

# Războiul contemporan și transformarea paradigmei militare globale

## *Contemporary Warfare and the Transformation of the Global Military Paradigm*

**Maior Doctorand Cristian-Alexandru SALAC\***

\*Ministerul Apărării Naționale  
e-mail: [salac\\_cristian@yahoo.com](mailto:salac_cristian@yahoo.com)

### Abstract

Articolul analizează transformarea paradigmei militare globale în contextul evoluțiilor tehnologice și strategice ale secolului XXI, utilizând o abordare calitativă, bazată pe analiza literaturii de specialitate și pe interpretarea conceptuală a conflictelor contemporane. Analiza folosește exemple ilustrative din războiul ruso-ucrainean, din conflictul din Nagorno-Karabakh și din domeniul operațiilor cibernetice pentru evidențierea transformărilor recente ale mediului operațional. Analiza arată că tehnologiile emergente – digitalizarea, inteligența artificială, dronele și infrastructurile orbitale – nu doar sprijină operațiile militare, ci reconfigurează criteriile de superioritate strategică, favorizând actorii capabili să integreze informația și inovația într-un mod coerent. Rezultatele evidențiază că războiul contemporan evoluează către un model multidimensional, precum și necesitatea adaptării structurilor militare la un model operațional multidomeniu, caracterizat de interdependență, viteză decizională și integrare tehnologică. Lucrarea contribuie la clarificarea conceptuală a războiului contemporan și evidențiază implicațiile strategice ale transformărilor în curs asupra securității globale.

*This article analyzes the transformation of the global military paradigm in the context of the technological and strategic developments of the 21st century, using a qualitative approach based on the analysis of specialized literature and the conceptual interpretation of contemporary conflicts. The analysis employs illustrative examples from the Russo-Ukrainian War, the Nagorno-Karabakh conflict, and the field of cyber operations in order to highlight recent transformations of the operational environment. The analysis shows that emerging technologies – digitalization, artificial intelligence, drones, and orbital infrastructures – not only support military operations, but also reshape the criteria of strategic superiority, favoring actors capable of coherently integrating information and innovation. The results highlight that contemporary warfare is evolving toward a multidimensional model, as well as the need to adapt military structures to a multidomain operational model characterized by interdependence, decision-making speed, and technological integration. This paper contributes to the conceptual clarification of contemporary warfare and emphasizes the strategic implications of ongoing transformations for global security.*

### Cuvinte-cheie:

război contemporan; război hibrid; securitate cibernetică; operații multidomeniu;  
tehnologii emergente; superioritate informațională.

### Keywords:

Contemporary Warfare; Hybrid Warfare; Cybersecurity; Multi-domain Operations;  
Emerging Technologies; Information Superiority.

### Info articol

Primit: 29 ianuarie 2026; Evaluat: 19 februarie 2026; Acceptat: 17 martie 2026; Disponibil online: 30 iunie 2026

Citare: Salac C.A. 2026. „Războiul contemporan și transformarea paradigmei militare globale.”

*Buletinul Universității Naționale de Apărare „Carol I”*, 15(2): 77-92. <https://doi.org/10.53477/2065-8281-26-14>



## Introducere

Evoluțiile mediului de securitate din ultimele decenii indică o transformare structurală profundă a naturii războiului și a modului în care puterea militară este concepută, organizată și utilizată. Conflictele contemporane nu mai pot fi analizate exclusiv prin prisma confruntărilor armate convenționale dintre state, ci trebuie înțelese ca procese multidimensionale, desfășurate simultan în domenii interconectate – fizic, informațional, economic, cibernetic și spațial (Freedman 2017, 45-52; Mazarr 2015, 3-7).

Concepte precum războiul hibrid, competiția în zona gri, operațiile informaționale și conflictele cibernetic devin esențiale pentru înțelegerea noilor dinamici ale securității internaționale. Tehnologiile digitale, inteligența artificială, sistemele autonome și infrastructurile orbitale nu mai reprezintă doar instrumente de sprijin, ci factori structurali care influențează distribuția puterii și arhitectura doctrinară a forțelor armate (Horowitz 2010, 4-8; Johnson 2022, 1397).

Scopul cercetării este de a analiza modul în care transformările tehnologice și strategice ale secolului XXI contribuie la redefinirea paradigmei militare globale și la configurarea unui model de conflict multidimensional persistent, caracterizat prin integrarea simultană a instrumentelor convenționale și nonconvenționale.

Pentru atingerea acestui scop, lucrarea are în vedere următoarele obiective de cercetare:

- identificarea principalelor caracteristici ale războiului contemporan, în raport cu paradigma tradițională;
- analiza rolului tehnologiilor emergente în transformarea conflictelor moderne;
- examinarea impactului dimensiunii cibernetic și informaționale asupra securității;
- evaluarea implicațiilor acestor transformări asupra organizării și funcționării forțelor armate moderne.

În vederea structurării demersului analitic, sunt formulate următoarele întrebări de cercetare:

1. În ce măsură transformările tehnologice actuale modifică natura conflictelor armate?
2. Care este rolul dimensiunii cibernetic și informaționale în redefinirea raporturilor de putere?
3. Cum influențează aceste evoluții organizarea și funcționarea armatei moderne?

Prin această abordare, lucrarea contribuie la clarificarea conceptuală a războiului contemporan și evidențiază implicațiile strategice ale transformărilor în curs asupra securității globale și organizării forțelor armate, în acord cu direcțiile recente, evidențiate în literatura de securitate și în studiile strategice (Manolache 2023, 164).

