

DEZVOLTAREA REZILIENȚEI STRATEGICE A MOBILITĂȚII MILITARE PRINTR-O ABORDARE CUPRINZĂTOARE, LA NIVELUL ÎNTREGULUI GUVERN

Conf. univ. dr. Maria CONSTANTINESCU

Departamentul Regional de Studii
pentru Managementul Resurselor de Apărare, Brașov
DOI: 10.55535/GMR.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;

INTRODUCERE

Definită ca fiind capacitatea forțelor armate de a deplasa rapid și eficient personal, materiale și echipamente pe diverse tipuri de teren și peste granițele naționale (Damen, 2025), mobilitatea militară este o piatră de temelie a apărării contemporane, a capacității de răspuns rapid și a executării cu succes a operațiunilor militare.

Scopul acestei lucrări este de a analiza provocările contemporane ale mobilității militare în România și în Europa și de a argumenta în favoarea adoptării unei perspective cuprinzătoare, la nivelul întregului guvern. Pentru a atinge acest scop, se urmăresc următoarele *obiective de cercetare*:

- Analiza provocărilor complexe care au un impact negativ asupra mobilității militare în Europa, cu referire la probleme mai vechi, cum ar fi infrastructura fizică inadecvată și complexitatea reglementărilor, dar și amenințările hibride contemporane, inclusiv atacurile cibernetice, campaniile de dezinformare și sabotajul.
- Identificarea principalelor cerințe pentru o mobilitate militară eficientă, într-o paradigmă la nivelul întregului guvern, cu accent pe dezvoltarea infrastructurii, armonizarea reglementărilor și strategii pentru atenuarea amenințărilor hibride.

Pe baza analizei provocărilor la adresa mobilității militare și a beneficiilor unei abordări integrate, se formulează următoarea *ipoteză de cercetare*: implementarea eficientă a unei abordări cuprinzătoare, la nivelul întregului guvern, care să cuprindă eforturile coordonate între organismele guvernamentale, entitățile din sectorul privat și organizațiile internaționale, îmbunătățește semnificativ mobilitatea militară și consolidează reziliența împotriva amenințărilor hibride în Europa.

Această cercetare va utiliza o *metodologie de cercetare* calitativă, utilizând, în principal, analiza de conținut pentru a aborda obiectivele stabilite. Sursele primare de date provin din analiza literaturii academice, rapoarte oficiale și analiza experților.

ANALIZA LITERATURII

Există o mare diversitate în ceea ce privește domeniile de interes, abordările metodologice și contextele geografice din literatura de specialitate care abordează multiplele domenii interconectate ale mobilității militare, examinând aspecte

diverse ale mobilității militare strategice, rezilienței și abordărilor la nivelul întregului guvern. Mai multe lucrări fundamentale examinează cadrul mobilității strategice (Drach, 1995), analizând cei patru piloni ai mobilității strategice: transportul aerian, transportul maritim, prepoziționarea și infrastructura.

Necesitatea integrării mobilității militare în diverse sectoare guvernamentale este abordată în literatura de specialitate din perspective diferite. Din perspectiva integrării organizaționale și tehnologice, studiile identifică necesitatea unei coordonări eficiente între sistemele de mobilitate strategică și cele din teatrele de operațiuni (Kee, 1996), în vederea alinierii structurii forțelor și a finanțării mobilității (Kokko, 1993) și pentru armonizarea doctrinelor logistice militare cu reglementările din sectorul civil (Gangotena-Bustamante, 2024). Rolul inteligenței artificiale, al modelării predictive, al vehiculelor autonome și blockchain-ului este evidențiat ca factor important care va influența mobilitatea militară în viitor (Gangotena-Bustamante, ib.). În ceea ce privește recomandările de politici, examinarea literaturii de specialitate a sugerat necesitatea consolidării structurilor de comandă, a dezvoltării unor organizații integrate la nivel inter-arme pentru gestionarea cunoștințelor și a încurajării unor campanii susținute de achiziție a cunoștințelor și de stabilire a contextului (Owen, 2017; Johnson, 2007). Deși lacunele în infrastructură sunt vizibile, fricțiunile „ușoare” (cum ar fi procedurile vamale sau aprobările de transport) pot impune întârzieri la fel de semnificative. Analize recente susțin că aceste obstacole administrative, dacă nu sunt rezolvate, ar putea întârzia desfășurările transfrontaliere de trupe cu zile sau săptămâni, subminând credibilitatea strategiilor bazate pe dizlocare rapidă (Comisia Europeană, 2022; Euractiv, 2024).

