ADVANCING THE STRATEGIC RESILIENCE OF MILITARY MOBILITY THROUGH A WHOLE-OF-GOVERNMENT APPROACH

Associate Professor Dr. Maria CONSTANTINESCU

Regional Departament for Defence Resources Management Studies, Brașov;
National Defence University "Carol I", Bucharest

DOI: 10.55535/RMT.2025.3.32

This research paper explores the contribution military mobility can have to ensuring strategic resilience, by adopting a comprehensive, whole-of-government (WoG) perspective, emphasizing its critical role as a strategic capability for timely and effective deployment and sustainment of forces. It argues that military mobility transcends purely military functions and requires coordinated engagement among various government ministries – including defense, interior, and transportation – and collaboration with private sector stakeholders managing transport infrastructure. Challenges such as infrastructure degradation, lack of standardization in cross-border movement, and cybersecurity threats underscore the need for resilient, interoperable transport systems. The research underlines the imperative of embedding military mobility into national and multinational defense planning to ensure readiness, deterrence, and operational success in complex and evolving security environments.

Keywords: military mobility; whole-of-government approach; strategic resilience; hybrid threats; infrastructure vulnerability;

INTRODUCTION

Defined as the capacity for armed forces to swiftly and efficiently move personnel, materiel, and assets across diverse terrains and national borders (Damen, 2025), military mobility is a cornerstone of contemporary defense, rapid response, and the successful execution of military operations.

The *aim* of this paper is to analyze the contemporary challenges of military mobility in Romania and U and to make the case for the adoption of a whole-of-government framework. In order to achieve this aim, the following *research objectives* are considered:

- To analyze the complex challenges negatively impacting military mobility in Europe, encompassing both traditional obstacles such as inadequate physical infrastructure and regulatory complexities, as well as contemporary hybrid threats including cyberattacks, disinformation campaigns, and sabotage.
- To identify key requirements for effective military mobility within a whole-of-government paradigm, focusing on infrastructure development, regulatory harmonization, and strategies for mitigating hybrid threats.

Based on the analysis of the challenges to military mobility and the proposed benefits of an integrated approach, the following *research hypothesis* is formulated: The comprehensive adoption and effective implementation of a whole-of-government approach, encompassing coordinated efforts across governmental bodies, private sector entities, and international organizations, significantly enhances military mobility and strengthens resilience against hybrid threats in Europe.

This research will employ a *qualitative research methodology*, primarily utilizing content analysis and desk research to address the stated objectives. The primary *data sources*are derived from the academic literature review, official reports, and expert analysis.

LITERATURE REVIEW

There is a wide diversity in focus areas, methodological approaches, and geographic contexts in the literature that address multiple interconnected domains of military mobility, examining various aspects of strategic military mobility, resilience and whole-of-government approaches. Several foundational works examine the strategic mobility framework, with early contributions (Drach, 1995) analyzing the four strategic mobility pillars of airlift, sealift, prepositioning, and infrastructure.

The need to integrate military mobility across various government sectors is addressed in the literature from different perspective. From the perspective of the organizational and technological integration, studies identify the need for seamless coordination between strategic and theater mobility systems (Kee, 1996), for aligning the force structure and mobility funding (Kokko, 1993) and for harmonizing the civil-military logistics doctrines (Gangotena-Bustamante, 2024). The role of artificial intelligence, predictive modeling, autonomous vehicles, and blockchain are highlighted as an important factors influencing military mobility in the future (Gangotena-Bustamante, ib.).In terms of policy recommendations, the examination of the literature suggested the need to consolidate command structures, develop multiservice knowledge-management organizations and encourage sustained knowledge acquisition and context-setting campaigns (Owen, 2017; Johnson, 2007). The human factors are considered a crucial component of resilient military mobility, with leadership, training, and professional development identified as essential for effective integration (Owen, 2013). While infrastructure gaps are visible, *"soft"* frictions (such as customs procedures, transport permits, and liability regimes) can impose equally significant delays. Recent analyses argue that these administrative hurdles, if unaddressed, could delay cross-border deployments by days or weeks, undermining the credibility of rapid reinforcement strategies (European Commission, 2022; Euractiv, 2024).