## 1. Metodologia cercetării

Prezenta lucrare se bazează pe o abordare calitativă de tip analitic și conceptual, adecvată studierii fenomenelor complexe din domeniul securității internaționale și al transformării conflictelor contemporane. Având în vedere caracterul dinamic și multidimensional al războiului modern, cercetarea urmărește identificarea și interpretarea principalelor tendințe strategice, tehnologice și doctrinare care influențează redefinirea paradigmei militare globale.

Unitățile de analiză utilizate în cercetare sunt reprezentate de conflicte contemporane relevante (războiul ruso-ucrainean și conflictul din Nagorno-Karabakh), de evoluții doctrinare recente (operațiunile multidomeniu) și de transformări tehnologice aplicate mediului militar (drone, capacități cibernetice și inteligență artificială). Analiza urmărește identificarea relațiilor dintre dezvoltarea tehnologică, modificarea mediului operațional și adaptarea doctrinară a actorilor militari.

Analiza comparativă a fost realizată prin raportarea cazurilor și evoluțiilor analizate la trei criterii principale: extinderea conflictului în domenii nonconvenționale, integrarea tehnologiilor emergente și transformarea proceselor decizionale și operaționale ale actorilor militari.

Demersul metodologic utilizează, în principal, analiza literaturii de specialitate (literature review), fiind selectate lucrări academice relevante din domeniul studiilor strategice, securității internaționale și tehnologiilor militare. Sursele analizate includ articole din reviste indexate, monografii și rapoarte de cercetare, care oferă atât perspective teoretice, cât și interpretări ale evoluțiilor recente din mediul de securitate. Selecția surselor a avut în vedere relevanța, actualitatea și contribuția acestora la înțelegerea transformărilor războiului contemporan.

În vederea creșterii consistenței analitice, cercetarea utilizează exemple ilustrative din conflictele recente pentru a evidenția aplicabilitatea practică a conceptelor analizate și modul în care transformările tehnologice influențează desfășurarea operațiilor contemporane.

În cadrul cercetării este folosită și metoda analizei comparative prin care sunt evidențiate diferențele și continuitățile dintre paradigma tradițională a războiului și formele contemporane de conflict, precum războiul hibrid, competiția în zona gri și confruntările din domeniul cibernetic. Această metodă permite identificarea elementelor de noutate și a factorilor determinanți ai schimbării, în special în relație cu dezvoltarea tehnologiilor emergente.

De asemenea, lucrarea recurge la analiza conceptuală, vizând clarificarea și delimitarea unor concepte-cheie, precum „război hibrid”, „operații multidomeniu”, „securitate cibernetică” sau „competiție strategică persistentă”. Această abordare contribuie la o înțelegere coerentă a cadrului teoretic și la integrarea diverselor perspective existente în literatura de specialitate.

Metodele de analiză a datelor sunt preponderent calitative, bazate pe interpretarea critică, corelarea informațiilor și identificarea relațiilor cauzale dintre variabilele analizate (tehnologie, strategie, actori, medii operaționale). Cercetarea nu utilizează metode cantitative sau instrumente statistice, întrucât obiectivul principal este explicarea și înțelegerea fenomenelor, nu măsurarea acestora.

Limitele cercetării derivă din caracterul predominant teoretic al analizei și din absența unor studii empirice extinse sau a unor seturi de date cantitative. Cu toate acestea, abordarea conceptual-analitică permite evidențierea tendințelor majore și formularea unor concluzii relevante pentru înțelegerea evoluției conflictelor contemporane.

Prin utilizarea acestor metode, cercetarea își propune să ofere o perspectivă integrată asupra transformării paradigmei militare globale și să contribuie la dezvoltarea cadrului conceptual necesar analizei războiului în secolul XXI.

## 2. Metamorfoza războiului în secolul XXI

Secolul XXI marchează o transformare profundă a războiului, nu doar în termeni tehnologici, ci și conceptuali și strategici. Analiza evoluțiilor recente din mediul de securitate evidențiază faptul că, nu mai pot fi reduse conflictele contemporane la confruntări militare convenționale între state, ci trebuie înțelese ca fenomene multidimensionale, în care domeniile fizic, informațional, economic și cibernetic interacționează permanent (Freedman 2017, 48-49).

Transformările analizate indică o transformare structurală a modului în care puterea este exercitată, în sensul extinderii câmpului de confruntare dincolo de dimensiunea militară clasică. Această evoluție sugerează că războiul contemporan capătă caracteristicile unui proces continuu, marcat de ambiguitate, interdependență și competiție persistentă sub pragul conflictului deschis (Mazarr 2015, 6-7). Relevanța strategică nu mai este determinată exclusiv de capacitatea de proiecție a forței, ci de abilitatea actorilor de a integra instrumente militare și nonmilitare într-un cadru coerent de influență.

### 2.1 *Tranziția de la conflictele convenționale la războaiele hibride*

Războaiele hibride reprezintă una dintre cele mai relevante manifestări ale transformării conflictului în secolul XXI. Literatura de specialitate indică faptul că aceste forme de conflict sunt caracterizate prin integrarea acțiunilor militare convenționale în tactici netradiționale, precum atacurile cibernetice, campaniile de dezinformare, presiunile economice și utilizarea actorilor proxy (Hoffman 2018, 30). Se observă că specificul războiului hibrid constă în sincronizarea adaptivă a acestor instrumente, orientată către exploatarea vulnerabilităților sistemice ale adversarului. În acest sens, obiectivul strategic nu mai este neapărat controlul teritorial imediat, ci destabilizarea politică și instituțională (Mazarr 2015, 10-11).

Conflictele recente, în special războiul din Ucraina, sugerează că acțiunile hibride pot preceda și însoți operațiile convenționale, confirmând caracterul lor integrat

și flexibil (Watling 2023, 5-6). Deci se confirmă ipoteza conform căreia războiul contemporan evoluează către un model multidimensional, în care instrumentele nonconvenționale devin esențiale.