Mobilitatea militară nu poate fi realizată eficient fără o infrastructură strategică rezilientă și capabilități cu dublă utilizare fiabile. Diverși autori (Drach, 1995; Gardner, 1996; Constantinescu, 2024) consideră infrastructura (porturi, aerodromuri, drumuri, căi ferate și rețele digitale) ca fiind un factor fundamental pentru proiecția și susținerea forțelor. Vulnerabilitatea acestor rețele la amenințările fizice, cibernetice și hibride este identificată ca o preocupare recurentă, mai ales că utilizările militare și civile se suprapun din ce în ce mai mult (Chung et al., 2024). Autorii subliniază necesitatea actualizării doctrinelor pentru a recunoaște infrastructura ca o componentă centrală a mobilității (Gardner, 1996), rolul crucial al investițiilor sporite în coridoarele de transport cu dublă utilizare (civil-militară) (Howell, 2020) și adoptarea unor standardelor uniforme în domeniu pentru a asigura compatibilitatea și reziliența (Gardner, 1996). Unele studii raportează că integrarea activelor comerciale, cum ar fi Flota Aeriană a Rezervei Civile și Acordul

Voluntar de Transport Intermodal Maritim, reprezintă atât un punct forte, cât și o vulnerabilitate, din cauza diminuării capacităților excedentare și a deficitului de forță de muncă în sectorul comercial (Gallagher, 2021). Literatura de specialitate identifică în mod constant blocajele fizice drept vulnerabilități critice în ceea ce privește infrastructura și rețelele de transport critice. Rapoartele Curții de Conturi Europene și ale Comisiei Europene notează că podurile care nu pot susține vehicule grele, rețelele feroviare cu ecartamente incompatibile și porturile care nu au o capacitate suficientă constrâng implementarea rapidă a măsurilor de îmbunătățire a mobilității militare (Comisia Europeană, 2022; Curtea de Conturi Europeană, 2023). Deși inițiativele UE în domeniul transporturilor au început să acorde prioritate coridoarelor de infrastructură cu dublă utilizare, finanțarea și termenele de implementare rămân insuficiente pentru a îndeplini cerințele strategice. Aceste chestiuni sunt ilustrate de auditurile independente, care subliniază că în ciuda atenției politice semnificative acordate subiectului, modernizarea infrastructurii continuă să rămână în urma nevoilor operaționale (Barigazzi, Herszenhorn, 2025).

Literatura academică și documentele oficiale acordă o atenție deosebită guvernantei, studiile subliniind faptul că exercițiile civil-militare de rutină sunt esențiale pentru depășirea separărilor instituționale și construirea unei culturi comune de pregătire (Kraśniewski, 2023; NATO, 2023). Cu toate acestea, barierele persistă, deoarece diferite agenții operează adesea cu diverse grade de toleranță a riscului, cicluri bugetare și regimuri de reglementare divergente, generând fricțiuni în situațiile care necesită rapiditate de decizie și reacție (Agenția Europeană de Apărare, 2022). Mecanismele necesare pentru o coordonare eficientă în domeniul mobilității militare sunt abordate prin intermediul mai multor studii, care evidențiază limitele abordărilor izolate și pledează pentru cadre integrate care valorifică capacitățile mai multor agenții guvernamentale, sectoare civile și parteneri internaționali. Unii autori (Burton, 2007; Manwaring, 2006) recomandă abordări interguvernamentale și multidimensionale, inclusiv modificări ale structurilor de comandă și stabilirea unor mecanisme cuprinzătoare de coordonare a politicilor, iar alții subliniază rolul agențiilor civile și al parteneriatelor public-private în sprijinirea operațiunilor militare, în special în logistică și infrastructură (Mars, 2016; Jacuch, 2020) și în spațiul cibernetic (Myers, 2011; Constantinescu, 2025), subliniind necesitatea unei guvernante integrate și a schimbului de informații în domeniul apărării și transporturilor.