Military mobility cannot be effectively achieved without a resilient strategic infrastructure and reliable dual-use capabilities. Multiple studies (Drach, 1995) (Gardner, 1996) (Constantinescu, 2024) identify infrastructure – ports, airfields, roads, rail, and digital networks – as fundamental to force projection and sustainment. The vulnerability of these networks to physical, cyber, and hybrid threats is identified as a recurring concern, especially as military and civilian uses increasingly overlap (Chung et al., 2024), the authors emphasizing the need to update doctrines as to recognize infrastructure as a core component of mobility (Gardner, 1996), the crucial role of increased investments in dual-use (civil-military) transport corridors (Howell, 2020) and to adopt industry standards to ensure compatibility and resilience (Gardner, ib.). Some studies report that the integration of commercial assets, such as the Civil Reserve Air Fleet and the Voluntary Intermodal Sealift Agreement, is both a strength and a vulnerability, due to declining excess capacity and workforce shortages in the commercial sector (Gallagher, 2021).

The literature consistently identifies physical bottlenecks as critical vulnerabilities in terms ofinfrastructure and critical transport networks. Reports from the European Court of Auditors and the European Commission note that bridges unable to support heavy vehicles, rail networks with incompatible gauges, and ports lacking sufficient capacity all constrain rapid deployment (European Commission, 2022; European Court of Auditors, 2023). While EU transport initiatives have begun prioritizing dual-use infrastructure corridors, funding and timelines remain insufficient to match strategic requirements. This aligns with independent audits and journalistic reporting, which stress that despite significant policy attention, infrastructure upgrades continue to lag behind operational needs (Barigazzi, Herszenhorn, 2025).

The governance dimension has received particular emphasis in both academic and policy literature. Studies highlight that routine civil-military exercises are essential to overcoming institutional silos and building a shared culture of preparedness (Kraśniewski, 2023; NATO, 2023). However, barriers persist, as different agencies often operate with divergent risk tolerances, budgetary cycles, and regulatory regimes, producing friction at moments when speed and clarity are most critical (European Defence Agency, 2022).The mechanisms required for an effective WoG coordination in the domain of military mobility are addressed through several studies, which highlight the limitations of siloed approaches and advocate for integrated frameworks that leverage the capabilities of multiple government agencies, civilian sectors, and international partners. Some authors (Burton, 2007; Manwaring, 2006) recommend cross-governmental and multidimensional approaches, including modifications to command structures and the establishment of comprehensive policy coordination mechanisms, and others emphasize the role of civilian agencies and public-private partnerships in supporting military operations, particularly in logistics and infrastructure (Mars, 2016) (Jacuch, 2020) and in cyberspace (Myers, 2011; Constantinescu, 2025), underscoring the need for integrated governance and information-sharing across defense, transport.

Crisis response and preparedness are central to the strategic resilience of military mobility, and several studies (Ring, 2008; Wiltse, 2012) critique the lack of clear, coordinated military strategies for disaster response and advocate for total force solutions that integrate active, guard, and reserve components with civilian agencies, with emphasis placed on pre-event planning, intergovernmental relationships, and flexible response design for both domestic and international contingencies.The importance of civil preparedness and sector resilience is highlighted, particularly for rapid deployment across Europe and reinforcement of the North Atlantic Treaty Organization’s Eastern Flank (Jacuch, 2020; Giurgiu et al.,

2024) and the development of dual-use infrastructure, simplification of cross-border procedures, and investment in logistics hubs are identified as practical strategies to enhance preparedness and responsiveness.

An emerging strand of literature explores the vulnerability of mobility to cyber and hybrid threats, with the conclusion that the resilience of military mobility must include cybersecurity, information integrity, and societal preparedness. This has reinforced calls for WoG cooperation between defence ministries, law enforcement agencies, and private operators of critical infrastructure (Giegerich, 2023; NATO, 2023).

CURRENT MILITARY MOBILITY CHALLENGES

The modern landscape of military operations is characterized by the continuing effects of legacy challenges (such as chronic underinvestment in dual use transport networks and legal obstacles), but also by increasingly complicated multifaceted threats that jeopardize the rapid and secure movement of forces and logistics.