Războiul ruso-ucrainean reprezintă unul dintre cele mai relevante exemple ale convergenței dintre operațiile convenționale și instrumentele hibride. Începând cu anexarea Crimeei în 2014 și continuând cu invazia din 2022, Federația Rusă a combinat operațiile militare clasice cu atacuri cibernetice, cu campanii de dezinformare și presiuni energetice. Utilizarea sincronizată a acestor instrumente a urmărit nu doar obținerea unor avantaje teritoriale, ci și destabilizarea politică și psihologică a adversarului.

### ***2.2. Actori statali și nonstatali în noile dinamici conflictuale***

Interacțiunea dintre actorii statali și cei nonstatali constituie un element definitoriu al conflictelor contemporane. Actorii nonstatali nu mai reprezintă doar entități periferice, ci actori relevanți, capabili să influențeze dinamica strategică la nivel regional și global (Salehyan 2009, 16-17).

Prin utilizarea rețelelor transnaționale, a mediului informațional și a vulnerabilităților infrastructurale, acești actori pot genera efecte strategice disproporționate, în raport cu resursele de care dispun. Această evoluție confirmă tendința de accentuare a asimetriei conflictelor, în care avantajul nu mai aparține exclusiv actorilor cu superioritate militară convențională (IISS 2024, 15-16).

Interdependența dintre actorii statali și nonstatali contribuie la creșterea complexității conflictelor, impunând dezvoltarea unor strategii integrate care să combine instrumente militare, politice și informaționale. În acest context, cooperarea internațională și mecanismele de securitate colectivă devin esențiale pentru gestionarea riscurilor emergente.

### ***2.3. Zona gri și competiția sub pragul confruntării directe***

Conceptul de „zonă gri” descrie un spectru de competiție strategică situat între pace și război, în care actorii urmăresc obținerea unor avantaje prin acțiuni ambigue, graduale și dificil de atribuit. Analiza conceptuală evidențiază că această formă de competiție reprezintă o caracteristică definitorie a mediului de securitate contemporan (Mazarr 2015, 6-7).

Operațiile desfășurate în zona gri, incluzând atacuri cibernetice, campanii de influență informațională și presiuni economice permit erodarea graduală a securității adversarului, fără declanșarea unui conflict deschis. Această abordare reduce riscul escaladării directe și complică procesele de descurajare și de răspuns strategic (NATO 2022, 5-7).

Documentele strategice recente ale NATO evidențiază faptul că amenințările hibride și competiția persistentă sub pragul conflictului armat reprezintă una dintre principalele provocări pentru securitatea euroatlantică, întrucât combină instrumente militare și nonmilitare într-o manieră dificil de atribuit și de contracarat (NATO 2022, 5-7).

Competiția din zona gri confirmă transformarea războiului într-un proces continuu, caracterizat prin presiune persistentă și multidimensională, iar ipoteza conform căreia

delimitarea tradițională dintre pace și război devine tot mai difuză, fiind înlocuită de un continuum al confruntării strategice, se demonstrează într-o mare măsură.

### **3. Tehnologia ca forță transformatoare în războiul contemporan**

Tehnologia reprezintă unul dintre principalii factori care determină transformarea profundă a războiului contemporan, influențând nu doar capacitățile tactice, ci și modul în care puterea militară este concepută și utilizată la nivel strategic. Analiza literaturii de specialitate evidențiază faptul că integrarea tehnologiilor emergente modifică distribuția puterii și avantajul competitiv dintre actori, favorizând pe cei capabili să adopte și să integreze rapid inovația (Horowitz 2010, 4-8).

Superioritatea militară nu mai este determinată exclusiv de resursele materiale sau de dimensiunea forțelor, ci și de capacitatea de a integra tehnologia în structuri operaționale coerente și de a exploata avantajele informaționale (Horowitz 2010, 15; Biddle 2022, 32).

#### **3.1. *Revoluția digitală și impactul asupra tacticilor militare***

Revoluția digitală constituie unul dintre principalii factori structurali ai transformării războiului contemporan, influențând simultan nivelul tactic, operativ și strategic. Integrarea tehnologiilor informaționale în structurile militare a generat un mediu operațional caracterizat de conectivitate extinsă și fluxuri continue de date. Acest proces permite analiza și folosirea în timp real a datelor provenite din multiple surse. Literatura recentă evidențiază faptul că digitalizarea redefinește modul în care este generată și utilizată puterea militară, depășind paradigma tradițională bazată pe superioritatea materială (Jensen, Valeriano și Maness 2019, 212-214).

Rezultatele analizei indică faptul că informația devine un multiplicator de forță esențial, iar succesul operațional depinde din ce în ce mai mult de capacitatea de a colecta, integra și exploata date într-un ritm superior adversarului. Integrarea tehnologiilor digitale conduce la comprimarea ciclului decizional și la creșterea relevanței superiorității informaționale, care permite actorilor să obțină avantaje strategice chiar și în condiții de inferioritate materială (Biddle 2022, 35).

În plan tactic, digitalizarea facilitează coordonarea unităților dispersate și integrarea sistemelor de armament în rețele comune, contribuind la creșterea flexibilității operaționale. Totodată, această dependență de infrastructurile digitale generează vulnerabilități semnificative, întrucât sistemele informatice devin ținte ale atacurilor cibernetice, capabile să producă efecte strategice disproporționate (Kello 2013, 18-21). Prin urmare, se confirmă ipoteza conform căreia revoluția digitală transformă fundamental logica acțiunii militare, deplasând accentul de pe superioritatea cantitativă pe superioritatea informațională.

