sciendo International Conference KNOWLEDGE-BASED ORGANIZATION
Vol. XXXI No 1 2025

BUILDING RESILIENCE AGAINST CYBERSECURITY RISKS IN MILITARY TRANSPORTATION NETWORKS

Maria CONSTANTINESCU

DRESMARA, National Defence University Carol I, Brașov, Romania
constantinescumaria.ro@gmail.com

Abstract: *The resilience of military transportation networks is critical to ensuring the effective deployment and sustainment of military forces, considering that the increasing reliance on digital technologies has made these networks highly vulnerable to cyber threats. This paper explores the evolving cybersecurity threat landscape affecting military mobility, identifying key attack vectors across sea, air, rail, road, and inland waterways. It examines how legacy systems, interoperability issues, and resource constraints hinder effective cyber defence. Through a comprehensive analysis of past cyber incidents and current vulnerabilities, the study proposes a multi-layered framework for cyber resilience that integrates technological innovation, robust governance, and enhanced civil-military collaboration. The findings underscore that cyber resilience in military transport is not merely a technical challenge, but a strategic priority requiring sustained investment and international cooperation.*

Keywords: military mobility, cyber-resilience, transportation networks

1. Introduction

The Ensuring the resilience of military transport networks is the foundation of military operations, as it ensures the timely delivery of troops, weapons and logistic support at the area of operations, ensuring the availability and sustainability of military capabilities. One crucial challenge in this respect is that military mobility, by its very nature, is not exclusively under the control of the armed forces. An effective transport network is the outcome of a whole of government endeavour, from infrastructure investments, procedural and regulatory harmonization, civil-military coordination, private sector best practices. Ensuring the resilience of military mobility requires cooperation between defence ministries, transport authorities, customs agencies, and private logistics providers and a coordinated planning and resource allocation. Without such integrated planning and political will sustained beyond short term considerations, across national and EU levels, inefficiencies in civilian infrastructure can undermine operational readiness and response times during crises or deployments.

Modern transportation is more vulnerable than ever to cybersecurity risks, due to the extensive use of Information Technology and Operational Technology, in all areas of operations. To ensure resilience against such risks, a structured approach integrating technological, organizational, and collaborative strategies is essential.

The aim of this paper is to examine the vulnerabilities of military transport networks to cyberattacks, and propose a framework for mitigating the risks.

DOI: 10.2478/kbo-2025-0008

The objectives of the paper consist in identifying the threat landscape, through the identification of the main attack vectors and potential malign actors, examining the key challenges and proposing a framework for cyber resilience, taking into account future directions and technological developments.
In support of the research goal and objectives, the following research questions have been considered:
(1) How can the integration of advanced technologies enhance cyber resilience in military transportation networks?
(2) What are the primary organizational and operational challenges to achieving interoperable cybersecurity standards among NATO and EU member states in military mobility?

2. The Cybersecurity Threat Landscape in Military Mobility

The transportation sector in general, and the military transport in particular, are increasingly confronted with cybersecurity threats targeting information and technology within the networks. These challenges are a result of increased interconnectivity, aging legacy systems, and the widespread integration of IoT devices. The adoption of technologies like AI, blockchain, real-time monitoring, network segmentation, and observability tools could provide advantages in the fight against cyber threats (in threat detection, incident response, regulatory compliance, workforce training), they could also be sources of vulnerabilities.
The main attack vectors which could be employed in order to compromise the functionality of military transport networks and disrupt military operations are discussed below.
Military transport by sea is essential for moving large quantities of military personnel, vehicles, and equipment across long distances. Sealift is vulnerable to cyberattacks mainly through the shipboard systems, port infrastructure, logistics and tracking systems and network integration.
Most NATO and EU countries ensure a significant portion of their military sea transport through civilian contractors, primarily via chartered commercial vessels and multinational assured access contracts. For example, the NATO Sealift Capability Package (SCP), which included up to 15 RoRo ships in 2021, was composed of both nationally chartered and commercial ships secured by multinational contract [1]. This is a source of vulnerabilities in terms of cybersecurity, as sealift operations often require interoperability between military and civilian systems, especially when using commercial ships and port facilities. This shared infrastructure inherits vulnerabilities from the commercial sector, including outdated software, inadequate patching, and weak cyber hygiene. The need to increase efficiency through digitalization and to automate processes, combined with the high costs of ensuring cybersecurity, compel some of the civilian companies to make tradeoffs between cost effectiveness and security.
Modern ships rely on interconnected digital systems for navigation, stability, propulsion, cargo management, and communications. These software systems can be targeted via satellite links, serial ports, or even infected USB drives, through the introduction of malware, enabling them to steal sensitive data, disrupt operations, or sabotage equipment.
Software that calculates the stability of a ship, moves rudders, or operates machinery can be hacked, effectively sabotaging the ship's operations. An example is the penetration test performed by the security company Naval Dome, who managed to hack into live, in-operation systems used to control a ships' navigation, radar, engines, pumps and machinery, shifting the ship's reported position, misleading the radar display, disabling the machinery, overriding the signals to fuel and ballast pumps and manipulating steering gear controls [2]. Another example was related to the capsizing of a roll-on/roll-off vehicle carrier

