

TEHNOLOGIILE EMERGENTE ȘI FLANCUL ESTIC AL NATO: PERSPECTIVE PENTRU ROMÂNIA

Căpitan Cătălin-Costel DUMITRIU

Academia Forțelor Terestre „Nicolae Bălcescu”, Sibiu

DOI: 10.55535/GMR.2025.3.17

This article examines how emerging technologies are reshaping security and defence on NATO's Eastern Flank, with particular attention to Romania. Building on a five-dimension analytical framework – command and control (C2), intelligence and situational awareness (ISR), decision speed, operational agility, and systemic resilience – originally distilled from Ukraine's experience, the study adapts and applies this grid to Romanian realities. Methodologically, it is qualitative and exploratory, triangulating specialised literature, NATO doctrinal documents, and close observation of recent developments in the Russia-Ukraine war. Findings reveal vulnerabilities in C2 infrastructure, logistics, and cyber resilience, alongside opportunities stemming from the accelerated integration of autonomous systems, digital infrastructures, and AI-assisted decision processes. The conclusions underscore the strategic salience of technological emergence for strengthening deterrence and defence, enhancing interoperability, and consolidating Romania's position as a pivotal state within NATO's regional security architecture.

Keywords: emerging technologies; Eastern Flank; decision speed; operational agility; resilience;

INTRODUCERE

Agresiunea militară declanșată de Federația Rusă împotriva Ucrainei în februarie 2022 a reprezentat un veritabil catalizator pentru reevaluarea paradigmelor tradiționale de securitate și apărare la nivel european și euroatlantic. Spre deosebire de conflictele convenționale din trecut, acest război a demonstrat, în timp real, că tehnologiile emergente nu constituie doar un element de sprijin marginal, ci un vector determinant al rezilienței operaționale și al capacității de adaptare strategică. Utilizarea extensivă a sistemelor aeriene fără pilot, a arhitecturilor de comunicații securizate, a platformelor de inteligență artificială dedicate sprijinirii procesului decizional și a instrumentelor de tip open-source intelligence a validat ipoteza conform căreia inovația tehnologică poate modifica semnificativ balanța de putere, chiar și în condițiile unei asimetrii evidente de resurse.

Pentru statele aflate pe flancul estic al NATO, inclusiv România, conflictul actual constituie un laborator strategic cu implicații majore. Proximitatea geografică, vulnerabilitatea structurală a regiunii Mării Negre și rolul de stat pivot în arhitectura defensivă aliată conferă României o poziție de expunere accentuată, dar și de responsabilitate strategică sporită. În aceste condiții, devine imperativ ca lecțiile desprinse din experiența Ucrainei să fie transpuse în politici de apărare coerente, în doctrină modernizată și în practici operaționale adaptate specificului național, dar perfect compatibile cu standardele și mecanismele NATO.

Scopul prezentului studiu este de a analiza impactul tehnologiilor emergente asupra securității și apărării pe flancul estic al NATO, cu o focalizare specială asupra României. În acest sens, se utilizează un cadru analitic multidimensional, dezvoltat anterior în literatura de specialitate, care cuprinde cinci dimensiuni esențiale pentru succesul operațional: (1) comandă și control; (2) intelligence și conștientizare situațională; (3) viteză decizională; (4) agilitate operațională și (5) reziliență sistemică. Acest cadru permite atât o evaluare comprehensivă a gradului de pregătire actual, cât și identificarea unor direcții de dezvoltare strategică pentru viitor.

Metodologia adoptată este de tip calitativ și exploratoriu, bazată pe triangularea mai multor surse: analiza comparativă a literaturii de specialitate, evaluarea documentelor doctrinare NATO (Strategic Concept 2022, NATO Warfighting

Capstone Concept 2021), precum și examinarea critică a experiențelor recente generate de conflictul ucrainean. Această abordare metodologică conferă studiului o ancorare solidă, asigurând atât validitatea teoretică, precum și relevanța practică a rezultatelor obținute.

Relevanța cercetării rezidă atât în plan teoretic, prin contribuția la consolidarea literaturii referitoare la revoluția tehnologică în domeniul militar și la evoluțiile contemporane ale artei războiului, cât și în plan practic, prin formularea unor recomandări concrete destinate întăririi rezilienței instituționale, modernizării doctrinei și consolidării interoperabilității României în cadrul NATO.

Într-o epocă definită de volatilitate strategică, incertitudine și complexitate sistemică, emergența noilor tehnologii se înscrie într-un proces mai amplu de transformare paradigmatică a războiului, pe care literatura de specialitate îl asociază cu așa-numita *revoluție în afacerile militare (RMA)*. Dacă, în trecut, schimbările tehnologice se manifestau preponderent prin introducerea unor platforme de luptă superioare din punct de vedere tehnic, realitatea contemporană indică o transgresare a frontierelor tradiționale ale conflictului. Astăzi, inovația nu se reduce la simple achiziții de echipamente, ci presupune integrarea simultană a infrastructurilor digitale, a algoritmilor de inteligență artificială, a instrumentelor de analiză big data și a mecanismelor de reziliență cibernetică, toate convergând spre o redefinire a ecuației dintre putere militară și competitivitate strategică.