#### **3.2. *Dronele și reducerea monopolului tehnologic***

Proliferarea vehiculelor aeriene fără pilot (UAV) reprezintă una dintre cele mai semnificative evoluții tehnologice ale războiului contemporan, contribuind la modificarea echilibrului de putere și la reducerea barierelor de acces la capacitățile

aeriene. Literatura de specialitate arată că dronele permit atât statelor, cât și actorilor nonstatali să desfășoare operații de supraveghere, recunoaștere și lovire de precizie, cu costuri relativ reduse (Boyle 2015, 4).

Aceste sisteme contribuie la reducerea monopolului tehnologic, redistribuind avantajul strategic și favorizând apariția unor forme de conflict asimetric. Conflictele recente, în special războiul din Ucraina, demonstrează rolul central al dronelor în modificarea tacticilor de luptă și în creșterea importanței operațiilor la distanță, unde precizia și adaptabilitatea devin factori decisivi (Watling 2023, 5-6).

Conflictul din Nagorno-Karabakh (2020) a evidențiat impactul major al dronelor asupra raportului de forțe la nivel tactic și operativ. Azerbaidjanul a utilizat drone Bayraktar TB2 și muniții loitering pentru neutralizarea sistemelor armene de apărare antiaeriană și a tehnicii blindate, demonstrând capacitatea unor sisteme relativ accesibile de a produce efecte strategice semnificative. Ulterior, războiul din Ucraina a confirmat această tendință prin folosirea pe scară largă a dronelor FPV pentru identificarea și lovirea țintelor în timp real.

Aceste evoluții sugerează că accesibilitatea tehnologiilor autonome reduce avantajul exclusiv al actorilor militari tradiționali și favorizează apariția unor forme de competiție asimetrică, bazate pe flexibilitate și adaptare rapidă.

Analizele realizate de Royal United Services Institute arată că utilizarea dronelor tactice în Ucraina a contribuit la reducerea timpului dintre identificarea țintei și executarea loviturii, crescând semnificativ eficiența artileriei și a operațiilor de recunoaștere (Watling 2023, 18-19).

Prin urmare, dronele nu reprezintă doar un instrument tehnologic, ci și un factor care influențează direct modul de desfășurare a conflictelor și distribuția puterii între actori.

### ***3.3. Inteligența artificială, sistemele autonome și automatizarea câmpului de luptă***

Integrarea inteligenței artificiale și a sistemelor autonome în domeniul militar marchează o etapă semnificativă în transformarea războiului contemporan. Aceste tehnologii permit analiza rapidă a datelor, identificarea tiparelor și optimizarea deciziilor operaționale în condiții de incertitudine ridicată (Scharre 2018, 37-38).

Rezultatele analizei indică faptul că inteligența artificială contribuie la accelerarea ciclului decizional și la creșterea eficienței operaționale, devenind un multiplicator de forță, bazat pe informație. Lucrările recente din domeniu subliniază că folosirea sistemelor autonome ridică provocări etice și strategice semnificative, în special în ceea ce privește responsabilitatea decizională și controlul uman asupra utilizării forței (Johnson 2022, 1397-1399).

Studiile recente asupra integrării inteligenței artificiale în domeniul militar sugerează că automatizarea proceselor de analiză și sprijin decizional poate modifica fundamental ritmul și logica desfășurării conflictelor contemporane (Payne 2021, 76-77). De asemenea, analizele recente privind integrarea inteligenței artificiale în domeniul militar sugerează că sistemele autonome vor influența semnificativ viteza decizională și arhitectura operațiilor viitoare (Konaev 2023, 15-16).

Prin urmare, analiza evidențiază că integrarea inteligenței artificiale transformă nu doar capacitățile militare, ci și natura deciziei în război.

### **3.4. Militarizarea spațiului și infrastructurile orbitale**

Spațiul cosmic a devenit un domeniu operațional esențial pentru desfășurarea operațiilor militare moderne, oferind avantaje strategice decisive în domeniul comunicațiilor, navigației și supravegherii. Analizele recente din domeniul studiilor strategice indică faptul că infrastructurile orbitale sunt integrate în mod direct în arhitectura operațiilor multidomeniu (Manolache 2023, 163).

Dependența de aceste infrastructuri generează vulnerabilități critice, întrucât perturbarea sau distrugerea sistemelor spațiale poate afecta capacitatea de comandă și control. În plus, dezvoltarea capabilităților antisatelit și a atacurilor cibernetice asupra sistemelor orbitale amplifică riscurile asociate securității spațiale.

Astfel, se confirmă tendința de extindere a conflictului în domenii noi, inclusiv în spațiul cosmic, consolidând caracterul multidimensional al războiului contemporan.

## **4. Dimensiunea cibernetică a conflictului: un vector în războiul contemporan**

Dimensiunea cibernetică a devenit o componentă centrală a conflictelor contemporane, redefinind modul în care puterea este exercitată în relațiile internaționale. Spre deosebire de domeniile tradiționale ale confruntării, spațiul cibernetic permite desfășurarea unor operații cu impact strategic semnificativ fără mobilizarea forței militare convenționale, modificând raportul dintre cost, atribuire și efect strategic în competiția contemporană (Kello 2013, 7; Schmitt 2017, 3).

Literatura de specialitate subliniază că operațiile cibernetice pot influența procesele politice, economice și sociale, afectând stabilitatea statelor fără a genera neapărat o reacție militară directă (Kello 2013, 8). Dificultatea atribuirii atacurilor, combinată cu costurile relativ reduse ale desfășurării acestora favorizează utilizarea instrumentelor cibernetice ca parte a unei competiții strategice persistente. În acest context, controlul infrastructurilor digitale și al fluxurilor informaționale devine un element esențial al puterii.