Cyberattacks represent a pervasive and escalating threat to the infrastructure underpinning military mobility, targeting critical components such as transport sector infrastructure, energy grids, supply chains, and command-and-control systems and causing physical damage, or compromising sensitive data.

Over the past five years, cyberattacks on railway systems globally have increased, indicating a growing focus by malicious actors on disrupting rail operations. The European Union Agency for Cybersecurity (ENISA) has consistently reported on the evolving cyber risk profile of the transport sector, noting an increase in attacks against European transport infrastructure, including airports, ports, and railways. The agency emphasizes that ransomware and data-related threats are particularly prevalent, targeting IT systems that support various operational aspects of rail transport. The cross-border nature of cyber threats means that an attack in one country can have wider implications for interconnected European networks, affecting overall military mobility and logistical capabilities (ENISA, 2023). The vulnerabilities exploited often include IT systems related to passenger services, ticketing, and mobile applications, with ransomware being a primary threat vector, accounting for 45% of cyberattacks in the rail sector (Secureworld.io., 2024, Rail Journal, 2023).

In 2023, Poland experienced cyber intrusions in railway communication systems in 2023, causing emergency stops and delays, which highlighted the vulnerability of critical communication infrastructure (Cybersecurity and Infrastructure Security Agency, 2023). In 2025, Ukraine's state railway service experienced a powerful cyberattack that disabled its online ticketing system, causing significant disruption, leading to long queues at stations as passengers were unable to purchase tickets online or via mobile applications (Reuters, 2025; The Record, 2025).

Cyberattacks are a major threat from a military mobility perspective, as they significantly impact the physical movement of military assets and personnel. Railway systems, being a cornerstone of military logistics for heavy equipment and large-scale troop movements, are particularly vulnerable. Attacks on operational technology (OT) systems, such as signaling, switching, and traffic control systems, can lead to widespread delays, rerouting, or even complete shutdowns of rail lines. A cyberattack that manipulates signaling systems could cause trains to halt, collide, or be misdirected, effectively creating bottlenecks and preventing timely deployment or redeployment of forces.

Cyberattacks can cripple the logistical planning and execution systems, with serious effects as modern military logistics rely heavily on sophisticated IT systems for inventory management, scheduling, route optimization, and supply chain coordination. A ransomware attack or data breach on these systems can render them inoperable, leading to a loss of situational awareness, inability to track assets, and severe delays in resupply efforts.

Cyberattacks are not solely aimed at disruption, they are increasingly used for intelligence gathering and surveillance, which indirectly impacts military mobility by compromising operational security. Adversaries can exploit vulnerabilities in transport networks to monitor the movement of military convoys, equipment, and personnel. By gaining access to scheduling systems, GPS data, or even public Wi-Fi networks used by military personnel, adversaries can infer troop movements, deployment patterns, and logistical vulnerabilities (Federal News Network, 2025).

Successful cyberattacks on critical infrastructure can erode public and military confidence in the security and reliability of transport systems, with significant psychological and operational consequences. Military commanders might become hesitant to rely on civilian infrastructure for critical movements, leading to slower, more cautious, and less efficient logistical planning. A loss of public trust can also lead to civil unrest or opposition to military movements, complicating operations that require civilian cooperation or access to public routes.

Responding to and recovering from cyberattacks on transport infrastructure can impose immense economic and resource strains, as the costs associated with system restoration, damage assessment, enhanced cybersecurity measures, and potential legal liabilities can divert significant funds and personnel away from other critical military priorities. Moreover, prolonged disruptions can lead to economic losses for civilian industries, which in turn can impact the broader economic stability necessary to support military operations. The need to invest heavily in cybersecurity for civilian-owned infrastructure that underpins military mobility, such as rail networks, commercial ports, and airports, is a recognized challenge, with insufficient cybersecurity being a persistent issue (Industrial Cyber, 2025). Another issue which enhances the severity of the threat is that these cyberattacks usually target civilian and private companies, who may not have the will and/or resources to invest significantly in increasing their level of cybersecurity, making them softer targets compared for example with military logistic bases servers.