Această mutație epistemologică obligă statele membre ale NATO, iar în mod particular România, să depășească logica incrementală a modernizării și să adopte o abordare proactivă, anticipativă și sistemică. Consolidarea securității naționale pe flancul estic nu mai poate fi concepută exclusiv în termeni de volum al forțelor sau de capabilități convenționale, ci trebuie să se fundamenteze pe interoperabilitate digitală, arhitecturi de comandă descentralizată și culturi organizaționale capabile să încurajeze inovarea rapidă.

Astfel, analiza de față își propune să contribuie la instituționalizarea unei dezbateri academice și doctrinare cu privire la modul în care România poate valorifica experiențele recente din Ucraina pentru a-și configura un profil strategic robust. În egală măsură, articolul se înscrie în direcțiile promovate de documentele de planificare strategică ale NATO, care subliniază importanța emergenței tehnologice nu doar ca oportunitate, ci și ca determinant critic al supraviețuirii instituționale și al eficienței operaționale. În această cheie de lectură, flancul estic devine nu doar un spațiu de apărare, ci și un laborator de testare a adaptabilității alianței la noile condiții ale conflictului contemporan. În consecință, prezentul studiu aspiră

să constituie un reper analitic pentru înțelegerea modului în care România și NATO pot transforma emergența tehnologică într-un vector de securitate și stabilitate durabilă.

TEHNOLOGIILE EMERGENTE ÎN APĂRARE: CADRUL ANALITIC

În analiza metamorfozelor războiului contemporan, devine evident că tehnologiile emergente funcționează nu ca simple multiplicatoare de putere, ci ca determinante structurale ale arhitecturii operaționale. Dincolo de dimensiunea strict tehnică, acestea configurează o veritabilă mutație epistemologică a războiului, în care cunoașterea, viteza și adaptabilitatea devin vectori definitorii ai eficacității militare. În acest context, propunerea unui cadru analitic integrator, articulat pe cinci dimensiuni – comandă și control (C2), intelligence și conștientizare situațională (ISR), viteză decizională, agilitate operațională și reziliență sistemică – permite nu doar o înțelegere comprehensivă a fenomenului, ci și o operaționalizare a teoriei RMA într-o cheie aplicativă, adaptată specificului NATO și al României.

Comandă și control (C2)

Dimensiunea C2 transcende logica tradițională a lanțurilor ierarhice rigide și se reconfigurează prin emergența ecologiilor informaționale distribuite, caracterizate prin redundanță, reziliență și interconectivitate permanentă. Dacă, în conflictele anterioare, accentul era pus pe transmiterea verticală a ordinelor, războiul contemporan demonstrează prevalența unor arhitecturi rețelizate, adaptative și descentralizate.

Exemple precum utilizarea rețelei Starlink în Ucraina au arătat că accesul la infrastructuri de comunicații reziliente și dispersate poate transforma radical dinamica conflictului, asigurând continuitatea C2 chiar și în condițiile distrugerii infrastructurilor convenționale (Kofman, Lee, 2022, pp. 10-18). Inteligența artificială contribuie la fuziunea datelor multisursă și la generarea de tablouri operaționale comune (Common Operational Picture), facilitând sincronizarea simultană a actorilor distribuiți (Alberts, Garstka, Stein, 1999, pp. 45-62).

Pentru România, provocarea constă în integrarea infrastructurilor naționale de C2 în meta-sistemele aliate NATO. Absența unei modernizări accelerate riscă să transforme statul într-un „*nod slab*” al rețelei. Soluția constă în digitalizarea integrală a lanțurilor decizionale, în implementarea arhitecturilor de cloud securizat și în cultivarea unei doctrine de conducere misionară (mission command) capabile să funcționeze în paralel cu sistemele automatizate (NATO, 2021, p. 27).

Intelligence și conștientizare situațională (ISR)

ISR devine centrul de gravitație al conflictelor moderne, în care superioritatea informațională precede și condiționează superioritatea operațională. Extinderea tehnologiilor emergente a creat premisele unei omnividențe operaționale, în care frontierele dintre teatrele de operații, spațiul cibernetic și cel cognitiv se estompează.

Astăzi, rețelele de senzori distribuiți, dronele comerciale militarizate, sateliții de observare privată și instrumentele OSINT configurează un spațiu ISR mult mai democratic, în care chiar și actori non-statali pot obține capacități similare celor ale marilor puteri (Horowitz, 2018, pp. 40-45). Aceasta subminează vechiul monopol informațional al statelor și impune noi mecanisme de filtrare, validare și integrare a datelor.