### **4.1. Atacuri cibernetice și vulnerabilitatea infrastructurilor critice**

Atacurile cibernetice asupra infrastructurilor critice evidențiază vulnerabilitățile generate de digitalizarea extinsă a societăților moderne. Sistemele energetice, financiare, de comunicații și transport sunt profund interconectate, iar această interdependență creează condițiile pentru apariția unor efecte în cascadă, în care perturbarea unui element poate afecta întregul sistem.

Un exemplu relevant îl reprezintă atacul cibernetic asupra infrastructurii energetice ucrainene din 2015, care a provocat întreruperi ale alimentării cu energie pentru aproximativ 230.000 de consumatori. Operațiunea a demonstrat că atacurile cibernetice pot genera efecte strategice semnificative fără utilizarea forței armate convenționale, evidențiind vulnerabilitatea infrastructurilor critice integrate digital. Analizele din literatura de specialitate arată că astfel de atacuri pot produce disfuncționalități majore fără utilizarea forței armate, afectând funcționarea serviciilor esențiale și generând instabilitate economică și socială (Kello 2013, 18-19). Exemplele recente, inclusiv operațiile cibernetice, asociate conflictului din

Ucraina evidențiază capacitatea acestor acțiuni de a amplifica efectele confruntării prin perturbarea infrastructurilor critice.

Caracterul asimetric al atacurilor cibernetice permite actorilor cu resurse limitate să genereze efecte strategice disproporționate. Această realitate modifică logica tradițională a conflictului, în care superioritatea materială nu mai garantează securitatea. În consecință, protecția infrastructurilor critice devine o prioritate strategică, iar securitatea cibernetică este integrată tot mai mult în politicile de apărare națională.

#### **4.2. Războaie informaționale: dezinformare și manipulare strategică**

Războaiele informaționale constituie o dimensiune esențială a conflictelor contemporane, în care influențarea percepțiilor devine un obiectiv strategic în sine. Dezvoltarea platformelor digitale și a rețelelor sociale a facilitat desfășurarea unor campanii de dezinformare capabile să afecteze coeziunea socială și procesele decizionale la nivel național și internațional.

Studiile recente evidențiază că manipularea informațională poate eroda încrederea în instituții, poate amplifica polarizarea socială și poate influența comportamentele electorale, contribuind astfel la destabilizarea internă a statelor (Jensen, Valeriano și Maness 2019, 219). Spre deosebire de propaganda tradițională, aceste operații utilizează algoritmi și mecanisme de amplificare digitală care permit diseminarea rapidă și largă a conținutului.

Această dinamică reflectă o schimbare semnificativă în modul de exercitare a puterii, în care controlul narativelor devine la fel de important ca superioritatea militară. În acest context, delimitarea dintre informație veridică și dezinformare devine tot mai dificilă, ceea ce complică procesele de răspuns și de contracarare.

#### **4.3. Apărarea cibernetică și dezvoltarea rezilienței naționale**

Creșterea complexității amenințărilor cibernetice a determinat o schimbare de paradigmă în abordarea securității, de la protecția strict tehnică a sistemelor către dezvoltarea rezilienței. Aceasta implică nu doar prevenirea atacurilor, ci și capacitatea de a absorbi impactul acestora și de a restabili rapid funcționarea sistemelor afectate. Literatura de specialitate subliniază că reziliența cibernetică presupune integrarea unor mecanisme instituționale, politici publice coerente și cooperare între sectorul public și cel privat. Interdependența infrastructurilor critice face ca securitatea să nu mai poată fi asigurată exclusiv la nivel național, fiind necesară coordonarea la nivel internațional.

În acest context, capacitatea statelor de a gestiona riscurile cibernetice devine un indicator esențial al securității. Adaptarea continuă la evoluția amenințărilor și dezvoltarea unor mecanisme de răspuns rapid sunt elemente fundamentale pentru menținerea stabilității în mediul digital.

#### **4.4. Integrarea ciberneticii în strategiile militare și geopolitice**

Dimensiunea cibernetică a fost integrată progresiv în strategiile militare și geopolitice, devenind un instrument de proiecție a puterii și influenței strategice. Statele dezvoltă capacități cibernetice ofensive care le permit să desfășoare operații

de spionaj, de perturbare și influență, fără a depăși pragul conflictului armat deschis. Această evoluție extinde logica competiției din zona gri, în care presiunea strategică este exercitată prin instrumente nonconvenționale, exploatând ambiguitatea și dificultatea atribuirii (Mazarr 2015, 3-7). În acest cadru, conflictul nu mai este limitat la episoade discrete de confruntare, ci capătă caracterul unui proces continuu.

Integrarea dimensiunii cibernetice în strategiile statelor influențează echilibrul de putere la nivel global, întrucât capacitățile digitale devin un element esențial al competitivității strategice. Această realitate impune dezvoltarea unor cadre doctrinare și juridice adaptate, precum și consolidarea cooperării internaționale pentru gestionarea riscurilor asociate.

Literatura recentă din domeniul dreptului internațional aplicabil spațiului cibernetic evidențiază dificultățile definirii pragului dintre operațiunile cibernetice și actele de agresiune, precum și problemele legate de atribuire și responsabilitate statală (Schmitt 2017, 11-12).

## 5. Transformarea armatei moderne

Transformarea armatei moderne reflectă adaptarea structurilor militare la un mediu de securitate caracterizat prin complexitate, interdependență și accelerarea schimbării tehnologice. Forțele armate nu mai pot fi analizate exclusiv prin prisma dimensiunii efectivelor sau a capacităților convenționale, ci ca sisteme integrate, capabile să opereze simultan în multiple domenii și să valorifice avantajele oferite de tehnologiile emergente.

