

Adrian LESENCIUC

Războiul informațional

Ediția a II-a, revizuită și adăugită

**Editura Academiei Forțelor Aeriene „Henri Coandă”
Brașov, 2025**

Editura Academiei Forțelor Aeriene „Henri Coandă”
Str. Mihai Viteazul nr. 160, Brașov, 500183
Telefon: 0268/423421, fax: 0268/422004
e-mail: editura@afahc.ro

Editură cu prestigiu recunoscut A2 în domeniile „Științe sociale”, „Științe militare, informații și ordine publică”

Războiul informațional Ediția a II-a, revizuită și adăugită -
Adrian LESENCIUC

Referenți științifici:

Prof.univ.dr. Marian PEARSICĂ

Academia Forțelor Aeriene „Henri Coandă”

Conf.univ.dr. Laurian GHERMAN

Academia Forțelor Aeriene „Henri Coandă”

Lector de carte:

Angela-Karina AVĂDĂNEI

Descrierea CIP a Bibliotecii Naționale a României
LESENCIUC, ADRIAN

Războiul informațional / Adrian Lesenciuc.-Ed. A 2-a,
reviz. Și adăug.. - Brașov: Editura Academiei Forțelor Aeriene
„Henri Coandă”, 2025

Conține bibliografie

ISBN 978-630-6507-39-9

355.013

Comanda nr.213/2025

Viza 0574/2025

Tiraj: 50 ex.

Cuprins

Cuprins	3
1. Războiul	5
1.1 Războiul și ceața terminologică a realismului politic	5
1.2 Războiul ca fenomen social	11
1.3 Război vs. conflict armat	17
1.4 Război vs. confruntare	27
1.5 Tipologii ale războaielor	32
1.5.1 Războaie juste și injuste	33
1.5.2 Războaie convenționale, neconvenționale și hibride	36
1.5.3 Războaie simetrice și asimetrice	39
1.5.4 Războaie absolute, totale și limitate	43
1.5.5 Alte tipologii conflictuale	46
1.6 Ultima „revoluție militară” și efectele ei asupra conflictului contemporan	50
2. Operațiile informaționale în conflictul contemporan	57
2.1 Operațiile întrunite	57
2.2 Operațiile informaționale ca funcție întrunită	67
2.3 Operațiile informaționale ca operații de influențare	73
3. Operațiile informaționale	77
3.1 Scop, obiective, principii	77
3.1.1 Scop și obiective	77
3.1.2 Principiile operațiilor informaționale	84
3.2 Relații de coordonare și cooperare	90
3.2.1 Filosofia StratCom	90
3.2.2 Relații de coordonare în cadrul Info Ops	94
3.2.3 Relații de cooperare cu structurile PR/ PA/ Mil PA/ Media Ops.....	101
3.2.4 Relații de cooperare cu CIMIC	107
3.2.5 Alte relații de cooperare	111
3.2.6 Fluxuri informaționale de informare și influență	113
4. Activități desfășurate în cadrul operațiilor informaționale	119
4.1 Tipuri de activități desfășurate în cadrul operațiilor informaționale	119
4.2 Activități de influențare	124
4.2.1 Operațiile psihologice (PsyOps)	124
4.2.2 Inducerea în eroare (MILDEC)	128
4.2.3 Prezența, postura și profilul (PPP). Conduita și	

standardele de comportament	130
4.2.4 Angajarea. Înțelegerea culturală	132
4.3 Activități de protecție a informațiilor	135
4.3.1 Securitatea operației (OPSEC)	135
4.3.2 Asigurarea informațiilor	137
4.4 Activități îndreptate împotriva conducerii adversarului și a capacității sale acționale	141
4.4.1 Operațiile cibernetice	141
4.4.2 Războiul electromagnetic	146
4.4.3 Distrugerea fizică	150
5. Războiul informațional	151
5.1 Conceptul actual de război informațional	151
5.2 De la conceptul de război la necesitatea de redefinire a conceptului de război informațional	157
5.3 Măștile războiului informațional	161
Abrevieri	169
Bibliografie	175

1. Războiul

La paix est plus importante que la guerre parce que le but de la guerre c'est la paix alors que le but de la paix n'est pas la guerre.

Sfântul Augustin din Hippona (354-430)

1.1 Războiul și ceața terminologică a realismului politic

Războiul este o formă de agresiune care presupune uzul forței organizate și al violenței fizice deschise. Cu toate acestea s-a răspândit, datorită promovării intense prin intermediul mijloacelor de comunicare de masă, o accepțiune largă a termenului „război” asociată oricărei forme de confruntare: psihologică, cognitivă, mediatică, informațională, hibridă, care nu contribuie la clarificări terminologice, ci mai degrabă la bulversarea înțelegerii. Această răspândire a accepțiunii *light* a termenului „război” se datorează fie necunoașterii conținutului din perspectiva câmpului de aplicare (științele securității, științe militare, științe politice), fie unei intenționate (sau neintenționate) afilieri la o paradigmă a relațiilor internaționale, fundamentată de realismul politic, o teorie pesimistă asupra raporturilor dintre state, în care aceste entități acționează rațional și luptă pentru putere. Din această perspectivă privind, în care raporturile dintre state au la bază competiția dintre ele, pacea și războiul sunt aparente, granițele dintre ele sunt fragile, există o stare de continuă competiție, iar pacea este garantată de echilibrul întregului sistem global de putere (adică de

reconfigurarea unei perspective bipolare sau multipolare la nivel global).

Filosoful american Jeff McMahan, una dintre figurile reprezentative în domeniul eticii militare, cu o contribuție remarcabilă în „teoria războiului drept” (*just war theory*), a rezumat (inclusiv din punct de vedere etic) problematică școlii de gândire a realismului politic după cum urmează:

Teoria care stă de obicei la baza formulării politicilor de securitate națională se numește „realism politic”. Conform acestei teorii, normele morale nu se aplică politicii externe, care ar trebui să fie ghidată în mod exclusiv de preocuparea pentru interesul național. (McMahan, 2006:414).

Din păcate această paradigmă a revenit în forță și alimentează nu numai gândirea politică a Federației Ruse – interesul național în limitele acestei paradigme se extinde la un spațiu de control care se suprapune peste un amplu teritoriu eurasiatic de influență istorică –, ci și cea specifică mișcărilor iliberale (a se înțelege prin iliberal situarea în afara paradigmei liberaliste) și suveraniste. Există în noul climat internațional voci majore care clamează înlocuirea ordinii mondiale liberal-progresiste cu ordinea mondială suveranistă, ceea ce, pentru a nu transfera problematica dezbaterii noastre în plan politic, înseamnă în primul rând setarea cadrului paradigmatic de dezbateri. Noua revenire în forță este cea a realismul politic, într-o nouă viziune și într-un alt tipar de agresivitate față de expresia de după încheierea celui de-Al Doilea Război Mondial, într-o formulă care actualizează viziunea lui Hans Morgenthau și Henry Kissinger, așezată pe un cadru teoretic din care nu lipsesc fundamentele politice ale lui Niccolò Macchiavelli, cele filosofice ale lui Thomas Hobbes, ori cele militare ale lui Carl von Clausewitz. Această proiecție clasică a realismului e mai degrabă una utopică și atotcuprinzătoare – teoreticianul britanic Ken Booth (2011:7) consideră că termenul „realism clasic” este

imprecis, cuprinzând nu neapărat o tradiție sau o școală de gândire politică universală, ci mai degrabă un cadru de afiliere la un grup autodefinit, care se exprimă în istorie prin lucrări aliniate ideologic pe durata a două milenii și jumătate, de la Tucidide până astăzi – care poate avea pretenția de autodefinire drept cadru paradigmatic, chiar dacă o școală similară de gândire a fost activă în anii 1930-1960, având reprezentanți în special în Statele Unite.

Din această perspectivă, a realismului clasic (atât în înțelesul său extins, paradigmatic, cât și în raport cu școala de gândire în domeniul relațiilor internaționale de la jumătatea secolului al XX-lea), pacea este posibilă doar ca rezultat al punerii în act a unui mecanism auto-reglator în lupta pentru putere pe scena internațională, ori ca impunere normativă internațională, așa cum fusese prefigurat de Hans Morgenthau încă din 1949:

Într-o lume a cărei forță motrice este aspirația la putere a națiunilor suverane, pacea poate fi menținută numai prin două mecanisme. Unul este mecanismul de autoreglare a forțelor sociale care se manifestă în lupta pentru putere pe scena internațională, adică echilibrul puterii. Celălalt constă în limitări normative ale acestei lupte sub forma dreptului internațional, a eticii internaționale și a opiniei publice mondiale¹ (Morgenthau, 1949:8-9),

dar echilibrul fragil al sistemului internațional organizat după principii realist-politice presupune aducerea în dezbatere și a

¹ In a world whose moving force is the aspiration for power of sovereign nations, peace can be maintained only by two devices. One is the self-regulatory mechanism of the social forces which manifests itself in the struggle for power on the international scene, that is, the balance of power. The other consists of normative limitations upon that struggle in the form of international law, international morality, and world public opinion [t.n.], în engleză în original

unui alt aspect: pacea și războiul se confundă în limitele acestei paradigme, ca, de exemplu, în proiecția unuia dintre profesorii din Departamentul de Politici Internaționale de la Aberystwyth, universitate în cadrul căreia s-a încheiat una dintre cele mai importante școli din domeniul științelor securității, Școala de la Aberystwyth²:

Deși „pacea” și „războiul” sunt considerate de obicei opuse, există un sens în care ambele devin aspecte ale conflictului endemic în întreaga viață socială. Războiul este pur și simplu un tip special de conflict care diferă de pace doar prin natura sa violentă.³ (Garnett, 2007:39).

Totuși, John Garnett lansase ideea încă din 1970, când rivalitatea dintre neorealism și neoliberalism caracteriza

² Școala de la Aberystwyth sau Școala Galeză este numele uneia dintre cele mai reprezentative grupări teoretice din domeniul studiilor securității, continuând linia deschisă de realismul politic și definind-o ca *emancipatory realism* (realism emancipator). Școala de la Aberystwyth propune o fuziune cu teoria critică a Școlii de la Frankfurt și continuă să fie interesată, în linia realismului originar, de sistemul de putere și de dinamica puterilor în societate. Ceea ce propune ca direcție analitică poartă numele de Critical Security Studies, din care se vor desprinde, mai târziu, Școala de la Copenhaga și Școala de la Paris. În rezumat, Școala de la Aberystwyth propune teoria ca element constitutiv al realității, adică: „The Aberystwyth School is a post-positivist approach that views theory as constitutive of reality. The relationship between the theory and its historical, social and political context is deemed very crucial. Furthermore, it is asserted that theory has a responsibility to guide the practice to enhance the security of humanity.” (Sezal, 2019:76), proiectând o înțelegere a lumii în dinamica schimbării emancipatoare în varii domenii de manifestare ale puterii soft. Școala se va separa de realism odată cu scrierile lui Ken Booth, care va avea o poziție tranșantă față de realismul clasic sau utopic și de „noul medievalism” în relațiile internaționale (Booth, 1991:527).

