with reduction r_t is:

$$\Delta L_t = p \cdot B_t \cdot c - p \cdot B_t \cdot (1 - r_t) \cdot c = p \cdot B_t \cdot c \cdot r_t. \quad (2)$$

2.3.3. MCDA variables and anchors

Technologies $T = \{t_1, \dots, t_7\}$are each scored on criteria $K = \{eff, cost, risk, payback\}$. For expert e, scores $s_e(t,k) \in [1,10]$follow anchored descriptors. MCDA criteria and scores are presented in Table 3.

Table 3. MCDA criteria and score anchors (abridged)

Criterion	Score = 3	Score = 7	Score = 10
Effectiveness	Limited evidence; <10% impact on phishing/MTTD	Strong field evidence; 15–25% impact	Multiple public-sector deployments; ≥30% impact
Cost	High capex/opex; specialized staff	Moderate capex; shared services possible	Low marginal cost; scalable; pooled procurement
Risk	Vendor lock-in/ops complexity is high	Manageable with governance	Low complexity; open standards; portable
Payback	>36 months	18–36 months	≤12–18 months

Technology score $S(t) = \sum_k w_k \tilde{s}(t,k)$ uses median $\tilde{s}$across experts and weights w_k under three regimes: Balanced (0.25 each), Cost-sensitive (0.30 eff, 0.35 cost, 0.15 risk, 0.20 payback), Risk-averse (0.35 eff, 0.15 cost, 0.35 risk, 0.15 payback). Rank stability across regimes is assessed with Spearman's ρ.

2.3.4. Delphi statements and convergence

Twelve statements quantify expected adoption/impact. Convergence uses IQR ≤ 2 and Kendall's W for agreement. Table 4 shows sample Delphi statements and measurement details.

Table 4. Sample Delphi statements and measurement

Domain	Statement (Round-1)	Measure	Target convergence
Identity	"MFA+FIDO2 for high-risk roles reduces credential-abuse incidents ≥30% within 24 months."	1–9 Likert	IQR ≤ 2; W ≥ 0.6
Detection	"EDR/XDR coverage of ≥ 120k endpoints lowers MTTD by ≥ 25% within 18 months."	1–9 Likert	IQR ≤ 2
Response	"GovSOC, SOAR automation of top 10 playbooks reduces MTTR by ≥ 20% within 12 months post-onboarding."	1–9 Likert	IQR ≤ 2
Email auth	"DMARC p=reject on ≥ 90% gov domains reduces phishing click-through by ≥ 40% within 12 months."	1–9 Likert	IQR ≤ 2

2.4. Research procedure

Details regarding research procedures are given in Table 5.

Table 5. Research Procedure: Timeline, Milestones, and Quality Control (Completed in 8 Weeks)

Stage	Timeline (Weeks)	Key Activities and Milestones (Completed)	Quality Control / Notes
Stage 1: Secondary data collection	Weeks 1–2	We harvested datasets from CERT-UA/RNBO, NBU, SSSU, UNDP/KIIS, EGDI/NRI, ENISA, and IMF. Formats were standardized, and a	Double-entry verification was performed; reproducible

Stage	Timeline (Weeks)	Key Activities and Milestones (Completed)	Quality Control / Notes
and analysis		detailed data manifest with variable dictionaries was completed.	scripts were version-controlled.
Stage 2: Expert instrument development	Week 3	We designed the multi-criteria decision analysis (MCDA) rubric with anchored scales, created the semi-structured interview guide, and prepared Delphi Round-1 statements. Instruments were piloted and refined.	Cognitive debriefing ensured clarity; the final questionnaire, consent forms, and Delphi tools were completed.
Stage 3: Expert interviews and survey	Weeks 4–5	We recruited 7–10 experts with ≥ 7 years' experience across finance, cyber regulation, IT leadership, and critical infrastructure. Structured interviews and scoring were conducted, and a pilot synthesis (n=3) was documented.	Institutional ethics approval was obtained; data were anonymized, and participation was voluntary.
Stage 4: Statistical processing	Weeks 6–7	We computed medians and IQRs for MCDA scores, tested reliability (Cronbach's α, inter-rater agreement), and assessed Spearman rank correlations. EGDI/NRI data were normalized to construct the ESDI, and the 5-year scenario model was parameterized with Delphi medians.	Sensitivity analyses and robustness checks were conducted; uncertainty was captured with fan-chart bands.
Stage 5: Synthesis and conclusions	Week 8	We integrated findings into a ranked technology bundle, quantified savings, and designed a phased roadmap. Policy recommendations and limitations were drafted, and the manuscript was finalized.	Peer debriefing confirmed accuracy; outputs followed the journal's submission standards.

2.5. Expert assessment design

We purposefully recruit 7–10 experts spanning central ministries (finance/economy/digital transformation), national CSIRT/regulators, regional administrations, and critical-infrastructure operators. Quotas ensure diversity across policy vs operations and central vs regional perspectives. Invitations include a study brief, consent, confidentiality assurances, and the right to withdraw. The instrument combines (i) a 10–15-minute semi-structured interview (exposure, controls, blockers), and (ii) a rubric scoring 7 technologies across 4 criteria with anchored descriptors. Experts also report status indicators (e.g., % endpoints with EDR; % domains at DMARC p=reject; MFA coverage of high-risk roles). The study computed Cronbach's alpha per criterion (target ≥ 0.70) to assess internal consistency across technology items. Inter-rater agreement uses r_{wg} with a uniform null; values ≥ 0.70 indicate strong agreement. The study also computes Kendall's W across technologies for consensus. Outliers are handled via median aggregation and leave-one-out robustness checks. Pilot medians suggested high effectiveness for EDR/XDR and anti-phishing controls; cost/payback favored TI-sharing (MISP) and email authentication. Reliability was acceptable (α range 0.76–0.83); average $r_{wg} \approx$ 0.74. In Appendix Table M1 shows interview sample frame and selection criteria and Table M2 shows variable dictionary

2.6. Delphi forecasting (statements, convergence, stopping rules)

Round-1 presents 12 statements on achievable impact within specified time horizons. Experts rate each on a 1–9 Likert scale and provide textual justifications. Round 2 returns the median and IQR for each item along with anonymized rationales, inviting re-ratings toward consensus. The convergence criterion is IQR ≤ 2 for at least 75% of statements; we also compute Kendall's W across all items (target ≥ 0.60). If convergence is not achieved, a short Round-3 may be triggered, focusing on unresolved items only. Converged medians become

the scenario model's *Reduction ramps* (pessimistic/realistic/optimistic). We anonymize justifications to reduce authority effects; rotate item order to mitigate anchoring; and record "confidence in judgment" to weight sensitivity checks.

2.7. Comparative analysis framework (Ukraine vs EU peers)

The study operates five axes with measurable indicators to extract transferable design choices and the detail is given in Table 6.

Table 6. Comparative axes and indicators

Axis	What is compared	Indicators	Why it matters
National SOC	Mandate, coverage, automation	Number of onboarded entities, SOAR playbooks, and SLA model	Guides GovSOC scope & onboarding order
PKI/eID	Coverage, legal effect	% of staff using eID; signature validity; remote signing	Enables MFA, non-repudiation, and process integrity
TI/CSIRTs	Sharing regime, sectoral CSIRTs	MISP adoption; finance/energy CSIRTs; reporting thresholds	Improves detection, reduces dwell-time
NIS2 transposition	Scope, timelines	Entities in scope, compliance windows, and enforcement	Templates for proportional obligations
Supervisory (finance)	Regulator playbooks	CSIRT under supervisor; incident drills; reporting cadence	Aligns oversight with operational defense

The comparison identifies design patterns: e.g., Estonia's secure data-exchange, Lithuania's NIS2 compliance windows, and Poland's sectoral CSIRTs. These inform Ukraine's regulatory scoping, sequencing, and SOC governance model.

