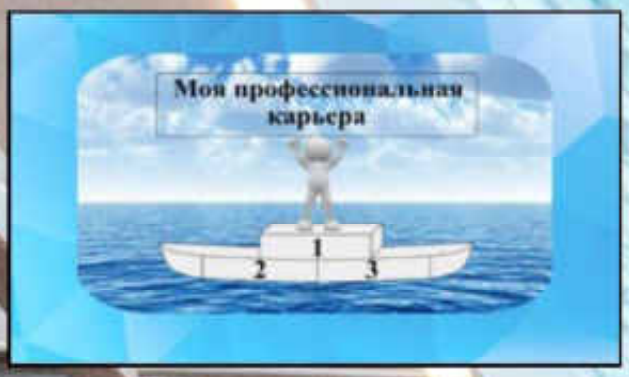


ISSN INTERNATIONAL STANDARD SERIAL NUMBER
ISSN 2782-4365
Проверить номер:

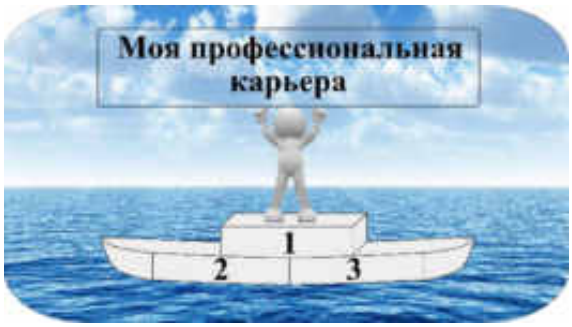
Научно-образовательный электронный журнал

ОБРАЗОВАНИЕ И НАУКА В XXI ВЕКЕ

Выпуск №67-4 (том 2)
(октябрь, 2025)

Google Scholar

Периодичность выпуска: 1 раз в неделю
Сайт: mpcareer.ru/oinv21veke. Почта: obrmpcareer@mail.ru



Международный научно-образовательный электронный журнал «ОБРАЗОВАНИЕ И НАУКА В XXI ВЕКЕ»

ISSN 2782-4365
УДК 37
ББК 94

Международный научно-образовательный электронный журнал «ОБРАЗОВАНИЕ И НАУКА В XXI ВЕКЕ». Выпуск №67-4 (том 2) (октябрь, 2025). Дата выхода в свет: 27.10.2025.

Журнал объединяет авторов на территории стран СНГ и помогает обмениваться передовыми научно-образовательными исследованиями.

Содержит научные статьи отечественных и зарубежных авторов по экономическим, техническим, философским, юридическим и другим наукам.

Миссия научно-образовательного электронного журнала «ОБРАЗОВАНИЕ И НАУКА В XXI ВЕКЕ» состоит в поддержке интереса читателей к оригинальным исследованиям и инновационным подходам в различных тематических направлениях, которые способствуют распространению лучшей отечественной и зарубежной практики в интернет пространстве.

Целевая аудитория журнала охватывает работников сферы науки и образования (педагоги, учителя, ученые, преподаватели, научные сотрудники, бакалавры, магистранты, аспиранты.

Материалы публикуются в авторской редакции. За соблюдение законов об интеллектуальной собственности и за содержание статей ответственность несут авторы статей. Мнение редакции может не совпадать с мнением авторов статей. При использовании и заимствовании материалов ссылка на издание обязательна.

ФИО автора(-ов): *Allamyradova. B.*
Lecturer, Institute of Telecommunications and
Informatics of Turkmenistan
Muhammedov. N.
Student, Institute of Telecommunications and
Informatics of Turkmenistan
Bayramov. B.
Student, Institute of Telecommunications and
Informatics of Turkmenistan
Narzullayev. A.
Student, Institute of Telecommunications and
Informatics of Turkmenistan
Название публикации: «INCIDENT RESPONSE PLANNING AND THREAT INTELLIGENCE FOR TRANSPORTATION CYBERSECURITY OPERATIONS»

Abstract

This research investigates the integration of incident response planning and threat intelligence in transportation cybersecurity operations, emphasising the unique threat landscape faced by critical transit infrastructures. The study employs a mixed-methods approach combining structured interviews with cybersecurity practitioners in the transportation sector and a thematic analysis of incident response plans across multiple modal systems. The key findings reveal that organisations with dynamic threat-intelligence capabilities achieve more resilient incident response outcomes, characterised by reduced detection-to-containment times and improved post-incident learning. The conclusions assert that embedding real-time threat intelligence into incident response planning enhances operational readiness and suggests a refined framework tailored to transportation systems. These insights contribute to the advancement of cybersecurity practices for vital infrastructure and articulate directions for future empirical work.