³ Though ‘peace’ and ‘war’ are usually regarded as opposites, there is a sense in which both are aspects of the conflict that is endemic in all social life. War is simply a special kind of conflict that differs from peace only by its violent nature, [t.n.], în engleză în original.

confruntarea paradigmatică din anii Războiului Rece, și când argumentele cele mai puternice ale realismului proiectau „ceață” conceptuală între termenii „pace” și „război” și viziunea limpede a necesității războaielor cauzate de imperfecțiunea lumii: „Războaiele sunt necesare pentru că trăim într-o lume imperfectă și sunt necesare politici mai puțin perfecte pentru a supraviețui în ea”⁴ (Garnett, 1970:30). Mai mult, sublinia Garnett (1970:30), gândirea strategică (în termeni realiști) presupune a nu crede în pace cu orice preț: „Deși majoritatea gânditorilor strategici au înclinații pacifiste, ei nu sunt de regulă pacifiști și nu cred în pacea cu orice preț”⁵.

În România realismul politic și expresia sa în plan militar, neoclausewitzianismul, au avut o puternică susținere și în perioada în care în plan internațional fuseseră repudiate. Generalul Mihail Orzeață, fost locțiitor al Șefului Statului Major General și profesor la Universitatea Națională de Apărare „Carol I”, este cel mai important reprezentant al acestei școli de gândire, fiind autorul unor lucrări în care extinde perspectiva lui Hans Morgenthau, Henry Kissinger și John Garnett, considerând pacea ca fiind o perioadă dintre două conflicte în care confruntarea continuă să existe, deși este nonviolentă (Orzeață, 2011). Evident, conceptul de *război continuu* promovat prin lucrarea omonimă, premiată de revista *Gândirea Militară Românească* – deși competiția și confruntarea interstatală la nivelul puterilor *soft* beneficiază de o abordare distinctă atât din punct de vedere teoretic, cât și doctrinar – a produs efecte asupra unei întregi școli de gândire. Această perspectivă preexista în școala de gândire românească – am realizat o radiografie mai amplă asupra acestei perspective a

⁴ Wars are necessary because we live in an imperfect world and less than perfect policies are required to survive in it, [t.n.], în engleză în original.

⁵ Though most strategic thinkers are pacifically inclined, that are not usually pacifists and they do not believe in peace at any price, [t.n.], în engleză în original.

Realpolitik-ului românesc în expresia sa neoclausewitzină în *Gândirea militară românească sub amprentă clausewitziană*, în subcapitolul „Poziționări neoclausewitziene. Războiul continuu” (Lesenciuc, 2019:69-76), evidențiind modul în care confruntarea informațională este interpretată în limitele permanenței conflictuale –, dar și-a găsit expresia extensiei confruntării permanente dincolo de competiția interstatală a realismului politic american prin lucrarea generalului Orzeacă, în care *războiul continuu* era definit drept confruntarea permanentă:

[...] dintre indivizi, dintre comunități (state, alianțe, entități religioase, etnice, profesionale etc.), dintre indivizi și comunități etc., pentru a-și impune interesele pe multiple planuri: putere, influență, teritorii și resurse (umane, materiale și financiare). (Orzeacă, 2011:31).

Evident, această proiecție poate fi citită în continuarea unei reinterpretări a raporturilor clausewitziene dintre politică și război prin ecuația răsturnată propusă de V.I. Lenin pentru a justifica Revoluția Socialistă, dar perpetuitatea conflictuală nu are justificare operațională pentru că nu contribuie la clarificări, ci induce anterior amintita ceață terminologică:

Războiul continuu, în înțelesul școlii românești de gândire militară, face trimitere la o integralitate socială, complexă, în care nu se poate distinge clar între pace și război. [...] Războiul continuu, în înțelesul de confruntare permanentă în planuri multiple, este rezultatul unei orientări neoclausewitziene a școlii de gândire militară a Universității Naționale de Apărare „Carol I”, care pune în prim-plan perspectiva sistemică, analiza unui continuum în care competiția și, în extrem, conflictualitatea definesc, în esență, o societate în căutarea căilor de acces la resurse și putere. (Lesenciuc, 2019:71, 75).

În ciuda propagării prin diferite lucrări științifice, preponderent fundamentate în liniile realismului clasic incert, așa cum fusese definit de Ken Booth, pacea și războiul nu au limite neclare. Chiar și acum, când un alt termen care contribuie la răspândirea ceții operaționale, conceptul de „război hibrid”, a început să producă nelămuriri și posibilitatea disimulării doctrine, „pacea” și „războiul” nu sunt termeni juxtapozabili, ci consecutivi, ușor de înțeles ca fiind distincți și din perspectiva științelor securității în ansamblu, dar și în ceea ce privește științele politice, cu atât mai mult privitor la științele militare. Într-un studiu din 2023, *Războiul hibrid sau întoarcerea prin disimulare la războiul absolut* arătam nu doar că aceste premise ale nebulozității semantice și, implicit, doctrine produc bulversare: „Odată cu invocarea conceptului de *război hibrid*, o ceață ideologică părea să se așeze și peste conceptele deja clarificate, prezente în strategii sau doctrine.” (Lesenciuc, 2023:11), ci și modul în care Federația Rusă se folosește de această nebulozitate pentru a realiza disimularea și surprinderea și pentru a transforma înainte de toate confruntarea hibridă într-un război al definițiilor, așa cum sesiza cercetătorul britanic Ofer Fridman (2019:67-84), intitulând un capitol din lucrarea care radiografiază fenomenul, *Hybrid Conflicts and Information Warfare. New Labels, Old Politics*, „A War of Definitions: Hybridity in Russia and the West”.

1.2 Războiul ca fenomen social

Războiul, în special în varianta diferendului internațional soluționat prin utilizarea forțelor armate, a tehnicii militare și armamentului din dotarea acestora, în ciuda aparentei frecvențe, este un fenomen destul de rar în ultimele două secole. J. David Singer (1989:202) a evaluat, după încheierea războaielor

napoleoniene, o medie de șase conflicte internaționale pe durata unui deceniu. Dacă ar fi să luăm în calcul această medie a manifestărilor conflictuale la nivelul global (ceea ce ar însemna, considerând doar conflictele interstatale, o medie de șase conflicte la sută de ani pentru fiecare dintre statele lumii,⁶) și perspectiva cunoscută în științele sociale drept *mitologia agresiunii*, datorată lui Goldstein (1989), conform căreia războiul este expresia instinctului agresiunii iar pacea o perioadă atipică între două războaie⁷, putem discuta despre un progres civilizațional remarcabil.

Războiul este expresia raționalizării politice a violenței, presupunând căutarea și articularea argumentelor necesare susținerii efortului de război. Politicul distinge între violența inacceptabilă și violența necesară și acționează pârghiile acceptării cauzei războiului de către populație. Spre exemplu, intrarea Statelor Unite în Războiul din Vietnam (5 august 1964), încurajată de deschiderea președintelui Lyndon B. Johnson față de soluționarea prin violență a „problemei comuniste” și provocată de atacul asupra distrugătorului american USS Maddox din Golful Tonkin⁸, a fost o problemă pusă pe agenda publicului de președintele american și s-a bucurat de susținerea populară. Ieșirea SUA din acest război,

⁶ Din păcate ultimul secol a presupus și existența a două conflicte mondiale, ceea ce înseamnă o creștere a mediei conflictelor în care au fost implicate statele lumii, ele însele în dinamică în ceea ce privește numărul lor. Actualmente numărul statelor a ajuns la 195 state suverane și independente (dintre care 193 membre ale Organizației Națiunilor Unite).

⁷ „War is an expression of the aggression instinct. It is unavoidable because humans have an inborn need to satisfy their aggressives urges. Peace is an aberration, a temporary period between wars. War has always been, and hence will always be, with us.” (Goldstein, 1989:11)

⁸ Atacarea și avarierea distrugătorului USS Maddox s-a produs în data de 2 august 1964. În data de 5 august 1964, Congresul SUA a adoptat „Rezoluția asupra Golfului Tonkin”, care i-a conferit președintelui american Lyndon Johnson posibilitatea să aprobe desfășurarea de operațiuni militare în Vietnam, fără a declara război.

provocată de ofensiva Têt, s-a produs ca urmare a voinței populare, a opoziției radicale a opiniei publice în raport cu războiul, care a pus presiune pe decidenții politici și a determinat implicit și schimbarea discursului politic american în raport cu războiul (decizia președintelui Johnson de a nu mai candida și de a începe tratativele de pace, promisiunile președintelui Nixon de retragere a trupelor americane din Vietnam, adică de „vietnamizare” a războiului).

Și în celelalte cazuri ale conflictelor contemporane importante din ultimele decenii, au contat și decizia politică, și influențarea publicului prin argumente necesare susținerii eforturilor de război. Obținerea bunăvoinței publicului larg în acest sens constituie în sine obiectivul unor activități planificate la nivel politic și militar. De exemplu, conceptul de operații mass-media (Media Ops), importat în aparatul doctrinar românesc din cel britanic, vizează promovarea înțelegerii și obținerea sprijinului public (atât cel intern, cât și cel internațional) pentru desfășurarea operațiunilor militare, în timp ce doctrina britanică a operațiilor mass-media (JDP 3-45.1), subsumată ulterior doctrinei operațiilor informaționale proiecta în mod similar efortul Media Ops cu scopul menținerii nivelului de susținere publică și politică:

Principalul efort al Media Ops în orice operațiune militară este acela de a comunica principalele teme și mesaje publicului adecvat, în urmărirea efectului dorit, rămânând în același timp sensibile la interesele mass-media. Acestea sunt o parte integrantă a oricărei operațiuni militare. Media Ops se concentrează în principal pe nevoia de a menține sprijinul public și politic și, prin urmare, libertatea de acțiune și manevră. Media Ops vor avea influență asupra adversarilor, aliaților și entitățile neutre și, prin urmare, este esențial ca personalul Media Ops și personalul Info Ops să colaboreze îndeaproape pentru a se

asigura că mesajul adecvat este transmis publicului adecvat.⁹ (JDP 3-45.1, 2007:I-3, art.109).

