István Paráda[1], István Bodnár[2]

CYBERSECURITY CHALLENGES AND DEFENCE STRATEGIES IN MILITARY AIR LOGISTICS: PERSPECTIVES ON NATO AIRLIFT CAPABILITIES

KIBERBIZTONSÁGI KIHÍVÁSOK ÉS VÉDELMI STRATÉGIÁK A KATONAI LÉGI LOGISZTIKÁBAN: NÉZŐPONTOK A NATO LÉGI SZÁLLÍTÁSI KÉPESSÉGEIRŐL

HTTPS://DOI.ORG/10.30583/2025-3-4-163

Abs*tract*

The growing digitalization of military air logistics operations has created unparalleled opportunities for efficiency, interoperability, and mission readiness across NATO airlift capabilities. Nonetheless, it has also widened the attack opportunities for cyberattacks targeting essential aviation infrastructure and logistics systems. This study analyzes cybersecurity issues associated with NATO's airlift missions and examines how cyber weaknesses in mission planning, communication systems, and logistics platforms can directly affect operational continuity. By analyzing NATO doctrines alongside the ENISA Threat Landscape 2025 report, the research emphasizes the emerging cybercrime strategies, supply-chain vulnerabilities, and data tampering in the air transport sector. The results indicate that cyber resilience has transitioned from a secondary IT issue to an essential logistics security function, crucial for maintaining NATO's mobility and quick-response capability. The document outlines a comprehensive cybersecurity defence framework that emphasizes risk assessment, secure network design, access management, incident response, supply

[1] PARÁDA, István PhD, NATO Support and Procurement Agency (NSPA). ORCID: https://orcid.org/0000-0002-3083-6015

[2] BODNÁR, István OF-2, National University of Public Service, Doctoral School of Military Engineering, Rheinmetall telecommunication engineer. ORCID: https://orcid.org/0000-0002-4761-1322

chain reliability, and ongoing staff training. Incorporating ENISA cyber threat intelligence into NATO's mission security framework underscores that the future success of military air logistics relies on the Alliance's capacity to uphold a secure, flexible, and resilient digital environment that can withstand evolving cyber threats.

Keywords: Cybersecurity, NATO Airlift, Military Logistics, ENISA, Mission Assurance, Cyber Resilience,

Absztrakt

A katonai légi logisztikai műveletek növekvő digitalizációja páratlan lehetőségeket teremtett a hatékonyság, az interoperabilitás és a missziós felkészültség terén a NATO légi szállítási képességeiben. Mindazonáltal kiszélesítette a támadási felületet a létfontosságú légi közlekedési infrastruktúrákat és logisztikai rendszereket célzó kiberkockázatok számára. Ez a publikáció elemzi a NATO légi szállítási küldetéseihez kapcsolódó kiberbiztonsági kérdéseket, és azt vizsgálja, hogy a missziótervezés, a kommunikációs rendszerek és a logisztikai platformok kiberbiztonsági gyengeségei hogyan befolyásolhatják közvetlenül a működési folytonosságot. A NATO-doktrínák és az ENISA 2025-ös kockázati jelentés együttes elemzésével a kutatás hangsúlyozza a kiberbűnözési stratégiák, az ellátási lánc sebezhetőségeinek és az adatmanipuláció összeolvadását a légi közlekedési ágazatban. Az eredmények azt mutatják, hogy a kiberbiztonsági ellenálló képesség a másodlagos informatikai kérdésből alapvető logisztikai biztosítási funkcióvá vált, amely kulcsfontosságú a NATO mobilitásának és gyors reagálási képességének fenntartásához. A dokumentum egy átfogó kiberbiztonsági védelmi struktúrát javasol, amely kiemeli a kockázatértékelést, a biztonságos hálózattervezést, a hozzáférés-kezelést, az incidenskezelést, az ellátási lánc megbízhatóságát és a folyamatos személyzeti képzést. Az ENISA kiberfenyegetésekkel kapcsolatos hírszerzési adatainak beépítése a NATO küldetésbiztosítási keretrendszerébe rávilágít arra, hogy a katonai légi logisztika jövőbeli sikere a Szövetség azon képességétől függ, hogy fenntartson egy biztonságos, rugalmas és ellenálló digitális környezetet, amely képes elviselni a változó kiberfenyegetéseket.

