HADMÉRNÖK
VÉDELEMINFORMATIKA
21. évfolyam (2026) 1. szám 41–55.
DOI: 10.32567/hm.2026.1.3

István Paráda[1]

Cyber Disruptions in Aviation Infrastructure

The CrowdStrike Outage

Abstract

This paper examines the intersection between civilian aviation cyber incidents and military logistics resilience, focusing on the systemic implications of the 2024 CrowdStrike global outage. Between 2018 and 2025, a series of airport IT and cybersecurity failures – ranging from ransomware to defence software malfunctions – exposed the vulnerabilities of dual-use infrastructures that serve both civil and military air mobility. The 2024 CrowdStrike event, which disrupted millions of systems worldwide, revealed the operational fragility of shared digital dependencies in air logistics networks. Drawing on data from FAA, ICAO and ENISA, this analysis identifies key lessons for defence logistics planners and cybersecurity policymakers seeking to enhance resilience against cascading failures.

Keywords: aviation cybersecurity, CrowdStrike incident, ENISA, NATO

Introduction: Cyber dependence and dual-use aviation logistics

Modern military logistics relies heavily on civilian aviation networks and digital infrastructure. Shared systems such as Jeppesen's MilPlanner and multinational airport IT environments blur the boundaries between civil and defence operations. This convergence enhances interoperability and efficiency, yet simultaneously creates tightly coupled digital dependencies that may amplify systemic vulnerability. Events such as the CrowdStrike 2024 outage highlight how a single commercial software update can propagate through defence logistics systems, affecting readiness, supply chain coordination and strategic mobility. Unlike conventional cyberattacks, this event originated from a non-malicious configuration failure, yet its operational effects resembled those of a coordinated systemic attack.

[1] CIS Operations Officer, NATO Support and Procurement Agency, e-mail: paradaistvan@gmail.com

This study examines aviation-related cyber and IT disruptions between 2018 and 2025 through a dual-use resilience lens. It addresses two research questions:

RQ1: What lessons does the CrowdStrike outage reveal about cybersecurity challenges in aviation and military operations?

RQ2: How have aviation and military organisations adapted to increasing cybersecurity dependency?

Literature review and methodology

The study adopts a qualitative, document-based analytical methodology. Empirical inputs are derived exclusively from publicly available institutional reports, incident reviews and regulatory publications issued by organisations such as ENISA,[2] FAA,[3] ICAO,[4] NATO CCDCOE[5] and NIST[6] between 2018 and 2025. Quantitative figures cited in the analysis are reproduced from these sources and are used illustratively rather than as independently generated datasets. Analytical inferences are explicitly distinguished from empirical observations. Documented incident characteristics – such as outage duration, affected systems and geographic scope – form the empirical baseline, while interpretations concerning cascading effects, logistics implications, and doctrinal relevance are derived through comparative analysis informed by resilience theory. Normative conclusions are presented as analytical implications rather than empirically verified causal claims.

A total of eleven significant aviation-related cyber and IT incidents were analysed, spanning the 2018–2025 period. Incident selection followed predefined inclusion criteria to enhance procedural transparency. Cases were incorporated into the dataset if they involved documented operational disruption affecting aviation IT or digital service infrastructure, were supported by official institutional reporting or credible post-incident documentation, included verifiable information regarding recovery duration, and demonstrated potential relevance for dual-use civilian–military aviation systems. Incidents lacking reliable documentation on operational scope or recovery timeframe were excluded from the comparative assessment.

Data collection was conducted through structured keyword searches in institutional databases and official publications using terms such as “aviation IT outage”, “airport ransomware”, “flight planning system failure” and “cybersecurity software update disruption”. Primary reliance was placed on institutional documentation issued by regulatory authorities and aviation agencies. Journalistic sources were used solely for contextual clarification and were not treated as primary evidentiary material.

Each incident was coded across three analytical dimensions forming the tri-axial model. The first dimension, Cyber Layer, categorises the documented technical origin of disruption, distinguishing among conventional software failures, malicious cyberattacks,

[2] European Union Agency for Cybersecurity.
[3] Federal Aviation Administration.
[4] International Civil Aviation Organization.
[5] NATO Cooperative Cyber Defence Centre of Excellence.
[6] National Institute of Standards and Technology.

security software malfunctions and cyber defence system malfunctions. Classification was based strictly on reported technical cause rather than inferred intent. The second dimension, Operational Reach, captures the geographic and organisational scope of impact and was assessed according to documented spread across local, sectoral, or global aviation systems. The third dimension, Recovery Time, reflects the duration required to restore operational functionality and was coded using consistent temporal thresholds based on documented restoration timelines.

Operationalisation of these variables followed uniform category definitions to ensure internal coherence across cases. Analytical interpretations are explicitly separated from empirical observations; documented incident characteristics constitute the evidentiary foundation, while resilience-related inferences are derived through structured comparison.