in 2019, due to the incorrect loading of the vehicles resulting from incorrect data fed into the shipboard stability calculation computer [3].

Ports and logistics hubs are increasingly automated and digitally managed and consequently, cyberattacks on port equipment (such as cranes, cargo tracking platforms, and inspection devices) can halt loading/unloading operations, disrupt scheduling, or even facilitate espionage. A famous example is the sophisticated, state-sponsored cyberattack NotPetya in 2017, disguised as ransomware but designed in reality as a data-wiping operation aimed at causing maximum disruption. Originating in Ukraine through a compromised software update, the malware quickly spread across borders, crippling global operations of multinational companies. Maersk, a major international shipping firm, whose IT systems were paralyzed, leading to significant delays and operational chaos at ports worldwide, suffered losses amounting to $250–$300 million dollars [4]. The attack exposed the fragility of global supply chains and the interdependence of transportation networks on digital infrastructure and demonstrated how a cyberattack, even if regionally targeted, could cascade across the globe, disrupting trade flows, delaying shipments.

In terms of port infrastructure, a relevant example of how vulnerable military transport is to cyberattacks is provided by the case of the Chinese-made cranes, particularly those manufactured by Shanghai Zhenhua Heavy Industries (ZPMC). Their widespread presence (they made up 80% of ship-to-shore cranes at U.S. ports) and built-in vulnerabilities (cellular modems and remote access capabilities) could be exploited for espionage or sabotage. Such features could allow the Chinese government to collect sensitive data on goods, including military shipments, or even remotely disable or manipulate critical port infrastructure in the event of a conflict [5].

In terms of logistics, platforms used for tracking containers and coordinating shipments can be compromised, providing adversaries with intelligence on military movements or enabling them to inject false data, causing confusion and delays. An example is LOGINK, a government supported Chinese logistic management platform, used for tracking containers and coordinating shipments, which could also provide surveillance data on its users and be used to coerce or disrupt port operators during a crisis or conflict [6].

Finally, the reliance of modern sea transport on cyber related systems such as the Global Navigation Satellite System (GNSS), Global Positioning System (GPS) and Automatic Identification System (AIS) is another source of vulnerability, as ship navigation could be targeted through spoofing and jamming attacks. An example is the 2017 Black Sea spoofing incident, when 20 ships reported their GPS positions inaccurately placed at an airport, with navigation systems showing impossible data such as antennas submerged underwater and abnormally high signal error rates [7].

Logistic hubs are essential for military mobility, and their increasing dependence on digital technologies like warehouse management systems (WMS), IoT devices, and robotics, used to streamline inventory control and operations, makes them vulnerable to cyber threats. Ransomware, denial-of-service (DoS) attacks, or to data breaches can disrupt operations and affect supply chains. Effective inventory management is crucial in military operations, as it ensures the timely and appropriate supply of a variety of goods, from food to weapon systems and ammunitions. Lack of effective logistic support can lead to operational losses and low sustainability, making this a potential target of choice for cyberattacks. These could alter inventory databases, changing item statuses or quantities, generating the delivery of faulty goods or supply chain

errors. Smart and automated technologies and devices, such as RFID scanners, could be spoofed or jammed, generating inaccurate or incomplete inventory data. Man-in-the-middle (MITM) attacks can be used to intercepting communications, with the purpose of exposing classified logistical data or disrupting operations [8].