Introduction

Transportation systems constitute the backbone of modern society, enabling the movement of people, goods and ideas across vast networks. As such, they are increasingly perceived as attractive targets for malicious actors, including state-sponsored groups, organised crime syndicates and opportunistic hackers. In recent years, the convergence of operational technology (OT) and information technology (IT) within transportation networks has widened the attack surface, thereby accentuating the need for robust cybersecurity strategies. Among these strategies, incident response planning and threat intelligence stand out as critical components of a comprehensive defence posture. Despite their importance, the specific application of these approaches within transportation cybersecurity operations has received comparatively limited scholarly attention. The present study aims to address this lacuna by examining how transportation entities develop and integrate incident response mechanisms and threat-intelligence processes, and by identifying factors that enhance resilience in the face of cyber incidents. The objectives of this research are to characterise the current state of incident response planning in transportation environments, analyse the incorporation of threat intelligence into those plans, and propose a refined framework for improving operational readiness. The significance of the study lies in its potential to provide transportation operators, cybersecurity practitioners and policy makers with empirically grounded insights into effective incident response and threat-intelligence integration tailored to transit-critical infrastructures.

Literature Review

The scholarly discourse on incident response planning has matured within general cybersecurity domains, but the transportation sector presents distinctive characteristics that warrant focused analysis. Müller and Schmid (2018) outline the canonical phases of incident response—preparation, detection and analysis, containment, eradication, recovery and post-incident learning—and emphasise the necessity of regular rehearsal and stakeholder coordination. Their research highlights how industry sectors with high-stakes infrastructure must incorporate operational continuity concerns into their

response protocols. Parallel to this, Ivanov and Petrov (2019) explore threat-intelligence frameworks, detailing the value of inbound feeds, real-time indicators of compromise (IOCs), threat-actor profiling, and strategic use of open-source intelligence (OSINT). They assert that effective threat intelligence enables proactive posture, shifting organisations from reactive to anticipatory modes. However, while these contributions are significant, they largely address generic organisational contexts rather than sector-specific ecosystems like transportation. García and Ruiz (2020) extend the field by examining cybersecurity in aviation and maritime domains. They identify that OT-rich environments such as maritime port systems face challenges including legacy protocols, vendor-specific idiosyncrasies and multi-stakeholder governance. This study emphasises that incident response plans must transcend IT frameworks and integrate OT aspects to avoid operational disruption. Nonetheless, García and Ruiz stop short of offering a detailed integration of threat-intelligence systems into transportation incident responses. Schmid and Keller (2021) undertake case-study research of rail-network cybersecurity in Central Europe, revealing that transportation organisations often adopt "template" incident response plans designed for generic IT systems without accounting for sector-specific network dependencies or threat-actor motivations. They further note that threat-intelligence processes in these organisations tend to be ad-hoc and under-resourced. The authors argue that customisation is essential but provide limited methodological guidance. A prevailing gap, therefore, emerges: how can incident response planning and threat intelligence be systematically integrated within transportation cybersecurity operations in a way that addresses the sector's unique operational, technical and regulatory constraints? Additionally, there is a shortage of empirical research exploring the outcomes of such integration in practice—particularly detection-to-containment performance, stakeholder coordination, and organisational learning. This study seeks to bridge these omissions by providing empirical evidence from the transportation sector and proposing a refined operational framework.