This study makes three distinct scholarly contributions to the fields of aviation cybersecurity and military logistics resilience. First, it conceptualises aviation-sector cyber and IT disruptions as dual-use systemic dependencies, demonstrating how failures originating in civilian commercial cybersecurity products can propagate into military logistics, mission planning and strategic air mobility systems. While prior studies have examined cyber threats or aviation disruptions separately, this paper analytically integrates these domains through a logistics-resilience perspective. Second, the study introduces a tri-axial analytical model, Cyber Layer – Operational Reach – Recovery Time, that enables structured comparison of heterogeneous cyber incidents across civilian and military aviation contexts. This model extends existing critical infrastructure resilience frameworks by explicitly linking technical failure modes (including non-malicious software errors) to operational and mission-level degradation. Third, through the case study of the 2024 CrowdStrike outage, the paper reframes endpoint cybersecurity software from a protective IT function into an operational dependency with doctrinal implications. The analysis demonstrates that cybersecurity mechanisms themselves can become systemic risk multipliers when deployed at scale without coordinated validation and resilience planning.

Cybersecurity challenges in civil and military airlift: A review of existing approaches and analytical gaps

The aviation sector has long been recognised as a critical infrastructure with increasing exposure to cyber risks due to its reliance on interconnected information and communication technologies. Existing literature and institutional analyses emphasise that aviation cybersecurity challenges extend beyond isolated technical vulnerabilities and involve systemic dependencies across airports, airlines, air navigation service providers, and supporting digital services.[7] Regulatory studies by ICAO, EASA[8] and ENISA primarily focus on threat identification, risk categorisation and compliance-based security management. While these works provide a comprehensive overview of threat

[7] Ukwandu et al. 2022; ENISA 2023.
[8] European Union Aviation Safety Agency.

landscapes and regulatory responses, they largely adopt a threat-centric perspective. Less attention is given to non-malicious failures originating from software updates, configuration errors, or internal system dependencies, despite their demonstrated operational impact on aviation continuity. A parallel body of literature addresses cyber resilience in complex socio-technical systems, emphasising concepts such as cascading failures, tight coupling and systemic vulnerability.[9] Resilience theory suggests that highly integrated systems may amplify disturbances, allowing localised technical failures to propagate across organisational and geographic boundaries. Studies on critical information infrastructure protection further argue that protective mechanisms themselves can become sources of disruption when improperly validated or centrally deployed.[10] These studies typically remain sector-agnostic or focus on energy, telecommunications, or industrial systems. Aviation-specific applications of cascading failure theory remain limited, and explicit links to military air mobility and logistics operations are rarely developed.

Military logistics literature increasingly recognises cyberspace as a critical enabler of operational readiness and strategic mobility. NATO doctrine and defence-focused analyses emphasise the shift from information assurance toward mission assurance, reflecting the understanding that digital systems underpin planning, coordination, and execution across domains.[11] Studies on defence supply chains highlight the growing dependence on civilian infrastructure and commercial software providers, particularly in airlift and transport operations. Despite this recognition, much of the military-focused literature treats cyber risk primarily as an external threat or intelligence problem. Civilian aviation systems and commercial cybersecurity products are often assumed to be reliable enablers rather than potential sources of systemic disruption. As a result, the operational implications of shared digital dependencies between civilian aviation and military logistics remain under-theorised, especially in the context of non-hostile cyber disruptions.

Taken together, existing literature provides substantial insight into aviation cybersecurity threats, resilience theory and military logistics assurance. However, these bodies of work largely remain analytically siloed. Aviation cybersecurity studies rarely extend their analysis into military logistics implications, while defence logistics literature seldom incorporates civilian cybersecurity failures as systemic risk factors. The present study addresses this gap by integrating these strands through a dual-use logistics resilience perspective. By analysing aviation cyber incidents – including non-malicious failures – across a multi-year dataset and applying a tri-axial analytical model, the study moves beyond narrative case description toward structured comparison. In doing so, it positions cybersecurity software and digital service dependencies as operational variables rather than purely technical considerations.

[9] Nowakowski et al. 2015; Johnson 2013: 61–92.
[10] McCreight 2019.
[11] Bhargava 2024; Haig–Kovács 2012.

Airport IT and cybersecurity disruptions (2018–2025): Patterns of systemic failure

The resilience of critical aviation infrastructure is challenged by a heterogeneous set of risk vectors. Traditional scholarship categorises these into external physical threats – such as natural disasters, power grid blackouts and kinetic terrorist acts – and internal technical vulnerabilities. However, the increasing digitisation of dual-use logistics has shifted the primary risk profile toward ICT[12] infrastructure dependencies. Recent studies emphasise that the most frequent causes of IT outages in complex operating systems are not necessarily external attacks, but rather Software Errors and Software Aging.[13] Software aging – the cumulative degradation of system performance due to resource exhaustion and error buildup – significantly increases the probability of catastrophic failure in systems that require high availability, such as ATM[14] and military C2[15] networks.[16]

The transition from a technical failure to a mission-level disruption is driven by downtime.

In the context of aviation:

- Breadth of impact: Because operating system outages affect all dependent applications, a kernel-level failure (like the CrowdStrike BSOD[17]) effectively decapitates the entire operational stack.
- Economic consequences: Unanticipated outages in major aviation hubs result in considerable loss of economic activity. For dual-use infrastructures, this translates into a loss of Mission Assurance, where the inability to process flight plans or ground handling data halts the movement of strategic assets.

