Securing Digital Corridors Under Hybrid Threats:Extending SDAF to Cybersecurity Governance of Critical Maritime Infrastructure in Geopolitical Flux

Rahid Zahid Alekberli * and Hikmat Karimov

Posted Date: 6 May 2026

doi: 10.20944/preprints202605.0307.v1

Keywords: cybersecurity governance; critical maritime infrastructure; Hybrid Threats; Strategic Data Alignment Framework (SDAF); big data and digital corridor; port community systems; cyber-resilience; supply chain risk management; regulatory convergence; Resource-Based View (RBV); geopolitical cybersecurity challenges

 doi:10.20944/preprints202605.0307.v1

Article

Securing Digital Corridors Under Hybrid Threats: Extending SDAF to Cybersecurity Governance of Critical Maritime Infrastructure in Geopolitical Flux

Rahid Zahid Alekberli * and Hikmat Kerimov

Institute of Defence Technologies and Cybersecurity, Azerbaijan Technical University, Baku, Azerbaijan

* Correspondence: ralekberli@gmail.com

Abstract

Maritime ports—now deeply digitalized and interdependent—face escalating cyber risk amid hybrid geopolitical pressures, complex vendor ecosystems, and widening social dependence on uninterrupted trade flows. Situated at the intersection of the Belt and Road Initiative and the Trans-Caspian International Transport Route, the Caspian Basin exemplifies both the promise of data-driven logistics and the vulnerability of fragmented cybersecurity governance. This study extends the Strategic Data Alignment Framework (SDAF), originally designed to align corporate strategy with data governance, into a cybersecurity governance model for critical maritime infrastructure under hybrid threat conditions. Using comparative policy analysis and benchmarking against contemporary global standards (e.g., NIS2-style obligations, maritime cyber guidelines, and digital trade principles), the study identifies systemic weaknesses in harmonization, institutional capacity, supply-chain assurance, and resilience planning. It reconceptualizes cyber-resilience as a strategic resource and proposes a five-step roadmap combining regional threat-intelligence sharing, vendor risk controls, standards alignment, AI-enabled detection, and stress-tested recovery. The findings underscore urgent needs for coordinated action to safeguard digital corridors and the societies they serve.

Keywords: cybersecurity governance; critical maritime infrastructure; Hybrid Threats; Strategic Data Alignment Framework (SDAF); big data and digital corridor; port community systems; cyber-resilience; supply chain risk management; regulatory convergence; Resource-Based View (RBV); geopolitical cybersecurity challenges

I. Introduction

Maritime ports have evolved into **critical digital infrastructures**, where physical operations increasingly depend on interconnected information technology (IT), operational technology (OT), Internet of Things (IoT) devices, and Port Community Systems (PCS). This digitalization improves efficiency and global connectivity, but it simultaneously widens the **attack surface for cyber threats**. Peer-reviewed studies consistently identify cyber risks in ports as systemic, spanning supply-chain vendors, IoT devices, and cyber-physical processes that underpin logistics operations .

The urgency of port cybersecurity has intensified amid **hybrid geopolitical threats**. Recent incidents of **AIS and GNSS spoofing** highlight vulnerabilities that adversaries exploit to mask illicit shipping, manipulate navigation, or disrupt regional stability . Parallel concerns arise in vendor ecosystems, where **third-party risks** and reliance on foreign-manufactured port equipment (e.g., cranes, sensors) complicate sovereignty and resilience debates. Scholarly reviews emphasize that fragmented approaches to supply-chain cyber governance leave maritime infrastructure disproportionately exposed to disruption .

Policymakers are responding unevenly. The **European Union's NIS2 Directive** imposes rigorous cybersecurity obligations, extending accountability to supply-chain partners and critical

 doi:10.20944/preprints202605.0307.v1

infrastructure operators, while the **International Maritime Organization's (IMO) guidelines** urge states and ports to integrate cyber risk management into safety systems. Yet compliance and enforcement remain inconsistent, particularly in emerging regional corridors, where resource constraints hinder adoption .

Against this backdrop, the **Caspian Basin** represents a high-stakes case. Positioned at the intersection of the **Belt and Road Initiative (BRI)** and the **Trans-Caspian International Transport Route (TITR)**, its ports are increasingly vital to Eurasian trade but face significant governance fragmentation [1–3]. Research highlights that while individual ports and states pursue digitalization, the region lacks a **harmonized cybersecurity governance framework**, leaving critical trade corridors vulnerable to cyberattacks and hybrid interference [1–6].