Inland waterway military transport suffers from the same vulnerabilities as the sea transport, due to the increased digitalization and automation of navigation systems, operational technology (OT), and IT networks that connect vessels, ports, and logistics systems. Attackers could compromise a lock's programmable logic controller (PLC) to manipulate gate operations, malware could reverse gate commands, causing simultaneous opening of upstream/downstream gates during a convoy's passage [9]. In another incident, attackers likely gained access via phishing and ransomware locked servers at an inland Columbia River port, disrupting operations for days [10].

Military air transport faces threats ranging from the compromise of avionics to data breaches. Many modern transport aircraft rely on complex communication and navigation systems like, which could be vulnerable to cyberattacks. Attacks on AI navigation systems, such as data poisoning or evasion attacks, could corrupt flight path algorithms [11] and GPS Spoofing/Jamming could misdirecting aircraft by falsifying GPS data, as in the case of sea transport.

Military air transport operations are also vulnerable to data breaches & espionage enabled by cyber means. Cyber intrusions can expose classified flight plans, cargo manifests, or troop movements, while ransomware attacks like the Port of Seattle's 2024 data breach, which affected the airport systems, have already demonstrated the risks to cargo logistics and operational continuity [12].

Denial of service (DDoS) attacks overload the communications systems between control towers and aircrafts, significantly disrupting operations. Although it was not the result of a cyberattack, the 2024 CrowdStrike software failure demonstrated the acute vulnerability of air transport to cybersecurity risks. A faulty update to CrowdStrike's Falcon Sensor security software caused approximately 8.5 million Windows computers worldwide to crash, resulting in massive disruptions across airlines, banks, hospitals, and other critical services, in what is considered the largest IT outage in history [13].

IoT exploits could also pose a threat, as compromised sensors in fuel systems or cargo monitors could falsify data, leading to in-flight failures, while AI-Powered malware could autonomously map and exploit network weaknesses in real time.

Negligent or malicious personnel with system access to the Air Traffic Management (ATM) systems also constitute a critical vulnerability.

Military rail transport is not immune to cyberattacks, as it is increasingly digitized and its effective functioning relies on interconnected operational and information technology systems. Cyberattacks could target signalling, control, and communication networks, disrupting train movements, manipulating switches, or even cause derailments. Data systems could be compromised, resulting in the unauthorized access to sensitive information about military logistics or troop movements, or ransomware could be used to halt rail operations. A lot of railway companies still rely on legacy equipment, the distributed nature of rail infrastructure, weak authentication protocols, exposure to the public internet, personnel shortages and lack of training are significant vulnerabilities. Many railways systems in Europe are still operated in a public-private partnership format, increasing the risks due to differences in regulations, procedures and lack of financial resources to increase cybersecurity. Cyberattacks can target third party suppliers (such as in 2022, when a

Danish software provider for the largest train company was hit by a ransomware attack)[14], or can target directly the railways systems, such as in the 2022 cyberattack by the Belarusian hacktivist group Cyber Partisans on Belarusian Railways. They encrypted servers and disrupting operations in an effort to hinder Russian military logistics and troop movements through Belarus amid rising tensions over Ukraine. [15] In the same year, following the events in Ukraine, pro-Russian hacker groups have "claimed responsibility for attacks on Romanian national operator CFR Calatori in April, on Lithuanian Railways and Latvian operator SJSC in June, and against Estonian Railways in August" [16].

Road military transport is also vulnerable, considering that many fleet management systems lack modern security features, which makes them susceptible to cyber intrusions and increases the challenges to integrate new security measures. As military vehicles adopt more onboard electronics, a digital control systems and fleet management systems, the attack surface of road military transport expands. Cyberattacks could target for instance vehicle control systems, potentially disrupting engines, brakes, steering, and communications. The use of modern communication systems, through wireless, Bluetooth, and vehicle-to-everything (V2X) systems generates risks related to confidentiality (as data breaches attacks can result in the leakage of sensitive information, such as troop movements and logistics data) and command and control.

Effective military road transport depends on the status of road networks, and traffic management systems are highly vulnerable to cyberattacks due to their reliance on interconnected digital components and wireless communication networks. Successful attacks on the traffic management systems could cause severe traffic congestion and compromise emergency logistics, with the additional benefit of plausible deniability. Critical components such as signal controllers, vehicle detectors, and roadside units can be physically accessed or remotely exploited through wireless channels, allowing attackers to manipulate signal timing or inject falsified data. Malware and denial-of-service (DoS) attacks can disrupt operations, while weak authentication protocols and misconfigurations create entry points for unauthorized access.