Between 2018 and 2025, eleven major aviation-related cyber incidents were identified and analysed (Table 1). The incidents span a range of geographic locations, threat vectors and technical origins, including conventional software failures, ransomware attacks, security software malfunctions, and defence-related cyber system errors. While several incidents originated in localised operational contexts, others produced sector-wide or global effects, underscoring the increasing interconnectedness of aviation digital infrastructure. The dataset confirms that aviation operates as a tightly coupled "system of systems", where failures at the IT or cybersecurity layer can propagate rapidly into operational disruption. Importantly, the dataset includes both malicious incidents (e.g. ransomware attacks) and non-malicious failures (e.g. faulty software updates), allowing comparative assessment of their respective operational impacts. This distinction is central to the analytical framework applied in this study.

[12] Information and Communication Technologies.
[13] Bovenzi et al. 2013.
[14] Air Traffic Management.
[15] Command-and-Control.
[16] Dos Santos – Matias 2017; Dos Santos et al. 2018; Noë et al. 2021.
[17] Blue screen of death: It is used to indicate a system crash, in which the operating system reaches a critical condition where it can no longer operate safely.

As shown in Figure 1, data-related threats and ransomware dominate the aviation cyber threat landscape, accounting together for over two-thirds of reported incidents. An examination of cybersecurity issues in the aviation sector in 2022 revealed that 71% of cybercriminals aimed to obtain login credentials to infiltrate IT systems. Out of those attacks, 25% were DDoS[18] incidents, while 4% of cybercriminals intended to compromise file integrity.[19] The transportation industry has witnessed an increase in cybersecurity incidents in the last seven years. Aviation, referred to as a "system of systems", consists of numerous technologies, individuals and procedures, making the supply chain vulnerable to risks. In 2025, a series of assaults targeted major U.S. and EU airlines in the aviation sector. The escalation of cyber threats against aviation infrastructure is a documented trend, with institutional reports indicating a consistent increase in incident frequency since 2019. Nevertheless, security experts cautioned that the issue will only become more severe. The operational stress placed on legacy aviation IT infrastructure has exposed latent vulnerabilities in high-demand environments. "Even in the absence of a cyberattack, antiquated technologies and vulnerable logistics can result in significant disruptions", said Jiwon Ma, senior policy analyst at FDD's[20] Center on Cyber and Policy Innovation.[21]

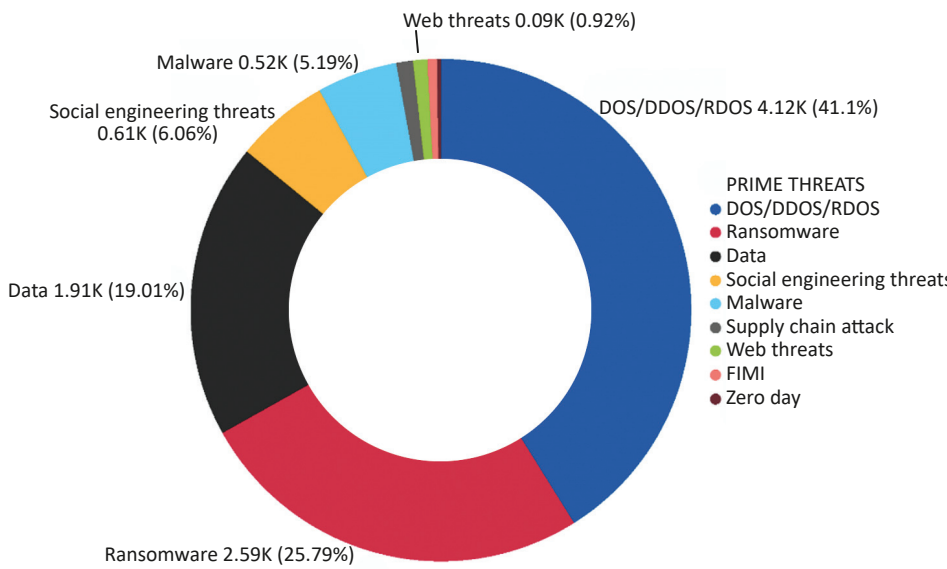

Figure 1: Distribution of incident by threats types (2023–2024)
Source: ENISA 2024

[18] Distributed Denial-of-Service attack is a cyberattack that overwhelms a targeted server, website, or network with a flood of malicious internet traffic from multiple compromised systems (a botnet) to disrupt normal service, making it unavailable for legitimate users.
[19] Thales 2025.
[20] Foundation for Defense of Democracies (FDD) publishes research on foreign policy and security issues, focusing on subjects such as nuclear non-proliferation, cyber threats, sanctions, illicit finance.
[21] Traynor 2025.

To illustrate the operational relevance of aviation cybersecurity disruptions, it is useful to examine a selection of documented incidents from recent years. Table 1 summarises major cyber and IT-related events affecting airports, air navigation services, and aviation-supporting digital infrastructure between 2018 and 2025. The selected cases demonstrate varying combinations of technical origin, operational reach and recovery duration, and several exhibit direct relevance for global aviation continuity and military air-mobility operations.