Kulcsszavak: kiberbiztonság, NATO légi szállítás, katonai logisztika, ENISA, küldetésbiztosítás, kiberbiztonsági ellenálló képesség,

I. Introduction

Today, both civil and military aviation rely heavily on highly digitalized avionics systems, real-time communication networks, and integrated mission-planning platforms. As technology becomes increasingly embedded in every phase of air operations, it has become imperative for both industry and military actors - particularly NATO - to treat cybersecurity not merely as a technical issue, but as a critical enabler of logistical readiness and mission continuity. The growing reliance on interconnected digital systems introduces new vulnerabilities that can directly affect the efficiency and operational security of air logistics. Cyber incidents can disrupt mission planning, flight routing, cargo allocation, and maintenance coordination - core elements of military air logistics that underpin NATO's strategic airlift capability. Therefore, understanding the cybersecurity landscape of air logistics is not only a technical necessity but also a strategic imperative for safeguarding operational resilience. The European Union Agency for Cybersecurity (ENISA) 2025 assessment underscores that the digitalization of transport systems - including military aviation logistics - has transformed the sector into a high-value cyber target, requiring mission-level resilience strategies across NATO operations.

This paper examines the relationship among military air logistics, NATO's airlift capabilities, and associated cybersecurity challenges, including the BOEING LockBit incident and the CrowdStrike incidents.[3] By analyzing potential vulnerabilities, assessing their operational impacts, and proposing mitigation strategies, the study highlights how cyber defence has become integral to maintaining uninterrupted air transport operations and sustaining mission assurance.

Two core hypotheses can be formulated:

1. Proactive cybersecurity risk management within Military Air Logistics and NATO Airlift Capabilities - including systematic vulnerability assessments and incident response planning – is an essential element to reduce the damage caused by cyberattacks and to sustain continuous air transport operations.

[3] Rosman, R. (2024).

2. The increasing integration and digitization of aviation systems expose air logistics operations to significant cyber threats. Addressing these challenges requires implementing advanced cybersecurity protocols, protecting IT and OT infrastructures, and providing continuous personnel training to ensure system resilience and mission safety.

This study employs a qualitative research methodology based on literature review, doctrinal analysis, and comparative threat assessment. The research draws on official NATO publications, cyber defence policies, and operational documents related to the Strategic Airlift Capability (SAC) and the Multinational Multi-Role Tanker Transport Fleet (MMF). Additionally, the analysis incorporates sector-specific threat intelligence from the ENISA Threat Landscape 2025, with particular emphasis on Sections 5.2 (Transport) and 6 (Cybercrime), to contextualize civilian–military interdependencies and evolving cyber risks in the aviation domain. The doctrinal analysis evaluates NATO's shift from information security to mission protection, examining how this paradigm influences cyber defence requirements in air logistics operations. The study further summarizes insights from academic and technical literature on aviation cybersecurity, air mobility operations, and supply-chain vulnerabilities. To enhance analytical expediency, the author developed a simplified cyber risk assessment model that integrates ENISA threat categories with NATO airlift operational dependencies. This model supports the identification of high-impact vulnerabilities and provides a structured framework for assessing cyber risks affecting military air logistics. The methodical approach does not aim to produce empirical measurements but rather to deliver a conceptual and doctrinally grounded assessment, suitable for informing strategic decision-making and future operational planning within NATO's air mobility ecosystem.

II. Incorporation of ENISA Threat Landscape Insights

Recent analyses by ENISA reinforce the urgency of developing robust cyber defence frameworks for military and dual-use transport systems. The ENISA Threat Landscape 2025 report identifies the transport sector as one of the most rapidly evolving targets of cyberattacks, driven by the growing convergence of IT, operational technology (OT), and cloud-based logistics infrastructures.[4] To implement

[4] ENISA (2025).

the ENISA findings within the context of NATO military airlift operations, this article applies a structured analytical framework that includes (1) vulnerability grouping and (2) impact assessment. First, the ENISA Threat Landscape 2025 dataset is categorized into thematic vulnerability groups relevant to aviation -such as ransomware and data extortion, supply-chain compromise, GNSS/GPS interference, and disruption of communication networks. Secondly, each vulnerability group is evaluated through a qualitative impact assessment that considers its potential impact on data integrity, system availability, and mission security in airlift operations.

According to ENISA, aviation and air transport networks are particularly vulnerable to:

- Ransomware and data theft campaigns targeting mission-critical scheduling and maintenance systems.
- Supply chain compromises in which malicious code or counterfeit components infiltrate avionics and ground systems.
- Disruption attacks (including Distributed Denial of Service, DDoS), aimed at operational coordination centers.
- Credential theft and phishing, exploiting personnel access in multinational logistics networks.