The EU cybersecurity agency ENISA, in its 2023 Transport Threat Landscape Report highlighted the fact that this is not only a hypothetical, future occurrence, registering a surge in incidents targeting the transport sector. The targets in the transport domain are authorities, infrastructure managers, railway undertakings and suppliers and service providers. Compared to 2022, in 2023 the DDoS attacks in the transport sector increased with 53%, the ransomware attacks with 19%, data harvesting with 14% and intrusion attack with 8% [17].

3. The Way Ahead – a Framework for Cyber-Resilience

Building cyber resilience in military transport systems requires the successful management of various challenges, such as outdated equipment and procedures systems, interoperability risks and resource constraints.

One of the most pressing issues to be solved it the reliance on **legacy operational technology systems,** often developed decades ago and ill-suited for the current cybersecurity challenges. Although they are functional in terms of basic operations, these systems are significant vulnerabilities for cyberattacks and the integration of these legacy systems with newer digital infrastructure (often done in a fragmented fashion) can augment these vulnerabilities. In addition, the scarcity of personnel with expertise in both cybersecurity and legacy OT compounds the challenge.

Secondly, by its very nature, military transportation is predominantly

international, generating **interoperability issues**. In joint operations or during multinational missions, data must be exchanged across diverse platforms, systems, and national boundaries. Each partner nation may have different cybersecurity standards, risk tolerances, and regulatory constraints, creating inconsistencies in the collective cyber defence posture, leading to an increased attack surface. Building resilience cyber coordinated measures across jurisdictions and organizations, harmonized policies, shared threat intelligence, and reliable communication channels, which must be constructed and refined over time, in order to ensure that all partners maintain equally rigorous cybersecurity practices.

Finally, **resource constraints** are a significant challenge. Achieving an effective trade-off between cybersecurity investments and operational readiness is a constant issue. In terms of military mobility, the outcome of allocating resources for modernizing IT infrastructure, conducting cyber training, or acquiring advanced detection tools has to be compared with the outcome generated by funding vehicles acquisition and maintenance, fuel, personnel, and mission-critical logistics. This constant trade-off often results in cybersecurity being considered as a "non-productive", secondary are, whose return on investment is not immediately visible. In operational environments where tangible operational outputs are paramount, cybersecurity efforts require constant advocacy.

In order to ensure the resilience of transport networks in the face of cyber threats, a multi-layered framework is required, encompassing technological innovation, governance standards, and collaborative capacity-building.

Technological solutions, artificial intelligence and machine learning could prove effective in monitoring network activity and equipment performance, by identifying unusual patterns in real-time and facilitating rapid detection of threats. The complex and distributed nature of military transport networks would benefit from the implementation of a Zero Trust Architecture, especially in environments where Information Technology and OT Operational Technology converge, for instance in autonomous systems, and command logistics platforms. Blockchain technology could reduce the risk of data manipulation or supply chain compromise by providing secure, transparent records of cargo movements, maintenance logs, and supply deliveries.

Building cyber resilience also requires a **common framework for governance**, relying on commonly agreed methodology and policies to identify, assess and mitigate cyber risks, especially considering the multitude of actors involved in ensuring military transportation. A robust collaboration with the private sector is essential to facilitate the sharing of threat intelligence, best practices, and technology solutions, helping bridge gaps in cybersecurity expertise and infrastructure, especially in areas where military systems rely on commercial transportation providers, satellite networks, or software platforms. Establishing formalized channels for information exchange can accelerate threat detection and mitigation efforts across the defence-industrial base.

As rapid recovery is vital to support military operations, predefined incident response plans are important to outline clear protocols for containment, eradication, recovery, and post-incident analysis. These plans should be regularly tested and adapted based on updated threat intelligence and all stakeholders should be kept up to date on the cybersecurity situation, in the limits of information classification.

4. Conclusions

The increased dependence of military transportation on modern technologies is a two edged sword, as it can simultaneously

increase efficiency and operational readiness, and generate vulnerabilities in all modes of military transport. The dynamic nature of the cyber threat landscape, combined with the complexity of multinational logistics operations and the reliance on civilian infrastructure and technologies, necessitates a whole of government, multi-layered approach to building cyber resilience, as military mobility is the result of a complex network of processes and actors.