Răspunsul și pregătirea la crize sunt esențiale pentru reziliența strategică a mobilității militare, iar mai multe studii (Ring, 2008; Wiltse, 2012) critică lipsa unor strategii militare clare și coordonate pentru răspunsul la dezastre și pledează

pentru soluții care să integreze componentele forțelor armate active și de rezervă cu structurile civile, punând accent pe planificarea anticipată, colaborarea inter-ministerială și inter-guvernamentală și un răspuns flexibil la situațiile neprevăzute interne sau internaționale. Importanța pregătirii civile și a rezilienței sectorului este subliniată, în special pentru desfășurarea rapidă a forțelor în Europa și consolidarea Flancului Estic al NATO (Jacuch, 2020; Giurgiu și colab., 2024).

O serie de articole mai recente explorează vulnerabilitatea mobilității la amenințările cibernetice și hibride, concluzionând că reziliența mobilității militare trebuie să includă securitatea cibernetică, integritatea informațiilor și pregătirea societății, ceea ce presupune o abordare la nivelul întregului guvern, implicând nu doar structurile de forță, ci și agenții specializate în combaterea amenințărilor cibernetice și nu în ultimul rând operatorii privați de infrastructură critică (Giegerich, 2023; NATO, 2023).

PROVOCĂRI ACTUALE PENTRU MOBILITATEA MILITARĂ

Mediul operațional actual este caracterizat de implicațiile încă nesoluționate ale unor provocări mai vechi (cum ar fi nivelul insuficient al investițiilor în rețelele de transport cu dublă utilizare sau obstacolele juridice), dar și de amenințări din ce în ce mai complexe și multi-fațetate, care afectează dislocarea rapidă și sigură a forțelor și a sprijinului logistic.

În ultimii cinci ani s-a înregistrat o creștere a atacurilor cibernetice asupra sistemelor feroviare la nivel global, indicând un interes crescut din partea unor actori statali și ne-statali pentru perturbarea operațiunilor feroviare. Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA) a raportat în mod constant despre profilul de risc cibernetic în evoluție al sectorului transporturilor, semnalând o intensificare a atacurilor împotriva infrastructurii de transport europene, inclusiv aeroporturi, porturi și căi ferate. Agenția subliniază că amenințările de tip ransomware sunt deosebit de răspândite, vizând sistemele IT care susțin diverse aspecte operaționale ale transportului feroviar. Natura transfrontalieră a amenințărilor cibernetice înseamnă că un atac într-o singură țară poate avea implicații mai ample pentru rețelele europene interconectate, afectând mobilitatea militară generală și capacitățile logistice (ENISA, 2023). Vulnerabilitățile exploatate vizează adesea sisteme IT legate de serviciile pentru pasageri, bilete și aplicații mobile, ransomware-ul fiind un vector principal de amenințare, reprezentând 45% din atacurile cibernetice din sectorul feroviar (Secureworld.io., 2024, Rail Journal, 2023).

În 2023, Polonia s-a confruntat cu intruziuni cibernetice în sistemele de comunicații feroviare, provocând opriri de urgență ale trenurilor și întârzieri semnificative, ceea ce evidențiază vulnerabilitatea infrastructurii critice de comunicații (Agenția pentru Securitatea Cibernetică și Infrastructură, 2023). În 2025, serviciul feroviar de stat din Ucraina a suferit un atac cibernetic puternic care a dezactivat sistemul său de bilete online, provocând perturbări semnificative și ducând la cozi lungi în stații, deoarece pasagerii nu au putut cumpăra bilete online sau prin intermediul aplicațiilor mobile (Reuters, 2025; The Record, 2025).

Atacurile cibernetice reprezintă o amenințare majoră din perspectiva mobilității militare, deoarece sunt relativ ușor de pus în aplicare, fără costuri semnificative, având însă un impact potențial major asupra dislocării echipamentelor și personalului militar. Sistemele feroviare, ca principală cale de transport pentru echipamente grele și dislocarea masivă de forțe, sunt deosebit de vulnerabile. Atacurile asupra sistemelor tehnologice operaționale, cum ar fi sistemele de semnalizare, comutare și control al traficului, pot duce la întârzieri generalizate, redirectionare sau chiar opriri complete ale liniilor feroviare. Un atac cibernetic care manipulează sistemele de semnalizare ar putea provoca oprirea, ciocnirea sau direcționarea greșită a trenurilor, generând blocaje și împiedicând desfășurarea la timp a forțelor.