Dimensiunea asumării sociale a războiului nu este singura în ceea ce privește înțelegerea acestuia ca fenomen social. Din perspectivă clausewitziană, societatea este direct implicată în război. O analiză a complexității sale în această angajare, datorată sociologului român Dimitrie Gusti încă din 1915, în *Sociologia războiului*, poate fi lămuritoare atât asupra nivelului efectelor asupra societății, cât și asupra modului în care societatea se reflectă în practicile sale. Din perspectiva lui Gusti, războiul este

[...] produsul simultan al unor nenumărate forțe materiale, morale, intelectuale și economice, cum ar fi: starea fizică a soldatului, starea sanitară, elan sau panică, aprovizionări, anotimp, teren, climă, întâmplare fericită ori întâmplare funestă. Războiul este mult mai mult decât o simplă chestiune de strategie, aprovizionări și armament, căci el rezumă o întreagă epocă istorică, toată știința, toată economia, toată cultura, toată tehnica unui timp se oglindește într-însul! Căci elementul pur omenesc al războiului din ce în ce mai mult este înlocuit cu unul rațional impersonal, care este instrumentul de luptă. Așa că adevăratul studiu adâncit al războiului ar conține o întreagă enciclopedie a timpului, la care ar trebui să contribuie toate științele: geografia, fizica, chimia, mecanica, meteorologia,

⁹ The main effort of Media Ops in any military operation is to communicate the principal themes and messages to the appropriate audiences in pursuit of the desired effect whilst remaining sensitive to media interests. This is an integral part of any military operation. Media Ops are primarily focused on the need to maintain public and political support and hence freedom of action and manoeuvre. Media Ops will have an influence on adversaries, allies and neutrals and it is therefore essential that Media Ops staff and Info Ops staff work closely together to ensure that the right message is put across to the right audiences. [t.n.], în engleză în original.

biologia, medicina, psihologia, etica, istoria, pedagogia, sociologia, dreptul s.a.m.d. (Gusti, 1970:138).

În raport cu perspectiva clausewitziană, conform căreia *războiul este o continuare a politicii cu alte mijloace*, ceea ce se poate traduce printr-o implicare totală a societății în conflict și prin resimțirea efectelor războiului indiferent în cadrul întregii societăți, războiul actual presupune o implicare a întregii societăți, dar nu numai ca societate spectatoare la o confruntare cu miză asemănătoare celei sportive. În condițiile unei virtualizări aproape totale a războiului conștientizată în urmă cu mai bine de două decenii, spre exemplu: „Războiul devine astfel virtual, nu doar pentru că pare să aibă loc pe ecran, ci pentru că angajează societățile doar în mod virtual”¹⁰ (M. Ignatieff, *apud* Angstrom, 2005:17), războiul actual presupune un altfel de amestec real-virtual prin *gamification of war* (Palatha, 2024; Danylyuk, 2025). Prin gamificare, teatrul de operațiuni devine scena reală a unei competiții specifice jocurilor în rețea, în care operatorii de drone sau de instrumente digitale intrați în joc beneficiază de puncte și recompense acordate pentru uciderea unui combatant ori pentru distrugerea unei piese de echipament militar din armata adversă, sunt în competiție și se realizează clasamente pentru stimularea acestei competiții. Prin gamificarea războiului se estompează pe de o parte limitele dintre real și virtual în războiul contemporan, iar pe de altă se ridică serioase probleme de natură etică.

Privitor la efectele sociale ale războiului, analizând evenimentele violente produse după Al Doilea Război Mondial, Monty G. Marshall (2002:70-72) propunea o scalare a magnitudinii. Cele zece categorii de conflicte rezultante sunt, în organizarea descendentă a magnitudinii efectelor, următoarele:

¹⁰ War thus becomes virtual, not simply because it appears to take place on screen, but because it enlists societies only in virtual ways, [t.n.], în engleză în original.

- categoria 10: exterminare și anihilare, presupunând distrugerea inamicului în mod extensiv, sistematic și nediscriminatoriu, începând de la identitatea socială care devine astfel țintă a distrugerii;

- categoria 9: război total, însemnând distrugerea masivă a resurselor umane și a infrastructurii fizice, ținând nediscriminatoriu elemente de infrastructură militară sau civilă și presupunând utilizarea a mai mult de 90% din resurse pentru efortul de război;

- categoria 8: război modern, vizând distrugeri masive, cu efecte mari pe termen mediu, fără a transforma noncombatanții în ținte sistematice și presupunând un efort de război cumulând între 60% și 90% din producția socială;

- categoria 7: război omniprezent (*pervasive warfare*), presupunând existența tehnologiilor de distrugere, dar limitarea capacității de producție, eventual dependența de resurse externe, dislocări de populații de peste 5 milioane, peste 1 milion de morți și peste 50% din producție pentru efortul de război;

- categoria 6: război extins, care înseamnă tehnologii de distrugere în masă limitate, dislocări de aproximativ 2 milioane de persoane, pierderi de vieți umane între 500.000 și un milion și circa 40 de procente din producția internă focalizate pentru efortul de război;

- categoria 5: război consistent și prelungit, bazat pe tehnologii de distrugere la un nivel ridicat, circa 1 milion de persoane dislocate, între 100.000 și 500.000 de victime și peste 25% din producție orientate spre efortul de război;

- categoria 4: confruntare îngrijorătoare (*serious warfare*), cuprinzând tehnologii de distrugere la nivel scăzut, obiective difuze sau indistincte, efecte limitate, operațiuni sporadice, dislocări de circa 100.000 de persoane și pierderi umane între 50.000 și 100.000;

- categoria 3: violență politică gravă (*serious political violence*), presupunând tehnologii de distrugere limitate,

manifestări sporadice ale conflictualității și un număr de victime între 10.000 și 50.000 de persoane;

- categoria 2: violență politică limitată, realizată prin utilizarea limitată a tehnologiilor militare, dislocări de populație pe termen restrâns și un număr de victime între 3.000 și 10.000 de persoane;

- categoria 1: violență politică sporadică, manifestată prin nivel scăzut de aplicare a tehnologiilor militare, prin prezența unor grupuri militante izolate, prin durată scăzută a dislocării unor persoane pentru un timp limitat și prin nu mai mult de 2.000 de victime directe.

Războiul, fenomen al cărui expresie fizică reprezintă lupta armată și care presupune, din perspectivă clausewitziană privind, utilizarea forței pentru impunerea voinței proprii asupra celei a adversarului manifestarea conflictului tinzând spre categoria 10 a taxonomiei Marshall, iar din perspectiva paradigmei Sun Tzu, înfrângerea voinței de a lupta a inamicului (tendința de eliminare a conflictului sau de expresie a sa în limitele inferioare ale scalei Marshall), a cunoscut mutații majore ca organizare și manifestare, dar și-a păstrat esența în ceea ce privește excedarea competiției raționale și intrarea în competiția impunerii voinței indiferent prin ce tip de metode. Din fericire, susține Marshall (2002:70), conflictele de după cel de-Al Doilea Război Mondial nu au atins valori mai mari decât cele specifice categoriei 7 de războaie,

1.3 Război vs. conflict armat

O primă diferență dintre război și conflictul armat derivă din înțelesurile asociate termenilor în dreptul internațional umanitar. Chiar dacă până nu demult legislația internațională a făcut trimitere la raporturile interstatale, mutațiile ultimelor decenii generate în special de amploarea ridicată a fenomenului

terorist și de asimetria morală a conflictelor contemporane au determinat o schimbare a focalizării. În termeni juridici, „conflictul armat” (*armed conflict*) este utilizat în locul celui de „război” (*war*) pentru a fi aplicat cu predilecție în situațiile în care statele sunt angajate în acțiuni militare îndreptate împotriva actorilor non-statali, cum ar fi grupările teroriste. Practic, după adoptarea Tratatului general de renunțare la război din 1928 și, în special, după adoptarea Cartei Națiunilor Unite în 1945, pentru a nu se pune problema încălcării acestora, termenul „conflict armat” s-a diferențiat semantic de „război”. Deși aparent depotențate de *jus ad bellum* (dreptul de a declara război) și de *facultas belland* (calitatea de beligerant), statele – individual sau în coaliții/ alianțe – utilizează termenul „conflict armat” pentru a se prevala de nevoia de răspuns adecvat unor provocări specifice ultimei jumătăți de secol. Spre exemplu, Protocolul I din 1977, adițional la Convenția de la Geneva din 1949, definit astfel:

[...] conflictul armat în care popoarele luptă împotriva dominației coloniale, a ocupației străine sau a regimurilor rasiste, exercitându-și dreptul la autodeterminare, așa cum este consacrat în Carta Națiunilor Unite și în Declarația privind principiile dreptului internațional privitoare la relațiile de prietenie și cooperare dintre state, în conformitate cu Carta Națiunilor Unite¹¹ (Adițional Protocol I, 1977: art.1, alin.4)

Practic, în termeni legali, cuvântul „război” a fost înțeles anterior celui de-al Doilea Război Mondial și, implicit, anterior

¹¹ [...] armed conflict in which peoples are fighting against colonial domination and alien occupation and racist regimes in the exercise of their right of self-determination, as enshrined in the Charter of the United Nations and the Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations, [t.n.], în engleză în original.

Convenției de la Geneva din 1949, în strânsă legătură cu declarația oficială de război, în timp ce după adoptarea Cartei Națiunilor Unite în 1945 declarația formală de război a devenit practic inexistentă. După adoptarea Convenției de la Geneva termenul „conflict armat” a apărut pentru a permite intervenția militară în scopuri umanitare, „pentru a transmite ideea că dreptul umanitar trebuia să se aplice ori de câte ori forțele armate se luptau între ele, indiferent clasificarea oficială”¹² (Paulus & Vashakmadze, 2009:98). În acord cu această perspectivă, agresiunea se definește ca utilizare a forțelor armate împotriva suveranității statale, integrității teritoriale și independenței politice a altui stat, reprezentând elementul central în ceea ce privește definirea termenului „război”. Din această perspectivă juridică, „războiul” menține întreaga conotație negativă a agresiunii statale, cu tot ceea ce derivă din ea, inclusiv consecințele rezultate din Carta Națiunilor Unite, în timp ce termenului de „conflict armat” i se asociază conotația pozitivă, umanitară, intervenția armată pentru pace.