References

[1] Strategic sealift. NATO. 2022. Available from: https://www.nato.int/cps/cz/natohq/topics_50104.htm.

[2] Tests Show Ease of Hacking ECDIS, Radar and Machinery. The Maritime Executive. Available from: https://www.maritime-executive.com/article/tests-show-ease-of-hacking-ecdis-radar-and-machinery.

[3] NTSB/MAR-21/03 PB2021-100930. NTSB Maritime Accident Report. Available from: https://www.ntsb.gov/investigations/AccidentReports/Reports/MAR2103.pdfDefense Industry Programme, Available from: https://defence-industry-space.ec.europa.eu/eu-defence-industry/edip-future-defence_en.

[4] McQuade, M. EU's The Untold Story of NotPetya, the Most Devastating Cyberattack in History. 2018. Available from: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

[5] WTAS: Joint Investigation into CCP-Backed Company Supplying Cranes to U.S. Ports Reveals Shocking Findings. March, 12, 2024. Available from: https://homeland.house.gov/2024/03/12/wtas-joint-investigation-intoccp-backed-company-supplying-cranes-to-u-s-ports-reveals-shocking-findings/#:~:text=The%20congressional%20probe%20discovered%20that,concerns%2C%20according%20to%20the%20WSJ .

[6] USCC Staff. LOGINK: Risks from China's Promotion of a Global Logistics Management Platform. September, 20, 2022. Available from: https://www.uscc.gov/sites/default/files/2022-09/LOGINK-Risks_from_Chinas_Promotion_of_a_Global_Logistics_Management_Platform.pdf .

[7] Goward, D. Mass GPS Spoofing Attack in Black Sea?. The Maritime Executive. 2017 Available from: https://maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea.

[8] Meggiato, G., Nterai, S., Skowronski, E., Gao, R., Rahman, M. Warehouses against Cyber-Attack Risks. Proceedings of the International Conference on Industrial Engineering and Operations Management Istanbul. 2022. Turkey.

[9] Good practice guide Cybersecurity in inland navigation". European Committee for drawing up Standards in the field of Inland Navigation (CESNI). 2023 Available from: https://www.cesni.eu/wp-content/uploads/2023/05/Guide_cybersecurite_en.pdf.

[10] Nicaise, V.. Cybermarétique: a short history of cyberattacks against ports. 10/15/2021. Available from: https://www.stormshield.com/news/cybermaretique-a-short-history-of-cyberattacks-against-ports/.

[11] Keller, J. How vulnerable is battlefield artificial intelligence (AI) to cyber and electronic warfare (EW) attack?. Military Aerospace. March, 27, 2025. Available from https://www.militaryaerospace.com/computers/article/55277563/vulnerabilities-of-artificial-intelligence-to-cyber-and-electronic-warfare-attack.

[12] Jones, D. Aviation sector faces heightened cyber risks due to vulnerable software, aging tech. Cybersecurity dive. April, 14, 2025. https://www.cybersecuritydive.com/news/aviation-cyber-risks-aging-tech/745273/.
[13] CrowdStrike: What the 2024 outage reveals about security. December, 17, 2024. Available at: https://www.privacyinternational.org/long-read/5507/crowdstrike-what-2024-outage-reveals-about-security.
[14] Paganini, P. A cyberattack blocked the trains in Denmark. November, 6, 2022. Available from: https://securityaffairs.com/138127/cyber-crime/cyberattack-blocked-trains-denmark.html.
[15] Culverwell, D. Belarusian hacktivists' cyberattack on railway system to disrupt movement of Russian troops. January, 25, 2022. Intellinews. https://www.intellinews.com/belarusian-hacktivists-cyberattack-on-railway-system-to-disrupt-movement-of-russian-troops-232859/.
[16] Preston, R. EU cybersecurity agency reports on threat to rail. International Rail Journal. 2023. https://www.railjournal.com/technology/eu-cybersecurity-agency-reports-on-threat-to-rail/#:~:text=Pro%2DRussian%20hacker%20groups%20have,against%20Estonian%20Railways%20in%20August.
[17] Theocharidou, M. ENISA Threat Landscape 2023: Transport sector. ENISA. 2023. Available from: https://www.enisa.europa.eu/sites/default/files/all_files/03-cooperation-information-sharing-03-enisa-theocharidou.pdf.