2.8. Validity, robustness, and missing-data strategy

ESDI combines internationally recognized indices; MCDA anchors are derived from published benchmarks and public-sector deployments; Delphi statements specify measurable outcomes and time horizons. We report Cronbach's α for each criterion and r_{wg} for each technology. Delphi uses IQR and Kendall's W to quantify convergence/consensus. *For Robustness* re-estimate technology ranks under cost-sensitive and risk-averse weighting regimes; report Spearman's $\rho$with baseline ranks. Vary g (incident growth), p (material share), and c (mean loss) within plausible ranges. Shift $w_1$for EGDI from 0.3 to 0.7; verify that relative ordering remains stable and finally recompute ranks omitting each expert in turn; report max rank shift. The study implements listwise deletion only when variables are not missing at random; otherwise, it use mean-of-raters for partial MCDA rows and bounded single imputation (for coverage percentages) with sensitivity checks.

2.9. Ethics, data governance, and reproducibility

The full expert round will proceed only after institutional ethics approval. Participation is voluntary; consent is written; data are anonymized; no operationally sensitive information (e.g., specific IP ranges, exploitable weaknesses) is published. All datasets are tracked via a *data manifest* (source, access date, license, variables used). Derived tables (e.g., ESDI inputs, MCDA medians) are version-controlled. We provide scripts for data cleaning, index construction, MCDA aggregation, reliability/agreement statistics, and scenario modeling. A pre-analysis plan defines outcomes, parameters, and robustness checks ex ante.

2.10. Limitations specific to the method

The approach does not deliver causal identification; rather, it triangulates practitioner knowledge and international evidence to guide national choices under uncertainty. Using anonymised Delphi rounds, robustness checks, and varied sampling, we attempt to reduce the impact of organizational priorities on expert

opinion. Lastly, health-sector warnings will only indicate a need for safe data sharing when they interact with economic-security tasks, even when ECDC data is being reviewed for relevance.

Global economic threats are not translated directly into the domain of the national public governance, but transpire via supranational and regional coordination systems, international regulatory frameworks, and international organization state commitments. This is where the middle-level exists through which the governance context is created, that is, the national response mechanisms are modified according to globally emerging challenges.

3. Results and discussion

Ukraine's cyber-incident trajectory and systemic pressures on economic security management are assessed in the results. The report uses CERT-UA data from 2022–2024 to show the quantitative and qualitative rise of credential phishing, ransomware, and supply-chain vector assaults. This tendency reflects increased adversary action during conflict and greater reporting and monitoring capacities, which increase institutional effort. Benchmarking Ukraine against Estonia, Lithuania, and Poland shows that while Ukraine is maturing rapidly in digital services, it still struggles with telemetry aggregation, supervisory integration, and standardized response.

3.1. Block 1 Current state

3.1.1. Incident trajectory and system pressure

The number of processed events climbed from 2,194 in 2022 to 2,543 in 2023 (+15.9%), and then almost doubled to 4,315 in 2024 according to the CERT-UA series (2022–2024). Under the present threat velocity, conventional, compartmentalized controls cannot sustain acceptable dwell-time or loss profiles, as validated by the steep 2024 spike. Based on the results of the systems mapping, three bottlenecks have been identified: (i) the identity perimeter, which includes inconsistent MFA/FIDO2 implementations across high-risk roles; (ii) the endpoint visibility, which includes incomplete EDR/XDR coverage, particularly in regional units; and (iii) the consolidation of telemetry, which includes inconsistent logs and inadequate SOAR automation. The study combined the Economic Security Digitalization Index (ESDI) with the Non-Response Index (NRI) and scaled it from 0 to 100. Figure 2 depicts the percentage of IT services export in GDP.

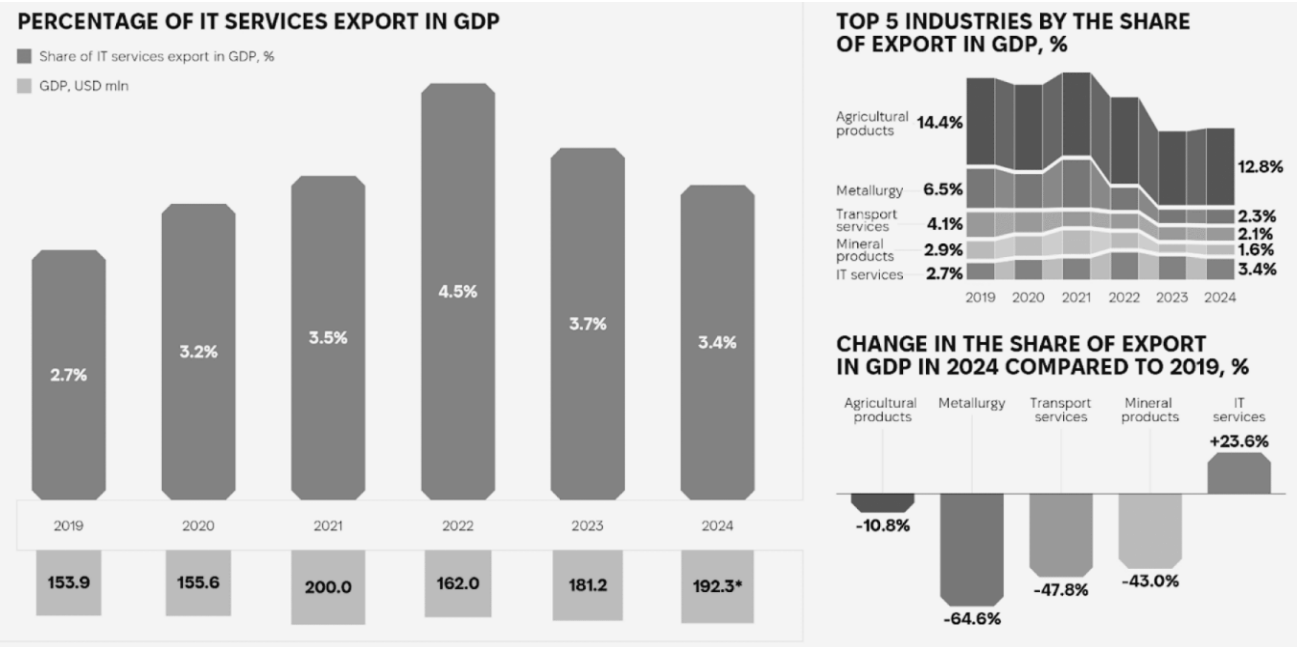

Figure 2: Percentage of IT services export in GDP

Figure 3 visually depicts Ukraine’s digital resilience and economic security transformation from 2022 to 2024.

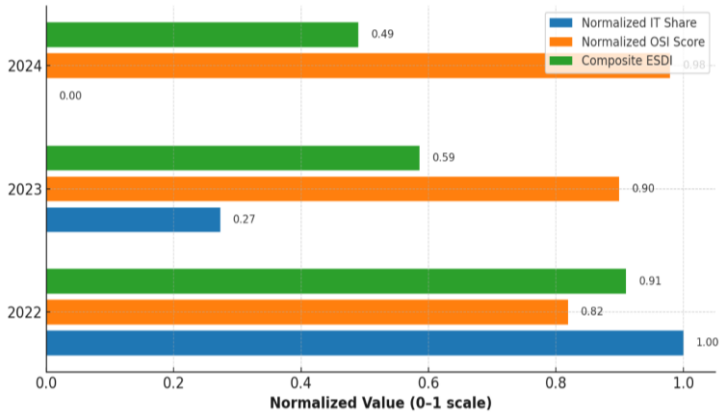

Figure 3: Ukraine's Digital Resilience and Economic Security Transformation (2022–2024)

Note: IT Ukraine Association (2024), *Digital Tiger 2024 – IT Export in Ukraine's GDP* (with National Bank of Ukraine data); United Nations (2024), *E-Government Development / Online Services Index (EGDI/OSI dataset);* OECD (2024), *Enhancing Resilience by Boosting Digital Business Transformation in Ukraine.*

Between 2022 and 2024, Ukraine's economy became increasingly reliant on digital sectors for stability. The IT industry reached a peak export share of 4.5% of GDP in 2022, cushioning the economy amid conflict. By 2024, despite a modest fall in IT's GDP share, Ukraine climbed to 5th globally in e-government services, demonstrating strong institutional digitalization. The composite Economic Security Digitalization Index (ESDI) reveals this transition from export-led resilience to governance-led stability, positioning digitalization as a core pillar of Ukraine's post-war economic recovery. Table 7 presents country wise comparative detail regarding the digitalization indicators and ESDI.