O a doua diferență constă în dimensiunea efectelor. The Stockholm International Peace Research Institute (SIPRI, *apud* Dianzenza, 2013) definește războiul în raport cu numărul victimelor rezultate în confruntarea militară prin aplicarea violenței directe, care trebuie să fie mai mare de 1.000:

Aceasta înseamnă că dacă părțile luptă pe o perioadă de o lună și o mie de oameni sunt uciși din cauza acestei violențe directe, atunci conflictul respectiv trebuie calificat drept „RĂZBOI”. Definiția nu ia în considerare alte persoane care ar fi putut muri din cauza acestor lupte ca o consecință indirectă a ei, cum ar fi lipsa alimentelor, a asistenței medicale ș.a.m.d.¹³

¹² to convey the idea that humanitarian law needed to apply whenever armed forces battled with each other, regardless the official classification, [t.n.], în engleză în original.

¹³ This means that if parties fighting over a period of a month and that a thousand people have been killed from that direct violence, then that

Această perspectivă ia în calcul tendința de scădere a densității de ocupare a câmpului de luptă în conflictele actuale, prin urmare reducerea naturală a numărului de victime directe în războaie. Anterior, începând cu 1987, în acord cu perspectiva Proiectului Ploughshares, iar ulterior cu perspectiva Uppsala Conflict Date Program (UCDP) al Universității din Uppsala, conflictele armate erau definite în raport cu următoarele caracteristici: (i) să fie conflicte politice; (ii) să presupună lupte armate purtate de armate regulate sau formațiuni paramilitare care urmăresc un scop politic și (iii) să existe cel puțin 1.000 de victime directe în confruntare și cel puțin 25 de victime pe an (Regehr, 2011). Actualmente, UCDP definește conflictul armat astfel:

Un conflict armat este o incompatibilitate contestată privitoare la guvern și/sau la teritoriu, în care utilizarea forței armate între două părți, dintre care una este guvernul unui stat, are ca rezultat cel puțin 25 de decese în cadrul luptelor într-un an calendaristic¹⁴ (UCDP, 2025).

în timp ce războiul păstrează coordonatele stabilite de SIPRI: „Un conflict sau o diadă la nivel statal care ajunge la cel puțin 1.000 de morți în cadrul luptelor într-un an calendaristic.”¹⁵ (UCDP, 2025).

conflict must be qualified as "WAR". The definition does not take into consideration other people who might have died by that fighting as an indirect consequence such as lack of food, medical and so on. [t.n.], în engleză în original.

¹⁴ A state-based armed conflict is a contested incompatibility that concerns government and/or territory where the use of armed force between two parties, of which at least one is the government of a state, results in at least 25 battle-related deaths in one calendar year, [t.n.], în engleză în original.

¹⁵ A state-based conflict or dyad which reaches at least 1000 battle-related deaths in a specific calendar year, [t.n.], în engleză în original.

Cea de-a treia diferență dintre termenii „război” și „conflict” derivă din condițiile obligatorii pe care trebuie să le îndeplinească un fenomen social violent pentru a putea fi numit război. În raport cu alte fenomene sociale care presupun confruntarea la nivelul puterilor *soft* (așa numitele „războaie” psihologice, informaționale, cognitive ș.a.), războiul presupune manifestarea explicită a violenței armate. Războiul se caracterizează prin violența armată, considerată condiție *sine qua non* pentru ca un fenomen de agresiune colectivă să poată fi astfel clasificat. Pentru a fi considerat război, un conflict necesită a fi un fenomen social de amploare, a avea largă răspândire, a presupune confruntare între două armate sau formațiuni paramilitare și a se face uz la declarația formală de război. Conflictul poate să fie o simplă neînțelegere dezvoltată până la limitele emergenței crizei sau o stare de confruntare prelungită și cu manifestarea izolată a violenței fizice directe. Violența fizică nu lipsește în cazul conflictului armat, dar diferența majoră este dată de amploarea acesteia, aspect subliniat de Uppsala Conflict Date Program. Totuși, distincția majoră este dată de o altă condiție obligatorie a războiului.

Cea mai clară demarcație terminologică în acest sens a fost realizată de Gaston Bouthoul, părintele polemologiei, care a identificat un set de trei condiții pentru ca un fenomen social violent să poarte numele de război: să existe (1) confruntare armată, implicând forțe armate sau paramilitare, armament și mijloace de luptă, care duc la îndeplinire obiective de natură politică; (2) confruntare între grupuri sociale organizate, intra-, inter- sau suprastatale, respectiv (3) confruntare presupunând utilizarea violenței fizice deschise: „atunci când nu comportă pierderea de vieți omenești, el [n.a.: războiul] nu este decât un conflict sau un schimb de amenințări. „Războiul rece” nu este război” (Bouthoul, 1978:54). Practic, Bouthoul insistă asupra

faptului că „războiul este o luptă¹⁶ armată și sângeroasă între grupuri organizate” (Bouthoul, 1978:54), ceea ce înseamnă că îndeplinirea simultană a celor trei condiții pentru ca un fenomen social violent să fie considerat război este obligatorie. În fig.1 am reprezentat această condiție prin raportare la necesitatea definirii unui plan (războiul) prin cel puțin trei puncte de susținere, condițiile menționate de Bouthoul, deși abordarea sociologului francez de origine tunisiană nu este restrictivă în înțelegerea actuală a conceptului de „războiul”.

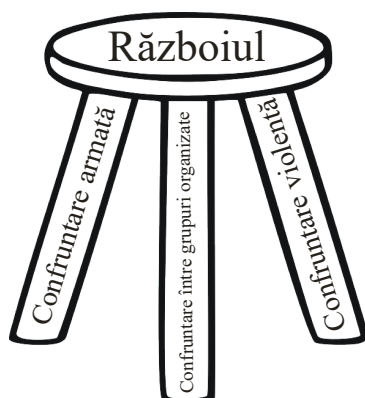


Fig.1 Condițiile necesare și obligatorii pentru ca un fenomen social să poată fi numit război. Interpretare după Bouthoul (1978:54), *apud* Lesenciuc (2014:114)

¹⁶ În lucrarea *Operațiile mass-media. Echilibrul instabil dintre logica militară și logica media*, făceam următoarele remarci privitoare la traducerea nesatisfăcătoare a textului în limba română: „Războiul este o luptă armată și sângeroasă între grupuri organizate” (Bouthoul, 1978:54). Traducerea românească este inexactă, atâta vreme cât în terminologia românească de specialitate lupta și războiul sunt operații desfășurate la nivel tactic, respectiv strategic, așadar concepte care diferă fundamental din perspectiva amplitudinii evenimentelor, trupelor și tehnicii militare implicate, respectiv obiectivelor vizate. În limba franceză în original definiția este următoarea: „la guerre est la lutte armée et sanglante entre groupements organisés” (Bouthoul, 1951:35). Termenul *lutte* înseamnă *luptă*, dar are și sensul de *confruntare*, traducere recomandabilă în acest caz (Lesenciuc, 2013:71).

În baza Raportului International Law Association (ILA, 2008) de la Rio de Janeiro, condiția esențială ca un fenomen social violent să fie numit conflict armat este apariția ostilităților, iar înțelegerea conflictului armat internațional presupune luarea în considerare a două condiții, după cum urmează:

Pentru ca un conflict non-internațional să se încadreze în definiția actuală trebuie îndeplinite două condiții. În primul rând, grupurile implicate în conflict trebuie să aibă o structură organizată. În al doilea rând, violența comisă trebuie calificată drept „prelungită”. Prin urmare, ostilitățile trebuie să atingă un anumit prag de intensitate și durată.¹⁷ (ILA, 2008:4).

În ceea ce privește conflictele armate care nu au caracter internațional, International Law Association le exemplifică prin revolte și alte forme de tulburări și tensiuni interne. Cu alte cuvinte, în afara distincției privitoare la amploarea violențelor fizice și a numărului de victime rezultate, conflictul armat poate să difere de război prin prima condiție dintre cele enumerate de Gaston Bouthoul, mai precis prin lipsa obligativității (pre)existenței unor structuri militare sau paramilitare, respectiv prin posibilitatea ca obiectivele politice care să anime confruntarea să lipsească (mai ales în cadrul conflictelor armate interne). Revoltele nu presupun explicit obiective de natură politică și nici forțe armate. Mai mult, acest raport din 2008 se referă la așa-numitele „non-international armed conflicts” prevăzute în cadrul articolului 3 al Convenției de la Geneva din 1949, dezvoltat, clarificat și adăugit ulterior, care a fost îmbogățit prin jurisprudența Tribunalului

¹⁷ For a non-international conflict to fall under the present definition, two conditions have to be met. First, the groups involved in the conflict have to feature an organized structure. Second, the violence committed must be qualified as “protracted”. Thus, the hostilities must meet a certain threshold of intensity and duration. [t.n.], în engleză în original.

Internațional pentru Crimele din Fosta Iugoslavie, după cum urmează:

un conflict armat există ori de câte ori se recurge la forța armată între state sau la violență armată prelungită între autoritățile guvernamentale și grupuri armate organizate sau între astfel de grupuri în cadrul unui stat ¹⁸ (Prosecutor v. Tadic, Case No. IZ 94-1, Decision on the Defense Motion for Interlocutory Appeal on Jurisdiction, P 70 (Oct. 2, 1995), para. 70., *apud* ILA, 2008:4),

fiind lămuritor în ceea ce privește distincția față de conceptul de război. Formula a fost adoptată și inclusă ulterior în Statutul de la Roma al Curții Penale Internaționale. Unele definiții ale conflictului armat includ obligativitatea confruntării dintre două grupări armate organizate, cum ar fi cea propusă de Theodor Meron (1999), plecând de la aceeași jurisprudență, dar punctul de vedere al juristului american, fost judecător la Curtea Penală Internațională, nu este una unanim acceptată.

International Law Association a definit conceptul luând în considerare amendamentul Meron, operând distincție între conflictele armate internaționale și celelalte conflicte armate, fără a considera grupările armate organizate ca fiind armate sau formațiuni paramilitare:

[...] o situație va fi considerată „conflict armat” dacă există:

- a) o confruntare între state, desfășurată prin forța armată (conflict armat internațional) sau
- b) violență armată prelungită în interiorul unui stat între autoritățile guvernamentale și grupuri armate organizate sau între astfel de grupuri (conflict armat non-internațional)¹⁹. (ILA, 2008:3).

¹⁸ an armed conflict exists, whenever there is a resort to armed force between States or protracted armed violence between governmental authorities and organized armed groups or between such groups within a State, [t.n.], în engleză în original.