În regiunea Mării Negre, România se află într-o zonă contestată, unde războiul electronic rusesc și capacitățile de negare a accesului (A2/AD) limitează libertatea ISR (Mareș, 2022, pp. 5-19). Totuși, participarea la mecanismele NATO de partajare a informațiilor, cum este NATO Intelligence Fusion Centre, poate compensa deficitele naționale. Astfel, România trebuie să investească în fuziunea ISR multisursă și să contribuie activ la construirea unei imagini operaționale comune regionale (Regional COP).

Viteză decizională

Într-o eră a conflictelor „*hiper-timpului*”, avantajul strategic aparține actorului capabil să comprime ciclurile decizionale OODA prin intermediul instrumentelor digitale și al inteligenței artificiale. Dacă, în secolul XX, câștigul era dat de masă și volum, în prezent, decisiv este ritmul cognitiv, adică viteza cu care informația este transformată în acțiune.

Sistemele predictive, analiza big data și instrumentele de suport decizional bazate pe AI transformă decizia într-un proces simultan, distribuit și anticipativ. Exemplele ucrainene arată că viteza decizională poate compensa chiar și inferioritatea numerică sau materială (Watling, Reynolds, 2022, pp. 42-51).

Pentru România, provocarea este dublă: tehnologică (integrarea sistemelor de suport decizional în C2) și culturală (adoptarea unei culturi organizaționale adaptative, care să reducă inerția birocratică). În NATO, viteza decizională este un criteriu de interoperabilitate critic: un partener care reacționează lent poate perturba sincronizarea întregii alianțe (NATO, 2022, p. 14).

Agilitate operațională

Agilitatea desemnează capacitatea forțelor armate de a reconfigura instantaneu structurile și procedurile în funcție de dinamica mediului operațional. Ea devine

posibilă datorită modularității platformelor, descentralizării logistice și utilizării de unități autonome. Agilitatea operațională nu se reduce la flexibilitate, ci presupune o plasticitate instituțională, prin care forțele sunt capabile să exploateze oportunități efemere și să neutralizeze amenințări emergente.

Exemplele recente arată că structurile militare capabile să opereze în rețea, cu unități descentralizate și autonome, reușesc să își păstreze inițiativa chiar în fața unor adversari superiori numeric (Murray, Knox, 2001, pp. 196-201). În cazul României, agilitatea implică o mutație doctrinară de la modelul liniar, centrat pe volum, la un model multidomeniu și distribuit, adaptat la operații descentralizate și contestate.

Reziliență sistemică

Reziliența reprezintă dimensiunea cardinală a supraviețuirii strategice. Ea presupune capacitatea de a menține funcțiile critice chiar și sub presiune maximă, în condiții de degradare sistemică. Spre deosebire de reziliența tactică, centrată pe unități sau echipamente, reziliența sistemică vizează ansamblul ecosistemului național și aliat: infrastructuri critice, rețele energetice, comunicații, lanțuri logistice și coeziune societală.

În Ucraina, adaptarea infrastructurilor civile pentru uz militar (de exemplu, rețelele energetice redundante) a arătat importanța fuziunii dintre reziliența militară și cea societală (Reznikova, 2022, pp. 45-63). Pentru România, aflată pe linia de contact al flancului estic, consolidarea rezilienței presupune integrarea eforturilor civile și militare, protecția infrastructurilor critice și crearea unui cadru societal al rezilienței capabil să susțină apărarea națională pe termen lung (Radin, 2023, p. 31).

Relevanța pentru NATO și România

Cadrul în cinci dimensiuni se aliniază cu prioritățile NATO stipulate în Strategic Concept 2022 și NATO Warfighting Capstone Concept 2021, în care superioritatea informațională, agilitatea multidomeniu și reziliența colectivă sunt identificate ca factori decisivi ai supraviețuirii instituționale (NATO, 2022, pp. 7-10; NATO, 2021, p. 27).

Pentru NATO, modelul oferă o grilă operațională de convergență doctrinară, în timp ce, pentru România, constituie o condiție de credibilitate strategică, indispensabilă consolidării rolului său de stat pivot pe flancul estic. Internalizarea acestui cadru echivalează cu un salt paradigmatic: de la modernizarea incrementală la integrarea anticipativă și sistemică în arhitectura de securitate euroatlantică (Radin, 2023, pp. 29-32).

ROMÂNIA PE FLANCUL ESTIC AL NATO

Poziția geostrategică și rolul României în securitatea colectivă

România se constituie într-un veritabil nod geostrategic în arhitectura de securitate euroatlantică, prin localizarea sa la confluența dintre Europa Centrală, Balcani și spațiul pontic. Flancul estic, din care România este parte integrantă, reprezintă astăzi nu doar o zonă periferică de apărare, ci un epicentru al confruntării dintre ordinea liberală internațională și dinamica revizionistă a Federației Ruse (Barros, 2023, pp. 7-10).