These patterns directly mirror the vulnerabilities observed in NATO's military airlift architecture, which increasingly depends on shared digital environments such as the Strategic Airlift Capability (SAC) and Multinational MRTT Fleet. The report emphasizes that data integrity, availability, and confidentiality are the most critical assets for the transport domain, aligning with NATO's emphasis on mission security over traditional information safety. Furthermore, ENISA's Section 6, "Cybercrime", highlights that organized cybercriminal groups are now acting as service providers, offering malware-as-a-service and data-extortion toolkits to state or non-state actors. This commercialized cybercrime ecosystem significantly lowers the barrier for sophisticated attacks on aviation logistics systems. It requires that NATO's logistics and support operations must adopt continuous threat intelligence and adaptive defence capabilities to counter both strategic and opportunistic intrusions.

Recorded incidents in the EU transport sector accounted for 7.5% of total incidents across all industries. It is noteworthy that 12% of the significant incidents reported under the NIS directive in 2024 occurred

in the transport sector.[5] Incidents affecting the transport sector in the EU are predominantly in air transport (58.4%), followed by logistics (20.8%). It is noteworthy that logistics encompasses organizations engaged in air, water, road, and rail transportation.

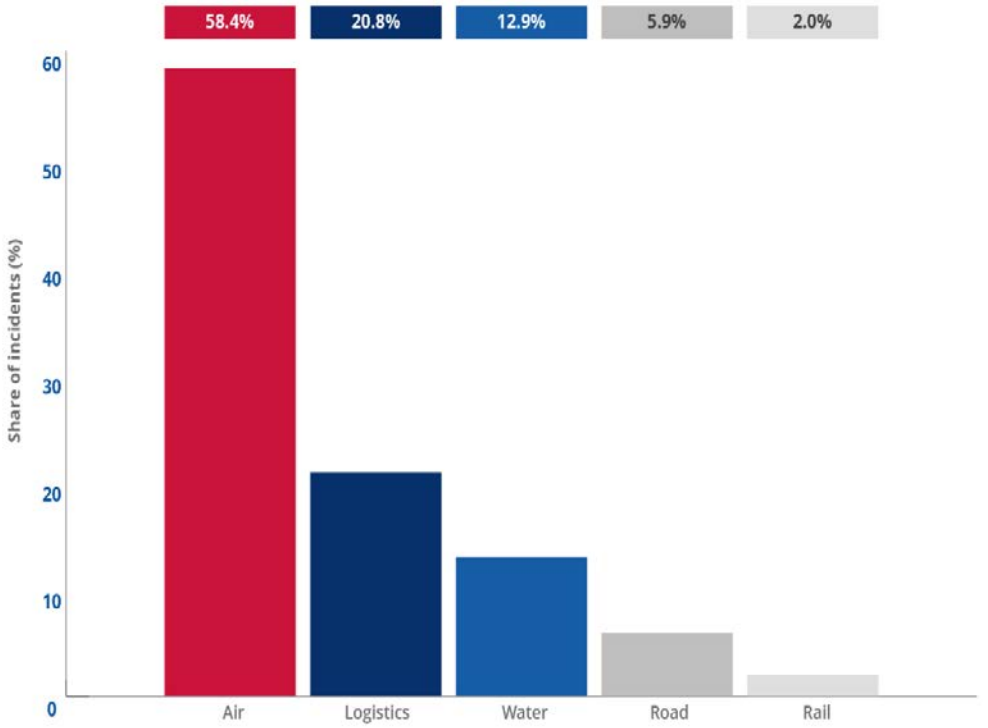

Figure 1. Distribution of incidents against the EU transport sector.

Source: ENISA: Threat Landscape 2025: Transport Sector and Cybercrime. European Union Agency for Cybersecurity, 2025. https://www.enisa.europa.eu/topics/threats

As shown in Figure 1, the EA transport sector was heavily affected by incidents, with most cyberattacks targeting air transport. Also, they were affected by hacktivist-led DDoS attacks (87.6%); the most active hacktivist groups against this sector included NoName057 (16) (36.4%), DarkStorm Team (15.4%), and Mysterious Team Bangladesh (6.2%).

As mentioned previously, increased activity was focused on specific EU national-level events and/or supra-national-level events. The increased activity is notably illustrated by NoName057 (16), with explicit announcements by Czechia, Latvia, and Poland regarding new bilateral security agreements with Ukraine as triggers for targeting transport

[5] ENISA (2024).

entities in these EU MSs.[6] In December 2024, Italy's Malpensa and Linate airport portals were briefly unreachable in attacks later claimed by NoName057[7], likely in the context of Italy's government decree authorizing the transfer of means, materials, and equipment to Ukraine. Cybercrime incidents against the transport sector accounted for 8.4% of all incidents, with ransomware accounting for 83.9% and data breaches accounting for 16.1%.