Literatura de specialitate evidențiază faptul că această transformare are o dimensiune dublă: pe de-o parte, tehnologică, prin integrarea sistemelor digitale și a inteligenței artificiale, iar pe de altă parte, organizațională, prin adaptarea doctrinelor și proceselor decizionale (Manolache 2023, 169-170). Ritmul accelerat al schimbării impune dezvoltarea unor structuri flexibile, capabile să răspundă rapid la evoluțiile mediului operațional.

### 5.1. Conceptul de operații multidomeniu (MDO)

Conceptul de operații multidomeniu (Multi-Domain Operations – MDO) reflectă evoluția gândirii militare către integrarea simultană a efectelor în domeniile terestru, aerian, naval, cibernetic și spațial. Această abordare depășește logica tradițională a operațiilor combinate, punând accent pe coordonarea rapidă și sincronizarea capacităților în medii operaționale complexe.

Strategiile doctrinare recente, dezvoltate de Departamentul Apărării al SUA, subliniază necesitatea integrării capacităților din toate domeniile operaționale într-o arhitectură comună de comandă și control, bazată pe schimb rapid de date și coordonare în timp real (U.S. Department of Defense 2022, 11-13).

Conceptul Multi-Domain Operations este reflectat în doctrina recentă a armatei SUA, care urmărește integrarea efectelor generate în domeniile terestru, aerian, naval, cibernetic și spațial într-un sistem unificat de comandă și control. Conflictul din Ucraina evidențiază aplicabilitatea acestui model prin integrarea imaginilor satelitare, a dronelor tactice și a artileriei de precizie într-un ciclu decizional accelerat.

Analizele recente subliniază că succesul operațional depinde de capacitatea de a integra informațiile provenite din multiple domenii și de a genera efecte convergente asupra adversarului (Manolache 2023, 165-166). Interconectivitatea sistemelor și viteza de procesare a datelor devin factori determinanți ai eficienței militare, iar superioritatea nu mai este asociată controlului unui singur domeniu, ci capacității de a acționa coerent în toate domeniile.

Această evoluție implică adaptări semnificative la nivel doctrinar și organizațional, inclusiv dezvoltarea unor structuri de comandă capabile să gestioneze complexitatea operațiilor multidomeniu.

### **5.2. Digitalizarea logisticii și optimizarea lanțurilor de aprovizionare**

Logistica militară a trecut printr-un proces accelerat de transformare, determinat de integrarea tehnologiilor digitale și de creșterea complexității mediului operațional. Sistemele moderne permit monitorizarea în timp real a resurselor, anticiparea necesarului logistic și adaptarea rapidă la schimbările din teren.

Studiile din domeniu arată că digitalizarea logisticii contribuie la creșterea eficienței operaționale prin reducerea incertitudinii și optimizarea distribuției resurselor. Lanțurile de aprovizionare devin mai transparente și mai flexibile, ceea ce permite susținerea operațiilor în medii contestate sau instabile.

Această transformare modifică rolul logisticii, care nu mai este doar o funcție de sprijin, ci un element strategic, capabil să influențeze direct rezultatul operațiilor. Capacitatea de a asigura continuitatea aprovizionării și de a gestiona perturbările devine un factor esențial al succesului militar.

### **5.3. Interoperabilitatea și modernizarea forțelor aliate**

Interoperabilitatea reprezintă o condiție fundamentală pentru funcționarea eficientă a alianțelor militare contemporane. Compatibilitatea tehnologică a sistemelor, armonizarea doctrinelor și standardizarea procedurilor permit desfășurarea operațiilor comune și reducerea fricțiunilor operaționale.

Literatura de specialitate evidențiază faptul că interoperabilitatea nu se limitează la aspectele tehnice, ci include dimensiuni organizaționale și culturale. Exercițiile multinaționale și schimbul de informații contribuie la consolidarea capacității de reacție colectivă și la creșterea coeziunii operaționale.

Modernizarea forțelor aliate este strâns legată de integrarea tehnologiilor emergente și de dezvoltarea unor sisteme comune de comandă și control. Această evoluție consolidează capacitatea alianțelor de a răspunde rapid și eficient la amenințările contemporane.

### **5.4. Rolul tehnologiilor emergente în transformarea mentalității militare**

Tehnologiile emergente influențează nu doar capacitățile tehnice ale forțelor armate, ci și modul în care este concepută gândirea militară. Integrarea inteligenței artificiale și a sistemelor autonome determină trecerea de la planificarea liniară la procese decizionale adaptative, bazate pe analiza continuă a datelor.

Studiile recente evidențiază că această transformare implică o redefinire a rolului factorului uman, care trebuie să gestioneze interacțiunea cu sisteme automatizate și

să înțeleagă limitările acestora (Johnson 2019, 1417-1418). Decizia militară devine rezultatul unei colaborări între om și tehnologie, ceea ce ridică provocări legate de responsabilitate și control.

Această evoluție impune dezvoltarea unei culturi organizaționale orientate spre inovare, învățare continuă și adaptabilitate. Forțele armate care reușesc să integreze aceste tehnologii în structuri flexibile pot obține avantaje semnificative într-un mediu strategic caracterizat prin incertitudine și competiție persistentă.

Analiza realizată sugerează că viitorul conflictelor globale va fi dominat de forme persistente de competiție multidomeniu, în care instrumentele informaționale, cibernetice și economice vor deveni la fel de relevante ca utilizarea directă a forței militare. Această tendință indică apariția unui model de conflict, caracterizat prin competiție strategică permanentă și integrarea simultană a presiunii în multiple domenii operaționale.