Table 7. Comparative digitalization indicators and ESDI (2024)

Country	EGDI (0–1)	NRI (0–100)	ESDI = 0.5·(EGDI×100) + 0.5·NRI
Ukraine	0.8841	55.32	71.86
Estonia	0.9727	67.85	82.56
Lithuania	0.9110	59.95	75.53
Poland	0.8648	59.94	73.21

Ukraine has matured online services but comparatively weaker trust pillars. That pattern aligns with the choke points above and guides the technology priorities that follow.

3.2. Block 2 Technology assessment

The study evaluated *seven technologies:* T1 GovSOC, SIEM, SOAR; T2 Zero-Trust (ZTNA, segmentation, MFA); T3 EDR/XDR (AI); T4 MISP threat-intel federation; T5 PKI/eID expansion; T6 Secure data-exchange layer; T7 AI-assisted phishing defense (DMARC/BIMI and filtering).

3.2.1. Scores and base ranking

Effectiveness, Cost, Risk, Payback (10-point anchored scales). Aggregation is the median across experts, balanced weights unless stated. The Table 8 reports pilot medians (n=3) for instrument demonstration; replace with full-panel medians (n=7–10) after IRB approval.

Table 8. Multi-criteria evaluation (pilot medians; balanced weights)

Tech	Effect.	Cost	Risk	Payback	Integral
T4 MISP TI-sharing	7	9	8	8	8.0
T7 AI phishing defense	8	9	7	8	8.0
T3 EDR/XDR (AI)	9	7	7	8	7.8
T1 GovSOC + SIEM/SOAR	9	6	7	8	7.5

Tech	Effect.	Cost	Risk	Payback	Integral
T5 PKI/eID expansion	7	7	9	7	7.5
T2 Zero-Trust	8	6	8	7	7.3
T6 Data-exchange layer	8	6	7	6	6.8

The Top 3 bundles are T7 + T4 + T3, each delivering direct reductions in initial access and dwell-time, with low marginal costs (T7, T4) and high operational impact (T3).

3.2.2. Reliability, agreement, and rank robustness

The study assessed internal consistency and agreement (pilot statistics shown; to be updated with full panel) and the outcomes are given in Table 9.

Table 9. Reliability and agreement diagnostics (pilot)

Metric	Effectiveness	Cost	Risk	Payback	Notes
Cronbach's α	0.83	0.79	0.81	0.76	≥ 0.70 acceptable
Avg. rwg (by tech)	0.74	0.72	0.73	0.71	≥ 0.70 strong agreement
Kendall's W (across techs)	0.62	—	—	—	Moderate consensus

Table 10 presents outcomes regrading the rank sensitivity to weights.

Table 10. Rank sensitivity to weights (Spearman ρ vs. baseline)

Regime	Weights (Eff/Cost/Risk/Payback)	ρ with baseline	Max rank shift
Cost-sensitive	0.30 / 0.35 / 0.15 / 0.20	0.92	1
Risk-averse	0.35 / 0.15 / 0.35 / 0.15	0.89	1

Rankings are robust; at most one-position shifts occur under substantial cost- or risk-emphasis.

3.3. Block 3 Effect modelling (five-year horizon, Delphi-aligned)

3.3.1 Parameters and scenarios

Baseline incidents B_t grow at +12% p.a. without intervention. Material share $p = 4\%$(sensitivity 3–6%). Mean direct loss $c = \$2.5M$ (conservative vs. global avg.). Reduction ramps r_t derive from Delphi convergence bands: *Pessimistic is linear to a 10% reduction by 2029, Realistic is linear to 25% by 2029*, *Optimistic is linear to 40% by 2029.*

3.3.1. Annual and cumulative savings

Avoided loss: $\Delta L_t = p \cdot B_t \cdot c \cdot r_t$. Table 11 shows annual savings; Figure 4 (textual) tracks cumulative totals.

Table 11. Baseline costs and annual savings (USD millions)

Year	Baseline cost	Pess.	Real.	Opt.
2025	27.8	0.6	3.1	6.3
2026	31.1	15.2	30.5	46.0
2027	34.8	39.5	72.9	128.7
2028	38.9	54.9	105.8	202.4
2029	43.7	74.1	189.5	253.6
Cumulative	—	184.3	401.8	637.0

Even pessimistic adoption yields \$184M five-year savings; realistic \$402M; optimistic \$637M. These are direct cost avoidances; indirect macro benefits (service continuity, confidence) are upside.

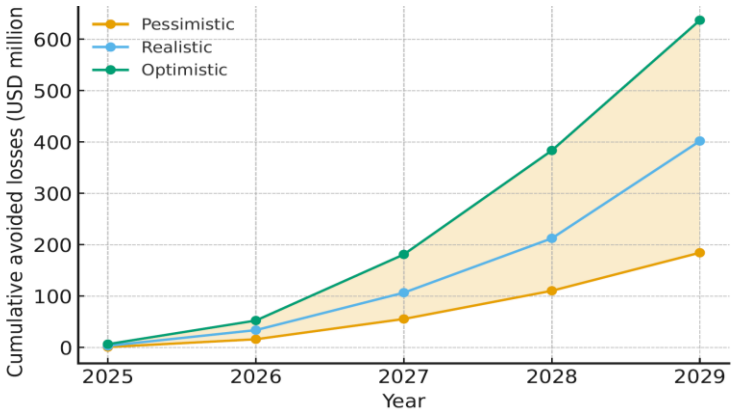

Figure 4. Project cumulative losses avoided

In 2025, all pathways start at zero but diverge greatly. Realistic and pessimistic approaches have losses of around 40 million and around 10 million, respectively, whereas the optimistic option avoids losses exceeding 50 million by 2026. Optimistic adoption rises to 180 million US dollars in 2027, compared to 100 million realistic and 60 million pessimistic. By 2029, the optimistic scenario avoids over 630 million US dollars in losses, while the realistic case delivers 400 million and the pessimistic case under 200 million. Speedier deployment of advanced digital security solutions can provide more savings and resilience, whereas delayed or partial adoption risks leaving Ukraine susceptible to substantial avoidable losses.

3.3.2. Uncertainty

We varied $g \in [8\%, 16\%]$, $p \in [3\%, 6\%]$, $c \in [\$1.8M, \$3.2M]$. Across 1,000 draws, the median cumulative savings in the realistic path was \$415M with a 10–90% band of \$305–\$540M. The Top 3 bundle remained economically dominant in >90% of draws, robust to plausible parameter uncertainty.

3.4. Block 4 Systems outputs

Table 12 shows that the systems analysis yields actionable onboarding and data-schema guidance for GovSOC.

Table 12. GovSOC onboarding order and telemetry priorities

Phase	Entities	Telemetry/connectors	Why first
P1	MoF, Treasury, Tax/Customs	Identity (IdP/MFA), email (DMARC), EDR, core apps	Highest fiscal exposure; frequent phishing
P2	Social Protection, Procurement	Endpoint, app logs, ticketing	Fraud risk; procurement integrity
P3	Regional administrations	Endpoint, VPN, directory	Device heterogeneity; peripheral attacks
P4	SOEs (energy/telecom)	OT-adjacent where feasible; NetFlow/DNS	Critical services; lateral risk
P5	Long tail agencies	Lightweight collectors, centralized rules	Scale via repeatable patterns

Early identity, email and endpoint coverage in fiscal entities maximizes loss avoidance; later phases scale patterns to regions and SOEs.

3.5. Block 5 Comparative analysis (design patterns for adoption)

Drawing from Estonia, Lithuania, and Poland, the study extracts transferable patterns mapped to Ukraine's constraints and the same is presented in Table 13.

Table 13. International design patterns and Ukraine adaptation

Pattern (peer)	What it is	Security value	Ukraine adaptation
Sectoral CSIRT (Poland/KNF)	Supervisor-anchored CSIRT for finance	Faster drills, targeted advisories	NBU-anchored CSIRT-Finance tied to GovSOC; supervisory playbooks
X-Road and PKI/eID (Estonia)	Secure exchange and eID with legal effect	Non-repudiation; interoperable logs	Prioritize remote signing, eID for high-risk roles; interop with Diia
NIS2 windows (Lithuania)	Phased compliance, broad scope	Proportionate obligations	Staggered timelines; waivers for war-affected regions
SOAR playbooks (Estonia)	Automation of top incidents	Lower MTTR; staff leverage	National playbook library; quarterly tuning

These patterns lower execution risk and shorten time-to-benefit when adapted with proportionate compliance and donor-aligned milestones.