The insights of the ENISA Threat Landscape 2025 highlight that the transport and aviation sectors are increasingly exposed to systemic cyber threats, such as ransomware, GPS/GNSS interference, supply-chain compromise, and disruption attacks on communication infrastructure. These vulnerabilities directly impact NATO's airlift operations, which rely on shared civilian–military networks, centralized planning systems, and multinational digital coordination platforms. While ENISA provides a macro-level overview of sectoral cyber risks, NATO's Strategic Airlift Capability (SAC) and the Multinational MRTT Fleet (MMF) represent operational-level manifestations of these challenges. The integration of IT, OT, and platform-specific systems within these programs illustrates how strategic airlift readiness is continuously shaped by the broader European threat environment described by ENISA. Thus, the ENISA assessment provides the external threat context, while the NATO airlift architecture represents the operational environment where these threats materialize. This linkage serves as the foundation for the following analysis.

III. NATO Airlift Capabilities[8]

"Effective strategic airlift capabilities are vital to ensure that NATO Allies and partners can rapidly deploy forces and equipment wherever required."[9] This principle underpins NATO's cooperative air logistics model, in which nations pool resources to maximize efficiency, interoperability, and cost-effectiveness. However, as these multinational systems become increasingly digitalized, the associated cybersecurity challenges directly affect logistical resilience and mission continuity.

[6] EUROPOL (2025).
[7] G.Piovaccari, J. Merriman (2024).
[8] Paráda István, Tóth András (2024).
[9] North Atlantic Treaty Organization (2024).

1. Strategic Airlift Capability (SAC)

The initiative, which aims to provide NATO allies and partners with access to strategic airlift, is the Strategic Airlift Capability (SAC), which has purchased three Boeing Globemaster III C-17 transport aircraft on behalf of a group of 12 NATO allies. The first C-17 was delivered in July 2009, followed by the second and third aircraft in September and October 2009. The aircraft is operated by the military Heavy Airlift Wing (HAW), the operational branch of SAC, at the 47th Air Base of the Hungarian Defence Forces in Pápa. Three military Boeing C-17 Globemaster III long-range cargo aircraft participating in the Strategic Airlift Capability (SAC), a multinational initiative, meet strategic and tactical airlift requirements. Each member nation owns a portion of the available flight hours and uses them to fulfill its national, NATO, UN, and EU commitments. [10] [11] [12]

HAW's multinational aircrew provides the full spectrum of C-17 air and ground missions, including aerial refuelling, one-ship airdrops, assault landings, and all-weather operations, day or night in low- and medium-threat environments. The HAW has flown more than 30,000 flight hours and achieved an exceptionally high (>80%) average mission capability in the SAC fleet with NAM maintenance support. A high deployment capability ratio means that aircraft are ready to carry out the SAC nation's mission without delay. HAW transported cargo and passengers to all continents.[13] [14] These figures demonstrate the logistical scale and digital complexity of operations. Mission planning, cargo routing, maintenance coordination, and aircrew scheduling all depend on interconnected information systems, such as flight-planning and EFB data-management platforms. Consequently, the SAC's operational success relies not only on physical readiness but also on cyber resilience. A disruption of flight planning systems could delay mission execution, impact load management, or compromise mission data integrity - highlighting that cybersecurity is now a logistics security function.

The SAC operates under the NATO Airlift Management Programme (NAMP), which provides financial, logistical, and IT support. Within

[10] J. D. Hood (2009).
[11] Szarvas László (2008).
[12] Siposné Kecskeméthy Klára (2019).
[13] Nyitrai Mihály (2016).
[14] Szászi Gábor (2015).

NAMP's digital infrastructure, secure data handling and access control are critical to maintain operational readiness.[15]

2. Multinational Multi-Task Tanker Transport (MRTT) Fleet (MMF)

The Multinational Multi-Role Tanker Transport (MRTT) Fleet, coordinated by the NATO Support and Procurement Agency (NSPA), provides strategic air-to-air refuelling, long-range transport, and medical evacuation. Operated from Eindhoven (Main Operating Base) and Cologne (Forward Operating Base), the MRTT fleet embodies NATO's digitally integrated air logistics concept. The program's "pooling and sharing" structure allows participating nations to share both costs and operational benefits. Each Airbus A330 MRTT aircraft has a fuel capacity of 111 tons and can deliver up to 2,200 litres per minute, servicing aircraft such as the F-16, F-35, C-17, Eurofighter, Tornado, and Gripen.

Yet, this technical integration also creates a broader cyber-attack surface. Mission scheduling, fuel distribution data, and maintenance coordination are processed through shared network environments managed by the NSPA. A disruption in these systems - whether caused by malware, insider threats, or communication failures - can have cascading effects across NATO's logistics chain. Thus, cyber defence must be included in every stage of MMF operations, including flight planning, data transmission, and post-mission reporting.