Table 1: Documented airport and aviation cyber incidents (2018–2025)

Year	Location	Incident description	Cyber layer	Recovery time	Operational reach
2018	Bristol (U.K.)	Ransomware attack	Cyberattack[22]	Prolonged	Sectoral
2019	Atlanta (USA)	CBP system failure	Software Failure[23]	Short	Local
2019	Heathrow & Gatwick (U.K.)	Windows update crash	Software Failure[24]	Short	Sectoral
2020	San Francisco (SFO)	Maze ransomware	Cyberattack[25]	Prolonged	Sectoral
2021	Global (Microsoft/Akamai)	Defender update (BSOD)	Security software error[26]	Medium	Global
2022	Jeppesen/Mil-Planner	Ransomware attack	Cyberattack[27]	Prolonged	Global
2023	FAA (USA)	Database corruption (NOTAM[28] failure)	Software failure[29]	Medium	Sectoral
2024	NATS (U.K.)	Flight parser failure	Software failure[30]	Medium	Sectoral
2024	Copenhagen (Denmark)	ESET update disruption	Security software error[31]	Medium	Sectoral
2024	Global (CrowdStrike Falcon)	Kernel driver crash (BSOD)	Cyber defence software error[32]	Prolonged	Sectoral
2025	Frankfurt (Germany)	Ransomware attack	Cyberattack[33]	Prolonged	Global

Source: compiled by the author

[22] Zanni 2018.
[23] Rockwell 2019.
[24] Jolly 2019.
[25] Cyble 2020.
[26] Sundaram 2021.
[27] Hunorfi et al. 2024: 101–120.
[28] Notice to Airmen is a notice containing information concerning the establishment, condition or change in any aeronautical facility, service, procedure or hazard, the timely knowledge of which is essential to personnel concerned with flight operations.
[29] Nolen 2023.
[30] Halliwell et al. 2024.
[31] Barrett 2024.
[32] CrowdStrike 2024.
[33] Paganini 2025.

A tri-axial model for assessing aviation cyber disruptions

To move beyond descriptive incident reporting, each disruption was analysed using the proposed tri-axial model, which links three analytical dimensions: cyber layer, operational reach, recovery time.

Cyber layer categorises the technical origin of the disruption as: software failure, cyberattack, security software malfunction, or cyber defence system malfunction. Operational reach captures the spatial and organisational scope of impact, classified as local, sectoral, or global. Recovery time reflects the duration required to restore operational functionality, categorised as short-term (hours), medium-term (days), or prolonged (weeks or longer).

Applying this model reveals clear structural patterns. Conventional software failures – such as the 2019 CBP[34] system outage in Atlanta – tended to remain locally contained and were resolved within short recovery periods. By contrast, ransomware incidents exhibited broader operational reach and longer recovery times due to system restoration requirements and forensic processes. Most notably, incidents originating in the security and defence software layer consistently demonstrated the widest operational reach. The 2022 Jeppesen/MilPlanner disruption and the 2024 CrowdStrike Falcon outage both propagated across national and alliance-level aviation systems, despite differing in intent and technical trigger. This finding indicates that centralised cybersecurity tools represent a distinct category of systemic risk within aviation and military logistics ecosystems.

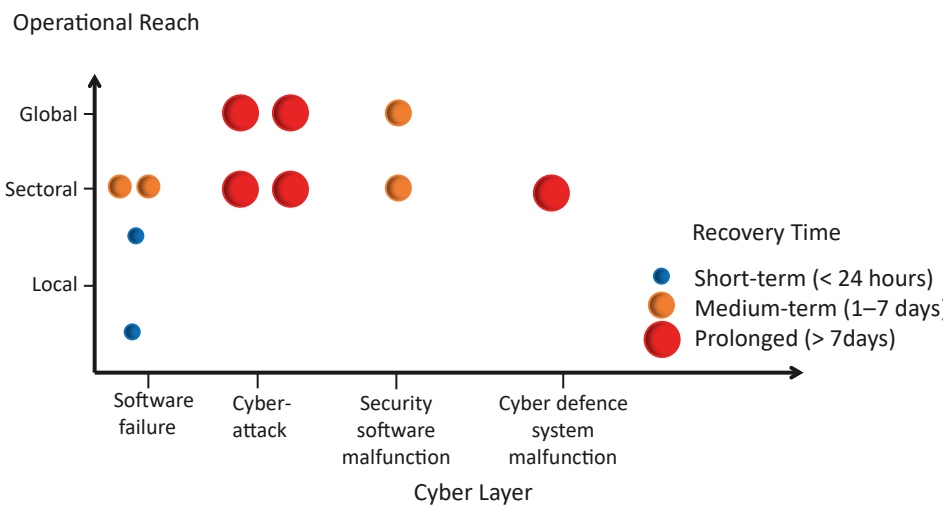

Figure 2: Tri-axial model for assessing aviation cyber disruptions

Source: compiled by the author based on incident data collected from ENISA, FAA, ICAO, and publicly available post-incident reports (2018–2025)

[34] Customs and Border Protection: Protecting the American people, safeguarding our borders and enhancing the nation's economic prosperity.