Poziția României, cu deschidere la Marea Neagră și vecinătate directă cu Ucraina, Republica Moldova și regiunea extinsă a Caucazului, îi conferă un rol de pivot strategic al Alianței. Statutul său de gazdă al unor capacități critice, precum sistemul Aegis Ashore de la Deveselu sau structurile multinaționale de comandă și control (NATO Force Integration Units, HQ MNC-SE), îi amplifică relevanța ca furnizor de securitate regională și ca pol de proiecție a descurajării colective (NATO, 2022, pp. 14-16). În acest sens, România devine un „*geopolitical hinge*” între spațiul euroatlantic și cel eurasiatic, iar reziliența sa națională se suprapune direct peste reziliența NATO, ca întreg.

Vulnerabilități structurale

În pofida acestei poziționări strategice, România continuă să manifeste vulnerabilități structurale care pot diminua eficacitatea contribuției sale la apărarea colectivă.

Comanda și controlul (C2) sunt încă parțial tributare unor infrastructuri convenționale fragmentate și insuficient digitalizate, ceea ce îngreunează integrarea completă în meta-sistemele de rețea ale NATO (Alberts et al., pp. 52-54). Lipsa unor arhitecturi distribuite, bazate pe redundanță și securizare digitală, amplifică riscul de a deveni un punct de fragilitate în lanțul aliat de comandă.

Logistica națională, cu precădere infrastructura de transport, prezintă constrângeri majore. Rețelele feroviare limitate, portul Constanța vulnerabil la blocaje și infrastructurile rutiere insuficient modernizate reduc mobilitatea strategică și capacitatea de a susține fluxuri logistice în caz de conflict de mare intensitate (Ti, Kinsey, 2023, pp. 28-31). Această fragilitate structurală amplifică dependența de sprijinul aliat și de coridoarele logistice regionale.

În ceea ce privește domeniul cybersecurity, România, deși sediu al Centrului European de Competențe în Securitate Cibernetică, rămâne supusă unor atacuri cibernetice persistente, atribuite unor actori statali ostili (Reznikova, 2022, pp. 50-52). Deficitul de cultură organizațională unitară și fragmentarea instituțională

limitează coeziunea eforturilor, ceea ce subminează reziliența digitală într-un mediu în care războiul hibrid și cel cibernetic devin dimensiuni permanente ale confruntării.

Inițiative în desfășurare

Pentru a contracara aceste vulnerabilități, România a demarat un proces complex și multidimensional de modernizare militară, doctrinară și instituțională.

Pe dimensiunea capabilităților convenționale, programele de achiziție de aeronave multirol F-16 și viitoarele F-35, integrarea sistemelor Patriot și HIMARS, precum și modernizarea componentelor navale ilustrează efortul de a realiza o tranziție de la o forță de apărare teritorială la una multidomeniu, interoperabilă și adaptată standardelor NATO (Kofman, Lee, 2023, pp. 22-26).

În plan aliat, România participă activ la consolidarea posturii NATO de descurajare și apărare, prin găzduirea de forțe multinaționale, participarea la exerciții de amploare precum „*Defender Europe*” și integrarea în inițiative precum Enhanced Forward Presence și Tailored Forward Presence (NATO, 2021, p. 34). Aceste demersuri conferă credibilitate angajamentului României de a acționa ca furnizor de securitate, nu doar ca beneficiar.

Pe dimensiunea cibernetică și tehnologică, România consolidează parteneriatele cu UE și NATO prin activitatea Centrului European de Competențe în Securitate Cibernetică și prin implicarea în inițiative de tip Smart Defence, orientate spre inovare și distribuirea costurilor de apărare (Galeotti, 2022, pp. 113-115). Aceste inițiative reflectă o mutație paradigmatică de la apărarea tradițională la o securitate comprehensivă, bazată pe reziliență societală și integrarea capabilităților emergente.

Analiza aplicată pe dimensiuni

❖ Comandă și control (C2): integrarea cu NATO, digitalizare, infrastructură

În paradigma conflictului contemporan, C2 transcende logica lineară a lanțurilor ierarhice și devine un ecosistem informațional distribuit, caracterizat prin redundanță și interconectivitate permanentă (Alberts et al., pp. 52-54). Pentru România, integrarea în meta-sistemele de comandă NATO presupune nu doar interoperabilitate tehnică, ci și convergență doctrinară cu principiul *mission command*, unde liderii locali beneficiază de autonomie decizională în condiții de incertitudine.

Limitările actuale derivă dintr-o dependență excesivă de infrastructuri convenționale, parțial digitalizate, vulnerabile la atacuri ciberneticе sau cinetice. Experiența Ucrainei a arătat că rețelele descentralizate (Starlink) pot menține funcționalitatea C2 chiar și în condiții de degradare sistemică. România, prin integrarea

în NATO Communications and Information Agency (NCIA), trebuie să accelereze digitalizarea lanțurilor decizionale, inclusiv prin implementarea unor cloud-uri tactice securizate și sisteme bazate pe AI, pentru fuziunea datelor multisursă.