¹⁹ [...] a situation shall be deemed an “armed conflict”, if there is

Rezumând, diferențele dintre război și conflict armat sunt următoarele (Tabelul 1) :

Tabelul 1 Diferențele dintre ariile semantice ale conceptelor de război și conflict armat

Condiții		Război	Conflict armat
Condiția 1	1.1 confruntare armată,	obligatorie	obligatorie
	1.2 implicând forțe armate sau paramilitare,	obligatorie	revoltele nu presupun forțe armate regulate sau neregulate
	1.3 armament și mijloace de luptă,	obligatorie	implicit obligatorie
	1.4 care duc la îndeplinire obiective de natură politică	obligatorie	conflictul armat nu presupune obligatoriu obiective de natură politică
Condiția 2	confruntare între grupuri sociale organizate, intra-, inter- sau suprastatale	obligatorie	obligatorie conform amendamentului Meron
Condiția 3	confruntare presupunând utilizarea violenței fizice deschise	obligatorie	obligatorie, dar fără să presupună aceeași amploare ca în cazul războiului

a) a confrontation between States, which is carried out by armed force, (international armed conflict) or

b) protracted armed violence within a State between governmental authorities and organized armed groups or between such groups (non-international armed conflict). [t.n.], în engleză în original.

Războiul este așadar un conflict armat care îndeplinește condiții suplimentare, precum cele proiectate de părintele polemologiei, sociologul Gaston Bouthoul, ori precum cele stabilite de Jessica Wolfendale, profesor universitar, specialist în etica violenței:

Un război există atunci când sunt îndeplinite următoarele condiții:

- (1) Există două sau mai multe grupuri organizate.
- (2) Aceste grupuri sunt angajate în ostilități intense.
- (3) Nicio parte la conflict și nicio altă parte terță nu are efectiv autoritatea de a decide între părțile adverse, de a pedepsi sau de a menține controlul în arena conflictului.²⁰ (Wolfendale, 2008:16),

în esență nu consistent diferite (în ciuda diferențelor dintre domeniile de referință), sau cele din setul de condiții sau caracteristici rezultate din analiza definițiilor războiului realizate de Psarros:

Violență

Caracter structurat

Purtat de unități militare sau miliții

Sub comandă politică civilă

În serviciul statelor sau organizațiilor similare statului

Având structură de comandă internă și reguli de angajare

Respectarea regulilor legale specifice privitoare la declarare și conduită

Respectarea regulilor privind utilizarea armelor

²⁰ A war exists when the following conditions are met:

- (1) There are two or more organized groups.
- (2) These groups are engaged in intense hostilities.
- (3) No party to the conflict and no other third party has the authority and ability to effectively adjudicate between the opposing sides, punish them, and otherwise maintain control in the arena of the conflict. [t.n.], în engleză în original.

Obligația de protejare a necombatantilor și a proprietății părților neutre

Respectarea integrității teritoriale a statelor neutre.²¹ (Psarros, 2023:460).

Indiferent de domeniul de referință și de unghiul sub care este privit războiul, de tipul de trăsături, caracteristici sau condiții identificate în numeroasele definiții ale fenomenului, există cel puțin distincții privitoare la amploare în ceea ce privește diferența dintre război și conflict armat, ultimul termen având o arie semantică mai amplă și reprezentând cel mai adesea genul proxim pentru definirea conceptului de război.

1.4 Război vs. confruntare

În literatura română de specialitate, confuziile dintre „război” și „conflict armat” nu sunt majore. Mai degrabă probleme de această natură apar în traducerea necorespunzătoare a altor termeni. Cum în acest moment limba-vehicul este engleza, foarte bogată în ceea ce privește terminologia asociată războiului, cele mai mari confuzii provin din traducerea unor termeni din această limbă, ale căror înțelesuri nu contribuie la limpezirea conceptuală, ci la efectul

²¹ Violence

Structured

Conducted by military or militia units

Under the command of civil political leaderships

In the service of states or state-like organisations

Have inner command and rules of engagement

Observation of specific legal rules regarding declaration and conduct

Observation of rules regarding the use of weapons

Obligation of protection of non-combatants and of citizens and property of neutral parties

Respect of the territorial integrity of neutral states. [t.n.], în engleză în original.

advers. Unul dintre acești termeni este „warfare”, ale cărui înțelesuri sunt complexe, iar traducerea nu este adecvată fiecărui context în parte. Spre exemplu, sintagma „information warfare” este tradusă în limba română prin „război informațional”, necorespunzător ca arie de acoperire, atâta vreme cât confruntarea violentă nu intră în extensiunea acestui termen.

Confuzia pleacă de la traducerea identică, *război*, a doi termeni din limba engleză, *war* și *warfare*, chiar dacă în limba sursă înțelesurile acestor termeni sunt diferite. Probleme de înțelegere și traducere produce îndeosebi cel de-al doilea, *warfare*, care are două paliere interpretative. În înțeles operațional, conceptul s-ar putea traduce prin „ansamblu de tehnici de luptă” și acoperă pe de o parte totalitatea tehnicilor folosite pentru întrebuințarea unei arme sau specializări militare, iar pe de alta totalitatea tehnicilor privitoare la măsuri militare sau funcții întrunite²². În înțeles strategic, conceptul se traduce prin „confruntare”, iar explicația cea mai adecvată din acest punct de vedere a adus-o profesorul emerit al Universității George Mason, Claudio Cioffi-Revilla.

Termenul „war”, tradus tot prin „război” în limba română, poate fi înțeles în raport cu coordonatele lui Gaston Bouthoul. În încercarea de a opera distincția „war” – „warfare”, Claudio Cioffi-Revilla (2000:254) utilizează o definiție a războiului propusă de Long-Range Analysis of War (LORANOW) Project al Universității din Colorado, proiect început în 1988 cu scopul de a asigura o înțelegere globală, operaționalizată a războiului de-a lungul istoriei (începând cu mileniul IX î.Hr., de când datează această formă de confruntare):

²² În primul caz s-ar încadra, pentru exemplificare, conceptele: *acoustic, amphibious, anti-air, antisubmarine, atomic/nuclear, biological, chemical, directed-energy, electronic, guerilla, mine, strike, surface*, sau *undersea warfare*, iar în cel de-al doilea: *C2, composite, information, irregular, multinational, network, partisan* sau *unconventional warfare*.

Un război (un „eveniment război”) este o situație de violență intenționată și letală între două sau mai multe grupuri sociale care urmăresc obiective politice conflictuale, care are ca rezultat victime, cu cel puțin un grup beligerant sub comanda unei conduceri autoritare²³.

O analiză diacronică a războiului, în raport cu o scală a beligeranței care propune anumite tipologii conflictuale, respectiv în raport cu o scală a procesualității, care propune o focalizare cronologică asupra gradului de soluționare, conduce la diferențieri și nuanțări. Dacă cea de-a doua scală presupune diferențieri între macro- și microprocese, prima constituie cadrul de operare cu cei doi termeni care nu sunt nuanțați în traducerea românești: „war” și „warfare”. Pe scala beligeranței se pot utiliza diferite dimensiuni: unitățile comportamentale ale analizei, tipul sau gradul de organizare a conflictului, complexitatea sau dimensiunile, durata, respectiv consecințele multidimensionale ale beligeranței (politice, economice, culturale/ simbolice). Din această perspectivă, termenul „war” desemnează conflictele interne, interstatale, internaționale (chiar mondiale) cu o durată de 10^2 - 10^3 zile, în timp ce termenul „warfare” privește procesele mai complexe dar mai puțin sistematizate decât precedentele, mai lungi ca durată: 10^3 - 10^4 zile, cu impact mai mare asupra civilizației în ansamblu, dar care nu se caracterizează, obligatoriu, prin intensitate ridicată a violenței:

Confruntarea (Warfare), pe de altă parte, este un proces agregat, relativ mai complex, care durează în general cel puțin decenii și

²³ A war (a 'war event') is an occurrence of purposive and lethal violence between two or more social groups pursuing conflicting political goals that results in fatalities, with at least one belligerent group organized under the command of authoritative leadership. [t.n.], în engleză în original.

care este mult mai sistematizat decât războaiele (10^3 - 10^4 zile). Sociologii și istoricii au acordat relativ mai puțină atenție acestei forme de beligeranță la scală mai mare – „confruntarea” –, deși se poate argumenta că aceasta este scara care are un impact mai mare asupra dezvoltării pe termen lung a societăților și civilizațiilor. *Dacă războiul este cel care „creează” un stat, confruntarea este cea care creează o întreagă civilizație.*²⁴ (Cioffi-Revilla, 2000:256).

Analizând comparat, după scala beligeranței, termenii „war” și „warfare” pot fi înțeleși astfel:

Tabelul 2 Scala beligeranței (apud Cioffi-Revilla, 2000:257)

	Războiul ('copacul')	Confruntarea ('pădurea')
Exemple istorice	• Războiul hispano-aztec • Cucerirea Tayasalului • Războiul franco-indian • Războiul franco-rus • Războiul Coreei • Războiul de șase zile	• Cucerirea spaniolă a Lumii Noi • Războiul franco-britanic • Războaiele napoleoniene • Războiul rece • Conflictul arabo-israelian
Unitate de acțiune:	Evenimentul	Procesul
Organizare:	Dezagregat	Agregat
Complexitate:	Relativ simplu	Relativ complex
Durată:	Ani/ 10^2 - 10^3 zile	Decenii/ 10^3 - 10^4 zile
Tipologie:	Civil, interstatal, hegemonic global, mondial	Prelungit, integralimitiv, dezintegrativ, sporadic

²⁴ *Warfare*, on the other hand, is an aggregate, relatively more complex process that generally lasts at least decades and is far less systematized than wars (10^3 - 10^4 days). Social scientists and historians have focused relatively less attention on this larger scale belligerence - 'warfare' - although arguably this is the scale that has greater impact on the long-range development of societies and civilizations. *If war is what forges' a state, warfare is what forges an entire civilization* [t.n.], în engleză în original.

Dacă luăm în discuție ambele perspective, a lui Gaston Bouthoul, care definește războiul în condiționarea sa triadică, respectiv a lui Claudio Cioffi-Revilla, constatăm că fenomenele sociale ample, care nu presupun stare de beligeranță declarată, un început și un sfârșit clar delimitate, respectiv manifestarea obligatorie a violenței fizice, cum este, de pildă, Războiul Rece (pe care Bouthoul îl dă drept exemplu de fenomen agresiv care nu are cum să fie considerat război), pot fi puse sub umbrela termenului „warfare”. Într-o traducere corespunzătoare, acest termen ar trebui să fie înțeles drept „confruntare”, desemnând conflictualitatea (uneori mocnită) mai puțin intensă, purtată la nivelul puterilor *soft*: politică, economică și simbolică.