This study extends the **Strategic Data Alignment Framework (SDAF)**, originally developed to align corporate strategy with Big Data governance [7,8], into the domain of **cybersecurity governance for critical maritime infrastructure**. By integrating SDAF with insights from the **Resource-Based View (RBV)**, the paper conceptualizes cyber-resilience not as a technical add-on but as a **strategic VRIN resource**—valuable, rare, inimitable, and non-substitutable [8]. The core research question guiding this paper is:

> *How can SDAF be adapted to strengthen cybersecurity governance in critical maritime infrastructure under conditions of hybrid threat and geopolitical uncertainty?*

The contribution is twofold. Theoretically, it expands SDAF into cybersecurity governance, linking digital resilience with strategic alignment [8]. Practically, it proposes a **five-step roadmap** that emphasizes regional cooperation, supply-chain assurance, AI-enabled defense, and alignment with international standards. In doing so, the paper aims to support both scholars and policymakers in advancing resilient, trusted digital corridors that safeguard global trade and the societies dependent on them.

II. Related Work

Cybersecurity in Maritime Infrastructure

Maritime ports have increasingly been conceptualized as **cyber–physical ecosystems**, where the interdependence of information technology (IT), operational technology (OT), and Port Community Systems (PCS) generates significant vulnerabilities. Recent scholarship emphasizes that cyber risks in ports are no longer confined to isolated IT incidents but extend across **critical infrastructures, logistics chains, and socio-technical systems**.[9]. A 2023 study proposed a comprehensive cybersecurity architecture for ports and harbors, underlining the need for integrated governance that spans standards compliance, layered technical controls, and continuous risk monitoring [9,10]. Small and medium-sized ports face particular challenges due to limited financial and human resources, resulting in uneven adoption of cybersecurity measures and increased vulnerability to cascading attacks [10].

Hybrid Threats and Navigation Integrity

Cybersecurity risks in maritime contexts are exacerbated by **hybrid threats**, which combine cyber operations with geopolitical objectives. Peer-reviewed studies have demonstrated the feasibility of **AIS (Automatic Identification System) spoofing**, where false signals are injected to manipulate ship identities, enable sanction evasion, or create navigational confusion [11]. Complementary research into GNSS (Global Navigation Satellite Systems) vulnerabilities has shown how spoofing and jamming can degrade situational awareness [12], posing both safety and security challenges for maritime operators [13]. These findings highlight navigation integrity as a domain where cyber and geopolitical risks converge, requiring governance frameworks that extend beyond purely technical solutions.

 doi:10.20944/preprints202605.0307.v1

Artificial Intelligence in Maritime Cyber Defence

Artificial intelligence (AI) is increasingly viewed as both an opportunity and a challenge for maritime cybersecurity. A 2025 systematic review identified AI-driven techniques such as anomaly detection, predictive analytics, and adversarial learning as central to emerging maritime cyber defence strategies, while also underscoring critical gaps in **dataset availability, adversarial robustness, and explainability** [14]. This duality suggests that while AI tools may enhance resilience, their integration must be governed by structured data management, quality assurance, and accountability mechanisms. Such insights directly reinforce the SDAF principle that **data governance must be strategically aligned with security objectives**.

OT/ICS Security and Port Community Systems

The integration of OT/ICS with PCS has amplified systemic risks within ports. Scholarly research has shown that cyber intrusions targeting industrial control systems can cascade into large-scale operational disruptions, underscoring the need for multi-layered governance and formalized **threat intelligence sharing** (Karagiannis et al., 2023). Given the growing sophistication of cyber–physical attacks, scholars argue that cybersecurity governance must evolve from compliance-oriented frameworks toward **proactive resilience models** that anticipate system-wide interdependencies.

Regulatory Convergence and Compliance Engineering

Regulatory developments are reshaping the landscape of maritime cybersecurity governance. The European Union's **NIS2 Directive** imposes binding obligations on critical infrastructure operators, extending accountability to supply-chain actors and mandating systematic risk assessments. Peer-reviewed legal analyses highlight how NIS2 reframes cybersecurity as a **governance issue tied to sovereignty, liability, and trust**, with implications for global trade corridors [15]. However, compliance engineering remains uneven across regions, with smaller ports in particular struggling to operationalize regulatory requirements.

Port Resilience and Governance Integration

Recent scholarship on **port resilience** emphasizes that cyber preparedness cannot be treated in isolation but must be integrated into broader governance models that also consider logistics continuity, stakeholder collaboration, and sustainability. A 2025 systematic review found that resilience-building requires combining digital technologies, governance mechanisms, and multi-stakeholder coordination, placing cybersecurity at the core of resilience rather than as an ancillary concern [16]. This perspective aligns closely with the SDAF principle of institutional cooperation as a strategic resource [7,8].