Polonia a realizat o integrare mai avansată a C2 în meta-sistemele NATO, beneficiind de o infrastructură robustă și de parteneriate consolidate cu SUA (inclusiv baza de la Redzikowo). În schimb, statele baltice, deși mai mici, au compensat prin digitalizare accelerată și prin doctrine de tip *mission command*. România rămâne parțial dependentă de infrastructuri convenționale, necesitând o tranziție către cloud-uri securizate și arhitecturi distribuite pentru a evita statutul de „*nod vulnerabil*” al rețelei aliate (Ib.).

❖ **Intelligence și situațional awareness (ISR): drone, sateliți, OSINT, centre de analiză**

ISR devine centrul de gravitație al conflictelor moderne, unde superioritatea informațională precede și condiționează superioritatea operațională (Horowitz, 2018, pp. 38-40). Războiul din Ucraina a demonstrat potențialul dronelor comerciale militarizate, al sateliților comerciali (Maxar, Planet Labs), dar și al OSINT, utilizat pentru verificarea și geolocalizarea rapidă a țintelor.

România se află într-o zonă contestată electronic, unde Federația Rusă dispune de capacități avansate de război electronic și de sisteme A2/AD în Crimeea (Watling, Reynolds, 2022, pp. 12-15). Integrarea cu NATO Intelligence Fusion Centre și extinderea parteneriatelor cu sectorul privat devin imperative pentru obținerea unei imagini operaționale comune. De asemenea, România trebuie să dezvolte centre naționale de analiză multisursă capabile să proceseze fluxuri mari de date din drone, sateliți și surse OSINT, evitând suprasaturarea cognitivă.

Statele baltice excelează prin integrarea OSINT și a rețelelor de senzori civili în arhitectura lor națională, bazându-se pe parteneriate cu sectorul privat și pe cultura digitală ridicată a populației. Polonia a investit masiv în drone și sateliți proprii, dezvoltând parteneriate cu SUA și Franța. România rămâne vulnerabilă la contestarea electronică rusă din Marea Neagră și depinde de partajarea NATO pentru obținerea unei imagini operaționale comune (Ib.).

❖ **Viteză decizională: leadership, AI, procese accelerate**

Într-un mediu strategic definit de hiper-timp, avantajul aparține actorului capabil să comprimate ciclurile OODA prin tehnologie și cultură organizațională adaptativă (Krepinevich, 1992, pp. 19-21). Dacă, în trecut, superioritatea era dată de masă și volum, astăzi ea depinde de ritmul cognitiv – abilitatea de a transforma informația în acțiune mai rapid decât adversarul.

România are nevoie de o reformă culturală în leadership militar, trecând de la un model birocratic la unul anticipativ și descentralizat. Integrarea instrumentelor AI – de la algoritmi de prognoză logistică la sisteme predictive pentru analiza câmpului de luptă – poate reduce inerția decizională și crește capacitatea de reacție. În NATO, viteza decizională nu este un atribut individual, ci o condiție de interoperabilitate: un stat care reacționează lent poate încetini sincronizarea întregii alianțe (Biddle, Friedman, 2022, pp. 9-12).

Polonia a adoptat o doctrină proactivă și o cultură organizațională bazată pe leadership descentralizat, ceea ce îi permite să reacționeze rapid. Statele baltice, prin structuri mai compacte și prin orientarea spre apărare teritorială, au dezvoltat mecanisme decizionale rapide și flexibile. România este încă tributară unei inerții birocratice, ceea ce încetinește procesele decizionale. Integrarea AI și a instrumentelor predictive este necesară pentru reducerea decalajului (Ib.).

❖ **Agilitate operațională: mobilitate, logistică, modularitate**

Agilitatea desemnează plasticitatea instituțională a forțelor armate de a se reconfigura instantaneu în funcție de dinamica mediului operațional (Murray, Knox, 2001, pp. 67-70). În Ucraina, structurile modulare și unitățile autonome au demonstrat că agilitatea poate compensa superioritatea numerică a adversarului.

Pentru România, această dimensiune este critică: infrastructura logistică limitată (rețele feroviare, poduri, porturi) afectează mobilitatea forțelor. Proiectele de modernizare (Rail2Sea, Via Carpathia) trebuie accelerate pentru a crea coridoare de mobilitate strategică. În plus, doctrina militară trebuie să privilegieze operațiile multidomeniu, cu unități distribuite, autonome și interconectate, capabile să exploateze oportunități efemere.

Polonia beneficiază de coridoare logistice extinse și de infrastructuri care permit mobilitate strategică rapidă, fiind principalul hub de sprijin pentru Ucraina. Statele baltice, în schimb, compensează infrastructura limitată prin structuri modulare și forțe dispersate, ceea ce le conferă reziliență. România, cu infrastructura feroviară și rutieră deficitară, trebuie să accelereze proiectele Rail2Sea și Via Carpathia pentru a asigura mobilitatea aliată pe flancul sudic (Ti, Kinsey, ib.).