Figure 2 visualises three analytical dimensions: cyber layer (x-axis), operational reach (y-axis) and recovery time (encoded by marker size). Recovery time categories are defined as short-term (< 24 hours), medium-term (1–7 days) and prolonged (> 7 days). The cyber layer axis is ordered according to increasing systemic coupling, from conventional software failures to centrally deployed cyber defence systems. The model illustrates those incidents originating in higher-order cyber layers that tend to combine wider operational reach with longer recovery periods, even in the absence of malicious intent. When mapped across the tri-axial dimensions, the incidents cluster into three analytically relevant patterns. First, localised software failures are frequent but operationally manageable. Although such failures can cause immediate delays and economic losses, their limited propagation potential and relatively rapid recovery reduce their strategic significance. Second, malicious cyberattacks, particularly ransomware, produce asymmetric operational effects. While not always global in reach, these incidents often result in prolonged recovery times and secondary impacts such as data exfiltration, regulatory exposure and reputational damage. Their relevance to military logistics lies primarily in contingency planning and redundancy rather than systemic interdependence. Third, and most critical, non-malicious failures in cybersecurity and defence software exhibit high-impact, low-frequency characteristics. These events combine global operational reach with prolonged recovery potential, despite originating from trusted and widely deployed systems. The model demonstrates that such failures bypass traditional threat-centric risk models, as their effects stem from architectural centralisation and automated propagation mechanisms rather than adversarial action. This pattern supports resilience theory arguments that tightly coupled systems are vulnerable to cascading "safe-mode" failures, where protective mechanisms inadvertently trigger operational paralysis.

The CrowdStrike 2024 outage was selected for in-depth case analysis due to its global reach, non-malicious origin, and direct relevance to both civilian aviation and military logistics systems. The case serves as an analytical stress test for the proposed model rather than as a representative incident.

Case study: The 2024 CrowdStrike outage as a systemic cyber failure

The CrowdStrike Falcon, recognised as a NGAV[35] cybersecurity platform, can aid different sectors. In contrast to traditional antivirus solutions that mainly depend on signature-based detection (recognising known malware by matching files with a signature database), NGAV utilises sophisticated technologies to deliver broader and more proactive security. Conventional antivirus systems have transformed into contemporary versions like Endpoint Detection & Response.[36] Through monitoring the actions of a programme (e.g. trying to reach sensitive files or execute unauthorised modifications), NGAV can detect possible threats by analysing behaviour patterns instead of depending only on recognised malware signatures. NGAV systems utilise

[35] Next Generation Antivirus.
[36] Basit Ajmal et al. 2022.

machine learning algorithms to identify patterns and irregularities in data. These algorithms draw from past and evolving threats, enhancing their capacity to detect new and unfamiliar malware. AI-powered NGAV can foresee and thwart attacks by examining extensive datasets and identifying possible vulnerabilities or attack vectors prior to their exploitation. NGAV typically incorporates EDR[37] features, enabling the identification, examination and reaction to security incidents on endpoints. EDR tools offer comprehensive insight into endpoint actions and allow quick reactions to possible threats. EDR capabilities assist in grasping the characteristics of an attack, its propagation, and the measures implemented, thereby helping to reduce future risks and enhance security posture.[38]

The 2024 CrowdStrike incident represents a high-impact systemic failure within globally distributed digital supply chains. Triggered by a faulty Falcon sensor update, the event caused over 8.5 million Windows-based systems to crash globally within hours.[39] The technical failure resulted in an immediate 11% reduction in the company's market capitalisation.[40] The effects of the global tech outage on Friday, 19 July 2024, persisted into Saturday, with employees from airlines, banks, hospitals, and other vital sectors focused on remediating operational backlogs resulting from the systemic disruption of Windows-based endpoint devices.[41] Numerous industries were affected by the tech failure, but none contain the public data found in the aviation industry. The kernel driver update, intended to enhance EDR capabilities, contained an invalid memory reference that caused immediate system crashes (BSOD) upon boot. The incident disrupted airline check-in systems, ground operations, logistics, and Service Desk platforms across major airports including Heathrow, Frankfurt, Sydney and Atlanta. Among those affected were Jeppesen's flight planning systems – integral to various military transport operations. This demonstrated the critical interdependence between civilian cybersecurity software vendors and defence operational continuity. According to ENISA's 2024 review, the outage temporarily degraded situational awareness in several European transport command centres. While the incident was not the result of a cyberattack, its systemic effects mirrored those of a coordinated disruption, revealing that resilience gaps persist even in peacetime. This reinforces the argument that digital supply chain assurance must become a core pillar of NATO's logistics doctrine.