Synthesis and Research Gap

The literature reviewed demonstrates that cybersecurity in maritime infrastructure has evolved into a **strategic governance challenge** shaped by hybrid threats, AI-driven risks, supply-chain vulnerabilities, and uneven regulatory compliance. Yet, no existing framework offers a **holistic alignment of strategy, data governance, and cybersecurity** tailored to critical maritime infrastructure. Current research remains fragmented—focusing on technical solutions, regulatory mandates, or resilience models in isolation.

This gap motivates the present study, which extends the **Strategic Data Alignment Framework (SDAF)** [7,8] into cybersecurity governance. By embedding cyber-resilience within a structured framework of strategy, governance, cooperation, and compliance, the study addresses the absence of an integrative approach capable of safeguarding digital corridors under hybrid threat conditions.

 doi:10.20944/preprints202605.0307.v1

III. Methods

Research Design

This study adopts a **qualitative comparative policy analysis (QCPA)** approach, which is appropriate for examining the governance dimensions of cybersecurity in critical maritime infrastructure. QCPA allows for the systematic comparison of national, regional, and international regulatory frameworks, highlighting both areas of convergence and fragmentation [17,18]. The method is particularly suited to contexts where **geopolitical factors and hybrid threats** shape policy choices, requiring an interpretive but structured lens.

Data Sources

The analysis draws on three categories of sources:

1. **Primary policy and regulatory documents**
   - National cybersecurity and maritime security strategies of Caspian Basin states.
   - Regional cooperation agreements and communiqués related to digital trade and transport.
   - International frameworks including the **EU NIS2 Directive**, the **IMO Guidelines on Maritime Cyber Risk Management**, and **WTO digital trade principles**.
2. **Peer-reviewed academic literature (2022–2025)**
   - Research on maritime cybersecurity ecosystems, supply-chain vulnerabilities, AIS/GNSS spoofing, AI-driven cyber defence, and resilience governance.
   - Systematic reviews providing conceptual clarity on resilience, governance integration, and compliance engineering.
3. **Expert validation**
   - Input from cybersecurity specialists and port governance practitioners was used to refine the thematic coding and validate findings. Expert consultation ensured contextual accuracy and practical relevance of the analytical results.

Analytical Framework

The study employs **thematic coding** [18] to identify recurring governance challenges across the data. Codes were developed deductively from SDAF dimensions and inductively from the literature. The coding categories included:

1. **Regulatory harmonization** – alignment with global frameworks (NIS2, IMO, WTO).
2. **Institutional capacity** – resources, organizational maturity, and human capital.
3. **Supply-chain and vendor risk management** – third-party security and assurance mechanisms.
4. **Navigation and OT integrity** – measures addressing AIS/GNSS spoofing and OT/ICS vulnerabilities.
5. **AI integration** – opportunities and risks in applying AI to maritime cybersecurity.
6. **Hybrid threat adaptation** – recognition and mitigation of state-linked or geopolitical cyber risks.
7. Each document was coded independently and then compared to establish cross-case patterns.

Benchmarking Procedure

To assess convergence, national and regional policies were benchmarked against **international standards**:

- **EU NIS2 Directive** served as the baseline for regulatory obligations and supply-chain accountability.
- **IMO Cyber Risk Management Guidelines** provided operational benchmarks for maritime-specific cybersecurity.
- **WTO digital trade principles** established expectations for cross-border trust and interoperability.

 doi:10.20944/preprints202605.0307.v1

This benchmarking enabled the identification of gaps between global expectations and regional practices in the Caspian Basin.

Validity and Reliability

Several strategies were employed to enhance the rigor of the study:

- **Triangulation:** Cross-validation across regulatory texts, scholarly literature, and expert interviews to ensure credibility.
- **Peer-reviewed evidence base:** Only recent (2022–2025) peer-reviewed studies were integrated into the analysis, ensuring the research reflects the latest scholarly consensus.
- **Expert validation:** Practitioners' feedback from cybersecurity and port sectors in the Caspian region confirmed the relevance of the coding results.
- **Audit trail:** Coding procedures and benchmarking criteria were documented to allow replication by future researchers.

Theoretical Integration

The **Strategic Data Alignment Framework (SDAF)** serves as the guiding theoretical lens. Originally developed for aligning corporate strategy with Big Data governance [7,8], SDAF is adapted here to assess cybersecurity governance. Its four dimensions—**strategic alignment, governance mechanisms, institutional cooperation, and compliance standards**—structure the coding schema. In this adaptation, cyber-resilience is explicitly positioned as a **VRIN resource** under the Resource-Based View [19], framing resilience not only as a technical outcome but as a **strategic advantage** in global digital corridors.