Disinformation campaigns may pose a significant threat to military mobility in Europe, especially in the context of heightened geopolitical tensions in Eastern Europe and the Baltic region, by undermining the integrity of strategic communications, destabilizing public trust, and complicating coordination among allied nations.

Disinformation campaigns often target the public and civil authorities to erode trust in military operations and government institutions, and false narratives about military build-ups, troop movements, or incidents involving infrastructure can lead to public unrest or opposition, thereby complicating command-and-control during crises. For example, a coordinated campaign on social media following the 2025 elections spread false reports claiming that Romania will send troops in Ukraine, with the result that even ordinary military convoys or planned military exercises were viewed with extreme suspicion by the population, considered as *"proof"* for that particular narrative (Inforadar, 2025). As a result of such disinformation campaigns, the movement of personnel and military material (NATO or national) on rail and roads may generate protests and in the event of a military operation, even lead to civil disobedience, distracting authorities and delaying mobilization.

Adversaries can use disinformation to distort or obscure real military developments, leading to confusion among decision-makers and false information about critical infrastructure damage or troop locations can mislead commanders, causing delays or misallocation of resources.

Disinformation campaigns can also falsely undermine the perception about transport infrastructure, influencing the movement of military logistics and supplies. For instance, rumors about unsafe rail routes or imminent attacks on key transport corridors might lead to unnecessary caution, rerouting, or closure of essential supply lines, or to crowding of essential military transport road routes by panicked civilians trying to flee certain areas.

In recent years, disinformation efforts targeting Europe have intensified, particularly surrounding the Russia-Ukraine conflict. For example, false claims about the destruction of key military infrastructure or false reports of troop withdrawals have periodically circulated, impacting strategic planning and public perception (European External Action Service, 2024). Similarly, manipulated satellite images and fake videos have been used to exaggerate or fabricate damage to critical transportation hubs, influencing decision-making and potentially delaying emergency or military responses.

Physical sabotage and covert actions inflict direct damage on infrastructure critical to military mobility, including roads, bridges, ports, and fuel supplies and can significantly impede logistical operations and rapid deployment capabilities. A specific characteristic of this type of hybrid warfare tool is the significant difficulty to demonstrate that a specific action was a deliberate sabotage, and to attribute it to a specific source/adversary. This feature makes this type of attacks particularly difficult to counter, as they may usually target civilian infrastructure and may mimic naturally occurring incidents. Malicious actors can lever ages legal loopholes and online recruitment of third-country nationals to execute these operations, complicating attribution and accountability.

A widely publicized incident of this nature was the railway sabotage in Germany in 2022, when cables crucial for train communication and safety were intentionally damaged, leading to a significant disruption in rail services across northern Germany, isolating key military and civilian infrastructure. (Rinke, Marsh, 2022). In 2024 the railway bridge at Elsfleth-Orth in Germany suffered irreparable damage when it was struck by a barge, causing severe economic repercussions for the region's ports (Boote Magazin, 2025). This bridge is also crucial from a military mobility perspective, as it is part of the route connecting the port of Nordenham, Germany and Miesau, home to the Theater Logistics Support Center Europe's ammunition depot, a crucial NATO logistic facility. A temporary bridge became functional in April 2024, but was again struck by a tanker barge in July 2024 (Shipwrecklog, 2024. A recent report by the International Institute for Security Studies has identified a significant increase in such incidents in Europe following the 2022, from 2 events in 2018 and 2019 to 12 events in 2022, 9 events in and a peak of 33 events, distributed across all sectors – Water, Communications, Military, and Transport in 2024 (Edwards, Seidenstein, 2025).

Europe'stransport *infrastructure limitations* are one of the main challenges to military mobility, as despite the fact that the continent is connected by an extensive transport infrastructure, this falls short of the requirements for rapid and large-scale military movements. After the fall of the USSR, the transport sector has been almost exclusively considered as a civilian matter, leading to decades of underinvestment and a lack of focus on dual-use standards have left critical vulnerabilities.