Within the dataset, the 2024 CrowdStrike outage represents an extreme but analytically revealing case. Classified under the tri-axial model as a cyber defence system malfunction with global operational reach and medium-to-prolonged recovery time, the incident illustrates how endpoint security software has become embedded in the operational fabric of aviation and military logistics. Unlike ransomware incidents, the CrowdStrike disruption did not involve data compromise or hostile intent. Nevertheless, its effects were comparable to a coordinated cyberattack, disrupting airline check-in systems, ground operations, Service Desk platforms, and flight-planning tools used in

[37] Endpoint Detection and Response.
[38] Pinheiro et al. 2019.
[39] Weston 2024.
[40] Coulter 2024.
[41] Rosman 2024.

both civilian and military contexts. The incident thus demonstrates that cybersecurity assurance failures can degrade mission assurance even in the absence of adversarial activity. From an analytical perspective, the CrowdStrike case validates the model's central claim: the cyber layer in which a failure originates is a stronger predictor of operational reach than the maliciousness of the event. This insight distinguishes the present analysis from narrative incident reporting and underscores the model's decision-support value for defence logistics planners.

Across the dataset, the tri-axial model enables systematic comparison of heterogeneous incidents and highlights a previously under-theorised risk category: centrally deployed defensive cyber dependencies. While aviation cybersecurity discourse often prioritises external threats, the results suggest that internal technological dependencies pose equal or greater risk to operational continuity. The analysis therefore reframes aviation cybersecurity from a threat-centric paradigm toward a dependency-centric resilience problem. For military air mobility, this implies that logistics resilience can no longer be assured solely through network hardening or threat detection. Instead, resilience must account for update governance, cross-domain testing, rollback capability, and the operational role of Service Desks as crisis management nodes.

The 2024 CrowdStrike incident serves as a pivotal reminder that cybersecurity tools themselves can be potential vectors of disruption. Future strategies should include rigorous sandbox testing, redundant Service Desk failover procedures, and internationally standardised incident response protocols aligned with ICAO Annex 19 and ISO/IEC 27035. Three strategic insights emerge from this assessment. First, civilian infrastructure and military logistics share a growing digital dependency that erodes traditional redundancy. Second, commercial cybersecurity products – though essential – introduce systemic risks when deployed without coordinated validation protocols across the systems. Third, information-sharing and pre-emptive sandbox testing between civilian IT vendors and defence agencies should be institutionalised under NATO and EU frameworks.

These findings align with RAND's (2023) and NIST's (2025) emphasis on cross-domain resilience: the ability of logistics networks to absorb and recover from disruptions regardless of origin. They also support ICAO's emerging guidance on dual-use cyber risk management within aviation ecosystems.[42]

Conclusions

Rather than treating the 2024 CrowdStrike outage as an isolated technical failure, this study interprets it as a systemic stress test of dual-use aviation logistics. The findings demonstrate that cybersecurity assurance has become inseparable from operational and mission assurance in both civilian and military airlift ecosystems. This section draws on the case study material discussed above to address the research questions set out in the introduction section.

[42] Lucas et al. 2024.

RQ1 inquired about the lessons the CrowdStrike outage reveals about cybersecurity challenges in aviation and military operations. The analysis demonstrates that cyber risk in aviation logistics is increasingly systemic rather than threat-driven. The 2024 CrowdStrike incident shows that non-malicious failures in widely deployed cybersecurity software can produce effects comparable to deliberate cyberattacks, disrupting mission planning, Service Desk operations, and logistics coordination across civilian and military domains. The key lesson is that digital protection mechanisms have become operational dependencies. As a result, resilience planning must extend beyond perimeter defence and threat detection to include update validation, rollback capability and cross-domain impact assessment. The lessons drawn from the CrowdStrike and earlier MilPlanner[43] outages reveal that cyber risk in aviation logistics is systemic, not incidental. Both events exposed a fundamental fragility in global air mobility: the lack of cross-domain testing, centralised update validation, and real-time incident coordination between civil and defence operators.

RQ2 examined how aviation and military organisations adapted to increasing cybersecurity dependency. The findings indicate a gradual but incomplete shift from information assurance toward mission assurance. While aviation and defence organisations increasingly recognise cyberspace as an operational domain, governance structures and validation practices remain fragmented. The CrowdStrike case illustrates that current adaptation efforts focus primarily on external threats, leaving internal technological dependencies insufficiently managed. Effective adaptation therefore requires integrating cybersecurity assurance into logistics doctrine, redefining the role of IT Service Desks as operational nodes, and institutionalising civil–military coordination mechanisms at alliance level.

At a strategic level, the CrowdStrike outage also redefined how alliances like NATO and the EU perceive logistics resilience. It exposed that cyber vulnerabilities are not confined to attacks but may emerge from trusted internal systems. This challenges the conventional dichotomy between threat defence and operational continuity. Future frameworks must integrate cybersecurity assurance into logistics doctrine, emphasising layered validation, redundant infrastructure and shared situational intelligence. Regular joint cyber exercises between civilian aviation partners, software providers, and defence logistics units could transform reactive recovery into proactive deterrence.

In conclusion, the 2024 CrowdStrike incident serves as a critical empirical case requiring the integration of digital supply chain resilience into logistics doctrines. It showed that worldwide military and civilian movement relies on a delicate network of digital dependencies that go beyond jurisdictional and organisational limits. The future of logistics resilience will depend on how quickly institutions adapt to this new reality: where cybersecurity, service continuity and strategic logistics are inseparable. The path forward demands a paradigm shift – from technology-centric security to mission-centric cyber governance – ensuring that the next global disruption becomes an opportunity for foresight rather than a failure of preparation.