IV. Results

The comparative policy analysis and benchmarking revealed a set of systemic governance challenges that undermine the cybersecurity resilience of critical maritime infrastructure in the Caspian Basin. The findings are presented according to the coding categories: regulatory harmonization, institutional capacity, supply-chain and vendor risk management, navigation and OT integrity, AI integration, and hybrid threat adaptation.

Regulatory Harmonization

The analysis identified **persistent fragmentation in regulatory frameworks** across the Caspian Basin. While Azerbaijan and Kazakhstan have made notable progress in drafting cybersecurity strategies that reference international obligations, these remain **loosely aligned** with the EU's NIS2 Directive [20,21]. By contrast, Russia and Iran maintain sovereignty-centered cybersecurity doctrines that prioritize national control over alignment with external standards, resulting in **limited interoperability** [22,23]. Turkmenistan's frameworks remain underdeveloped, with minimal evidence of structured cyber risk management [24–26].

Benchmarking revealed that none of the regional frameworks fully incorporate the **supply-chain accountability provisions mandated by NIS2**, nor do they adequately reflect the **operational controls recommended by the IMO cyber guidelines** [27]. This divergence suggests that while international norms are recognized, they are **not systematically translated into enforceable national practices**.

Institutional Capacity

Institutional maturity varied significantly across cases. Larger ports, such as Baku International Sea Trade Port, demonstrated **emerging organizational structures** for cyber risk management, including nascent Security Operations Centers (SOCs) and port community systems with embedded monitoring functions. However, small and medium-sized ports across the region exhibited **severe**

 doi:10.20944/preprints202605.0307.v1

capacity gaps, lacking specialized personnel, budgetary allocation, and technical infrastructure [7,8,27].

This capacity deficit leads to an **implementation gap**, where national strategies that aspire to international compliance fail to materialize in operational environments. Expert validation confirmed that even when policies exist, local enforcement mechanisms remain weak, reflecting a disconnect between strategic ambition and institutional reality.

Supply-Chain and Vendor Risk Management

A critical weakness across all examined cases was the absence of robust supply-chain risk management mechanisms. Ports remain heavily reliant on foreign-manufactured equipment (e.g., cranes, IoT sensors, and PCS software) without systematic certification or vetting processes [8,27].

This reliance introduces vulnerabilities at two levels:

1. **Technical risk**, as embedded components may lack security assurance.
2. **Strategic risk**, as geopolitical dependencies on external vendors could be exploited during periods of heightened tension.

Comparative analysis against NIS2 requirements highlighted a **regulatory gap**: while NIS2 obliges operators to assess third-party risks, no Caspian state has adopted comparable accountability measures. This absence underscores the urgent need for **vendor certification and assurance frameworks** as part of regional governance [8,27].

Navigation and OT Integrity

The findings confirm that **navigation integrity remains insufficiently addressed** in regional governance frameworks. Evidence from expert validation highlighted incidents of **AIS manipulation** and GPS interference in the Caspian Sea, which create both safety hazards and opportunities for illicit activities such as sanctions evasion [11,12].

Despite growing scholarly consensus on the need for cryptographic authentication of AIS and advanced GNSS spoofing detection techniques, none of the reviewed national frameworks mandate such measures. Furthermore, industrial control systems (ICS) used in port operations remain highly exposed due to outdated architectures and inadequate segmentation from enterprise IT networks [11,12]. These vulnerabilities expose Caspian ports to potential **cyber–physical disruption scenarios**, including crane manipulation or PCS shutdowns.

AI Integration

The analysis revealed that while AI-driven security solutions are increasingly recognized in strategic documents, **their integration remains limited and experimental**. Larger ports reference the potential of AI-based anomaly detection for PCS monitoring, yet lack the data governance structures and robust datasets required for effective deployment.

This gap aligns with broader scholarly findings that **AI in maritime cybersecurity is constrained by limited data availability and adversarial robustness**. Without proper governance, reliance on AI tools risks generating false confidence rather than genuine resilience.

Hybrid Threat Adaptation

Perhaps the most significant gap lies in the **lack of explicit recognition of hybrid threats** within regional policies. None of the reviewed frameworks explicitly integrate scenarios involving **state-linked cyber operations, coordinated disinformation campaigns, or cross-domain attacks targeting both digital and physical infrastructure**.