Atacurile cibernetice pot paraliza sistemele de planificare și execuție logistică, cu efecte grave, deoarece logistica militară modernă se bazează, în mare măsură, pe sisteme IT sofisticate pentru planificare, gestionarea stocurilor, optimizarea rutelor și coordonarea lanțului de aprovizionare. Un atac ransomware sau un acces neautorizat la datele din aceste sisteme le poate face inoperabile, afectând cunoașterea situației și generând imposibilitatea de a urmări activele și întârzieri semnificative în eforturile de re-aprovizionare.

Atacurile cibernetice nu vizează doar perturbarea activității, fiind utilizate și pentru colectarea de informații și pentru supraveghere, cu impact indirect asupra mobilității militare prin compromiterea securității operaționale. Adversarii pot exploata vulnerabilitățile rețelelor de transport pentru a monitoriza mișcarea convoaielor militare, a echipamentelor și a personalului. Prin obținerea accesului la sistemele de programare, datele GPS sau chiar la rețelele Wi-Fi publice utilizate de personalul militar, adversarii pot deduce mișcările trupelor, modelele de dislocare și vulnerabilitățile logistice (Federal News Network, 2025).

Atacurile cibernetice reușite asupra infrastructurii critice pot eroda încrederea publicului și a militarilor în siguranța și fiabilitatea sistemelor de transport, cu consecințe psihologice și operaționale semnificative. Comandanții militari ar putea ezita să se bazeze pe infrastructura civilă pentru acțiuni critice, ceea ce

ar putea duce la o planificare logistică mai lentă, mai precaută și mai puțin eficientă. Pierderea încrederii publice poate duce, de asemenea, la tulburări civile sau la mișcări de opoziție față de convoaiele militare, complicând operațiunile care necesită cooperare civilă sau acces la rute publice.

Răspunsul la atacurile cibernetice asupra infrastructurii de transport și acțiunile de remediere a efectelor acestora pot impune presiuni economice și un consum de resurse semnificativ, deoarece costurile asociate cu repunerea în funcțiune a sistemului, evaluarea daunelor, măsurile sporite de securitate cibernetică și potențialele răspunderi legale pot devia fonduri și personal de la alte priorități militare critice. Mai mult, perturbările prelungite pot duce la pierderi economice pentru industriile civile, ceea ce, la rândul său, poate afecta stabilitatea economică necesară pentru sprijinirea operațiunilor militare. Necesitatea de a investi masiv în securitatea cibernetică pentru infrastructura civilă cu dublă utilizare care stă la baza mobilității militare, cum ar fi rețelele feroviare, porturile comerciale și aeroporturile, rămâne o provocare importantă (Industrial Cyber, 2025). Un alt factor care sporește gravitatea amenințării este că aceste atacuri cibernetice vizează, de obicei, companii civile și private, care pot să nu aibă interesul și/sau să nu dispună de resursele necesare pentru a investi suficient în creșterea nivelului lor de securitate cibernetică, ceea ce le face ținte mai vulnerabile pentru atacatori comparativ cu unitățile militare.

Campaniile de dezinformare pot reprezenta o amenințare semnificativă la adresa mobilității militare în Europa, în special în contextul tensiunilor geopolitice accentuate din Europa de Est și regiunea baltică, prin subminarea integrității comunicațiilor strategice, destabilizând încrederea publică și complicând coordonarea dintre națiunile aliate. Acestea vizează, adesea, publicul și autoritățile civile pentru a eroda încrederea în operațiunile militare și instituțiile guvernamentale, iar narațiunile false despre acțiunile militare, mișcările de trupe sau incidentele care implică infrastructura pot duce la tulburări ale ordinii publice, complicând astfel comanda și controlul în timpul crizelor. Un exemplu recent îl constituie campania desfășurată pe rețelele de socializare după alegerile din 2025, prin care s-au răspândit informații false care susțineau că România va trimite trupe în Ucraina, rezultatul fiind că până și convoaiele militare obișnuite sau exercițiile militare planificate au fost privite cu extremă suspiciune de către populație, considerate „dovezi” în sprijinul respectivei narațiuni (Inforadar, 2025). Ca urmare a unor astfel de campanii de dezinformare, circulația personalului și a materialelor militare (NATO sau naționale) pe căile ferate și pe drumuri poate genera proteste și, în cazul unei operațiuni militare, poate