[43] Paráda–Tóth 2024: 167–182.

References

Barrett, Michael (2024): How has the Global IT Outage Affected Denmark? *The Local,* 19 July 2024. Online: www.thelocal.dk/20240719/how-is-global-it-outage-affecting-denmark#:~:text=Danish%20rail%20operator%20DSB's%20website%20is%20down,as%20the%20effects%20of%20the%20outage%20rippled

Basit Ajmal, Abdul – Khan, Shawal – Jabeen, Farhana (2022): Defeating Modern Day Anti-Viruses for Defense Evaluation. *2022 International Conference on Frontiers of Information Technology,* 255–260. Online: https://doi.org/10.1109/FIT57066.2022.00054

Bhargava, Amit Kumar (2024): Cybersecurity in Aerospace: A Military Perspective. *Blue Yonder,* 1(1). Online: https://journals.capsindia.org/index.php/byj/article/view/48/47

Bovenzi, Antonio – Lopez, Javier Alonso – Yamada, Hiroshi – Russo, Stefano – Trivedi, Kishor S. (2013): Towards Fast OS Rejuvenation: An Experimental Evaluation of Fast OS Reboot Techniques. *2013 IEEE 24th International Symposium on Software Reliability Engineering,* 61–70. Online: https://doi.org/10.1109/ISSRE.2013.6698905

Coulter, Martin (2024): CrowdStrike Chaos Could Prompt Rethink among Investors, Customers. *Reuters,* 20 July 2024. Online: www.reuters.com/technology/cybersecurity/crowdstrike-chaos-could-prompt-rethink-among-investors-customers-2024-07-19/

CrowdStrike (2024): Preliminary Post Incident Review (PIR): Content Configuration Update Impacting the Falcon Sensor and the Windows Operating System (BSOD). *CrowdStrike,* 24 July 2024. Online: www.crowdstrike.com/en-us/blog/falcon-content-update-preliminary-post-incident-report/

Cyble (2020): SFO Struck by a Web Compromise. *Cyber News,* 13 April 2020. Online: https://cyble.com/blog/sfo-struck-by-a-web-compromise/

Dos Santos, Caio A. R. – Matias, Rivalino Jr. (2017): An Empirical Study on Patterns of Failure Causes in a Mass-market Operating System. *Proceedings of the ACM Symposium on Applied Computing,* 1542–1547. Online: https://doi.org/10.1145/3019612.3019740

Dos Santos, Caio A. R. – Prince, Marcela A. – Matias, Rivalino Jr. – Fonseca Maciel, Vinicius (2018): Reliability Assessment of Commercial Off-the-shelf Operating System Software: An Empirical Study. *Brazilian Symposium on Computing Systems Engineering,* 201–206. Online: https://doi.org/10.1109/SBESC.2018.00038

ENISA (2023): *ENISA Threat Landscape 2021–2022.* Online: https://doi.org/10.2824/553997

ENISA (2024): *ENISA Threat Landscape 2024.* Online: https://doi.org/10.2824/0710888

Federal Aviation Administration (FAA) (2024): *After Action Report on January 2023 Notice to Air Missions Database Failure.* Online: www.governmentattic.org/55docs/FAAaarJan2023NTAMdbfail2023.pdf

Haig, Zsolt – Kovács, László (2012): *Kritikus infrastruktúrák és kritikus információs infrastruktúrák* [Critical Infrastructures and Critical Information Infrastructures]. Budapest: Nemzeti Közszolgálati Egyetem. Online: https://hhk.uni-nke.hu/document/hhk-uni-nke-hu/kovasz-tanulmany.pdf

Halliwell, Jeff – Chambers, Sarah – Cropper, Phil – Foulsham, Mark (2024): *Independent Review of NATS (En Route) Plc's Flight Planning System Failure on 28 August 2023.* Online: www.caa.co.uk/publication/download/23337

Hunorfi, Péter – Paráda, István – Farkas, Tibor (2024): Kiberbiztonsági kihívások a légi közlekedésben – Kronológiai folyamat a Boeing elleni kibertámadások tükrében [Cybersecurity Issues in Aviation – Timeline of Cyber Crimes against Boeing]. *Hadmérnök,* 19(1), 101–120. Online: https://doi.org/10.32567/hm.2024.1.6

ICAO (2025): *Doc 10213 — Unrestricted. Global Cyber Risk Considerations.* Online: www.icao.int/sites/default/files/sp-files/aviationcybersecurity/Documents/Doc-10213-Unedited-Global-Cyber-Risk-Considerations.EN_.pdf

Johnson, Chris W. (2013): Lessons from Major Incidents Influencing and Influenced by Telecoms Failures. In Théron, Paul – Bologna, Sandro (eds.): *Critical Information Infrastructure Protection and Resilience in the ICT Sector.* Hershey: IGI Global, 61–92. Online: https://doi.org/10.4018/978-1-4666-2964-6.ch004