Given the Caspian Basin's geopolitical sensitivity, this omission represents a critical blind spot. Expert feedback confirmed that while practitioners are aware of hybrid threats, they lack institutional mandates or playbooks for response [12–14,16]. This leaves ports vulnerable to **strategically motivated cyberattacks** that exploit regional fragmentation.

 doi:10.20944/preprints202605.0307.v1

Summary of Findings

In sum, the analysis demonstrates that cybersecurity governance in Caspian maritime infrastructure is characterized by:

1. Fragmented regulatory frameworks with limited harmonization.
2. Severe institutional capacity gaps, particularly in smaller ports.
3. Absence of supply-chain assurance mechanisms, exposing ports to vendor-based risks.
4. Unaddressed vulnerabilities in navigation integrity and OT/ICS systems.
5. Underdeveloped AI integration, hindered by data governance deficits.
6. Neglect of hybrid threat adaptation, despite clear geopolitical exposure.

These findings highlight the urgency of extending the **Strategic Data Alignment Framework (SDAF)** to cybersecurity governance [7,8]. SDAF provides a structured pathway to align strategy, governance, institutional cooperation, and compliance with global standards—addressing the exact weaknesses observed in the empirical analysis.

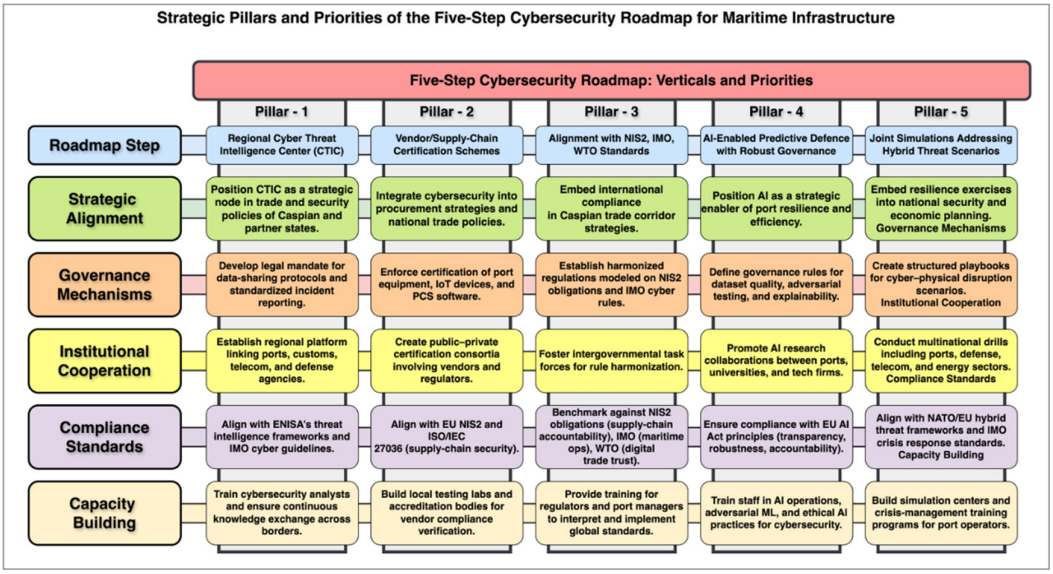
V. Discussion

Extending SDAF to Cybersecurity Governance

The results demonstrate that fragmented governance, weak institutional capacity, and unaddressed hybrid threats leave Caspian ports acutely vulnerable. These challenges align directly with the dimensions of the **Strategic Data Alignment Framework**. Originally developed to align corporate strategies with Big Data governance [7,8,28,29], SDAF emphasizes the need for **strategic alignment, governance mechanisms, institutional cooperation, and compliance standards** [8,9]. Extending SDAF into cybersecurity governance offers a structured means to address the shortcomings identified in this study.

Structured Strategic Data Alignment Framework Based on the Five-Step Cybersecurity Roadmap and Its Strategic Verticals

- The diagram illustrates thematic priorities across strategic alignment, governance mechanisms, institutional cooperation, compliance standards, and capacity building, adapted from the Strategic Data Alignment Framework [8,28] and aligned with NIS2, IMO, and WTO principles.



 doi:10.20944/preprints202605.0307.v1

Five-Step Cybersecurity Roadmap Verticals for Critical Maritime Infrastructure

The extended framework illustrates how SDAF's dimensions can be adapted to integrate cyber-resilience:

- **Strategic alignment** → embedding cybersecurity into national and corporate trade strategies.
- **Governance mechanisms** → enforcing compliance with NIS2, IMO, and WTO standards.
- **Institutional cooperation** → creating regional cyber threat intelligence platforms.
- **Compliance standards** → translating international obligations into enforceable local mandates.

This extension ensures that cybersecurity is not treated as an isolated technical issue but as an integral element of strategic governance for digital corridors.