duce chiar la proteste civile, distrăgând atenția autorităților și întârziind dislocarea de forțe. Adversarii pot folosi dezinformarea pentru a distorsiona sau ascunde evoluțiile reale ale situației, generând confuzie în rândul factorilor de decizie, iar informațiile false despre daunele aduse infrastructurii critice sau amplasarea trupelor pot induce în eroare comandanții, provocând întârzieri sau decizii greșite de alocare a resurselor.

Campaniile de dezinformare pot submina și percepția privind siguranța infrastructurii de transport, influențând mobilitatea militară. De exemplu, zvonurile despre rute feroviare nesigure sau atacuri iminente asupra coridoarelor cheie de transport ar putea duce la prudență inutilă, redirectionarea sau închiderea liniilor de aprovizionare esențiale sau la aglomerarea rutelor rutiere importante pentru transportul militar, prin supraaglomerarea cu populația civilă panicată, care încearcă să fugă din anumite zone.

În ultimii ani, eforturile de dezinformare care vizează Europa s-au intensificat, în special în jurul conflictului Rusia-Ucraina. De exemplu, au circulat periodic afirmații false despre distrugerea infrastructurii militare cheie sau despre retragerile de trupe, afectând planificarea strategică și percepția publică (Serviciul European de Acțiune Externă, 2024). În mod similar, au fost folosite imagini din satelit manipulate și videoclipurile false pentru a exagera sau a inventa daune aduse nodurilor critice de transport, influențând procesul decizional și întârziind reacția la situații de urgență sau operațiunile militare.

Sabotajul fizic și acțiunile sub acoperire pot provoca daune semnificative infrastructurii esențiale pentru mobilitatea militară, inclusiv drumuri, poduri, porturi și facilitățile de aprovizionare cu combustibil și pot împiedica semnificativ operațiunile logistice și capacitatea de dislocare rapidă. O caracteristică specifică a acestui tip de instrument de război hibrid este dificultatea semnificativă de a demonstra că o anumită acțiune a fost un sabotaj deliberat și de a o atribui unei anumite surse/adversar. Această caracteristică face ca acest tip de atacuri să fie deosebit de dificil de contracarat, deoarece vizează de obicei infrastructura civilă și pot imita incidente naturale. Actorii rău intenționați pot valorifica lacunele legale și recruta online cetățeni din țări terțe pentru a executa aceste operațiuni, complicând atribuirea și responsabilitatea.

Un incident de acest gen, larg mediatizat, a fost sabotajul feroviar din Germania din 2022, când cablurile cruciale pentru sistemele de comunicații feroviare au fost deteriorate intenționat, ceea ce a dus la o perturbare semnificativă a serviciilor feroviare din nordul Germaniei, izolând infrastructura militară și civilă cheie. (Rinke,

Marsh, 2022). În 2024, podul feroviar de la Elsfleth-Orth din Germania a suferit daune ireparabile după ce a fost lovit de o barjă, provocând repercusiuni economice grave pentru porturile din regiune (Boote Magazin, 2025). Acest pod este crucial însă și din perspectiva mobilității militare, deoarece face parte din ruta care leagă portul Nordenham, Germania, de Miesau, care găzduiește depozitul de muniții al Centrului de Sprijin Logistic al Teatrului de Operațiuni din Europa, o facilitate esențială pentru NATO. Un pod temporar a fost dat în folosință în aprilie 2024, dar a fost lovit din nou de o barjă-cisternă în iulie 2024 (Shipwrecklog, 2024). Nu există nicio posibilitate de a dovedi oficial că aceste incidente au fost sabotaj și nu doar efectul slabei pregătiri a echipajelor barjelor, însă un raport recent al Institutului Internațional pentru Studii de Securitate a identificat o creștere semnificativă a unor astfel de incidente în Europa după 2022, de la 2 evenimente în 2018 și 2019 la 12 evenimente în 2022, 9 evenimente în 2023 și un vârf de 33 de evenimente, distribuite în toate sectoarele - Apă, Comunicații, Armată și Transporturi în 2024 (Edwards, Seidenstein, 2025).