Jolly, Jasper (2019): Passenger Anger as Tens of Thousands Hit by BA Systems Failure. *The Guardian,* 7 August 2019. Online: www.theguardian.com/business/2019/aug/07/british-airways-it-glitch-causes-disruption-for-passengers-delays

Lucas, Rebecca – Ekström, Thomas – Fusaro, Paola – Hastings Roer, Elizabeth – Retter, Lucia (2024): *Toward Defense Supply Chain Disruption Management. A Research Agenda for Defense Supply Chain Resilience*. RAND Research Report. Online: www.rand.org/content/dam/rand/pubs/research_reports/RRA2500/RRA2504-1/RAND_RRA2504-1.pdf

McCreight, Robert (2019): Grid Collapse Security, Stability and Vulnerability Issues: Impactful Issues Affecting Nuclear Power Plants, Chemical Plants and Natural Gas Supply Systems. *Journal of Homeland Security and Emergency Management,* 16(1). Online: https://doi.org/10.1515/jhsem-2018-0021

Noë, Nyala – Tuzovic, Emina – McArthur, Frederik S. – Thompson Carroll, Angus (2021): Improving Loss Prevention in High Hazard Industries Through the Evaluation of Safety Culture and Error Traps from Structured and Unstructured Data Using Machine Learning. *Institution of Chemical Engineers Symposium Series,* (168). Online: www.icheme.org/media/27736/hazards-31-paper-40-noe.pdf

Nolen, Billy (2023): *The Federal Aviation Administration's NOTAM System Failure and its Impacts on a Resilient National Airspace.* Statement of Billy Nolen, Acting Administrator Federal Aviation Administration Hearing before the United States Senate Committee on Commerce, Science, and Transportation Notice to Air Missions System, February 15, 2023. Online: www.transportation.gov/federal-aviation-administrations-notam-system-failure-and-its-impacts-resilient-national-airspace

Nowakowski, Tomasz – Młyńczak, Marek – Jodejko-Pietruczuk, Anna – Werbińska-Wojciechowska, Sylwia eds. (2015): *Safety and Reliability. Methodology and Applications.* Boca Raton: CRC Press. Online: https://doi.org/10.1201/b17399

Paganini, Pierluigi (2025): Safepay Ransomware Group Claims the Hack of Professional Video Surveillance Provider Xortec. *Security Affairs,* 26 October 2025. Online: https://securityaffairs.com/183868/malware/safepay-ransomware-group-claims-the-hack-of-professional-video-surveillance-provider-xortec.html

Paráda, István – Tóth, András (2024): A NATO katonai légi szállítási képességek kibervédelmi aspektusai [Cybersecurity Challenges for NATO Military Air Transport Operations]. *Hadmérnök,* 19(4), 167–182. Online: https://doi.org/10.32567/hm.2024.4.12

Pinheiro, Ricardo – Lima, Sidney – Fernandes, Sergio – Silva, Sthéfano H. M. T. (2019): Next Generation Antivirus Applied to Jar Malware Detection Based on Runtime Behaviors Using Neural Networks. *2019 IEEE 23rd International Conference on Computer Supported Cooperative Work in Design,* 28–32. Online: https://doi.org/10.1109/CSCWD.2019.8791864

Rockwell, Mark (2019): Software Bug Caused CBP Airport System Outage. *FCW,* 19 August 2019. Online: www.nextgov.com/modernization/2019/08/software-bug-caused-cbp-airport-system-outage/210982/

Rosman, Rebecca (2024): Disruptions Continue after an IT Outage Affects Millions around the Globe. *NPR,* 20 July 2024. Online: www.npr.org/2024/07/20/g-s1-12487/crowdstrike-microsoft-outage-update

Sundaram, Mani (2021): Akamai Summarizes Service Disruption. *Akamai,* 22 July 2021. Online: www.akamai.com/blog/news/akamai-summarizes-service-disruption-resolved

Thales (2025): *Aviation Sector Sees 600% Year-on-year Increase in Cyberattacks.* Online: www.thalesgroup.com/en/news-centre/press-releases/aviation-sector-sees-600-year-year-increase-cyberattacks

Traynor, Orlaith (2025): *The Global Impact of Aviation Cyberattacks.* Online: https://cybelangel.com/blog/the-global-impact-of-aviation-cyberattacks/

Ukwandu, Elochukwu – Ben-Farah, Mohamed A. – Hindy, Hanan – Bures, Miroslav – Atkinson, Robert – Tachtatzis, Christos – Andonovic, Ivan – Bellekens, Xavier (2022): Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends. *Information,* 13(3). Online: https://doi.org/10.3390/info13030146

Weston, David (2024): Helping our Customers through the CrowdStrike Outage. *Official Microsoft Blog,* 20 July 2024. Online: https://blogs.microsoft.com/blog/2024/07/20/helping-our-customers-through-the-crowdstrike-outage/

Zanni, John (2018): Ransomware Attack against Bristol Airport Shows Need for Smart, Secure Digital Infrastructure in Transportation. *Acronis,* 19 September 2018. Online: www.acronis.com/en/blog/posts/ransomware-attack-against-bristol-airport-shows-need-smart-secure-digital-infrastructure/