❖ **Reziliență sistemică: cyber, infrastructuri critice, reziliență societală**

Reziliența nu se reduce la nivel tactic, ci reprezintă coloana vertebrală a supraviețuirii strategice. Ea implică menținerea funcțiilor critice în condiții de șoc sistemic – de la infrastructuri energetice și comunicații la coeziunea societală (Reznikova, 2022, pp. 46-49).

În Ucraina, fuziunea dintre infrastructurile civile și cele militare – precum adaptarea rețelelor energetice și integrarea OSINT în structurile oficiale –

a demonstrat că reziliența societală este inseparabilă de reziliența militară. Pentru România, vulnerabilitățile din infrastructurile critice (energie, transport, comunicații) necesită o strategie *whole-of-society*, în care instituțiile civile, mediul privat și cetățenii participă la consolidarea rezilienței naționale.

În plus, România, prin găzduirea Centrului European de Competențe în Securitate Cibernetică, are oportunitatea de a deveni un hub regional de reziliență digitală, integrat în strategia NATO de apărare cibernetică.

Statele baltice sunt considerate modele de reziliență societală: guvernele lor au dezvoltat programe de apărare totală (Total Defence) care integrează populația civilă în arhitectura de securitate. Polonia a investit masiv în infrastructuri critice și securitate cibernetică, consolidând capacitatea de reziliență. România, deși găzduiește Centrul European de Competențe în Securitate Cibernetică, rămâne vulnerabilă la atacurile hibride și la fragmentarea instituțională, fiind necesară o strategie *whole-of-society* pentru a îmbina reziliența militară cu cea societală (Reznikova, 2022).

Pentru a întregi analiza multidimensională, *tabelul 1* prezintă o sinteză comparativă a poziționării României, Poloniei și statelor baltice, evidențiind atât zonele de convergență doctrinară și instituțională, cât și vulnerabilitățile structurale specifice fiecărui stat.

*Tabelul 1: Analiză comparativă pe dimensiuni
(România – Polonia – Statele baltice) (adaptare proprie)*

Dimensiune	România	Polonia	Statele baltice
C2 (Comandă și control)	Infrastructuri parțial digitalizate; integrare incompletă în meta-sistemele NATO; risc de „nod slab”	Integrare avansată cu SUA și NATO (ex. Redzikowo); infrastructură robustă	Arhitecturi distribuite; digitalizare accelerată; doctrină mission command
ISR (Intelligence și situațional awareness)	Vulnerabilitate la război electronic rus în Marea Neagră; dependență de partajarea NATO	Investiții în drone și sateliți; parteneriate strategice cu SUA și Franța	Integrare OSINT și senzori civili; cultură digitală ridicată
Decizie (Viteză decizională)	Procese birocratice lente; AI insuficient integrat; cultură organizațională rigidă	Leadership descentralizat; procese anticipate și proactive	Structuri compacte; mecanisme flexibile; reacții rapide

Dimensiune	România	Polonia	Statele baltice
Agilitate (Mobilitate și logistică)	Infrastructură deficitară (feroviar, rutier, portuar); proiecte Rail2Sea și Via Carpathia în derulare	Hub logistic principal pentru Ucraina; infrastructuri extinse	Structuri modulare, dispersate; reziliență logistică prin dispersie
Reziliență (Cyber, infrastructuri critice, societal)	Vulnerabilități cibernetice și instituționale; fragmentare societală; potențial prin Centrul European Cyber	Investiții masive în infrastructuri critice și cyber; reziliență consolidată	Modele de Total Defence; integrare societală în apărare; coeziune ridicată

Tabelul 1 arată că Polonia deține poziția de lider regional prin infrastructuri robuste și integrare avansată cu NATO, în timp ce statele baltice reprezintă un laborator de reziliență societală și digitală. România se află într-o poziție intermediară: deși este un pivot strategic la Marea Neagră, persistă vulnerabilități în infrastructură, C2 și reziliență cibernetică. Prin urmare, consolidarea interoperabilității digitale, accelerarea mobilității logistice și dezvoltarea unei strategii *whole-of-society* devin imperative pentru a transforma România dintr-un „*nod vulnerabil*” într-un actor-cheie al securității colective.

IMPLICAȚII PENTRU NATO ȘI ROMÂNIA

Alinierea României la NATO Strategic Concept (2022) și NATO Warfighting Capstone Concept (2021)

NATO Strategic Concept (Madrid, 2022) a marcat o schimbare de paradigmă: Rusia este definită explicit ca amenințare directă, iar China este menționată ca rival sistemic. Această redefinire a mediului strategic impune o consolidare fără precedent a flancului estic. În paralel, NATO Warfighting Capstone Concept (2021) anticipează mediul de securitate din 2040, introducând operațiile multi-domeniu (MDO) ca nou cadru de gândire militară, cu accent pe convergența între domeniul terestru, aerian, maritim, cibernetic și spațial (NATO, 2021, pp. 12-15).