Many European roads and bridges are not designed to withstand the weight and size of modern heavy military equipment, leading to significant delays and forced detours that directly impact the speed and efficiency of military deployments. These infrastructure limitations mean that moving military equipment and troops from Western Europe to the East can currently take weeks, and in some cases, months, a timeframe that is unacceptable for rapid response scenarios (Todd, 2025). A significant example comes from Germany, where 4,500 of its 40,000 bridges are in insufficient or deficient condition, rendering them incapable of handling heavy military vehicles (Hartmann, 2024).

The situation of the European rail networks also presents substantial challenges. A recent evaluation from Deutche Bahn found that 23% of its 33,000 kilometers of track were in *"extremely bad condition"*, along with 48% of signaling control centers, 42% of level crossings, and over 25% of railroad switches, contributing to an average of one in three trains being delayed in 2022 (Hartmann, 2024). Another study concluded that, despite some progress and increased investments, the European rail system remains fragmented, with significant portions of the networks failing to fulfill the requirements set out in the EU's core infrastructure policy, the Trans-European Transport Network (TEN-T). For instance, less than 20% of TEN-T corridors are equipped with the European Train Control System (ETCS) and the average speed of rail lines often remains low, with eight member states achieving a maximum speed of only 80 km/h on the majority of their lines, far below the goal of 160 km/h for the TEN-T (Rico, Heyl, 2025).

Inland waterways, including canals and rivers, also play a role in military logistics, but their aging infrastructure poses challenges. Locks and weirs are on average 65 years old, leading to frequent component failures and the closure of entire waterway sections, often without alternative routes. (Hartmann, 2024).

The resilience of military mobility in Europe is also challenged by bureaucratic hurdles and fragmented national regulations, which significantly affect the timely movement of military forces across European borders. A report by the European Court of Auditors (European Court of Auditors, 2025) has identified the problems generated by extensive red tape from fragmented procedures and a lack of coordinated effort at the EU level, as military equipmentoften faces restrictions at national borders due to exceeding local weight limits or encountering infrastructure (like bridges) not designed for heavy loads. Another hurdle is related to the slow progress on *"Military Schengen"* as the EU's first Military Mobility Action Plan (2018) experienced delays, and despite a subsequent plan (2021) allocating 1.69 billion euros to this purpose, there is still a significant funding gap. A final issue identified is the persistent lack of cohesive cross-border investment, as nations tend to neglect infrastructure along their borders, often viewing it as a neighbor's responsibility. A significant challenge is also the absence of centralized coordination and effective information sharing mechanisms among EU member states, generating inefficiencies in planning and executing military movements and makes it difficult to implement military mobility plans in a targeted manner (Van Rensbergen, 2025).

Another area that needs to be considered in the efforts to increase the resilience of military mobility is the way the domain is going to be impacted by *emerging technologies*, such as artificial intelligence (AI), drones, and autonomous systems, which are increasingly being leveraged by adversaries and can disrupt traditional logistical and operational models. The conflict in Ukraine since 2022 has generated numerous lessons regarding the profound impact of drones not only on ground combat operations, but also through direct attacks on logistical convoys and supply routes (Hollenbeck, 2025) and through the use of low-cost sea drones to effectively challenge naval operationsas seen with the Russian Black Sea fleet (Navy Lookout, 2025), opening the way for their use against naval transport. This widespread use of drones by adversaries can create a highly contested logistical space, forcing military movements to adapt to constant surveillance and potential interdiction, thereby slowing down deployments and increasing risks to personnel and equipment.

The integration of AI and autonomous systems by adversaries can introduce new layers of complexity and vulnerability to military mobility. While militaries are exploring AI for optimizing their own logistics and supply chain management, adversaries can exploit these technologies for disruptive purposes. For example, AI-enhanced intelligence can be used to analyze enemy doctrines and forecast responses, allowing for more precise targeting of logistical nodes and movement corridors. The threat of *"data poisoning"* could also compromise the integrity of AI-driven logistical planning and decision-making, leading to inefficiencies or misallocations of resources. Autonomous ground vehicles, while beneficial for reducing risk in high-danger operations, also present a new vector for attack if compromised or countered by adversary autonomous systems, potentially disrupting critical resupply efforts and creating chokepoints in military mobility (Lopez, 2024). Advancements in fields like quantum technology hold the potential to break asymmetric encryption and enable navigation systems that are resilient to GPS disruption, further complicating military mobility and logistics by challenging existing technological advantages (Kirichenko, 2025).