Limitările infrastructurii de transport din Europa reprezintă una dintre principalele provocări la adresa mobilității militare, deoarece, în ciuda faptului că Europa este conectată printr-o infrastructură de transport extinsă, aceasta nu satisface cerințele pentru mișcări militare rapide și la scară largă. După căderea URSS, sectorul transporturilor a fost considerat aproape exclusiv o chestiune civilă, ceea ce a dus la decenii de investiții insuficiente, iar lipsa de interes privind îndeplinirea standardelor de dublă utilizare a generat vulnerabilități critice.

Multe drumuri și poduri europene nu sunt proiectate să reziste greutății și dimensiunilor echipamentelor militare grele moderne, ceea ce duce la întârzieri semnificative și alegerea de rute alternative, cu impact direct asupra vitezei și eficienței transporturilor militare. Aceste limitări ale infrastructurii generează un timp inacceptabil de mare pentru transportul echipamentelor militare și a trupelor din Europa de Vest către Est (săptămâni și, în unele cazuri, chiar luni de zile), în cazul necesității unui răspuns rapid (Todd, 2025). Un exemplu semnificativ vine din Germania, unde 4.500 din cele 40.000 de poduri sunt într-o stare considerată insuficientă sau deficientă din perspectiva asigurării mobilității militare, acestea nefiind capabile să suporte greutatea vehiculelor militare (Hartmann, 2024).

Situația rețelilor feroviare europene prezintă, de asemenea, provocări substanțiale. O evaluare recentă realizată de Deutsche Bahn a constatat că 23% din cei 33.000 de kilometri de cale ferată ai Germaniei se aflau într-o „*stare extrem de proastă*”, alături de 48% din centrele de control al semnalizării, 42% din trecerile

la nivel cu calea ferată și peste 25% din macazurile de cale ferată, contribuind la o medie a întârzierii unuia din trei trenuri în 2022 (Hartmann, 2024). Un alt studiu a concluzionat că, în ciuda unor progrese și a investițiilor sporite, sistemul feroviar european rămâne fragmentat, porțiuni semnificative ale rețelelor neîndeplinind cerințele stabilite în politica de infrastructură de bază a UE, Rețeaua Transeuropeană de Transport (TEN-T). De exemplu, mai puțin de 20% din coridoarele TEN-T sunt echipate cu Sistemul European de Control al Trenurilor (ETCS), iar viteza medie a liniilor feroviare rămâne adesea scăzută, opt state membre atingând o viteză maximă de doar 80 km/h pe majoritatea liniilor lor, mult sub obiectivul de 160 km/h pentru TEN-T (Rico, Heyl, 2025).

Căile navigabile interioare, inclusiv canalele și râurile, joacă, de asemenea, un rol în mobilitatea militară, dar infrastructura lor îmbătrânită prezintă provocări. În cazul Germaniei, ecluzele au în medie, o vechime de 65 de ani, ceea ce duce la defecțiuni frecvente ale componentelor și la închiderea unor secțiuni întregi de căi navigabile, adesea fără rute alternative (Hartmann, 2024).

Reziliența mobilității militare în Europa este afectată de obstacolele birocratice și de reglementările naționale fragmentate, care afectează semnificativ mișcarea în timp util a forțelor militare peste granițele europene. Un raport al Curții de Conturi Europene (Curtea de Conturi Europeană, 2025) a identificat probleme generate de proceduri fragmentate și de lipsa unui efort coordonat la nivelul UE, deoarece echipamentele militare se confruntă adesea cu restricții la frontierele naționale din cauza depășirii limitelor de greutate locale sau a problemelor de infrastructură (cum ar fi podurile), care nu sunt proiectată pentru transporturi grele. Un alt obstacol este legat de progresul lent în ceea ce privește „*Schengenul militar*”, deoarece primul Plan de acțiune privind mobilitatea militară al UE (2018) a înregistrat întârzieri și, în ciuda unui plan ulterior (2021), care a alocat 1,69 miliarde de euro în acest scop, există încă un deficit semnificativ de finanțare. O altă problemă identificată este lipsa persistentă a unor investiții transfrontaliere coordonate, deoarece națiunile tind să negligeze infrastructura de-a lungul frontierelor proprii, considerând-o, adesea, ca fiind responsabilitatea țării vecine. O provocare semnificativă este, de asemenea, absența unei coordonări centralizate și a unor mecanisme eficiente de partajare a informațiilor între statele membre ale UE, ceea ce generează ineficiențe în planificarea și executarea mișcărilor militare și face dificilă implementarea planurilor de mobilitate militară într-un mod ținut (Van Rensbergen, 2025).