NATO airlift capability	SAC	MRTT	SALIS
Aircraft type	Boeing Globemaster III C-17	Airbus A330-200	Antonov An-124-100
Length	53,04 m	59 m	68.96 m
Wingspan	51,74 m	62 m	73.3 m
Height	16,79 m	16,8 m	21.08 m
Maximum takeoff weight	265 352 kg	242 000 kg	405 000 kg
Cargo/Passenger capacity	77 500 – 170 000 kg	253 - 277 passengers	150 000 kg
Maximum speed	830 km/h	913 km/h	850 km/h

Figure 2. Comparison of NATO Airlift Capability Aircraft pool

[15] Strategic Airlift Capability (2024).

The MMF's digital infrastructure, maintained through the Multinational Tanker Transport Fleet Support Partnership, demonstrates NATO's recognition that cybersecurity is fundamental to operational sustainability. Network segmentation, access control, and continuous monitoring must therefore be integral to NSPA's management model.[16] [17]

IV. Cyber Dependency in Airlift Logistics

Both SAC and MMF illustrate how NATO's logistical efficiency now depends on interconnected digital systems. The fusion of IT, operational technology (OT), and platform-specific systems creates a cyber-dependent logistics network in which data accuracy, secure communication, and system availability are vital. Any compromise within this network - such as a data corruption in mission planning or a denial-of-service (DoS) attack on communication links - can disrupt sortie generation, reduce fleet readiness, and jeopardize mission assurance. Accordingly, cybersecurity must be considered an integral part of NATO's air logistics doctrine, not an isolated IT responsibility.[18] [19]

Cybersecurity Domain	***Air Logistics Function***	***Operational Impact if Compromised***
Network Infrastructure Security	Mission planning and routing	Flight delays; loss of situational awareness
Data Integrity & Access Control	Cargo and fuel management	Incorrect load data; resource misallocation
Communication Resilience	Aircrew coordination	Mission disruption; reduced interoperability
OT Platform Protection	Maintenance and ground operations	Equipment downtime; reduced readiness

Figure 3. Relationship between Cybersecurity Layers and Air Logistics Functions

[16] Isaiah Oppelaar (2012).
[17] North Atlantic Treaty Organization (2022).
[18] W. D. Bryant (2016).
[19] M. Kalivoda and A. DeFazio (2017).

This table illustrates how disruptions in different cybersecurity layers translate directly into operational degradation across NATO airlift functions. Vulnerabilities in the network system impede mission planning and routing, resulting in delays and a loss of situational awareness. At the same time, compromised data integrity affects core logistics processes, such as cargo allocation and fuel management, leading to miscalculations that undermine mission efficiency. Likewise, weaknesses in communication systems and OT platform protection can disrupt aircrew coordination and ground operations, demonstrating that even localized cyber incidents can cascade into broader readiness and mission-assurance failures across the entire air logistics ecosystem.

In summary, NATO's airlift capabilities - while technologically advanced and logistically efficient - are increasingly dependent on the integrity of their cyber infrastructure. Protecting these systems ensures not only data security but also the continuity of NATO's military air logistics operations.

V. The importance and challenges of cybersecurity in military airlift operations

In the digital era, modern military operations depend extensively on advanced technologies, data-driven systems, and real-time network connectivity. Among these, military airlift capabilities form a cornerstone of global mobility and power projection, enabling the rapid deployment of personnel, materiel, and humanitarian supplies to critical locations. However, as these systems become increasingly automated and interconnected, they are simultaneously exposed to new forms of cyber vulnerabilities that threaten their reliability, continuity, and mission effectiveness.

The cyber threat areas of interest facing military airlift operations are dynamic and multidimensional. Adversaries such as state-sponsored actors, organized cybercriminals, and hacktivist networks actively seek to exploit weaknesses in aviation and logistics networks. Successful intrusions can lead to the disruption of strategic transport operations, unauthorized extraction of sensitive information, manipulation of flight planning or logistics data, and, in the most extreme cases, interference with aircraft control systems. These threats are not theoretical; they are increasingly facts of life in operations. The digital dependencies within airlift command, logistics coordination, and mission management systems have created new attack vectors. For instance, malware targeting mission planning platforms or service desk systems can cascade through the logistics

chain, delaying deployments or causing data synchronization failures. Thus, cyber resilience is now a key determinant of operational readiness.[20]

NATO's experience in recent conflicts - particularly those influenced by hybrid and cyber warfare - has underlined that cyberspace is an operational domain, not merely a technical environment. This recognition has prompted a doctrinal shift from traditional information assurance (focused on data protection) to mission assurance, in which cyber defence is embedded directly into the planning, execution, and sustainment phases of military operations. This paradigm shift demands that cybersecurity be accepted as a core logistics function. Protecting information networks ensures not only data integrity but also the uninterrupted flow of mission-critical logistics processes such as aircrew scheduling, route optimization, and cargo allocation. The Ukrainian conflict further illustrated that cyberattacks can have tangible kinetic consequences, disrupting communication and command chains that underpin logistics operations.