## 6. Perspective asupra viitorului conflictelor globale

Evoluția conflictelor globale indică o transformare structurală a modului în care competiția strategică este desfășurată, marcând o tranziție de la confruntările convenționale de mare intensitate către forme persistente de competiție multidimensională. Interdependențele economice, digitalizarea accelerată și dezvoltarea tehnologiilor emergente contribuie la configurarea unui mediu de securitate în care presiunea strategică poate fi exercitată continuu, fără depășirea pragului conflictului armat deschis (Mazarr 2015, 3-7; NATO 2022, 5-7).

Această evoluție reflectă o schimbare de logică în desfășurarea conflictului, în care acumularea graduală a efectelor asupra infrastructurilor, percepțiilor și proceselor decizionale devine mai relevantă decât obținerea unor victorii decisive pe câmpul de luptă. Studiile recente subliniază că actorii statali preferă din ce în ce mai mult utilizarea unor instrumente indirecte, capabile să genereze avantaje strategice, fără escaladare militară directă (Jensen, Valeriano și Maness 2019, 212-214).

Un element central al conflictelor viitoare îl reprezintă integrarea profundă a dimensiunii cibernetice în strategiile geopolitice. Spațiul digital oferă oportunități pentru desfășurarea unor operații de influență, sabotaj și culegere de informații, toate caracterizate de dificultăți de atribuire și de costuri reduse. Această realitate favorizează dezvoltarea unor strategii bazate pe presiune continuă, în care instrumentele cibernetice, informaționale și economice sunt folosite într-o manieră integrată pentru a modifica echilibrul de putere.

În plan operațional, conflictele viitoare vor fi caracterizate de accelerarea ciclului decizional și de integrarea sistemelor autonome în procesele de luptă. Capacitatea de a corela rapid informațiile provenite din multiple surse și de a genera efecte coordonate în mai multe domenii devine un factor determinant al eficienței militare. Literatura de specialitate evidențiază faptul că superioritatea nu mai este asociată exclusiv masei forțelor, ci capacității de a integra tehnologia, informația și structurile organizaționale într-un sistem coerent (Manolache 2023, 168-170).

Un alt element definitoriu îl constituie creșterea rolului actorilor nonstatali și a conflictelor asimetrice. Aceștia pot exploata vulnerabilitățile infrastructurale și informaționale ale statelor, generând efecte strategice, fără a dispune de capacități militare convenționale comparabile. Această tendință contribuie la complexitatea mediului de securitate și la dificultatea gestionării conflictelor.

Pe termen lung, stabilitatea internațională va depinde de capacitatea actorilor de a gestiona echilibrul dintre inovarea tehnologică și mecanismele de reglementare. Dezvoltarea accelerată a inteligenței artificiale, a sistemelor autonome și a capacităților cibernetice ridică probleme legate de control, responsabilitate și predictibilitate. Lipsa unor cadre normative clare poate amplifica riscurile și poate conduce la creșterea instabilității sistemice.

Viitorul conflictelor globale va fi definit de competiția persistentă, în care diferența dintre pace și război devine tot mai dificil de delimitat. Capacitatea statelor de a integra tehnologia, de a dezvolta reziliența și de a gestiona complexitatea mediului de securitate va reprezenta un factor decisiv în menținerea avantajului strategic.

## Concluzii

Analiza realizată confirmă faptul că războiul contemporan a suferit o transformare structurală, evoluând de la paradigma confruntărilor convenționale către un model multidimensional, în care domeniile cibernetic, informațional, economic și spațial capătă o importanță comparabilă cu dimensiunea militară tradițională. Această evoluție susține ipoteza conform căreia natura conflictului în secolul XXI este definită de interdependență, ambiguitate și competiție persistentă sub pragul confruntării directe.

Examinarea rolului tehnologiilor emergente evidențiază faptul că digitalizarea, inteligența artificială și sistemele autonome nu reprezintă doar instrumente de eficientizare operațională, ci factori care reconfigurează raporturile de putere și modul de desfășurare a conflictelor. Capacitatea de a integra și de a exploata informația devine un determinant central al avantajului strategic, ceea ce confirmă ipoteza privind transformarea criteriilor de superioritate militară.

Exemplele analizate, precum războiul ruso-ucrainean, utilizarea dronelor în conflictul din Nagorno-Karabah și operațiile cibernetice asupra infrastructurilor critice, evidențiază faptul că avantajul strategic este determinat tot mai mult de capacitatea de integrare multidomeniu și de exploatarea rapidă a informației. Dimensiunea cibernetică și informațională demonstrează că perturbarea infrastructurilor critice și exploatarea vulnerabilităților digitale permit exercitarea unei presiuni strategice continue, fără escaladare militară directă.

Din punct de vedere metodologic, utilizarea unei abordări calitative de tip analitic și conceptual, bazată pe analiza literaturii de specialitate și pe comparația dintre formele tradiționale și contemporane de conflict a permis identificarea unor

tendințe coerente și a unor relații cauzale între tehnologie, strategie și transformarea paradigmei militare. Această abordare oferă un cadru interpretativ relevant pentru înțelegerea evoluției conflictelor în secolul XXI.

Contribuția teoretică a lucrării constă în integrarea conceptelor de război hibrid, operații multidomeniu și competiție în zona gri într-un model interpretativ unitar al conflictului contemporan. Analiza susține ideea că războiul actual evoluează către o formă persistentă de competiție strategică multidimensională, în care delimitarea dintre pace și conflict devine tot mai dificil de realizat.