O altă provocare pentru eforturile de creștere a rezilienței mobilității militare este modul în care acest domeniu va fi afectat de *tehnologiile emergente*, cum ar fi

inteligența artificială (IA), dronele și sistemele autonome, care sunt din ce în ce mai mult utilizate de adversari și pot perturba modelele logistice și operaționale tradiționale. Conflictul din Ucraina, din 2022, a oferit numeroase lecții cu privire la impactul profund al dronelor asupra operațiunilor de luptă la sol, prin atacuri directe asupra convoaielor logistice și rutelor de aprovizionare (Hollenbeck, 2025) și prin utilizarea dronelor maritime cu costuri reduse pentru operațiuni navale, așa cum s-a văzut în cazul flotei rusești de la Marea Neagră (Navy Lookout, 2025), deschizând calea pentru utilizarea lor împotriva transportului naval. Această utilizare pe scară largă a dronelor de către adversari poate crea un spațiu logistic extrem de contestat, forțând transporturile militare să se adapteze la supravegherea constantă și la potențialele interdicții, încetinind, astfel, dislocarea forțelor și crescând riscurile pentru personal și echipamente.

Utilizarea IA și a sistemelor autonome de către adversari poate crește complexitatea și genera noi vulnerabilități în ceea ce privește mobilitatea militară. În timp ce forțele armate explorează inteligența artificială pentru optimizarea propriei logistici și a managementului lanțului de aprovizionare, adversarii pot exploata aceste tehnologii în scopuri disruptive. De exemplu, inteligența artificială poate fi utilizată pentru a analiza doctrinele și mișcările inamice și a prognoza răspunsuri, permițând o identificare mai precisă a nodurilor logistice și a coridoarelor de mișcare. Amenințarea „*otrăvirii datelor*” ar putea, de asemenea, compromite integritatea planificării logistice și a luării deciziilor bazate pe inteligență artificială, ducând la ineficiențe sau alocări greșite de resurse. Vehiculele terestre autonome, deși benefice pentru reducerea riscurilor în operațiunile cu pericol ridicat, reprezintă, de asemenea, un nou vector de atac dacă sunt compromise sau contracarate de sistemele autonome ale adversarilor, perturbând potențial eforturile critice de reprovizionare și creând puncte de blocare în mobilitatea militară (Lopez, 2024). Progresele înregistrate în domeniul tehnologiei cuantice au potențialul de a sparge criptarea asimetrică și de a permite apariția unor sisteme de navigație rezistente la perturbările GPS, complicând și mai mult mobilitatea și logistica militară prin contestarea avantajelor tehnologice existente (Kirichenko, 2025). *Războiul electromagnetic* este un alt factor care trebuie luat în considerare în construirea rezilienței, deoarece vizează direct sistemele critice de comunicații și navigație, reprezentând o amenințare semnificativă pentru mobilitatea militară. O vulnerabilitate principală constă în Sistemul de Poziționare Globală (GPS), care este foarte sensibil la bruiaj și falsificare de semnale, putând dezorienta forțele și perturbând convoaiele logistice. Războiul electromagnetic este deja utilizat

de ambele părți combatante în Ucraina, având impact atât asupra sistemelor militare, cât și asupra celor civile dependente de GPS (Turgeon, 2024). Un incident recent de acest tip a evidențiat acest risc, când sistemul de navigație al unui avion care o transporta pe Ursula von der Leyen în Bulgaria a fost perturbat din cauza unei suspiciuni de interferență rusească, piloții fiind nevoiți să aterizeze avionul folosind hărți pe hârtie (Davies, Vernon, 2025). Războiul electromagnetic poate oferi adversarilor informații critice despre mișcările de trupe și tacticile militare, permițând o identificare mai eficientă a eventualelor punctelor de blocare logistică sau a convoaielor vulnerabile (NATO, 2023).