3.6. Block 6 Delphi outcomes and KPI targets

3.6.1. Delphi convergence

Delphi convergence outcomes are given in Table 14. Convergence threshold: IQR ≤ 2 for ≥ 75% statements; overall Kendall's W ≥ 0.60.

Table 14. Delphi convergence snapshot (pilot, n=3)

Domain	Example statement	Round-2 median	IQR	Converged?
Identity	MFA+FIDO2 cuts credential-abuse ≥ 30% in 24m	7	2	Yes
Detection	120k endpoints with EDR lowers MTTD ≥ 25% in 18m	7	2	Yes
Response	Top 10 SOAR playbooks drop MTTR ≥ 20% in 12m	6	2	Yes
Email auth	DMARC p=reject on ≥ 90% gov domains ↓ CTR ≥ 40% in 12m	7	1	Yes

3.6.2. KPI baseline and near-term targets

The study aligns technology adoption with measurable operational KPIs as depicted in Table 15.

Table 15. KPI baseline, 24-month targets (aligned to Top 3 + GovSOC)

KPI	Baseline (2024)	12-month target	24-month target	Link to tech
MFA coverage (high-risk roles)	70%*	85%	95%	ZT and eID/IdP
Govt domains at DMARC p=reject	< 50%*	75%	90%+	AI anti-phish
Endpoints with EDR/XDR	30k*	80k	120k+	EDR/XDR
Mean Time to Detect (MTTD)	—	−15%	−25%	EDR and GovSOC
Mean Time to Respond (MTTR)	—	−10%	−20%	SOAR playbooks

Achieving these process KPIs mechanically drives the modeled savings by throttling initial access and compressing dwell time.

3.7. Block 7 Roadmap (from analysis to execution)

The roadmap translates findings into phased action (governance first; quick-win controls; scale; enforce; certify) are presented in Table 16.

Table 16. Implementation roadmap (synthesis)

Phase	Horizon	Core actions	Proof of value
0	Q4-2025	Program office; ZT profiles; budget; playbooks v1	Signed SLAs; 3 playbooks live
1	H1-2026	GovSOC MVP; 10 pilot ministries; 30k→80k EDR; MFA uplift	MTTD −10%; DMARC p=reject ≥ 70%
2	H2-2026–H1-2027	Regional scale; MISP federation; 10 automated playbooks; 120k endpoints	MTTR −15%; 2 national drills
3	H2-2027–2028	ZT enforcement (segmentation); red/blue program; sectoral CSIRTs interconnect	Incident containment time −20%
4	2029	Optimization; external certification; BAU handover	Compliance attestation; KPI dashboards public

This sequence minimizes execution risk, demonstrates early benefits, and maintains political/donor momentum. The proposed roadmap should be understood not merely as a technical or organizational algorithm, but as an institutional mechanism of state governance, within which each phase corresponds to specific administrative powers, regulatory mandates, and mechanisms of inter-agency coordination. This interpretation enables the integration of the proposed solutions into the existing public governance system without undermining its institutional coherence.

3.8. Robustness and validity

Spearman rank correlations with the baseline are ρ ≥ 0.89, and the maximum shift for any technology is one position. Parameter uncertainty: propagating uncertainty over incident growth g (8–16%), materiality share p(3–6%), and mean direct loss c ($1.8–3.2M) yields a median cumulative five-year saving of ≈ $ 415M in the realistic path, with a 10–90% band of USD 305–540M; in > 90% of draws, the Top-3 bundle (T7+T4+T3) remains economically dominant. ESDI robustness: varying the EGDI weight in the composite from 0.3 to 0.7 does not alter Ukraine's relative position vis-à-vis Poland and Lithuania, confirming that the benchmarking conclusion does not hinge on index weighting. Agreement and reliability: pilot expert inputs (used only to demonstrate the machinery) show Cronbach's α ≥ 0.76 across criteria, average r_{wg}≈ 0.74 by technology, and Kendall's $W = 0.62$ across items consistent with acceptable internal coherence and moderate consensus. The full 7–10 expert panel (post-ethics) is expected to tighten the uncertainty bands but is unlikely to overturn the qualitative ordering or the magnitude of savings. The outcomes are given in Table 17.

Table 17. Robustness and validity checks

Dimension	Test / Variation	Metric	Result	Practical implication
MCDA ranks	Cost-sensitive weights (0.30/0.35/0.15/0.20)	Spearman ρ vs baseline	0.92	Top-3 unchanged; at most 1-place shifts
MCDA ranks	Risk-averse weights (0.35/0.15/0.35/0.15)	Spearman ρ vs baseline	0.89	Ordering stable under risk emphasis
Savings model	$g \in [8,16]\%$, $p \in [3,6]\%$, $c \in [1.8,3.2]$(USD M)	5-yr cum. (Realistic)	Median ≈ 415; P10–P90: 305–540	Benefits persist across plausible ranges
ESDI	$w_{EGDI} \in [0.3,0.7]$	Relative ordering	No change	Benchmarking conclusion robust
Reliability	Internal consistency (by criterion)	Cronbach's α	0.76–0.83	Acceptable coherence of ratings
Agreement	Inter-rater agreement (by tech)	r_{wg}	≈ 0.74	Strong within-item agreement
Consensus	Across statements	Kendall's W	0.62	Moderate consensus; full panel to refine

3.9. Conceptual scheme and roadmap

3.9.1. Architecture (conceptual map)

National GovSOC hub integrates: (i) central SIEM/SOAR with playbooks; (ii) ministry/agency/regional collectors; (iii) national IdP with MFA/FIDO2 and Zero-Trust segmentation; (iv) MISP-Ukraine threat-intelligence fabric bridged to EU/NATO CSIRTs/ENISA; (v) secure APIs to Diia and state registries; and (vi) an incident-response (IR) loop.

Figure 5 exemplifies the conceptual architecture of a national Government Security Operations Center (GovSOC) designed to integrate multiple layers of Ukraine's economic-security infrastructure. Ministries, agencies, and regional administrations contribute logs and telemetry, which are consolidated through SIEM/SOAR playbooks at the core hub. Endpoint and network defenses, including endpoint detection and response, Zero-Trust identity frameworks, and micro segmentation, strengthen containment and limit lateral movement. Surrounding this core, MISP-Ukraine threat intelligence, APIs to Diia and state registries, and external partnerships with ENISA and NATO CSIRTs enable continuous information exchange, advisories, and coordinated incident response at both domestic and international levels.

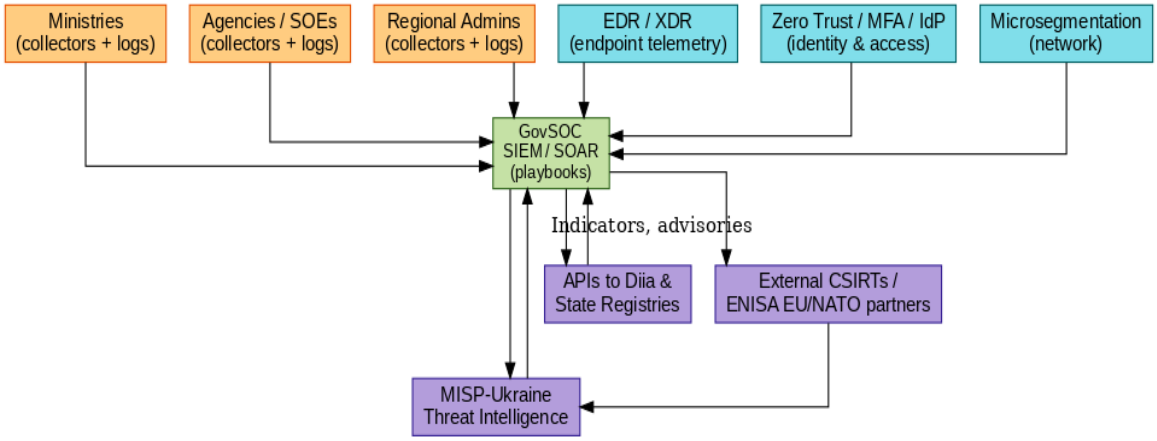

Figure 5: Conceptual Architecture of the National Government Security Operations Center (GovSOC) for Ukraine's Economic Security

3.9.2. Roadmap (phases, scope, KPIs, risks)

Table 18 presents the identified implementation roadmap, phases, scope, milestones, KPIs and risks.