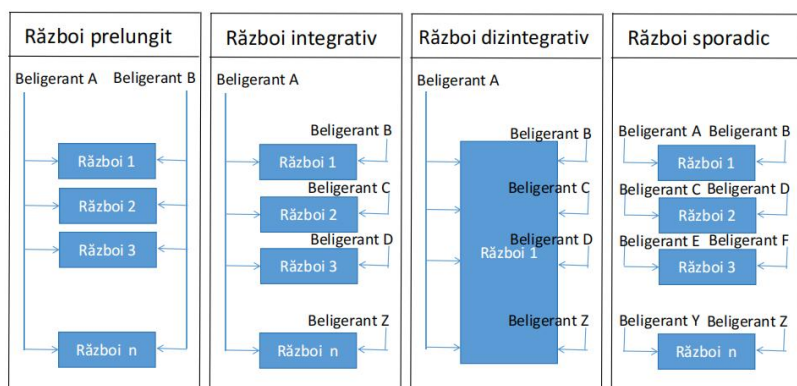


Fig.2 Tipologia confruntărilor, *apud* Cioffi-Revilla (2000:261)

Din această perspectivă, „confruntarea” (*warfare*) cunoaște forme distincte de manifestare (fig.2): confruntare prelungită (*protracted warfare*), presupunând angajarea în timp, în războaie diferite, a acelorași doi actori beligeranți (A și B); confruntare integrativă (*integrative warfare*) sau prin fuziune, în care același actor beligerant A se angajează în diferite conflicte, decalate în timp, cu actorii B, C, ..., Z, presupunând menținerea controlului politic asupra foștilor actori beligeranți

autonomi; confruntare dezintegrativă (*disintegrative warfare*) sau prin fisiune, în care un actor beligerant se angajează simultan în raport cu actorii B, C, ..., Z; respectiv confruntarea sporadică (*sporadic warfare*), în care actori beligeranți distincți se confruntă între ei în diferite conflicte în același interval de timp (A-B; C-D; ...; Y-Z).

O astfel de înțelegere a raporturilor „război” – „conflict armat”, respectiv „război” (*war*) – „confruntare” (*warfare*), permite o eliminare a posibilelor surse de eroare în interpretarea fenomenelor sociale violente, cum este și cazul termenului *information warfare* tradus prin sintagma „război informațional”.

1.5 Tipologii ale conflictelor

Războiul, constituind un fenomen complex – cea mai complexă formă de conflictualitate socială –, necesită un cadru analitic de cel puțin aceeași complexitate și, implicit, abordări transdisciplinare. Tipologiile războiului sunt de asemenea complexe și presupun cel mai adesea luarea în considerație a unor criterii combinate/ încrucișate, provenind din arii disciplinare distincte. Pentru realizarea unei taxonomii în raport cu unul sau cu mai multe criterii, este nevoie de o cunoaștere adecvată a fenomenului război și de înțelegerea caracterului războaielor în raport cu contextul (spațial, temporal, psihologic etc.) al producerii acestora. Profesorii Mircea-Dănuț Chiriac, Emil Ion și Dănuț Manta de la Universitatea Națională de Apărare „Carol I”, autori ai unei scheme tipologice a conflictelor armate, au ajuns la concluzia că:

Scopul cognitiv general al tipologiei în strategia militară este înțelegerea caracterului războaielor într-o epocă dată, descifrarea trăsăturilor celor mai semnificative ale acestora de care depind formele și metodele de organizare, pregătire și

întrebuințare a forțelor armate, elaborarea doctrinelor strategice, întreaga politică militară a statului (Chiriac *et al.*, 2007:60).

Schema propusă de cercetătorii români constă în prezentarea unei sinteze a școlilor doctrinare franceză, americană și sovietică din a doua jumătate a secolului XX. Autorii proiectează o schemă tipologică prezentă în literatura română de specialitate, ea însăși sinteză a influențelor gândirii militare răsăritene, iar apoi apusene, fără să pună în discuție posibilitatea existenței unei școli românești de gândire militară. În construcția tipologiei celor trei profesori, construcția are la bază 10 criterii: criteriul moral-politic; raporturile dintre forțe/mijloace; caracteristicile strategice ale acțiunilor militare; amploarea scopurilor; amploarea spațială; cadrul intern/extern; durata; sistemul de alianțe și beligeranța parțială (Chiriac *et al.*, 2007:62).

1.5.1 Războaie juste și injuste. După criteriul moral (politic), războaiele sunt drepte (juste) sau nedrepte (injuste). Angajarea justă în conflict a făcut obiectul analizei prin intermediul a numeroase studii, unele chiar gravitând în jurul acestei teme (spre exemplu, Ryan, 2012 sau Brooks, 2013). În baza acestui criteriu²⁵, războaiele drepte vizează cauza dreaptă, scopul (politic) al intrării în conflict: apărarea drepturilor și libertăților fundamentale cetățenești, apărarea independenței, suveranității, unității teritoriale a statului. Fundamentarea provine din domeniul eticii militare și a dreptului internațional umanitar, având drept pilon de referință teoria războiului drept (*just war theory*). De referință este lucrarea *Just and Unjust Wars* a filosofului american Michael Walzer (1977), care a

²⁵ Criteriul moral(-politic) este, de fapt, cel mai controversat dintre toate criteriile, atâta vreme cât, din perspectivă etică, justificarea războiului la nivelul statului sau al organizației suprastatale se realizează pe alt nivel și în raport cu alte criterii decât justificarea războiului la nivelul individual, al persoanelor direct implicate (combatanți sau necombatanți).

înlocuit teoria dreptului natural (moștenită de la Hugo Grotius) cu o abordare liberală, focalizată pe drepturi individuale.

Această teorie, în conexiune directă cu punerea în aplicare a criteriului moral al războiului, constituie de fapt un cadru de referință al eticii militare, oferind instrumente de lucru în ceea ce privește justificarea morală a războiului, atât în esența sa politică (privitor la dreptul de a declara și declanșa războiul, adică *jus ad bellum*), cât și militară (referitor la comportamentul combatanților în război, adică *jus in bello*), dar și mixtă, politico-militară (aplicabilă în etapa post-conflict, adică în ceea ce privește *jus post bellum*). Rezumând altfel perspectiva, teoria războiului drept presupune o proiecție teleologică, adică o teorie a scopurilor, care definește condițiile în care se poate recurge la război, și o proiecție privitoare la mijloacele utilizate în război, adică definind limitele comportamentului acceptat în timpul confruntării armate. Această proiecție rezumativă a filosofului Jeff McMahan evidențiază faptul că în ceea ce privește dimensiunea teleologică, adică *jus ad bellum*, de referință este „cerința ca războiul să fie declanșat pentru o cauză dreaptă” (McMahan, 2006:416). Totodată, în limitele realismului politic în revenire în disputa paradigmatică actuală, justificarea se rezumă la interesul național: „Din perspectivă realistă, războiul este justificat atunci când servește interesului național și nejustificat atunci când este împotriva acestuia” (McMahan, 2006:415), iar justificarea războiului este corelată direct cu justetea sa.

Așadar, justificarea războiului, focalizată pe cauza dreaptă (a interesului național sau a altor tipuri de interese în interpretări diferite, în raport cu paradigme de securitate diferite), nu se rezumă la apărarea teritoriului, ci presupune și apărarea unui alt stat împotriva agresiunii externe, ori a drepturilor fundamentale ale unei populații, respectiv pedepsirea unor agresiuni nejustificate. În conflictele actuale,

este considerată justă intervenția unei coaliții în scopul construirii păcii și a apărării anterior amintitelor drepturi și valori fundamentale (cum ar fi, de exemplu, cazul luptei împotriva terorismului). Pentru a înțelege complexitatea nivelurilor diferite de angajare în raport cu acest criteriu, am făcut apel la studiul lui Bazargan (2013:18), *The permissibility of aiding and abetting unjust wars*:

[...] spre deosebire de guvern, civilii și combatanții luați individual nu au de obicei puterea de a alege ce scopuri va avea un război. Deoarece un actor poate fi obligat moral să facă doar ceea ce este capabil să facă, un individ obișnuit nu poate fi obligat moral să schimbe obiectivele unui război nedrept purtat de guvernul său.²⁶

În esența lor, toate războaiele sunt injuste, dar acest punct de vedere este condamnat din perspectiva realismului politic ca fiind unul absolutist²⁷. Cauze juste sunt clamate distinct și

²⁶ [...] unlike the government, individual civilians and combatants typically do not have the power to choose what aims a war will have. Because an agent can be morally required to do only what that agent is capable of doing, a typical individual cannot be morally required to change the aims of an unjust war fought by her government. [t.n.], în engleză în original.

²⁷ Jeff McMahan rezumă această perspectivă, întâlnită, de altfel, și la John Garnett (2007:39): „Faptul că pacea nu este un panaceu explică de ce, atunci când sunt confrunțați cu alegerea imposibil de evitat între pace și război, liderii aleg uneori războiul. Unele forme de pace – sub dictatură, de exemplu – pot fi mai rele decât unele forme de război. În consecință, deși toți doresc pacea, aproape nimeni (cu excepția pacifiștilor convinși) nu dorește doar pacea sau pacea cu orice preț” (The fact that peace is not a panacea explains why, when confronted with the stark choice of peace and war, leaders sometimes choose war. Some kinds of peace – under dictatorship, for example – may be worse than some kinds of war. In other words, although everyone wants peace, almost no one (apart from strict pacifists) wants only peace or peace at any price, în original), în următorii termeni: „Persoanele care au opinii absolutiste în raport cu războiul se

antagonic de fiecare dintre părțile angajate în conflict. În majoritatea conflictelor actuale, în care au fost angajate forțe și mijloace de luptă ale coalițiilor, războiul a fost utilizat drept *ultima ratio*, caz în care poate fi clamată justetea apelului la această formă de impunere a voinței. Totuși, în toate războaiele nedrepte există obiective (parțiale) drepte.