Pentru România, această aliniere înseamnă:

- *Transformare doctrinară: trecerea de la un model liniar de apărare teritorială la o arhitectură multidomeniu și anticipativă, cu accent pe interoperabilitate și integrarea tehnologiilor emergente.*

- *Modernizare infrastructurală: rolul său ca hub logistic și strategic în Marea Neagră impune investiții masive în infrastructuri critice (porturi, coridoare feroviare, spațiu aerian securizat).*
- *Rol pivot în securitatea regională: spre deosebire de Polonia (hub nordic) și statele baltice (avanposturi), România este bastionul sudic al flancului estic, ceea ce îi conferă responsabilitatea de a asigura coeziunea sudului aliat.*

Contribuții practice ale României pentru securitatea regională

România nu se limitează la a primi securitate de la NATO, ci și proiectează securitate, prin:

- **Structuri multinaționale:** găzduiește Comandamentul Multinațional de Divizie Sud-Est (HQ MNC-SE) și Unitățile de Integrare a Forțelor NATO (NFIU). Aceste structuri sunt esențiale pentru planificarea și desfășurarea rapidă a operațiilor.
- **Capabilități antirachetă:** sistemul Aegis Ashore de la Deveselu este parte integrantă a apărării balistice a NATO, ceea ce transformă România într-o țintă strategică, dar și într-un furnizor de securitate la nivel aliat.
- **Exerciții multinaționale:** participarea și găzduirea de exerciții precum Defender Europe, Saber Guardian și Sea Breeze demonstrează capacitatea României de a asigura interoperabilitate operațională.
- **Inițiative energetice și infrastructurale:** proiectele BRUA și Neptun Deep consolidează independența energetică și securitatea regională, reducând dependența de gazul rusesc.

Prin aceste contribuții, România funcționează ca un nod de securitate integrată la Marea Neagră, completând rolul Poloniei din zona baltică.

Lecții pentru interoperabilitate și inovație

Conflictul din Ucraina a evidențiat că interoperabilitatea tehnologică și inovarea doctrinară sunt vitale pentru supraviețuirea colectivă.

Pentru România, trei lecții sunt esențiale:

- **Interoperabilitatea digitală:** România trebuie să treacă de la infrastructuri convenționale la arhitecturi distribuite de C2, integrând cloud-uri tactice și algoritmi AI. Spre comparație, statele baltice sunt deja avansate în digitalizare societală, iar Polonia a investit în **infrastructuri robuste compatibile cu SUA**.
- **Inovația accelerată:** România trebuie să folosească statutul de gazdă a Centrului European de Competențe în Securitate Cibernetică pentru a deveni un hub regional al inovației tehnologice militare. Acest lucru

presupune nu doar apărare, ci și dezvoltarea de soluții proprii (dronă, software, infrastructuri cyber).

- **Reziliența societală:** statele baltice oferă modelul de Total Defence, unde întreaga societate participă la apărare. România are nevoie de o strategie *whole-of-society*, în care cetățenii, mediul privat și instituțiile civile sunt integrate în arhitectura de reziliență.

Astfel, România poate depăși statutul de „*nod vulnerabil*” și poate deveni un pilon inovator și rezilient al flancului estic, contribuind la transformarea NATO într-o alianță multidomeniu, adaptivă și anticipativă.

CONCLUZII ȘI RECOMANDĂRI

Analiza a demonstrat că tehnologiile emergente nu reprezintă simple multiplicatoare de putere, ci determinanți structurali ai rezilienței și eficacității operaționale. Cadrul analitic în cinci dimensiuni – comandă și control, intelligence și conștientizare situațională, viteză decizională, agilitate operațională și reziliență sistemică – a permis o evaluare comprehensivă a modului în care România, comparativ cu Polonia și statele baltice, se poziționează în arhitectura de securitate a flancului estic.

Rezultatele confirmă că România deține un rol pivot strategic în Marea Neagră, dar persistă vulnerabilități structurale în domeniile C2, infrastructurii logistice și rezilienței cibernetice. În același timp, oportunitățile de integrare în inițiativele NATO și UE, precum și statutul de gazdă a Centrului European de Competențe în Securitate Cibernetică, pot transforma aceste vulnerabilități în avantaje comparative.

Din punct de vedere teoretic, studiul contribuie la consolidarea literaturii privind *revoluția în afacerile militare*, demonstrând că tranziția spre un mediu multidomeniu și digitalizat nu este doar un deziderat, ci o realitate empirică deja validată de conflictul ucrainean.

Pe plan epistemologic, articolul susține ideea că paradigma informațională și cognitivă devine centrul de gravitație al războiului contemporan, înlocuind, treptat, paradigma industrială bazată pe volum și masă. Astfel, rezultatele cercetării confirmă tendințele recente din teoria strategică și le completează cu o perspectivă aplicată asupra specificului României și flancului estic.