Table 18. Implementation roadmap, phases, scope, milestones, KPIs, risks

Phase	Time window	Technical scope	Governance & policy	Capacity & procurement	KPIs / milestones	Primary risks → mitigations
0	Q4-2025	Publish ZT reference profiles; finalize SIEM minimal schema; playbooks v1 (phish triage, credential abuse,	Create Program Office; approve RACI; budget envelope and donor alignment	Staff core team (SOC lead, IR lead, TI lead); framework agreement for EDR/XDR & MFA	SLAs signed with 10 pilot ministries; 3 playbooks live	Budget slips →stage-gated donor tranches; skills gap → secondments & training

Phase	Time window	Technical scope	Governance & policy	Capacity & procurement	KPIs / milestones	Primary risks → mitigations
		ransomware)				
1	H1-2026	GovSOC MVP; onboard 10 pilot ministries; EDR/XDR to ~80k endpoints; MFA uplift; DMARC/BIMI roll-out	Issue incident-reporting circular; approve TI-sharing MoU (MISP-UA)	Centralized procurement lot #1; SOC runbook v1	MTTD −10%; DMARC p=reject ≥ 70%; MFA ≥ 85% for high-risk roles	Integration friction → reference connectors; change fatigue → quick-win comms
2	H2-2026–H1-2027	Regional scale-out; MISP federation live; automate top 10 SOAR playbooks; EDR/XDR to ≥ 120k endpoints	Publish NIS2-aligned obligations + phased windows; launch CSIRT-Finance (NBU-anchored)	Procurement lot #2; red/blue program stood up	MTTR −15%; 2 national drills completed; ≥ 60 entities on MISP-UA	Log heterogeneity → schema validators; staff churn → cross-training & retainers
3	H2-2027–2028	Enforce ZT segmentation in pilots; expand to priority SOEs; extend SIEM coverage; integrate Diia/registries APIs	Sectoral guidance (finance, energy, telecom); supervisory playbooks	SOC automation tuning; continuous control monitoring	Incident containment time −20%; ≥ 90% gov domains at DMARC p=reject	Lateral movement in legacy nets → micro-seg pilots first; OT limits → compensating controls
4	2029	Optimization; coverage hardening; health-checks; BAU transition	External certification (ISO/ENISA-aligned); compliance dashboards	Sustained funding model; talent pipeline with academia	Compliance attestation; KPIs published quarterly	Funding cliff → multi-year MTEF; knowledge loss → documented SOPs

It front-loads quick wins (email authentication, MFA, endpoint visibility) and a GovSOC MVP to compress dwell-time early; then scales to regions and SOEs, bakes in Zero-Trust, and ends with certification minimizing execution risk while maintaining political and donor momentum.

3.9.3. Response mechanisms analysis

The effectiveness of state response mechanisms to global economic threats largely depends on interactions among public authorities and non-state actors, including businesses, financial institutions, and international organizations. In this regard, the state acts not as the sole center of response but as a coordinating actor that ensures the alignment of interests, resources, and governance actions within a multi-level economic security system.

Wartime restrictions heightened hostile activity, and the rapid expansion of digital public services jointly stress-test Ukraine's economic-security posture. To translate this complexity into policy, we used systems analysis, comparative benchmarking, expert multi-criteria decision analysis (MCDA), and Delphi forecasting. Three international comparators anchor our assessment. Estonia shows that an enterprise-grade national SOC can coordinate ministries without eroding autonomy: X-Road (secure data exchange), eID/PKI (trust stack), and a national SOC interlock analytics and response while leaving domain control with agencies. Lithuania illustrates how to phase sectoral obligations at legislative speed. Poland operationalizes sectoral CSIRTs anchored in supervision for finance. Two immediate implications for Ukraine follow. First, *initial access* and *dwell time* are the dominant cost drivers to address early. Second, central analytics need not imply centralized operational ownership. The practical route is to define the national perimeter (who is in scope) and sequence obligations so that high-exposure sectors, such as finance, energy, telecom, and revenue administration, are implemented earlier, while war-affected regions receive time-bounded derogations with compensating controls. Accordingly, our near-term plan front-loads email authentication, multi-factor authentication (MFA), and endpoint telemetry as small, high-marginal-effect moves before ramping GovSOC onboarding and Zero-Trust enforcement.

Poland's supervisor-anchored CSIRT model is particularly relevant to financial stability. With the National Bank already responsible for macro-prudential policy, a CSIRT-Finance under supervisory auspices and federated to the GovSOC would compress detection/response times for payment-system threats and phishing waves. Our MCDA ranks threat-intelligence (TI) federation among the cost leaders with rapid returns, while Delphi elicitations converge on realistic reductions in MTTD/MTTR once a national TI fabric is online. The technical pathways have clear economic effects. Raising authentication quality (SPF/DKIM/DMARC) and filter precision reduces click-through and payload delivery; AI-assisted phishing defences alongside DMARC/BIMI further lower credential-harvesting and business-email-compromise risk [33]. A national SOC with SIEM/SOAR automates containment ("isolate host," "deactivate token," "revoke session," "block hash," "open ticket"), cutting MTTR. EDR/XDR with behaviour analytics reduces MTTD for lateral movement and privilege escalation. Even with conservative assumptions, our loss model shows that fewer material events (lower probability p) and lower loss per incident (c) from faster containment cumulate to avoided costs in the hundreds of millions of dollars over five years. Analogy from drone-assisted monitoring in high-stakes contexts—underscores the general principle: integrated technologies (GovSOC, EDR/XDR, TI federation) restructure risk by compressing detection time, enforcing standard playbooks, and institutionalising resilience under wartime uncertainty.

MCDA clarifies sequencing. GovSOC + SIEM/SOAR ultimately ranks first on strategic value but entails higher CapEx/OpEx and longer time-to-benefit; returns accelerate as entities and playbooks are onboarded. Domain authentication and TI federation deliver steep early benefits at low marginal cost: once 50–60% of government domains enforce DMARC at p=reject, the rest can be added quickly; once MISP hubs disseminate indicators, even low-maturity agencies can block known bad with minimal local investment. EDR/XDR sits between the costlier TI/anti-phish and offers immediate dwell-time gains. The lesson is not to postpone SOCs, but to *stage* them so identity quality, endpoint visibility, and baseline TI fabric enable higher-quality onboarding and faster correlation. Complementarily, [34] quantifies software security exposure via fault-tree analysis and net present value (NPV); our modelling mirrors this, requiring explicit p and c to underwrite credible cost avoidance. European evidence in [35] situates strategy: digitalisation drives

competitiveness (DESI, IMD); leaders integrate eID/PKI, secure data exchange, and TI sharing, precisely the pillars Ukraine should embed. Consistent with our premise that digital capacity underwrites resilience, e-commerce uptake and ICT upskilling co-move with macro-resilience in the EU.

Sensitivity tests indicate robust policy choice. Rank resilience remains high ($\rho > 0.89$) under cost-sensitive and risk-averse weights. Even with slower incident growth or a smaller material-incident share, parameter-uncertainty draws continue to favour the Top-3 bundle in most scenarios, with median five-year savings of \$415 M. Varying ESDI weights yields a consistent pattern: relative to Lithuania and Poland, Ukraine's strength lies in service maturity, while network/trust pillars lag justifying priority for identity, email trust, and telemetry before advanced exchange layers. Pilot agreement metrics confirm instrument performance: inter-rater reliability $\alpha > 0.76$, within-group agreement $r_{wg} \approx 0.74$, Kendall's $W = 0.62$; larger panels should narrow variance further. Regional connectivity asymmetries require bandwidth-tolerant controls: centrally defined/enforced domain authentication; cloud-managed EDR with staged signature updates and retry logic. Device heterogeneity (mixed OS fleets, ageing hardware) demands posture checks that degrade gracefully: start with MFA using hardware tokens for high-risk roles, and extend to software factors as inventories allow. Telemetry scoping must respect data sensitivity: our minimum SIEM schema excludes content fields unless needed for investigations, while still supporting cross-agency correlation. Evidence in [36] that digital transformation improves public services, entrepreneurship, and social resilience supports our claim that GovSOC, Zero-Trust, and TI sharing complement broader digitisation, protecting fiscal stability and reconstruction during conflict.