1.5.2 Războaie convenționale, neconvenționale și hibride. După mijloacele de luptă utilizate, războaiele pot fi clasice (cu utilizarea armamentului convențional) sau cu utilizarea armelor de distrugere în masă (*weapons of mass destruction*, WMD), deliberată sau accidentală, care presupune violarea distincției dintre combatanți și noncombatanți în acțiunea militară propriu-zisă, adică tot aspecte de ordin moral. Această clasificare nu necesită o aprofundare a înțelegerii, deși conceptul de „război convențional” a suferit nuanțări. Practic, odată cu luarea în considerare a mediului virtual în confruntările contemporane, conceptul de „confruntare convențională” (*conventional warfare*) se complexifică:

Este clar că există o diferență uriașă între prima definire a războiului și cea actuală. Convingerea că războiul trebuie să se poarte între două state independente cu intenția de a lupta este acum subminată de atacurile teroriste internaționale. În ciuda acestui fapt, statele se străduiesc să atribuie atacurile nu contează cărei țări. După rezolvarea problemei atribuirii, intră în joc dreptul la autoapărare. După cum se vede în analiza tehnică a evenimentelor care au avut loc în mediul cibernetic, structura complexă a Internetului, din care derivă atacurile cibernetice într-un înțeles tradițional, face necesară reexaminarea regulilor tradiționale ale conflictului.²⁸ (Kuru, 2017:18).

numesc pacifiști. Ei cred că războiul nu este niciodată justificat” (McMahan, 2006:416)

²⁸ It is clear that there is a huge difference between the first definition of the war and the present one. The belief that the war needs to be between two

Deși conceptul de „confruntare convențională” (*conventional warfare*) se modifică, cel de „război convențional” (*conventional war*) nu impune ajustări, decât în sensul înțelegerii unei anumite forme a hibridizării acțiunii. Probabil o mai adecvată clasificare ar presupune luarea în considerare, pe lângă războaiele convenționale și cele neconvenționale și a celor hibride, care presupun acțiunea nediscriminatorie în anumite medii ale câmpului de luptă (în anumite domenii ale confruntării), fără ca efectele să fie letale.

Conceptul de război hibrid (*hybrid warfare*), presupunând „confruntare hibridă”, adică inserția în punerea în aplicare în limitele puterii *hard* (a puterii militare) a unor instrumente provenind din aria puterilor *soft* (mai precis a unor instrumente ale puterii simbolice), este suficient de imprecis. Pentru Frank Hoffman (2005, împreună cu James N. Mattis; 2007), părintele conceptului de „război hibrid” – insist asupra aceste sintagme românești deoarece în forma primă, termenul sa impus ca *hybrid war*, ulterior devenind mai cunoscut drept *hybrid warfare* –, impunerea termenului a fost posibilă din nevoia de a defini combinația acțiunilor militare convenționale cu cele neconvenționale (altele decât cele privitoare la utilizarea armelor de distrugere în masă), respectiv a forțelor regulate și neregulate, a unui mix de metode militare și non-militare, pe care Hoffman le rezumă astfel în momentul în care definește agresorul hibrid:

independent states with the intention of fighting is now weakened by international terrorist attacks. Despite this, the states are striving to attribute the attacks to any country. After solving attribution problem, the right to self-defence comes into play. As seen in the technical analysis of the events that took place in the cyber environment, the complex structure of the internet, which derives attacks from cyber space in a traditional sense, makes it necessary to re-examine the traditional rules of conflict. [t.n.], în engleză în original.

Orice adversar care folosește simultan și adaptativ un amestec combinat de arme convenționale, tactici neregulate, terorism și comportament criminal în spațiul de luptă pentru a atinge obiectivele politice.²⁹ (Hoffman, 2007:29)

În esență, conceptul occidental de „război hibrid” este diferit de cel rusesc, *ghibridnaia voina*, dat fiind faptul că mixul de mijloace și metode utilizat de armata Federației Ruse se realizează depășind limitele legale și etice ale confruntării, iar acolo unde nu sunt stabilite asemenea limite prin legislația internațională, încălcându-se norme morale evidente. În încercarea de a chestiona hibriditatea războiului din Ucraina (camuflat sub numele de „operațiune militară specială”), am subliniat în lucrarea *Războiul hibrid sau Încercarea de disimulare doctrinară prin războiul absolut* modul în care această tentativă de camuflare evidențiază, la o analiză mai atentă, ceea ce Ruiz Palmer (2015:9) a definit a fi „Vin sovietic vechi în sticle rusești noi”³⁰:

Plecând de la originea termenului și de la felul în care el poate servi în urma operaționalizării conceptuale în aparatul doctrinar, răspunsul este simplu: actuala invazie din Ucraina este *ghibridnaia voina*, dar nu și *hybrid warfare*. Războiul hibrid în înțeles occidental, asociat unei forme a hibridității conflictuale specifice zilelor noastre, s-a încheiat odată cu exercițiul ZAPAD 2021 și odată cu debutul „operațiunii militare speciale”. *Hybrid warfare* este o formă de conflict limitat, care nu își propune distrugerea totală a adversarului și care presupune utilizarea amestecului de mijloace și instrumente, care nu se încadrează în paradigma clausewitziană. *Ghibridnaia voina* este „lupul în piele de oaie”, războiul absolut camuflat în ceața conceptuală și

²⁹ Any adversary that simultaneously and adaptatively employs a fused mix of conventional weapons, irregular tactics, terrorism, and criminal behaviour in the battlespace to obtain the political objectives, [t.n.], în engleză în original.

³⁰ Old Soviet wine in new Russian bottles, [t.n.], în engleză în original.

ideologică a hibridității, proiectat să contribuie la distrugerea totală a inamicului, la distrugerea rațiunii acestuia de a fi, a fundamentelor istorice, a referințelor și ancorelor identitare. *Ghibridnaia voina* nu este o formă de război hibrid, ci una de război total, un război masificat, „de ieri”, mimând forma iluzorie a războiului viitorului. (Lesenciuc, 2023:128).

Privitor la războaiele neconvenționale (cu armament neconvențional), merită făcută o remarcă privitor la faptul că nu numai armamentul nuclear face obiectul încadrării în categoria *weapons of mass destruction*, ci și, de exemplu, armele biologice și chimice, respectiv că nu numai cel de-Al Doilea Război Mondial se încadrează în această tipologie conflictuală în baza acestui criteriu, deși de referință rămâne această conflagrație, prin acțiunile totale atât de pe fronturile europene, răsăritean și apusean, cât mai ales din teatrul de operațiuni din Pacific.

1.5.3 Războaie simetrice și asimetrice. După forțele și mijloacele implicate în război, după doctrină și nivelul de instruire, se poate face distincție între conflicte simetrice și asimetrice. Practic, amintita distincție simetric/ asimetric aplicabilă războiului are la bază raporturile de putere dintre entitățile care iau parte la conflict. În calificarea războaielor ca fiind simetrice sau asimetrice intră o serie de aspecte care țin explicit de manifestarea în limitele puterii *hard*, dar uneori sunt luate în considerare și aspecte ale manifestării puterilor *soft*. Într-o abordare cuprinzătoare, confruntarea asimetrică poate fi definită astfel:

Confruntarea asimetrică este o confruntare nontradițională, centrată pe populație, purtată între o putere militară superioară și una sau mai multe puteri inferioare, care cuprinde toate aspectele care urmează: evaluarea și înfrângere amenințărilor asimetrice, desfășurarea operațiunilor asimetrice, înțelegerea

asimetriei culturale și evaluarea costurilor asimetrice.³¹
(Buffaloe, 2006:17),

Din această perspectivă privind, problematica asimetriei conflictuale atrage după sine aspecte mai puțin abordate în studiile românești, cum ar fi asimetria costurilor, plecând de la o altă asimetrie în analiza binomului insurgență/contrainsurgență (Galula, 1964/2006: 3), ori asimetria culturală:

Incapacitatea de a înțelege cultura inamicului – presupunând că inamicul gândește la fel ca tine și împărtășește valorile tale – va duce la eșec în obținerea victoriei, deoarece nu vei putea identifica „centrul său de greutate”.³² (Buffaloe, 2006:14).

Această abordare propune o ecuație a confruntării asimetrice/ *asymmetric warfare* (AW):

$$AW = AT + AO + CA + AC \quad [1]$$

unde AT reprezintă amenințările asimetrice/ *asymmetric threats*, incluzând terorismul, insurgența, operațiunile informaționale, amenințările așa numit „disruptive” (un termen operațional împrumutat, dar fără acoperire semantică în limba română) și amenințările necunoscute; AO sunt operațiunile asimetrice/ *asymmetric operations*, în care se încadrează schimbările asimetrice, valorificarea avantajului asimetric, dar și instrumentele esențiale ale puterii naționale: diplomatic,

³¹ Asymmetric warfare is population-centric nontraditional warfare waged between a militarily superior power and one or more inferior powers which encompasses all the following aspects: evaluating and defeating asymmetric threat, conducting asymmetric operations, understanding cultural asymmetry and evaluating asymmetric cost. [t.n.], în engleză în original.

³² Failure to understand an enemy's culture—assuming that the enemy thinks as you do and shares your values—will lend to a failure to achieve victory because you are unable to identify his “center of gravity”. [t.n.], în engleză în original.

informațional, militar și economic; CA presupune asimetria culturală/ *cultural asymmetry* și include asimetria valorilor, normelor și regulilor, dar și înțelegerea populației țintă și operațiile informaționale, iar AC reprezintă costurile asimetrice/ *asymmetric cost*, incluzând activele, costurile apărării, costurile de întreținere a acțiunilor și, încă o dată, operațiile informaționale (Buffaloe, 2006:18).

Confruntarea asimetrică presupune în esență o formă de alterare a practicilor războiului, susține Pauline M. Kaurin, profesor de etică militară la Pacific Lutheran University:

Văd războiul asimetric (în special versiunea contemporană a acestuia) ca pe o încercare de a modifica discursul și regulile de bază despre ce reprezintă războiul, cum trebuie purtat și ce se consideră succes sau eșec”³³ (Kaurin, 2014:9),

inclusiv o formă de alterare a înseși esenței războiului.

Confruntările simetrice presupun existența unui echilibru de putere între părți, cel mai bun exemplu din istorie fiind cel al Primului Război Mondial, în care coalițiile s-au angajat sub raport numeric, tehnologic și doctrinar în ponderi comparabile. În ceea ce privește conflictele asimetrice, acestea se caracterizează, în ceea ce privește cel puțin unul dintre mai sus-menționatele aspecte, printr-o balanță dezechilibrată. De-a lungul istoriei, războaiele de cucerire, de anexare, de rapt și de colonizare au fost cele care au adus în discuție disproporția, fie la nivel numeric din punctul de vedere al forțelor implicate, fie la nivel doctrinar și al instruirii, fie la nivelul tehnologiilor utilizate (de exemplu armamentul de foc în raport cu arcurile cu săgeți, în cazul colonizărilor). În zilele noastre, acțiunile asimetrice au dezvoltat posibilități de angajare dezechilibrată în

³³ I see asymmetrical warfare (especially the contemporary version of it) as an attempt to alter the discourse and ground rules about what constitutes war, how it is to be waged and what counts as success or failure. [t.n.], în engleză în original.

raport cu valorile și principiile democratice și umanitare, cum ar fi în cazul acțiunilor teroriste.