Military airlift operations do not exist in isolation; they are highly integrated, technologically interdependent within a global aviation ecosystem. Civil aviation networks - air traffic control (ATC), meteorological systems, NOTAM databases, and communication links - are frequently shared or interfaced with military operations. This civil–military interdependence creates additional layers of cyber risk. A vulnerability in civilian infrastructure can propagate across connected systems, potentially undermining air traffic safety and mission reliability. Therefore, cybersecurity in military airlift must extend beyond national defence measures to include international coordination, joint protocols, and standardized incident response frameworks. NATO's operational doctrine increasingly emphasizes this shared responsibility, encouraging collective cyber resilience across partner states and civil aviation entities.

While technology forms the visible component of cyber defence, human and procedural factors often determine success or failure. Insider threats - whether malicious or unintentional - can compromise logistics systems, while insufficient training or poor cyber hygiene can magnify vulnerabilities. Accordingly, cybersecurity education and awareness must be integrated into training in all units involved in airlift and logistics operations. Personnel in planning, maintenance, and command functions should receive continuous training in secure data handling, phishing detection, and incident reporting. Moreover, leadership engagement

[20] u.o.

is crucial: cyber defence cannot remain the exclusive domain of IT departments; it must be integrated into command-level decision-making and readiness assessments.[21] [22]

Ensuring the security of military airlift capabilities requires a comprehensive and layered cyber defence strategy, combining preventive, adaptive, and reactive measures:

- Preventive: Hardening critical systems, segmenting networks, and enforcing authentication and encryption standards.
- Adaptive: Continuously monitoring for anomalies and integrating threat intelligence into logistics decision-making.
- Reactive: Developing robust incident response and recovery protocols to restore operations swiftly after a cyber event.

To address the identified gap in structured empirical analysis, this paper proposes a simplified Cyber Risk Assessment Matrix tailored specifically for NATO military airlift operations. The model integrates threat categories from the ENISA Threat Landscape 2025 with operational dependencies of the Strategic Airlift Capability (SAC) and the Multinational MRTT Fleet (MMF).

Threat–Vulnerability–Impact Matrix

Threat Type	***Key Vulnerability***	***Operational Impact***	***Risk Level***
Ransomware targeting mission-planning systems	Centralized planning & flight data dependency	Sortie delays, incorrect routing, loss of mission assurance	Critical
GPS spoofing / GNSS interference	Navigation reliance & limited redundancy	Misrouting, aborts, airspace violations	High
Supply-chain malware in avionics or ground IT	Third-party vendor dependencies	Fleet grounding, data corruption	High
Insider misuse of credentials	Access control weaknesses	Unauthorized changes, data theft	High
DoS attack on logistics or comms	Network centralization	Loss of situational awareness, degraded command flow	Medium–High

[21] D. Kiss and L. Weissenbach (2020).
[22] C. St-Pierre and S. Ryan (2022).

VI. Cyber Defence Aspects and Addressing Challenges to Military Airlift Capabilities

Effective protection of NATO's airlift capabilities requires a comprehensive and integrated cyber defence framework that links technical safeguards with operational logistics flexibility. Military airlift operations depend on a complex digital system that spans aircraft systems, command networks, logistics databases, and multinational coordination platforms. To sustain readiness and mission assurance, these systems must be continuously protected, monitored, and adapted to evolving threats.

The first step in strengthening cyber defence is the systematic identification and evaluation of vulnerabilities within the airlift environment. Risk assessments should consider not only technical components - such as mission-planning systems, communications networks, and maintenance databases - but also human, procedural, and supplier-related risks. This holistic approach allows for targeted mitigation strategies and informed investment in cybersecurity resources.

Military airlift operations rely on interlinked information and operational-technology systems. Establishing a secure network architecture with firewalls, intrusion detection and prevention systems, segmentation, and redundancy minimizes adversaries' opportunities to intervene. Network zoning between mission-critical and administrative systems is essential to prevent cross-domain compromise. [23]

Because airlift missions involve constant information exchange - flight plans, cargo manifests, weather data, and command directives - data confidentiality and integrity are vital. Implementing strong encryption, Virtual Private Networks (VPNs), and end-to-end authentication mechanisms ensures that information remains shielded from interception or manipulation during transmission.