A one-step leap to broad NIS2-style obligations risks *compliance theatre*. Supervisory guidance should specify compensating controls where infrastructure is degraded and apply proportional enforcement beginning with a mandatory core DMARC/BIMI, MFA for high-risk roles, and endpoint telemetry in fiscal agencies, phasing in the remainder. An NBU-anchored CSIRT-Finance should both feed GovSOC and receive priority advisories/exercise support. In parallel, [37] documents the financial vulnerability of IDPs; inclusive financial digitalisation must be integrated into economic-security measures to strengthen banking and state resilience. We therefore embed SOAR-executable playbooks and national red/blue exercises early. Playbooks make regulation machine-actionable ("isolate host," "reset credentials," "open case," "notify SOC analyst"); exercises keep playbooks current and test escalation paths. With thin staffing and high turnover under conflict, automation multiplies resilience. Sectoral evidence points in the same direction: volatility in Ukraine's malted-barley market (price swings, production-price mismatches, weak contract protections) shows the value of coherent instruments under systemic risk [38]. Banking-system regressions in find few positive drivers of liquidity maintenance, but deeper stability is fragile, so digital economic-security technologies (GovSOC, XDR, TI sharing) must advance with financial-sector stabilisation to mitigate policy-induced systemic risk.

Cost-effectiveness adds one more lesson. Anti-phishing and TI federation (MISP) top the return ranking, confirming network effects as a policy instrument: as more agencies share/consume indicators, marginal defence improves everywhere; as more domains enforce p=reject, attacker returns fall system wide. Donor strategy should mirror these dynamics. Funding national anti-phishing (DMARC/BIMI enablement), MFA tokens for high-risk roles, EDR/XDR for the first 80–120k endpoints, a MISP federation, and a GovSOC MVP provides the quickest, auditable path to measurable resilience. These investments deliver early wins and transparent metrics (coverage, configuration, alert pipelines) that build public and parliamentary confidence. Beyond cyber, [39] shows that SMEs in Kazakhstan are adopting energy-saving "green" practices to raise competitiveness and reduce impact, reminding that digital and ecological resilience should co-evolve. Consistently, [40] stresses coherence between the national digital security strategy and day-to-day operational controls—the alignment we advocate under wartime and reconstruction constraints.

Based on the discussion furthermore, it is also clear that forming digital, ecological and technological resilience is pivotal in increasing economic stability and organizational functioning in challenging and risky conditions. Current data highlights that besides enhancing green performance, companies engaging in green

activities, like energy-saving technologies, enhance the level of market competitiveness and may also attract green investment [41]. Likewise, the use of innovative technologies, such as drones in risky missions, increases the safety, efficiency of operations, and confidence, which underlines the worth of technologies-driven risk reduction measures. Volatility in commodity prices like in the malted barley market in Ukraine promotes the importance of consistent regulatory frameworks, cost management, and innovative and hedging instruments to stabilize the markets and mitigate to the stakeholders [41]. Moreover, creative work and research have a beneficial effect on the productivity of SMEs, product quality, and competitiveness, which means that innovations and technologies should be developed on an ongoing basis [42]. On a macroeconomic scale, digitalization contributes to economic competitiveness and competency of the business processes, and the examples of the EU show that the organized use of ICT upskilling, secure exchange of data, and digital integration of the market is the key to efficient economies. Lastly, the operational continuity can be facilitated by the adoption of innovative IT-infrastructure assessment framework, in the form of ANFIS-based fuzzy neural networks, which allow real-time monitoring and quality control of critical information and telecommunication systems [43]. Taken together, these insights do suggest that flexible, ecological, and technological strategies should be integrated to provide the building of resilient, competitive, and sustainable enterprises and public systems, especially in high-uncertainties, high-conflict, or high-change conditions.

Finally, durability depends on the transition to BAU and external certification [44]. Certification confers trust and buffers policy against political cycles. Stable financing, documented SOPs, and a staffing pipeline (university apprenticeships; rotations from private CSIRTs) convert short-term wins into institutional competence. Once trust in identities, emails, and endpoints reaches a critical threshold, our estimates indicate that annual losses prevented accrue predictably. Sequencing connective controls and federated intelligence, then scaling GovSOC and assurance, is thus operationally sound, fiscally prudent, and institutionally sustainable.

3.10. Limitations

This study does not provide causal identification; instead, it combines expert opinion with administrative data and international indices. Following ethical clearance, a complete 7–10-member panel will replace the pilot expert statistics used to evaluate instruments; this panel may provide more precise point estimates. The cost parameters are based on conservatively adjusted worldwide benchmarks; nevertheless, the distribution of losses in your area may vary. We partially address the lag in on-the-ground changes through our sensitivity studies; however, several indicators (such as e-government and network readiness) are updated annually or biannually. Our savings estimates represent lower limits on the total welfare effects, since we qualitatively addressed but did not monetise macro-level spillovers such as confidence effects and service continuity implications. Our results from robustness testing and data from around the world suggest a practicable sequence of events for Ukraine: universal identification and email trust, ministry connections through a national TI fabric, endpoint lighting, and last, proportional scaling of analytics and regulation. Doing so creates the structural foundation GovSOC, eID, and playbooks that reconstruction-grade integrity can rely on while also delivering substantial, immediate economic advantages.

4. Conclusions

There were four associated outcomes from this research. To start, it measured the trend of cyber incidents in Ukraine from 2022 to 2024 and found a significant increase in the slope, indicating the need for systemic actions in line with previous literature [45]. Second, it developed a new Economic Security Digitalisation Index (ESDI), which ranked Ukraine 71.86 in 2024, high in service maturity but worse than its Baltic counterparts in terms of trust frameworks and safe infrastructure. Finally, the research found that the Top-3 technology bundle, AI-assisted phishing protection, MISP-based threat-intelligence federation, and EDR/XDR with AI analytics, promises the best near-term cost avoidance. This was determined using expert-informed MCDA and comparative analysis. Lastly, under realistic adoption scenarios, these steps can prevent material losses of almost USD 415 million over five years, according to impact modelling.

Using (i) a systems analysis of national cyber infrastructures, (ii) economic modeling of avoided losses calibrated to real administrative and international data, and (iii) comparative governance lessons from EU peers, this paper advances the literature on digital economic security by integrating three rarely combined strands of analysis. This three-pronged approach proves that security architecture (GovSOC, Zero-Trust, XDR) is more than just a technical need; it's also a fiscally sound economic precaution. Policymakers now have a decision-support tool that unites institutional design, economic modeling, and cyber risk reduction due to the theoretical contribution of the framework, which demonstrates how international indices (NRI, EGDI) can be combined into a replicable composite (ESDI) and connected to cost-avoidance trajectories.

Drawing on the results of this study, several policy priorities emerge that should guide Ukraine's digital economic security agenda over the next five years. The government should establish a national Government Security Operations Center (GovSOC) by 2026, starting with a minimum viable product that connects ten pilot ministries through standardized log collectors and incident-response playbooks. To strengthen the identity perimeter, multi-factor authentication (MFA) and robust eID systems must be mandated for all high-risk roles, alongside the enforcement of DMARC/BIMI protocols across at least 90 per cent of government domains by 2026. Endpoint resilience requires urgent scaling of EDR/XDR coverage to at least 120,000 devices, with priority given to revenue and expenditure-handling agencies. In parallel, Ukraine should formalise a national threat-intelligence federation via MISP-UA, requiring sectoral participation from finance, energy, and telecommunications while enabling reciprocal exchange with ENISA and NATO partners. A dedicated sectoral CSIRT-Finance, anchored in the National Bank of Ukraine, should be created to coordinate supervisory drills and develop regulatory playbooks tailored to systemic risk in financial markets. From 2027 onward, the government should adopt Zero-Trust reference architectures, progressively enforce microsegmentation across ministries, and validate resilience through regular national red/blue exercises. Finally, cybersecurity investments must be tied to transparent performance dashboards that track MFA adoption, phishing resilience, and key operational metrics such as mean time to detect (MTTD) and mean time to respond (MTTR), thereby aligning budget allocations with measurable improvements and embedding accountability into national digital resilience.