Electromagnetic warfare (EW) is another factor to be seriously considered in building resilience, as it directly targets critical communication and navigation systems, posing a significant threat to military mobility. A primary vulnerability lies in the Global Positioning System (GPS), which is highly susceptible to jamming and spoofing, potentially disorienting forces and disrupting logistical convoys. EW is already used by both parties in Ukraine, impacting both military and civilian GPS-dependent systems (Turgeon, 2024). A recent incident of this type has highlighted this risk, when the navigation system of a plane carrying Ursula von der Leyen to Bulgaria was disrupted due to suspected Russian interference, with the pilots having to land the plane using paper maps. (Davies, Vernon, 2025). EW can also involve electronic masking, probing, and reconnaissance, providing adversaries with critical intelligence on military movements and intentions, allowing for more effective targeting of logistical chokepoints or vulnerable convoys (NATO, 2023).

CONCLUSIONS AND RECOMMENDATIONS

The findings confirm the research hypothesis that the comprehensive adoption and effective implementation of a Whole-of-Government (WoG) approach is indispensable for significantly enhancing military mobility and strengthening resilience against these evolving threats. A WoG framework necessitates coordinated engagement across diverse governmental ministries – including defense, interior, transportation, foreign affairs, and finance – as well as robust collaboration with private sector stakeholders who manage critical transport infrastructure. This integrated strategy moves beyond siloed departmental efforts, recognizing that the resilience of military mobility is intrinsically linked to civilian preparedness, harmonized regulatory environments, and a shared understanding of security imperatives across society. The paper highlights that successful military mobility hinges on high-level political and military engagement, effective planning that seamlessly integrates civilian and military logistics, and the consistent application of WoG frameworks across enabling nations. Ultimately, advancing military mobility through a WoG approach is paramount for ensuring readiness, bolstering deterrence, and achieving operational success in an increasingly complex and unpredictable global security environment.

BIBLIOGRAPHICAL RESOURCES:

1. Barigazzi, J., Herszenhorn, D.M. (2025). *EU military mobility plan hampered by delays, lack of funding*. Politico, https://www.politico.eu, retrieved on 2 August 2025.
2. Boote Magazin (2025). *Millions in damages, Captain on trial after bridge crash,* https://www.boote-magazin.de/en/travel-and-charter/territories/millions-in-damages-captain-on-trial-after-bridge-crash/, retrieved on 12 August 2025.

3. Burton, A. (2007). *Developing a Whole-of-Government Approach to Complex Problems.*
4. Chung, S., Sardak, D., Cegan, J., Linkov, I. (2024). *Assessing the Robustness and Resilience of U.S. Strategic Highways: A Network Science Perspective.*
5. Constantinescu, M. (2025). *Building Resilience against Cybersecurity Risks in Military Transportation Networks*. International conference Knowledge-Based Organization.
6. Council of the European Union (2022). *Conclusions on military mobility*. Brussels: General Secretariat of the Council.
7. *Cyber hackers target Polish rail network, cause operational disruptions*, https://industrialcyber.co/transport/cyber-hackers-target-polish-rail-network-cause-operational-disruptions/, retrieved on 22 August 2025.
8. Damen, H. (2025). *Logistics and Mobility: The Backbone of Military Success*. Insparcom, https://insparcom.nl/logistics-and-mobility-the-backbone-of-military-success, retrieved on 2 August 2025.
9. Davies, M, Vernon, W. (2025). *EU chief von der Leyen's plane hit by suspected Russian GPS jamming*. BBC news, https://www.bbc.com/news/articles/c9d07z1439zo, retrieved on 22 August 2025.
10. Drach, A. 1995. *The Strategic Mobility Shortfall: Underrepresented, Underfunded, and Unresolved*.
11. Edwards, C., Seidenstein, N. (2025). *The Scale of Russian Sabotage Operations against Europe's Critical Infrastructure*, The International Institute for Strategic Studies.
12. *ENISA Threat Landscape: transport sector*, https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape, retrieved on 2 August 2025.
13. Euractiv (10 March 2024). *EU struggles with military transport bureaucracy despite action plan*, https://www.euractiv.com, retrieved on 22 August 2025.
14. European Commission (2022). *Action Plan on Military Mobility 2.0* (JOIN(2022) 49 final). Brussels: European Commission.
15. European Commission (2025), https://transport.ec.europa.eu/news-events/news/commission-supports-military-mobility-projects-eu807-million-2024-01-24_en, retrieved on 22 August 2025.
16. European Commission. *Military mobility*, https://transport.ec.europa.eu/transport-themes/military-mobility_en, retrieved on 22 August 2025.
17. European Court of Auditors (2023). *Special Report: The EU's action on military mobility – Slow progress in removing obstacles*. Luxembourg: Publications Office of the European Union.
18. European Court of Auditors (2025). *EU military mobility – Full speed not reached due to design weaknesses and obstacles en route*, https://www.eca.europa.eu/ECAPublications/SR-2025-04/SR-2025-04_EN.pdf, retrieved on 2 August 2025.
19. European Defence Agency (2022). *Defence implications of a whole-of-government approach*. Brussels: EDA.
20. European External Action Service (2024). *Disinformation and Strategic Deception in the Ukraine War*, https://eeas.europa.eu/, retrieved on 2 August 2025.
21. Federal News Network (19 August 2025). *Weaponized infrastructure: The overlooked digital threat to US forces*, https://federalnewsnetwork.com/commentary/2025/08/weaponized-infrastructure-the-overlooked-digital-threat-to-us-forces/, retrieved on 22 August 2025.