Cyber-Resilience as a VRIN Resource

The **Resource-Based View (RBV)** provides a powerful lens for interpreting cyber-resilience as a strategic resource. Under RBV, resources must be **valuable, rare, inimitable, and non-substitutable (VRIN)** to confer sustainable competitive advantage [19]. The analysis suggests that regulatory convergence and cyber-resilience satisfy these conditions:

- **Valuable:** Enhances trust, reduces costs from disruptions, and safeguards trade flows.
- **Rare:** Few regional trade corridors achieve meaningful cybersecurity harmonization.
- **Inimitable:** Building resilience requires historical cooperation, institutional trust, and complex coordination that cannot easily be replicated.
- **Non-substitutable:** No technical substitute exists for governance-based resilience.

By framing cyber-resilience as a VRIN resource, the study advances theoretical understanding of cybersecurity not merely as risk management, but as a source of **strategic advantage for ports and regions**.

Policy and Practical Implications

The findings and SDAF extension yield a **five-step roadmap** for strengthening cybersecurity governance in Caspian maritime infrastructure:

1. **Establish a Regional Cyber Threat Intelligence Center (CTIC).**

A shared platform would enable real-time information exchange, ensuring that ports are not isolated in responding to threats.

2. **Implement Vendor and Supply-Chain Certification.**

A regional framework for certifying equipment, software, and third-party providers would reduce dependence on insecure or politically sensitive vendors [13].

3. **Align with International Standards (NIS2, IMO, WTO).**

Translating global principles into enforceable obligations within national legal systems would enhance interoperability and global trust.

4. **Adopt AI-Enabled Anomaly Detection and Predictive Defence.**

AI systems, governed by structured data policies, would allow proactive monitoring while ensuring explainability and robustness [14].

5. **Conduct Joint Hybrid Threat Simulations and Resilience Testing.**

Regular drills and scenario-based exercises would prepare institutions for state-linked cyberattacks and multi-domain disruptions [16].

Together, these measures operationalize SDAF in the cybersecurity domain, linking strategic priorities with regulatory enforcement and institutional practice.

 doi:10.20944/preprints202605.0307.v1

Contribution to Scholarship and Practice

This study contributes to scholarship by **extending SDAF into cybersecurity governance**, bridging a gap between strategic management and cyber policy in critical infrastructure. It also reframes **cyber-resilience as a VRIN resource**, offering a novel theoretical justification for investment in governance-based security. Practically, the five-step roadmap provides policymakers and practitioners with an actionable pathway to address vulnerabilities in Caspian ports and, by extension, other emerging trade corridors.

VI. Conclusions

This study has examined the cybersecurity governance of critical maritime infrastructure in the Caspian Basin, with a particular focus on the vulnerabilities introduced by hybrid threats, fragmented regulation, and supply-chain dependencies. Through a comparative policy analysis and benchmarking against global standards such as the EU's NIS2 Directive, IMO cyber risk management guidelines, and WTO digital trade principles, the research identified systemic gaps in **regulatory harmonization, institutional capacity, vendor assurance, navigation integrity, AI integration, and hybrid threat preparedness**.

To address these shortcomings, the study extended the **Strategic Data Alignment Framework (SDAF)**, originally designed for corporate data governance, into the domain of **cybersecurity governance for critical infrastructure**. This extension demonstrates that SDAF's four dimensions—strategic alignment, governance mechanisms, institutional cooperation, and compliance standards—can provide a structured pathway to embed cyber-resilience into national and regional strategies. In doing so, the paper reconceptualizes cyber-resilience as a **VRIN resource** under the Resource-Based View, highlighting its value as a source of strategic advantage rather than a purely technical safeguard.

The practical contribution of this study is a **five-step roadmap**: establishing a regional cyber threat intelligence center, certifying vendors and supply chains, aligning with international standards, deploying AI-enabled anomaly detection, and conducting joint hybrid threat simulations. These measures collectively provide a governance-based approach to strengthening digital corridors, with immediate relevance for Caspian ports and broader applicability to other emerging trade corridors worldwide.

Looking forward, **future research** should build on these findings by:

1. Developing **quantitative resilience metrics** to measure the effectiveness of governance interventions.
2. Conducting **simulation-based studies** to test hybrid threat scenarios under different regulatory conditions.
3. Expanding comparative analysis to include **other regional corridors**, such as the Black Sea and Mediterranean, to assess transferability of the SDAF extension.

In synthesizing theory and practice, this paper contributes to both academic scholarship and policy discourse. It underscores that cybersecurity governance is not a peripheral technical concern but a **strategic necessity** for safeguarding global trade and ensuring societal resilience in an era of hybrid threats and geopolitical uncertainty.