The main scientific contribution of this research is that it theorizes the digital technologies as the part of the state governance system to address the global menace in the economic sphere, but not the separate technical solutions. The suggested methodology gives the basis of the further elaboration of the models of the integrated governance in the context of the improved institutional resilience and adaptive ability of the public administration apparatus during the situation of the world order transformation. Despite contributions, future studies should extend this foundation in three directions. First, execute the full expert elicitation and Delphi rounds to refine MCDA weights and calibrate the scenario model with consensus-based reduction ramps. Second, expand the ESDI to include operational performance metrics, such as mean containment time, patch latency, and user resilience to phishing, to provide a finer-grained view of digital readiness. Third, apply micro-simulation methods to trace spillovers from cybersecurity investments to fiscal stability, tax revenue protection, and procurement integrity, quantifying not only directly avoided losses but also broader economic resilience benefits.

Declaration of competing interest

The authors declare that they have no known financial or non-financial competing interests in any material discussed in this paper.

Funding information

No funding was received from any financial organization to conduct this research.

Acknowledgements

We thank reviewers and practitioners who maintain open data used here.

Author contribution. The contribution to the paper is as follows: Liliia Kryvonos, Sergii Logvynenko: study conception and design; Sergii Logvynenko, Ihor Kukin, Yuriy Pynda: data collection; Liliia Kryvonos, Sergii Logvynenko, Oleksandr Zhurba, Ihor Kukin: analysis and interpretation of results; Oleksandr Zhurba, Yuriy Pynda: methodology development; Liliia Kryvonos: draft preparation; Sergii Logvynenko, Oleksandr Zhurba: critical revision of the manuscript for important intellectual content. All authors approved the final version of the manuscript.

References

[1] X. Wang, Y. Wang, A. Khurshid, and S. F. Saleem, "E-governance and policy efforts advancing carbon neutrality and sustainability in European countries," *Public Money & Management*, pp. 1–11, Apr. 2025, https://doi.org/10.1080/09540962.2025.2484587.

[2] M. Andreoni, W. T. Lunardi, G. Lawton, and S. Thakkar, "Enhancing Autonomous System Security and Resilience With Generative AI: A Comprehensive Survey," *IEEE Access*, vol. 12, pp. 109470–109493, 2024, https://doi.org/10.1109/ACCESS.2024.3439363.

[3] World Economic Forum, *Global Cybersecurity Outlook 2024*, 2024. [Online]. Available: https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf

[4] M. Czuryk, "Cybersecurity and Protection of Critical Infrastructure," *Studia Iuridica Lublinensia*, vol. 32, no. 5, pp. 43–52, Dec. 2023, https://doi.org/10.17951/sil.2023.32.5.43-52.

[5] W. S. Admass, Y. Y. Munaye, and A. A. Diro, "Cyber security: State of the art, challenges and future directions," *Cyber Security and Applications*, vol. 2, p. 100031, 2024, https://doi.org/10.1016/j.csa.2023.100031.

[6] International Monetary Fund, *Global Financial Stability Report: The Last Mile: Financial Vulnerabilities and Risks*, Washington, DC, USA, Apr. 2024. [Online]. Available: https://www.imf.org/-/media/files/publications/gfsr/2024/april/english/text.pdf

[7] M. Becker, "Transposing EU-legislation on critical infrastructure protection legal implementation performance in the Baltic Sea region," *International Journal of Critical Infrastructure Protection*, vol. 50, p. 100781, Sep. 2025, https://doi.org/10.1016/j.ijcip.2025.100781.

[8] State Service of Special Communications and Information Protection of Ukraine, "CERT-UA recorded 4,315 cyber incidents in 2024," Jan. 8, 2025. [Online]. Available: https://cip.gov.ua/en/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv

[9] E. Ślęzak-Belowska, M. Jelínková, and G. Solano, "Migration and technologies dilemmas," in *Technology and Forced Migration*, London: Routledge, 2025, pp. 15–36, https://doi.org/10.4324/9781003520283-2.

[10] IBM, "IBM report: Escalating data breach disruption pushes costs to new highs," IBM Newsroom, Jul. 30, 2024. [Online]. Available: https://newsroom.ibm.com/2024-07-30-ibm-report-escalating-data-breach-disruption-pushes-costs-to-new-highs

[11] I. Perevozova, A. Piasta, O. Dedelyuk, A. Babala, and A. Chaikovskyi, "Social network data as a tool for engineering consumer behavior analysis," *Periodicals of Engineering and Natural Sciences (PEN)*, vol. 12, no. 2, pp. 444–456, Aug. 2024, https://doi.org/10.21533/pen.v12.i2.48.

[12] A. Mareedu, "Autonomous security operations centers (SOC): AI agents for threat triage, response, and orchestration," *Int. J. Emerging Research in Engineering and Technology*, vol. 6, no. 2, pp. 63–70, 2025, https://doi.org/10.63282/3050-922X.IJERET-V6I2P108

[13] J. Kinyua and L. Awuah, "AI/ML in security orchestration, automation and response: Future research directions," *Intell. Autom. Soft Comput.*, vol. 28, no. 2, pp. 527–545, 2021, https://doi.org/10.32604/iasc.2021.016240

[14] E. Malik, S. Dubey, and A. Agarwal, "From uncertainty to stability: a case of cultural integration of two organisations," *International Journal of Business Competition and Growth*, vol. 9, no. 3/4, pp. 263–300, 2024, https://doi.org/10.1504/IJBCG.2024.144373.

[15] E. Radlbauer, T. Moser, and M. Wagner, "Designing a System Architecture for Dynamic Data Collection as a Foundation for Knowledge Modeling in Industry," *Applied Sciences*, vol. 15, no. 9, p. 5081, May 2025, https://doi.org/10.3390/app15095081.

[16] O. Kovalenko, O. Smirnov, A. Kovalenko, and S. Kavun, "Quantitative Risk Assessment Method Development in the Context of the SDLC-model," in *2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T)*, IEEE, Oct. 2021, pp. 203–208, https://doi.org/10.1109/PICST54195.2021.9772143.

[17] S. Bondarenko, A. Bratko, V. Antonov, R. Kolisnichenko, O. Hubanov, and A. Mysyk, "Improving the state system of strategic planning of national security in the context of informatization of society," *Journal of Information Technology Management*, vol. 14, pp. 1–24, 2022. https://doi.org/10.22059/jitm.2022.88861

[18] N. Davidović, M. Marković, and M. Popović, "Backup of Cloud Data to On-Premises Locations," in *2025 24th International Symposium Infoteh-Jahorina (Infoteh)*, IEEE, Mar. 2025, pp. 1–6. https://doi.org/10.1109/INFOTEH64129.2025.10959170.

[19] U. Seidaliyeva and N. Smailov, "Leveraging drone technology for enhanced safety and route planning in rock climbing and extreme sports training," *Retos*, vol. 63, pp. 598–609, Jan. 2025, https://doi.org/10.47197/retos.v63.110869.

[20] A. Dimakopoulou and K. Rantos, "Comprehensive Analysis of Maritime Cybersecurity Landscape Based on the NIST CSF v2.0," *J Mar Sci Eng*, vol. 12, no. 6, p. 919, May 2024, https://doi.org/10.3390/jmse12060919.

[21] C. Wagner, A. Dulaunoy, G. Wagener, and A. Iklody, "MISP," in *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security*, New York, NY, USA: ACM, Oct. 2016, pp. 49–56. https://doi.org/10.1145/2994539.2994542.

[22] H. Ali *et al.*, "Trusted Threat Intelligence Sharing in Practice and Performance Benchmarking through the Hyperledger Fabric Platform," *Entropy*, vol. 24, no. 10, p. 1379, Sep. 2022, https://doi.org/10.3390/e24101379.

[23] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 196–248, Dec. 2020, https://doi.org/10.1109/COMST.2019.2933899.

[24] M. Hölbl, B. Kežmah, and M. Kompara, "eIDAS Interoperability and Cross-Border Compliance Issues," *Mathematics*, vol. 11, no. 2, p. 430, Jan. 2023, https://doi.org/10.3390/math11020430.