Robust access management reduces the risk of insider misuse and credential theft. Multi-factor authentication, role-based privilege allocation, and periodic credential audits limit exposure of sensitive aviation systems. Access policies must apply across all network layers, including third-party maintenance and logistics partners integrated through NATO's support programs.

[23] F. L. Greitzer et al. (2014).

Given the inevitability of attempted intrusions, well-defined incident response plans are indispensable. These should include detection, containment, eradication, and recovery phases, supported by pre-approved communication protocols and decision chains. Conducting regular cyber-resilience exercises - both simulated and live - tests the ability of logistics and IT personnel to sustain operations during digital disruption.

Human reliability underpins technical defence. Continuous education programs on phishing recognition, data-handling protocols, and secure device usage foster a cyber-aware culture among pilots, logistics officers, and maintenance crews. Training must also address cross-national coordination within NATO, ensuring that cyber standards are uniformly applied across participating nations.

The military airlift supply chain comprises numerous contractors that provide aircraft components, software updates, and logistical services. Third-party risk management - including vendor vetting, software integrity checks, and contractual cybersecurity clauses - reduces the likelihood of compromised elements entering NATO's operational ecosystem. The introduction of a zero-trust model across procurement channels can further limit exposure.

Cyber defence in the airlift environment cannot be static. Continuous monitoring, vulnerability scanning, and penetration testing are required to detect anomalies and emerging threats. Integrating threat intelligence alerts into NATO's command and control centers enhances situational awareness and enables proactive mitigation. Regular audits ensure that lessons learned are incorporated into future defence upgrades.[24]

Furthermore, this kind of defence in military airlift operations extends beyond protecting IT systems - it safeguards the logistical lifeline of NATO's mobility. By integrating technical controls, human preparedness, and resilient logistics design, airlift operations can maintain continuity even under cyber-contested conditions. Each of these measures, taken together, transforms cybersecurity from a support function into an operational capability that directly underpins NATO's strategic readiness.

[24] DoD (2022).

VII. Conclusions

The growing digital convergence of the civilian and military aviation sectors has established highly interconnected networks among aircraft systems, logistical frameworks, and air traffic management systems. These interconnections, while improving operational efficiency, also bring considerable cybersecurity risks. Consequently, NATO must protect its aviation capabilities through a comprehensive defence strategy that integrates defence-in-depth, operational flexibility, and sophisticated, adaptive defence approaches.

The ENISA Threat Landscape 2025 highlights that both next-generation and legacy systems are becoming increasingly reliant on networks, broadening the potential attack surface for state and non-state entities. Consequently, cyber defence validation should be a vital part of the airworthiness certification process for NATO and its member nations, ensuring that cybersecurity is a critical component from planning through the operational phases.

Safeguarding military airlift capabilities-vital to NATO's worldwide mobility and crisis response framework-requires a comprehensive strategy that includes risk evaluation, secure network design, encrypted communication, access management, incident response, personnel training, supply chain security, and ongoing monitoring. Ongoing adjustments to new threats will remain crucial for sustaining operational dominance on a swiftly changing digital battleground.

Ultimately, the reliance between civil and military aviation indicates that neither sector can achieve comprehensive cybersecurity on its own. An assault on civil aviation facilities will inevitably undermine NATO's military preparedness. This reliance showed that cybersecurity and logistics are not separate functions but interlinked foundations of operational preparedness. Consequently, future military logistics systems must embed cybersecurity as an essential feature, guaranteeing that both mission continuity and logistical flexibility remain intact even in potential hostile cyber environments. The findings of this study confirm the central hypotheses formulated in the introduction. First, the analysis demonstrates that NATO's military airlift capabilities indeed require proactive cyber risk management and continuous protection of their IT and OT infrastructures, validating Hypothesis 1. Second, the examination of ENISA threat trends and operational interdependencies shows that increasing digitalization significantly elevates exposure to

cyber threats, and that advanced cybersecurity protocols and ongoing personnel training are essential, thereby confirming Hypothesis 2. [25] [26]

VIII. References

Bryant, William D.: "Mission Assurance through Integrated Cyber Defense" Winter 2016 edition of Air and Space Power Journal 2016. pp. 10-14. [Online]. Available: https://www.airuniversity.af.edu/Portals/10/ASPJ_Spanish/Journals/Volume-29_Issue-3/2017_3_04_bryant_s_eng.pdf

Bryant, William D.: Resiliency in Future Cyber Combat. Strategic Studies Quarterly, 2015 Winter, 87–107. [Online]. Available: https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-09_Issue-4/Bryant.pdf

C. St-Pierre and S. Ryan: "Integrating Cyber Awareness into NATO Command Structures," NATO Review, 2022.

D. Kiss and L. Weissenbach: "Cybersecurity Challenges in Aviation: Civil-Military Interdependencies," Air & Space Power Journal–Europe, vol. 8, no. 4, 2020.