CONCLUZII ȘI RECOMANDĂRI

Rezultatele cercetării confirmă ipoteza conform căreia adoptarea și implementarea eficientă a unei abordări cuprinzătoare la nivelul întregului guvern sunt indispensabile pentru sporirea semnificativă a mobilității militare și întărirea rezilienței împotriva acestor amenințări în continuă evoluție. Aceasta necesită o implicare coordonată a diverselor ministere guvernamentale – inclusiv apărarea, internele, transporturile, afacerile externe și finanțele –, precum și o colaborare robustă cu părțile interesate din sectorul privat care gestionează infrastructura critică de transport. Această strategie integrată depășește eforturile departamentale izolate, recunoscând că reziliența mobilității militare este intrinsec legată de pregătirea civilă, de mediile de reglementare armonizate și de o înțelegere comună a imperativelor de securitate în întreaga societate. Lucrarea subliniază faptul că succesul mobilității militare depinde de un angajament politic și militar la nivel înalt, de o planificare eficientă care integrează perfect logistica civilă și militară și de aplicarea consecventă a cadrelor abordării cuprinzătoare în toate națiunile care oferă acest sprijin. În cele din urmă, promovarea mobilității militare printr-o abordare cuprinzătoare este esențială pentru asigurarea pregătirii, consolidarea descurajării și obținerea succesului operațional într-un mediu de securitate global din ce în ce mai complex și imprevizibil.

REFERINȚE BIBLIOGRAFICE:

1. Barigazzi, J., Herszenhorn, D.M. (2025). EU military mobility plan hampered by delays, lack of funding. Politico, <https://www.politico.eu>, accesat la 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/>, accesat la 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/>, accesat la 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>, accesat la 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>, accesat la 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>, accesat la 2 august 2025.
13. Euractiv (10 martie 2024). *EU struggles with military transport bureaucracy despite action plan*, <https://www.euractiv.com>, accesat la 22 august 2025.
14. European Commission (2025), https://transport.ec.europa.eu/news-events/news/commission-supports-military-mobility-projects-eu807-million-2024-01-24_en, accesat la 2 august 2025.
15. European Commission (2022). *Action Plan on Military Mobility 2.0 [JOINT(2022) 49 final]*. Brussels: European Commission.
16. European Commission. *Military mobility*, https://transport.ec.europa.eu/transport-themes/military-mobility_en, accesat la 22 august 2025.
17. 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, accesat la 2 august 2025.
18. 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.
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/>, accesat la 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/>, accesat la 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 regiones inestables*, în *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*, în *Survival*, 65(4), pp. 121-140.
26. Giurgiu, T., Virca, I., Noja, G. (2024). *Military Mobility in the Vision of NATO and European Union*, în revista *Romanian Military Thinking*.
27. Hartmann, J. (2024). *Military Mobility*. DGAP, <https://dgap.org/en/research/publications/military-mobility>, accesat la 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/>, accesat la 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>, accesat la 18 ianuarie 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-sprrijinului-pentru-ucraina, accesat la 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>, accesat la 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/>, accesat la 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 challenge*, *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/>, accesat la 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, accesat la 2 august 2025.
42. NATO (2023). *Resilience and civil preparedness*. Brussels: NATO Headquarters, <https://www.nato.int>, accesat la 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/>, accesat la 2 august 2025.
44. Owen (2017). *US Air Force Airlift and the Army's Relevance*. Parameters
45. Rail Journal (22 martie 2023). *EU cybersecurity agency reports on threat to rail*, <https://www.railjournal.com/technology/eu-cybersecurity-agency-reports-on-threat-to-rail/>, accesat la 2 august 2025.
46. Reuters (24 martie 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/>, accesat la 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>, accesat la 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/>, accesat la 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>, accesat la 2 august 2025.
51. The Record (24 martie 2025). *Cyberattack hits Ukrainian state railway, disrupting online ticket system*, <https://therecord.media/ukraine-railway-ukrзалізниця-cyberattack-online-ticket-system>, accesat la 2 august 2025.
52. Todd, S. (16 septembrie 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>, accesat la 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>, accesat la 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, accesat la 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/>, accesat la 2 august 2025.
57. <https://www.iiss.org/research-paper/2025/08/the-scale-of-russian--sabotage-operations--against-europes-critical--infrastructure/>, accesat la 2 august 2025.