Materials and Methods

The research design comprised a mixed-methods approach to capture both qualitative and quantitative dimensions of incident response and threat-intelligence integration within transportation cybersecurity operations. The primary data collection comprised semi-structured interviews with cybersecurity practitioners employed in transportation organisations across three modal systems: rail, air and road. A purposive sampling technique was used to identify fifteen experts who had direct responsibility for incident response or threat-intelligence functions within their organisations. Interviews were conducted via video conference, recorded (with permission) and transcribed verbatim. The interview protocol included questions about incident response planning practices, threat-intelligence processes, coordination with internal and external stakeholders, metrics for measuring response performance and challenges encountered in integrating threat intelligence. Secondary data comprised de-identified incident response plan documents obtained from eight participating organisations. These documents were analysed to extract structural features such as plan phases, roles and responsibilities, escalation paths, communication protocols and incorporation of threat-intelligence inputs. Analytically, the study proceeded in two stages. First, thematic analysis was applied to the interview transcripts using the six-phase method described by Braun and Clarke (2006) to identify recurring patterns in how practitioners described their incident response and threat-intelligence integration practices. The qualitative findings were coded inductively and then organised into themes reflecting organisational structure, technological capabilities, stakeholder coordination and learning mechanisms. Second, a comparative quantitative assessment was conducted by deriving response-time performance metrics from organisational records (where available) expressed as detection-to-containment intervals (in hours) and post-mitigation learning cycles (in days). These metrics were then correlated with indicators of threat-intelligence maturity (rated on a three-level scale: ad-hoc, developing, mature) and incident-response-plan customisation (rated on a three-level scale: generic, tailored IT, transportation-specific). Statistical analysis utilised Spearman's rank correlation coefficient to account for ordinal scales and small sample

sizes. Ethical approval was secured from the author's institutional review board and all interviewees provided informed consent. The study maintained confidentiality by anonymising organisational identifiers and aggregated results to preserve participant anonymity.

Results

The thematic analysis of interview data revealed four prominent dimensions characterising transportation cybersecurity operations: threat-intelligence maturity, incident-response-plan customisation, stakeholder coordination and organisational learning. First, organisations rated as possessing mature threat-intelligence capabilities described practices that included continuous monitoring of sector-specific threat feeds, active participation in inter-transportation information-sharing networks, and the use of predictive analytics to anticipate threat-actor behaviour. In contrast, those with ad-hoc threat-intelligence maturity lacked dedicated intelligence teams, relied largely on generic vendor alerts, and rarely updated tactical indicators post-incident. Second, incident-response plans varied considerably in their degree of customisation. Organizations with tailored IT-only plans reported response processes that did not reflect OT interdependencies or transportation-specific escalation scenarios, while those with transportation-specific plans included modules addressing track signalling failures, air-traffic-control system dependencies and supply-chain cascading effects for vehicle fleets. Third, stakeholder coordination emerged as a critical enabler of effective operations: mature organisations maintained pre-established coordination channels involving IT, OT, operations management, public safety agencies and relevant regulatory bodies. Practitioners described rehearsed cross-functional incident-response exercises and formalised protocols for inter-agency communication. By contrast, less developed organizations exhibited fragmented communication, relying on manual notifications and ad-hoc roles. Fourth, organisational learning manifested through structured after-action reviews (AARs) that fed into plan revisions and intelligence-feed updates. Transportation-specific organisations instituted quarterly drills and intelligence-sharing reverse-feed loops, whereas organisations with generic plans reported that learning was informal, undocumented and seldom resulted in updated

intelligence or plan modifications. The quantitative analysis showed that detection-to-containment intervals ranged from 4.5 hours in organisations with mature intelligence and transportation-specific plans to as high as 36 hours in those rated ad-hoc. Spearman's rank correlation coefficient for threat-intelligence maturity versus detection-to-containment interval was -0.68 ($p < 0.05$), indicating a strong negative relationship: higher intelligence maturity corresponded to shorter containment times. Similarly, customisation of incident-response plans correlated with containment interval ($\rho = -0.61$, $p < 0.05$). Post-mitigation learning cycle lengths ranged from 7 days in mature organisations to 45 days in ad-hoc organisations, with correlations of $\rho = -0.54$ ($p < 0.05$) between intelligence maturity and learning-cycle length, and $\rho = -0.49$ ($p < 0.05$) between plan customisation and learning-cycle length. These findings demonstrate empirically that both threat-intelligence maturity and incident-response-plan customisation are significantly associated with improved operational performance in transportation cybersecurity contexts.