De asemenea, analiza subliniază că avantajul strategic nu mai este determinat exclusiv de resursele materiale, ci de capacitatea de a integra tehnologia, informația și procesele decizionale într-un sistem coerent și adaptabil. Această concluzie are implicații directe asupra modului în care statele își configurează strategiile de apărare și își dezvoltă capabilitățile militare.

Lucrarea oferă o perspectivă analitică asupra transformării războiului contemporan și contribuie la clarificarea relației dintre tehnologie, strategie și securitate, evidențiind direcțiile principale de evoluție ale conflictelor globale.

Pe baza analizei realizate, lucrarea propune interpretarea războiului contemporan prin conceptul de „conflict multidimensional persistent”, definit ca o formă de competiție strategică, desfășurată simultan în domeniile militar, cibernetic, informațional, economic și spațial, caracterizată prin continuitate, ambiguitate strategică și integrare tehnologică. Spre deosebire de paradigma clasică a confruntării convenționale, acest model evidențiază faptul că avantajul strategic este determinat, în principal, de capacitatea actorilor de a integra informația, tehnologia și presiunea exercitată simultan în multiple domenii într-un mecanism coerent de influență și adaptare operațională.

Prezenta cercetare prezintă însă anumite limitări, generate de caracterul său predominant conceptual și de absența unor analize empirice cantitative sau a unor studii de caz aprofundate. Deși abordarea utilizată permite identificarea unor tendințe majore și formularea unor concluzii relevante, integrarea unor date empirice ar putea consolida validitatea rezultatelor.

Cercetările viitoare ar putea viza analiza comparativă a unor conflicte recente, utilizarea metodelor mixte (calitative și cantitative) și evaluarea impactului tehnologiilor emergente asupra diferitelor tipuri de actori. De asemenea, explorarea relației dintre inteligența artificială, autonomie decizională și stabilitate strategică reprezintă o direcție relevantă pentru dezvoltarea ulterioară a domeniului.

## Referințe

**Biddle, Stephen.** 2022. “Back in the Trenches: Why Attrition Still Dominates the Battlefield.” *International Security* 46(4): 32-35. <https://direct.mit.edu/isec/article/46/4/7/109111/Back-in-the-Trenches-Why-Attrition-Still>.

- Boyle, Michael J.** 2015. “The Legal and Ethical Implications of Drone Warfare.” *International Journal of Human Rights* 19(2): 4. <https://doi.org/10.1080/13642987.2014.991210>.
- Freedman, Lawrence.** 2017. *The Future of War: A History*. New York: PublicAffairs.
- Hoffman, Frank G.** 2018. “Examining Complex Forms of Conflict: Gray Zone and Hybrid Warfare.” *PRISM* 7(4): 30–47. <https://ndupress.ndu.edu/Media/News/Article/1680696/examining-complex-forms-of-conflict-gray-zone-and-hybrid-challenges/>.
- Horowitz, Michael C.** 2010. *The Diffusion of Military Power: Causes and Consequences for International Politics*. Princeton, NJ: Princeton University Press.
- International Institute for Strategic Studies (IISS).** 2024. “The Military Balance 2024.” *The Military Balance* 124(1): 15–16. London: Routledge. <https://doi.org/10.4324/9781003485834>.
- Jensen, Benjamin M., Brandon Valeriano și Ryan C. Maness.** 2019. “Fancy Bears and Digital Trolls: Cyber Strategy with a Russian Twist.” *Journal of Strategic Studies* 42(2): 212–219. <https://doi.org/10.1080/01402390.2018.1559152>.
- Johnson, James.** 2019. “Artificial Intelligence & Future Warfare: Implications for International Security.” *International Affairs* 95(6): 1397–1418. <https://doi.org/10.1093/ia/iiz125>.
- Manolache, Ionela Cătălina.** 2023. “The Role of Multi-Domain Operations in Modern Warfare.” *Land Forces Academy Review* 28(3): 163–170. <https://doi.org/10.2478/raft-2023-0020>.
- Kello, Lucas.** 2013. “The Meaning of the Cyber Revolution: Perils to Theory and Statecraft.” *International Security* 38(2): 7–21. [https://doi.org/10.1162/ISEC\\_a\\_00138](https://doi.org/10.1162/ISEC_a_00138).
- Konaev, Margarita.** 2023. *The Future of Conflict: Autonomous Systems and Artificial Intelligence*. Washington, DC: Center for Security and Emerging Technology (CSET).
- Mazarr, Michael J.** 2015. *Mastering the Gray Zone: Understanding a Changing Era of Conflict*. Santa Monica, CA: RAND Corporation. <https://doi.org/10.7249/RR1003>.
- NATO.** 2022. “NATO Strategic Concept.” Brussels: North Atlantic Treaty Organization. <https://www.nato.int/content/dam/nato/webready/documents/publications-and-reports/strategic-concepts/2022/290622-strategic-concept.pdf>.
- Payne, Kenneth.** 2021. *I, Warbot: The Dawn of Artificially Intelligent Conflict*. London: Hurst Publishers.
- Salehyan, Idean.** 2009. *Rebels without Borders: Transnational Insurgencies in World Politics*. Ithaca, NY: Cornell University Press. <https://www.degruyterbrill.com/document/doi/10.7591/9780801459214/html>.
- Scharre, Paul.** 2018. *Army of None: Autonomous Weapons and the Future of War*. New York: W. W. Norton & Company.
- Schmitt, Michael N.** 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press. <https://doi.org/10.1017/9781316822524>.

**U.S. Department of Defense.** 2022. "Joint All-Domain Command and Control (JADC2) Strategy." <https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.pdf>.

**Watling, Jack.** 2023. *The War in Ukraine and the Evolution of Modern Warfare*. London: Royal United Services Institute (RUSI).