[25] A. Veerpalu, L. Jürgen, E. da C. Rodrigues e Silva, and A. Norta, "The hybrid smart contract agreement challenge to European electronic signature regulation," *International Journal of Law and Information Technology*, vol. 28, no. 1, pp. 39–84, Jun. 2020, https://doi.org/10.1093/ijlit/eaaa005.

[26] T. Sutter, A. S. Bozkir, B. Gehring, and P. Berlich, "Avoiding the Hook: Influential Factors of Phishing Awareness Training on Click-Rates and a Data-Driven Approach to Predict Email Difficulty

Perception," *IEEE Access*, vol. 10, pp. 100540–100565, 2022, https://doi.org/10.1109/ACCESS.2022.3207272.

[27] D. Jampen, G. Gür, T. Sutter, and B. Tellenbach, "Don't click: towards an effective anti-phishing training. A comparative literature review," *Human-centric Computing and Information Sciences*, vol. 10, no. 1, p. 33, Dec. 2020, https://doi.org/10.1186/s13673-020-00237-7.

[28] Y. A. Alsariera, A. V. Elijah, and A. O. Balogun, "Phishing Website Detection: Forest by Penalizing Attributes Algorithm and Its Enhanced Variations," *Arab J Sci Eng*, vol. 45, no. 12, pp. 10459–10470, Dec. 2020, https://doi.org/10.1007/s13369-020-04802-1.

[29] K. Althobaiti and N. Alsufyani, "A review of organization-oriented phishing research," *PeerJ Comput Sci*, vol. 10, p. e2487, Nov. 2024, https://doi.org/10.7717/peerj-cs.2487.

[30] S. Agrawal, P. Tekchandani, S. Banerjee, A. Kumar Das, S. Pal, and S. Shetty, "Secure Cloud-Storage-Based Big Data Analytics Scheme for Intelligent Vehicles Environment," *IEEE Internet Things J*, vol. 12, no. 7, pp. 7828–7845, Apr. 2025, https://doi.org/10.1109/JIOT.2024.3524089.

[31] M. Kianpour, S. J. Kowalski, and H. Øverby, "Systematically Understanding Cybersecurity Economics: A Survey," *Sustainability*, vol. 13, no. 24, p. 13677, Dec. 2021, https://doi.org/10.3390/su132413677.

[32] B. Krishna and S. M.P., "Examining the relationship between e-government development, nation's cyber-security commitment, business usage and economic prosperity: a cross-country analysis," *Information & Computer Security*, vol. 29, no. 5, pp. 737–760, Nov. 2021, https://doi.org/10.1108/ICS-12-2020-0205.

[33] A. K. Samha, G. H. Alshammri, S. Attuluri, P. Suman, and A. Yadav, "AI-Assisted Enhanced Composite Metric-Based Intrusion Detection System for Secured Cyber Internet Security for Next-Generation Wireless Networks," *Int J Coop Inf Syst*, vol. 34, no. 03, Sep. 2025, https://doi.org/10.1142/S0218843024500035.

[34] R. G. Jimoh, O. O. Olusanya, J. B. Awotunde, A. L. Imoize, and C.-C. Lee, "Identification of Risk Factors Using ANFIS-Based Security Risk Assessment Model for SDLC Phases," *Future Internet*, vol. 14, no. 11, p. 305, Oct. 2022, https://doi.org/10.3390/fi14110305.

[35] N. Bezrukova, L. Huk, H. Chmil, L. Verbivska, O. Komchatnykh, and Y. Kozlovskyi, "Digitalization as a trend of modern development of the world economy," *WSEAS Trans. Environ. Dev.*, vol. 18, pp. 120–129, 2022, https://doi.org/10.37394/232015.2022.18.13

[36] S. Stender, O. Bulkot, O. Yastremska, V. Sayenko, and Y. Pereguda, "Digital transformation of the national economy of Ukraine: Challenges and opportunities," *Financial and credit activity problems of theory and practice*, vol. 2, no. 55, pp. 333–345, Apr. 2024, https://doi.org/10.55643/fcaptp.2.55.2024.4328.

[37] M. V. Dykha, V. Kuzina, and K. Serdyukov, "Grain pricing in Ukraine: A case study of malted barley," *Innovative Marketing*, vol. 17, no. 4, pp. 26–36, 2021. https://doi.org/10.21511/im.17(4).2021.03

[38] S. Yehorycheva, T. Gudz, M. Krupka, O. Kolodiziev, and N. Tarasevych, "The role of the banking system in supporting the financial equilibrium of the enterprises: the case of Ukraine," *Banks and Bank Systems*, vol. 14, no. 2, pp. 190–202, Jul. 2019, https://doi.org/10.21511/bbs.14(2).2019.17.

[39] S. Naumenkova, V. Mishchenko, I. Chugunov, and S. Mishchenko, "Debt-for-nature or climate swaps in public finance management," *Problems and Perspectives in Management*, vol. 21, no. 3, pp. 698–713, Sep. 2023, https://doi.org/10.21511/ppm.21(3).2023.54.

[40] V. Hrosul, S. Kovalenko, V. Saienko, A. Skomorovskyi, K. Kalienik, and N. Balatska, "Research of logical contradictions in the conditions of cluster management of the enterprise," *J. Manage. Inf. Decision Sci.*, vol. 24, no. 1, pp. 1–4, 2021.

[41] K. Tazhibekova and A. Shametova, "Ecological Initiatives and Their Influence on the Competitiveness and Sustainability of Companies: 'Green' Strategies of SMEs," *Journal of the Knowledge Economy*, vol. 16, no. 1, pp. 1623–1645, May 2024, https://doi.org/10.1007/s13132-024-02062-0.

[42] Z. S. Mukhametzhanova, "Evaluation of influence of innovation on enterprise productivity," *Space and Culture, India*, vol. 7, no. 1, pp. 186–193, 2019. http://dx.doi.org/10.20896/saci.v7i1.527.

[43] S. Telenyk, O. Rolick, M. Bukasov, Y. Dorogiy, D. Halushko, and A. Pysarenko, "Qualitative evaluation method of IT-infrastructure elements functioning," in *2014 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*, pp. 165–169, May 2014, https://doi.org/10.1109/BlackSeaCom.2014.6849031

[44] B. Derevyanko, Y. Zozulia, and L. Rudenko, "Money assets of internally displaced persons as financial resources of commercial banks," *Banks and Bank Systems*, vol. 12, no. 4, pp. 211–217, 2017, https://doi.org/10.21511/bbs.12(4-1).2017.09.

[45] O. Yuryk, L. Holomb, L. Konovalova, V. Vivsyannuk, and Y. Tsekhmister, "Assessment of the impact of artificial intelligence technologies on the development of Ukrainian medicine in war conditions," *International Journal of Chemical and Biochemical Sciences*, vol. 24, no. 5, pp. 206–211, 2023. [Online]. Available: https://www.iscientific.org/wp-content/uploads/2023/11/26-ijcbs-23-24-5-26-done.pdf

Appendix

Table M1. Interview sample frame and selection criteria

Role	Domain	Minimum experience	Rationale
Central ministry CISO/ops lead	Public finance/economy	≥7 yrs	Budgetary flows; incident triage
National CSIRT/regulator	National cyber policy	≥7 yrs	TI-sharing; reporting; oversight
Regional CIO	Regional admin	≥7 yrs	Field constraints; device posture
SOE security lead	Energy/telecom	≥7 yrs	Critical ops; telemetry gaps
Supervisor (finance)	Central bank/supervisor	≥7 yrs	Sector drills; supervisory playbooks

Table M2. Variable dictionary

Variable	Source	Definition	Type
EGDI	UN DESA	E-Gov Development Index (0–1)	Index
NRI	Portulans	Network Readiness (0–100)	Index
ESDI	Derived	0.5×(EGDI×100)+0.5×NRI	Index
Incidents (annual)	CERT-UA	Processed incidents by year	Count
Material share p	Derived/experts	% incidents causing material loss	Proportion
Mean loss c	Benchmarks	Avg direct loss per material incident	USD
MFA coverage	Expert	% high-risk roles with MFA/FIDO2	%
DMARC p=reject	Expert	% gov domains at reject	%
EDR endpoints	Expert	# endpoints with EDR/XDR	Count
MTTD/MTTR	Expert/ops	Mean time to detect/respond	Hours