DoD: Zero Trust Reference Architecture v2.0, Washington, D.C., 2022. [Online]. Available: https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf

ENISA: Threat Landscape 2025: Transport Sector and Cybercrime. European Union Agency for Cybersecurity, 2025. [Online]. Available: https://www.enisa.europa.eu/topics/threats

ENISA: CIRAS incident reporting, 2024. [Online]. Available: https://ciras.enisa.europa.eu/ciras-consolidated-reporting

EUROPOL: Global operation targets NoName057(16) pro-Russian cybercrime network, 2025. [Online]. Available: https://www.europol.europa.eu/media-press/newsroom/news/global-operation-targets-noname05716-pro-russian-cybercrime-network

F. L. Greitzer et al.: "Analysis of Insider Threats to Information Systems," MITRE Tech. Rep., 2014.

[25] Bryant, William D. (2015).
[26] Bryant, William D. (2016).

G. Piovaccari, J. Merriman: Cyber attack on Italy's Foreign Ministry, airports claimed by pro-Russian hacker group, 2024 Reuters [Online]. Available: https://www.reuters.com/technology/cybersecurity/cyber-attack-italys-foreign-ministry-airports-claimed-by-pro-russian-hacker-2024-12-28/

Hunorfi Péter, Paráda István, Farkas Tibor: Kiberbiztonsági kihívások a légi közlkedésben - Kronológiai folyamat a Boeing elleni kibertámadások tükrében, Hadmérnök 19. évfolyam (2024) 1. szám 101-120.

Isaiah Oppelaar: "NATO's Multinational MRTT Unit: An Update and Case Study for Future Defence Cooperation" The Journal of the JAPCC 2023. pp. 25-31. [Online]. Available: https://www.japcc.org/articles/natos-multinational-mrtt-unit/

J. D. Hood: "NATO Strategic Airlift: Capability or Continued US Reliance?" AIR COMMAND AND STAFF COLLEGE AIR UNIVERSITY 2009, pp.68–73. [Online]. Available: ADA539589.pdf

Kalivoda, Michal, and Alexander DeFazio: "Defending NATO's Aviation Capabilities from Cyber Attack "Journal of the JAPCC 2017. pp. 104-109. [Online]. Available: JAPCC Journal Ed. 23

North Atlantic Treaty Organization: "Multi Role Tanker Transport Capability (MRTT-C) Factsheet" 2022. pp. 1-2. [Online]. Available: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/9/pdf/2209-factsheet-mrtt.pdf

North Atlantic Treaty Organization: "Strategic airlift" 2024. [Online]. Available: NATO - Topic: Strategic airlift

Nyitrai Mihály: “Eredmények a szövetséges stratégiai légi és tengeri szállítóképesség erősítése terén” Hadtudományi Szemle 2016. pp.84-87. [Online]. Available: Hadtudományi szemle - 9. évf. 2. sz. (2016)

Paráda István, Tóth András: A NATO katonai légi szállítási képességek kibervédelmi aspektusai. HADMÉRNÖK, 19(4), 167-182. http://doi.org/10.32567/hm.2024.4.12

Rosman, R.: Disruptions continue after IT outage affects millions worldwide. Retrieved July 21, 2024, [Online] Available: https://www.npr.org/2024/07/20/g-s1-12487/crowdstrike-microsoft-outage-update.

Siposné Kecskeméthy Klára: “A NATO Biztonsági Beruházási Programja Magyarországon” Honvédségi Szemle 2019. pp.32-33. [Online]. Available: https://real.mtak.hu/125189/

Strategic Airlift Capability 2024. [Online]. Available: https://sacprogram.org/default

Szászi Gábor: “A Magyar Honvédség légiszállító képességének változása napjainkig, a fejlesztés jövőbeni lehetpségei” ECONOMICA 2015. pp. 221-222. [Online]. Available: https://ojs.lib.unideb.hu/economica/article/view/4607/4392

Szarvas László: “Stratégiai Légi Szállítási képesség - egy új többnemzeti megoldás” Nemzet és biztonság 2008. pp.60–71. [Online]. Available: https://www.nemzetesbiztonsag.hu/cikkek/szarvas_laszlo-strategiai_legi_szallitasi_kepesseg___egy_uj_tobbnemzeti_megoldas.pdf