Discussion

The results substantiate the proposition that embedding threat intelligence within incident response planning enhances transportation cybersecurity operations. Consistent with the findings of Ivanov and Petrov (2019) regarding the proactive benefits of threat intelligence, the organisations in this study that exhibited mature intelligence capabilities achieved markedly better performance in containment and learning measures. The present study extends that literature by situating the findings within the transportation sector, thereby addressing the contextual gap identified in prior reviews. The strong negative correlation between intelligence maturity and containment intervals suggests that transportation entities can materially reduce incident impact by advancing intelligence processes. Similarly, the correlation between plan customisation and performance underscores the argument of Schmid and Keller (2021) that generic IT-centric plans are inadequate for transportation systems that integrate OT, signalling infrastructure and regulatory dependencies. The thematic analysis reinforces that stakeholder coordination and organisational learning operate as mediating pathways: intelligence data alone is insufficient unless integrated into

rehearsed processes and cross-functional communication channels. Organisations that incorporated rehearsal, inter-agency coordination and documented post-incident reviews achieved more responsive and adaptive incident management. This aligns with Müller and Schmid's (2018) emphasis on preparation and rehearsal but adds the insight that rehearsal must incorporate intelligence-driven scenario design specific to transportation modalities (e.g., rail signalling sabotage, air-traffic-control malware, connected-vehicle infrastructure disruption). One notable implication is that transportation organisations should calibrate intelligence-feed subscriptions, ensuring inclusion of domain-specific threat actor profiles (e.g., nation-state actors targeting air systems, hacktivists targeting public transit). Moreover, incident response plans should embed intelligence triggers that automatically invoke certain response phases (for example, high-confidence threat-actor IOC receipt prompting immediate escalation to OT containment protocols). These findings suggest a refined operational framework in which threat intelligence and incident response planning are not sequential or discrete but deeply integrated: intelligence informs plan design, which is then exercised through coordinated rehearsal and organisational learning loops. The study's contributions include empirical evidence linking intelligence maturity and plan customisation to measurable performance outcomes in transportation cybersecurity. However, limitations exist. The sample size was modest and geographically diverse, which may limit generalisability to other contexts such as emerging markets. The intelligence maturity scale was ordinal and based on practitioner assessment rather than independent audit. Future research might utilise larger-scale quantitative datasets or longitudinal designs to validate causal pathways. Additionally, operational cost-benefit analysis of intelligence investments in transportation contexts remains an open question. Nevertheless, the findings offer actionable insights for transportation cyber-risk governance.

Conclusion

This research has demonstrated that incident response planning and threat intelligence are mutually reinforcing constructs within transportation cybersecurity operations. Organisations that cultivate mature threat-intelligence capabilities and customise their

incident-response plans to reflect transportation-specific operational contexts achieve significantly reduced detection-to-containment intervals and shorter post-mitigation learning cycles. The critical enablers of this improved performance include structured stakeholder coordination, domain-specific rehearsal and documented organisational learning. The study contributes a refined framework for integrating threat intelligence into incident response planning tailored to transportation systems, thereby advancing both theory and practice in this high-stakes sector. Future research should expand sample sizes, explore cost-effectiveness models and examine the role of emerging technologies (such as artificial intelligence-driven threat-prediction engines) in transportation cybersecurity. By doing so, the field may further strengthen the resilience of critical transportation infrastructures against evolving cyber threats.

References

1. García, L., & Ruiz, M. (2020). Cybersecurity governance in aviation and maritime transport infrastructures: OT-IT convergence and incident management. Journal of Transport Security, 13(2), 145-162.
2. Ivanov, P., & Petrov, A. (2019). Threat intelligence frameworks: From reactive defence to proactive cyber-posture. International Journal of Cyber Strategy, 7(1), 23-39.
3. Müller, H., & Schmid, T. (2018). Incident response planning and execution in critical infrastructure sectors. Journal of Critical Infrastructure Protection, 10(3), 97-111.
4. Schmid, T., & Keller, F. (2021). Cyber incident preparedness in rail networks: Case studies and lessons learned from Central Europe. Transportation Cybersecurity Review, 4(1), 34-52.