Pornind de la concluziile analizei, se pot formula următoarele direcții strategice pentru consolidarea profilului de securitate al României:

- Investiții în reziliența cibernetică – dezvoltarea unor infrastructuri distribuite și redundante, capabile să reziste atacurilor hibride și să asigure continuitatea funcțiilor critice în caz de conflict.

- Consolidarea logisticii descentralizate – implementarea unor modele modulare și flexibile de sprijin, inspirate din experiența Ucrainei, care să permită reconfigurarea rapidă a fluxurilor logistice în medii contestate.
- Parteneriate tehnologice – valorificarea poziției României în cadrul NATO și al UE pentru a dezvolta alianțe industriale și tehnologice, orientate către drone, inteligență artificială și infrastructuri de comunicații securizate.
- Formarea unei culturi de inovație militară – stimularea experimentării doctrinare și a proceselor de învățare instituțională rapidă, prin crearea unor laboratoare operaționale și integrarea mediului academic și privat în ecosistemul de apărare.
- Integrarea unei strategii *whole-of-society* – adaptarea modelului baltic de apărare totală la specificul românesc, prin implicarea societății civile și a mediului privat în asigurarea rezilienței și continuității naționale.

În ansamblu, studiul confirmă că succesul strategic pe flancul estic al NATO depinde de capacitatea statelor membre de a integra tehnologiile emergente într-un mod coerent, multidimensional și anticipativ. Pentru România, acest proces implică depășirea vulnerabilităților structurale prin investiții în reziliență, inovare doctrinară și parteneriate tehnologice, consolidând, astfel, nu doar propria securitate, ci și credibilitatea colectivă a Alianței. Într-o epocă marcată de volatilitate strategică și accelerare tehnologică, adaptabilitatea va reprezenta criteriul fundamental al supraviețuirii și eficienței operaționale.

REFERINȚE BIBLIOGRAFICE:

1. Alberts, D.S., Garstka, J.J., Stein, F.P. (1999). *Network centric warfare: Developing and leveraging information superiority*. Washington, DC: CCRP Publication Series.
2. Barros, G. (2023). *Ukrainian military innovation: Tactical and technological lessons*. Washington, DC: Institute for the Study of War.
3. Biddle, S., Friedman, J.A. (2022). *The battle of Donbas and the future of conventional warfare*, în *Survival*, 64(4), pp. 7-30, <https://doi.org/10.1080/00396338.2022.2090705>, accesat la 22 august 2025.
4. Galeotti, M. (2022). *The weaponisation of everything: A field guide to the new way of war*. New Haven, CT: Yale University Press.
5. Horowitz, M.C. (2018). *Artificial intelligence, international competition, and the balance of power*, în *Texas National Security Review*, 1(3), pp. 36-57, <https://tnsr.org/2018/02/artificial-intelligence-international-competition-and-the-balance-of-power/>, accesat la 30 septembrie 2025.
6. Kofman, M., Lee, R. (2022). *Preliminary lessons in conventional warfighting from Russia's invasion of Ukraine: February-July 2022*. Arlington, VA: CAN, <https://www.cna.org>, accesat la 30 septembrie 2025.

7. Kofman, M., Lee, R. (2023). *The evolving character of war: Ukraine and the future of military innovation*. Washington, DC: Center for Strategic and International Studies, <https://www.csis.org>, accesat la 30 septembrie 2025.
8. Krepinevich, A.F. (1992). *The military-technical revolution: A preliminary assessment*. Washington, DC: Center for Strategic and Budgetary Assessments.
9. Mareš, M. (2022). *Hybrid threats in the context of the war in Ukraine*. *Vojenské rozhledy*, 31(4), pp. 5-19, <https://doi.org/10.3849/2336-2995.31.2022.04.005>, accesat la 22 august 2025.
10. Murray, W., Knox, M. (2001). *The dynamics of military revolution, 1300-2050*. Cambridge: Cambridge University Press.
11. NATO (2021). *NATO warfighting capstone concept*. Norfolk, VA: Allied Command Transformation, <https://www.act.nato.int>, accesat la 30 septembrie 2025).
12. NATO (2022). *Strategic concept*. Madrid: NATO Summit, <https://www.nato.int>, accesat la 30 septembrie 2025.
13. Radin, A. (2023). *Technological resilience in modern conflict: Case studies from Ukraine*. Santa Monica, CA: RAND Corporation, <https://www.rand.org>, accesat la 30 septembrie 2025.
14. Reznikova, O. (2022). *National resilience and technological innovation during wartime*, în *Ukrainian Journal of Security Studies*, 8(3), pp. 45-63.
15. Ti, K., Kinsey, C. (2023). *Adaptive logistics in contested environments: Lessons from Ukraine*, în *Journal of Military Logistics*, 14(1), pp. 22-36.
16. Watling, J., Reynolds, N. (2022). *The Russian way of war: Lessons from Ukraine*. London: Royal United Services Institute, <https://rusi.org>, accesat la 30 septembrie 2025.