Acknowledgments: The author gratefully acknowledges the institutional support of the Azerbaijan Technical University and the Defense Technologies and Cybersecurity Institute, which provided the academic environment and resources for this research. Special appreciation is extended to **cybersecurity experts and port governance practitioners from the Caspian region**, whose perspectives on hybrid threats, supply-chain vulnerabilities, and regulatory implementation offered valuable insights into the realities of maritime digital infrastructure. The author also acknowledges the contributions of **international experts and comparative policy dialogues**, which helped situate the study within the broader landscape of global best practices. Their input provided critical perspectives on aligning regional governance models with international frameworks such as

 doi:10.20944/preprints202605.0307.v1

the NIS2 Directive, IMO guidelines, and WTO digital trade principles. The collective contributions of these experts enriched the analytical process, strengthened the thematic validation, and informed the practical recommendations presented in this paper.

References

1. D. Ş. Polat, "Zengezur Koridoru: Türkiye-Azerbaycan İlişkileri Bağlamında Stratejik, Ekonomik ve Bölgesel Çıkarımlar," *İstanbul Kent Üniversitesi Siyasal, Sosyal ve Stratejik Araştırmalar Dergisi*, vol. 1, no. 1, pp. 144–173, Apr. 2025, Accessed: Oct. 16, 2025. [Online]. Available: https://dergipark.org.tr/en/pub/kentusamder/issue/91382/1681617
2. K. Abdullayev, P. Hasanov, A. Aliyeva, N. Aliyeva, and A. Mustafayev, "The non-oil sector of the Republic of Azerbaijan's economy: Prospects and directions for development within the framework of contemporary economic policy," *Economics of Development*, vol. 4, no. 23, pp. 82–94, 2024, doi: 10.57111/econ/4.2024.82.
3. A. Yermekbayev, L. Delovarova, and A. Kaliyeva, "Trans-Caspian International Transport Route: A Kazakhstani Perspective on Challenges, Opportunities, and Prospects," *International Journal*, vol. 79, no. 2, pp. 312–329, June 2024, doi: 10.1177/00207020241257636.
4. M.-A. Pădureanu and I. Oneașcă, "From synergy to strategy in the black sea region: Assessing opportunities and challenges," EIR Working Papers Series, Working Paper 51, 2024. Accessed: Oct. 16, 2025. [Online]. Available: https://www.econstor.eu/handle/10419/300147
5. E. Kaya, Y. Karakuş, and G. Onat, "Azerbaijan and Turkey's Tourism Ties: The Role of Zangezur Corridor," *Journal of Hospitality and Tourism Issues*, vol. 6, no. 1, pp. 16–27, June 2024, doi: 10.51525/johti.1406400.
6. H. Nurlu, "TRT World - Zangezur Corridor, a century-long artery between rivalry and resilience." Accessed: Oct. 16, 2025. [Online]. Available: https://www.trtworld.com/article/2859d3513152
7. R. Alekberli (Alakbarli), "Integrating Big Data Governance and Corporate Strategies in Small and Medium Caspian Basin Seaports," *Walden Dissertations and Doctoral Studies*, Sept. 2024, [Online]. Available: https://scholarworks.waldenu.edu/dissertations/16316
8. R. Z. Alekberli and R. E. Haussmann, "Integrating Big Data Governance and Corporate Strategies in Small and Medium Caspian Basin Seaports," in *2024 IEEE Global Conference on Artificial Intelligence and Internet of Things (GCAIoT)*, Nov. 2024, pp. 1–6. doi: 10.1109/GCAIoT63427.2024.10833594.
9. J. Pöyhönen and M. Lehto, "Comprehensive cyber security for port and harbor ecosystems," *Front. Comput. Sci.*, vol. 5, Oct. 2023, doi: 10.3389/fcomp.2023.1154069.
10. Y. Chen, "A study on the system of influential factors for high-quality development of Chinese cultural and tourism small towns: Insights from W town," *Dissertations and Theses Collection (Open Access)*, pp. 1–244, Mar. 2023, [Online]. Available: https://ink.library.smu.edu.sg/etd_coll/480
11. A. Androjna, I. Pavić, L. Gucma, P. Vidmar, and M. Perkovič, "AIS Data Manipulation in the Illicit Global Oil Trade," *JMSE*, vol. 12, no. 1, p. 6, Dec. 2023, doi: 10.3390/jmse12010006.
12. S. Singh et al., "Detection and Mitigation of GNSS Spoofing Attacks in Maritime Environments Using a Genetic Algorithm," *Mathematics*, vol. 10, no. 21, p. 4097, Nov. 2022, doi: 10.3390/math10214097.
13. G. Wimpenny, J. Šafář, A. Grant, and M. Bransby, "Securing the Automatic Identification System (AIS): Using public key cryptography to prevent spoofing whilst retaining backwards compatibility," *J. Navigation*, vol. 75, no. 2, pp. 333–345, Mar. 2022, doi: 10.1017/S0373463321000837.
14. C. V. Ribeiro, A. Paes, and D. D. Oliveira, "AIS-based maritime anomaly traffic detection: A review," *Expert Systems with Applications*, vol. 231, p. 120561, Nov. 2023, doi: 10.1016/j.eswa.2023.120561.
15. I. De La Peña Zarzuelo, M. J. Freire Soeane, and B. López Bermúdez, "Industry 4.0 in the port and maritime industry: A literature review," *Journal of Industrial Information Integration*, vol. 20, p. 100173, Dec. 2020, doi: 10.1016/j.jii.2020.100173.
16. G. T. Tsoulfas, "Port resilience: a systematic literature review," *Marit Econ Logist*, July 2025, doi: 10.1057/s41278-025-00326-3.
17. B. Rihoux and C. Ragin, *Configurational Comparative Methods: Qualitative Comparative Analysis (QCA) and Related Techniques*. 2455 Teller Road, Thousand Oaks California 91320 United States: SAGE Publications, Inc., 2009. doi: 10.4135/9781452226569.