22. Gallagher, R.E., Burch, G.F., Batchelor, J.H. (2021). *United States Civil Reserve Air Fleet (CRAF): A Brief History – Formation, Functionality, and Future*. Transportation Research Record.
23. Gangotena-Bustamante, J.B. (2024). *Diseño de sistemas logísticos resilientes para fuerzas desplegadas en regions inestables*, in *Space Scientific Journal of Multidisciplinary.*
24. Gardner, G. (1996). *Infrastructure, the Fourth Element of Strategic Mobility*.
25. Giegerich, B. (2023). *Cyber and hybrid threats to mobility and logistics in Europe*, in Survival, 65(4), pp. 121-140.
26. Giurgiu, T., Virca, I., Noja, G. (2024). *Military Mobility in the Vision of NATO and European Union*, in *Romanian Military Thinking.*
27. Hartmann, J. (2024). *Military Mobility*. DGAP, https://dgap.org/en/research/publications/military-mobility, retrieved on 22 August 2025.
28. Hollenbeck, N. (2025). *How to Transform the Army for Drone Warfare*. Army War College, https://warroom.armywarcollege.edu/articles/transform-for-drones/, retrieved on 2 August 2025.
29. Howell, R. (2020). *Transportation Infrastructure: A Critical Component for Deterrence in Europe*, U.S. Army Command and General Staff College, https://apps.dtic.mil/sti/pdfs/AD1159121.pdf, retrieved on 18 January 2024 (In-text citation Howell, 2020).
30. Industrial Cyber (2025). *Cyber threats to rail, ports and airports could cripple US military mobilization*, FDD report warns.
31. Inforadar, *Dezinformare pe tema sprijinului pentru Ucraina*, https://inforadar.mapn.ro/tema/104_dezinformare-pe-tema-sprijinului-pentru-ucraina, retrieved on 2 August 2025.
32. Jacuch, A. (2020). *Security and defense challenges – civil preparedness in NATO.*
33. Johnston, M. (1996). *Strategic Mobility: An Assessment*, https://apps.dtic.mil/sti/html/tr/ADA308551/index.html, retrieved on 2 August 2025.
34. Kee, R.A. (1996). *Bridging the Gulf between Theater and Strategic Air Mobility.*
35. Kirichenko, D. (2025). *Artificial intelligence's growing role in modern warfare*. Army War College, https://warroom.armywarcollege.edu/articles/ais-growing-role/, retrieved on 2 August 2025.
36. Kokko, R.W. (1993). *Strategic Mobility for the National Military Strategy.*
37. Kraśniewski, P. (2023). *Interagency coordination for defence logistics: A whole-of-government chal*lenge. Security &Defence Quarterly, 42(3), pp. 33-47.
38. Lopez, T. (2024). *DOD Needs Solutions for the Proliferation of Autonomous Vehicles, Defense Officials Say*. Defense Logistic Agency, https://www.dla.mil/About-DLA/News/News-Article-View/Article/3869110/dod-needs-solutions-for-the-proliferation-of-autonomous-vehicles-defense-offici/, retrieved on 2 August 2025.
39. Manwaring, M. 2006. *Defense, Development, and Diplomacy (3D): Canadian and U.S. Military Perspectives.*
40. Mars, H. (2016). *How the Department of Transportation Supports the DOD.*
41. NATO (2023). *Electromagnetic warfare*, https://www.nato.int/cps/en/natohq/topics_80906.htm, retrieved on 2 August 2025.
42. NATO (2023). *Resilience and civil preparedness*. Brussels: NATO Headquarters, https://www.nato.int, retrieved on 2 August 2025.