 doi:10.20944/preprints202605.0307.v1

18. J. Saldana, "The coding manual for qualitative researchers," pp. 1–440, 2021, Accessed: July 13, 2024. [Online]. Available: https://www.torrossa.com/en/resources/an/5018667
19. B. Wernerfelt, "A resource-based view of the firm," *Strat. Mgmt. J.*, vol. 5, no. 2, pp. 171–180, Apr. 1984, doi: 10.1002/smj.4250050207.
20. Azerbaijan, "The Strategy of the Republic of Azerbaijan on Information Security and Cybersecurity for 2023–2027 | Digital Watch Observatory." Accessed: Oct. 13, 2025. [Online]. Available: https://dig.watch/resource/the-strategy-of-the-republic-of-azerbaijan-on-information-security-and-cybersecurity-for-2023-2027
21. e-G. Academy (Estonia), "National Cyber Security Index (NCSI): Azerbaijan." 2024. [Online]. Available: https://ncsi.ega.ee/country/az/
22. G. Lopez-Rodriguez, I. Moreno-Lopez, and J.-C. Hernández-Gutiérrez, "Cyberwarfare against Critical Infrastructures: Russia and Iran in the Gray Zone," *Applied Cybersecurity & Internet Governance*, vol. 2, no. 1, pp. 1–19, Dec. 2023, doi: 10.60097/ACIG/162865.
23. *Russia's Strategy in Cyberspace*. Riga [Latvia]: NATO Strategic Communications Centre of Excellence, 2021.
24. Z. Mungalova, "Economic Development in the Commonwealth of Independent States Challenges and Opportunities," Apr. 16, 2023, *Social Science Research Network, Rochester, NY*: 5161189. doi: 10.2139/ssrn.5161189.
25. K. A, N. A, O. Y, and R. R, "A BRIEF OVERVIEW OF SYSTEMS ENGINEERING AND ITS RELATIONSHIP TO PROJECT MANAGEMENT," *Символ науки*, no. 5-1–3, pp. 55–57, 2024, Accessed: Oct. 16, 2025. [Online]. Available: https://cyberleninka.ru/article/n/a-brief-overview-of-systems-engineering-and-its-relationship-to-project-management
26. B. Zehir and F. Odabaşı, "DIGITAL TRANSFORMATION IN CENTRAL ASIA: OPPORTUNITIES AND RISKS IN A LATE START," *DISEM*, vol. 2, no. 1, pp. 3–14, July 2025, Accessed: Oct. 16, 2025. [Online]. Available: https://dergipark.org.tr/en/pub/disem/issue/94049/1706515
27. M. Nilsson, *Aligning EU Cybersecurity Regulations with ICS Security Standards : A Systematic Literature Review*. 2025. Accessed: Oct. 16, 2025. [Online]. Available: https://urn.kb.se/resolve?urn=urn:nbn:se:his:diva-25899
28. R. Alekberli, "Developing a Data-Driven Radio Frequency Administration for Spectrum-Sharing, Strategic Utilization and Sharing-Readiness in Azerbaijan as a Case Example," Master's Thesis, The University of Liverpool (United Kingdom), 2019. Accessed: Jan. 27, 2025. [Online]. Available: https://search.proquest.com/openview/6925c6af1de3bc498adc7bec4c5747ad/1?pq-origsite=gscholar&cbl=18750&diss=y
29. R. Alekberli and R. Alguliev, "Internets copy: Current state, problems and perspectives," in *2014 IEEE 8th International Conference on Application of Information and Communication Technologies (AICT)*, IEEE, 2014, pp. 1–7. doi: 10.1109/ICAICT.2014.7035938.