43. Navy Lookout (2025). *Black Sea battle: how Ukraine's drones overpowered the Russian Navy,* https://www.navylookout.com/black-sea-battle-how-ukraines-drones-overpowered-the-russian-navy/, retrieved on 2 August 2025.
44. Owen (2017). *US Air Force Airlift and the Army's Relevance*. Parameters
45. Rail Journal (22 March 2023). *EU cybersecurity agency reports on threat to rail,* https://www.railjournal.com/technology/eu-cybersecurity-agency-reports-on-threat-to-rail/, retrieved on 2 August 2025.
46. Reuters (24 March 2025). *Ukraine sees Russian effort to sow chaos as cyberattack hits railway online systems*, https://www.reuters.com/world/europe/ukraine-railway-says-its-online-systems-targeted-large-scale-cyberattack-2025-03-24/, retrieved on 2 August 2025.
47. Rico, C., Heyl, B. (2025). *Transport & Environment. The State of the EU's Rail Infrastructure: Investment priorities for more connected and resilient networks*, https://www.transportenvironment.org/articles/the-state-of-the-eus-rail-infrastructure, retrieved on 2 August 2025.
48. Ring, K. (2008). *Military Disaster Response: Strategy, Leadership, and Actions-Closing the Gap.*
49. Rinke, A., Marsh, S. *Malicious and targeted sabotage halts rail traffic in northern Germany*, https://www.reuters.com/world/europe/rail-northern-germany-standstill-due-technical-issue-2022-10-08/, retrieved on 2 August 2025.
50. Secureworld.io. (20 August 2024). *Cyber Attacks on Railway Systems Increase by 220%,* https://www.secureworld.io/industry-news/railway-cyber-attacks, retrieved on 2 August 2025.
51. The Record (24 March 2025). *Cyberattack hits Ukrainian state railway, disrupting online ticket system*, https://therecord.media/ukraine-railway-ukrzaliznytsia-cyberattack-online-ticket-system, retrieved on 2 August 2025.
52. Todd, S. (16 September 2025). *EU Military Mobility Package addresses long-standing weaknesses in Europe's transport networks,* https://www.ajot.com/premium/ajot-eu-military-mobility-package-addresses-long-standing-weaknesses-in-europes-transport-networks, retrieved on 2 August 2025.
53. Turgeon, T. (2024). *GPS Spoofing at Russia's Borders: What to Know. GNSS jamming*, https://www.gnssjamming.com/post/gps-spoofing-report-october-2024, retrieved on 2 August 2025.
54. Van Rensbergen, A. (2025). *Red tape and underfunding slow down EU 'military Schengen'.* The Parliament Magazine, https://www.theparliamentmagazine.eu/news/article/bureaucracy-and-underfunding-undermine-eu-military-mobility, retrieved on 2 August 2025.
55. Wiltse, J. (2012). *Before the Next Hurricane Katrina: A Strategic Approach to Enhancing Military Capabilities.*
56. https://shipwrecklog.com/log/tag/elsfleth-bridge/, retrieved on 2 August 2025.
57. https://www.iiss.org/research-paper/2025/08/the-scale-of-russian--sabotage-operations--against-europes-critical--infrastructure/, retrieved on 2 August 2025.