Există acțiuni asimetrice din multiple puncte de vedere, atât din perspectiva cantității de forțe dislocate, a aspectelor de ordin doctrinar și al instruirii, cât și a aspectelor de natura nivelului tehnologic, al mijloacelor și armamentelor utilizate în război, cum ar fi cazul intervențiilor structurilor suprastatale sau a coalițiilor de state în Balcanii de Vest, Afganistan, Irak etc. În cazul atentatelor teroriste, angajarea disproporționată și fără scrupule se datorează unei asimetrie morale, privitoare la valori, principii și practici, dar și această disproporționalitate valorică, judecată în raport cu un sistem de convingeri și credințe apropiat spațiului occidental, poate fi înțeleasă în anumite cazuri ca fiind falsă angajare asimetrică:

Suntem destul de tentați să spunem că asimetria puterii maschează o simetrie a valorilor. Cei doi actori nu valorează de fapt unul mai mult decât altul din motive diferite, dar asimetria puterii este totuși pe deplin manifestă.³⁴ (Badiou, 2006:155).

Din perspectiva eticii militare, asimetria morală ia în considerare în special practicile asimetrice:

Asimetria morală se referă la diferențele dintre practicile și normele morale care stau la baza strategiilor și tacticilor pe care conflictul este dispus să le utilizeze în război.³⁵ (Kaurin, 2014:5),

³⁴ Nous sommes assez tentés de dire que la dissymétrie des puissances recouvre une symétrie des valeurs. Les deux protagonistes en réalité ne valent pas beaucoup plus cher l'un que l'autre pour des raisons différentes, mais la dissymétrie de puissances n'en est pas moins entièrement déployée. [t.n.], în franceză în original.

³⁵ Moral asymmetry relates to the differences in moral practices and the moral norms, that undergird those strategies and tactics the conflict are willing to utilize in war. [t.n.], în engleză în original.

dar, din păcate, nu se bucură de o foarte mare atenție în lucrările de specialitate și este adusă în discuție cel mai adesea în contextul altor tipuri de asimetrie (Kaurin, 2014:6).

Angajarea asimetrică este firească prin raportare la valorile civilizației, odată ce valorile culturale diferă considerabil în anumite situații. În esență, delimitarea simetric/asimetric utilizată pentru a descrie tipul de război presupune o proiecție tipologică multicriterială.

1.5.4 Războaie absolute, totale și limitate. După amploarea scopurilor politico-militare urmărite, războaiele au fost clasificate în războaie cu caracter limitat și totale. Această tipologie are la bază concepția clausewitziană. Generalul prusac a introdus pentru prima dată conceptul de război absolut (adică limita extremă de manifestare), care presupune violența absolută, a cărui finalitate este extremă: distrugerea/ anihilarea/ nimicirea inamicului, în raport cu care a construit conceptul de război real:

Repetăm, deci, teza noastră: războiul este un act de violență și în folosirea acesteia nu există limite; astfel, fiecare parte îi impune celeilalte legea sa, rezultând o acțiune reciprocă, care, conform definiției, trebuie să ajungă la extrem. Aceasta este *prima acțiune reciprocă și primul fenomen extrem* pe care îl întâlnim. (Clausewitz, 1982:55)

De la această clasificare, care a alimentat dorința de punere în aplicare a conceptului de război absolut în înțelesul său nediluat, continuatorii gândirii clausewitziene au proiectat acțiunea militară extremă, până la limita neîmplinirii tragice a acestei proiecții: exterminarea în lagărele naziste și bombardamentele nucleare de la Hiroshima și Nagasaki din cel de-al Doilea Război Mondial. În fapt, războiul real nu se produce cu scopul atingerii limitelor războiului absolut, ci doar în orizontul acestuia, atâta timp cât factorul politic introduce

elemente de raționalitate în conflict, propunând scopuri limitate și delimitând, totodată, cadrul de aplicare și de angajare, după cum considera Clausewitz.

În concepția strategică americană, din încrucișarea ultimelor două criterii, a rezultat conceptul de „ripostă flexibilă”, propus de generalul Maxwell D. Taylor, ca răspuns la strategia „represaliilor masive”, intitulată *New Look*, a președintelui Dwight D. Eisenhower³⁶. După adoptarea conceptului de „ripostă flexibilă” în strategia americană în 1961, având la bază *The National Military Program of Flexible Response* propus de generalul Taylor, structurat pe patru piloni:

1. Îmbunătățirea planificării și antrenamentul pentru război limitat.
2. Exploatarea rachetei balistice cu rază medie de acțiune.
3. O mai bună protecție pentru Comandamentul Aerian Strategic.
4. Un program limitat de adăposturi antiatomice.³⁷ (Taylor, 1960:139),

în cadrul strategiei a fost inclusă și distincția pe care a propus-o generalul american, între războiul general și războiul limitat. Prin război general se înțelege, în doctrina americană a

³⁶ Strategia „represaliilor masive” presupune utilizarea armamentului nuclear doar pentru descurajarea strategică și recomandarea utilizării armamentului convențional în confruntări așa-numite limitate. În raport cu strategia americană și cu amploarea scopurilor politico-militare, există puncte de vedere diferite. De exemplu, Brian W. Brennan (2002:9) consideră că Statele Unite au adoptat o strategie de război limitat în Războiul Coreei, odată cu refuzul președintelui Harry S. Truman de a utiliza armamentul nuclear împotriva Coreei de Nord și a Chinei.

³⁷ 1. Improved planning and training for limited war.

2. Exploitation of the intermediate Range Ballistic Missile.

3. Better protection for the Strategic Air Commandment.

4. A limited fall-out shelter program. [t.n.], în engleză în original.

administrației Kennedy, confruntarea nucleară între cele două mari superputeri ale Războiului Rece, S.U.A. și U.R.S.S., în timp ce războiul limitat înseamnă orice altă confruntare convențională, inclusiv cea între cele două puteri deja menționate. Totuși, pentru a reveni la criteriul anterior, nici măcar în acest document posibilitatea utilizării armamentului nuclear tactic nu este exclusă, aspect ce diferențiază clasificarea război general – război limitat de precedenta clasificare, război clasic – război cu utilizarea WMD.

În ambele clasificări după amploarea scopurilor politico-militare, atât în raport cu războiul absolut, cât și cu cel total (sau general) se definește războiul limitat, înțeles astfel după limitarea (politică) a obiectivelor sale. Această delimitare se realizează pe trei paliere distincte: (i) din punct de vedere geografic, (ii) din perspectiva finalităților și obiectivelor războiului și (iii) în ceea ce privește mijloacele utilizate (Freedman, 1994:201), presupunând o clarificare precisă a limitelor politico-militare ale conflictului. Într-o altă expunere a criteriilor în raport cu care pot fi definite războaiele ca fiind limitate, celor trei paliere deja menționate mai sus se adaugă un al patrulea, „țintele împotriva cărora sunt îndreptate ostilitățile”³⁸ (Clarke, 1988:58-59, *apud* Cable, 1993:555).

În plus, literatura de specialitate americană propune, după intensitatea și amploarea acțiunilor militare, distincția dintre conflictul de mare intensitate, de intensitate medie și de mică intensitate. Această tipologie este transcriterială, presupunând deopotrivă angajarea din perspectiva tipului obiectivelor propuse sau a scopurilor politico-militare urmărite (Chiriac *et al.*, 2007:64-65). Conflictul de mare intensitate presupune angajarea părților în conflict în raport cu obiectivele totale, decisive, de nimicire a adversarului, iar conflictele de medie și

³⁸ the targets against which hostilities are directed, [t.n.], în engleză în original.

mică intensitate angajează în conflict state ale căror obiective sunt limitate:

- Conflictul de mare intensitate reprezintă un război între două state și aliații lor care își propun obiective decisive, utilizarea tehnologiei moderne și toate categoriile de armament, inclusiv ANM³⁹;
- Conflictul de intensitate medie reprezintă un război între două state sau coaliții în care se propun obiective limitate, iar pentru realizarea lor se utilizează, în principal, mijloace convenționale, sunt de durată, însă sunt limitate la dimensiunile zonelor geografice relativ reduse (...);
- Conflictul de mică intensitate reprezintă un război limitat care se duce pentru realizarea unor obiective politice, sociale, economice și psihologice incluzând presiuni diplomatice, economice și sociale, până la terorism și mișcare insurecțională. (Chiriac *et al.*, 2007:62)

În ceea ce privește clasificarea conflictelor în raport cu intensitatea, există o literatură foarte bogată și scalări în trepte multiple a intensității, cum este cea realizată de Monty G. Marshall (2002:70-72), anterior prezentată, sau cum există numeroase studii care propun măsurarea intensității conflictuale (de exemplu, Cusack *et al.*, 2021).

1.5.5 Alte tipologii conflictuale. Celelalte clasificări nu necesită o detaliere suplimentară. După amploarea spațială (după aria de desfășurare), războaiele pot fi locale, regionale sau mondiale. Distanța este clară între aceste tipuri de conflicte. Ceea ce trebuie înțeles este faptul că, în raport cu acest criteriu, un război se poate transforma, parcurgând etape distincte ale amplitudinii spațiale, ca în cazul celui de-Al Doilea Război Mondial, în care de la niște acțiuni locale (Războiul Civil din Spania, invadarea Poloniei de către trupele naziste), s-

³⁹ *Weapons of mass destruction, WMD.*

a ajuns la acțiuni de mai mare amploare, regionale (fiind implicate Scandinavia și statele occidentale), apoi continentale, prin deschiderea frontului răsăritean, și în cele din urmă mondiale.

După durată, războaiele pot fi de scurtă sau de lungă durată. Istoria consemnează conflicte foarte scurte, cum ar fi cele dintre Anglia și Zanzibar din 1896, cu o durată de 45 de minute, dintre Israel, pe de o parte, și Egipt, Siria și Iordania din 1967, cu o durată de 6 zile (cunoscut, de altfel, ca *Războiul de șase zile*), dintre India și Pakistan din 1971, cu o durată de 13 zile, sau războiul ruso-georgian din august 2008, cu o durată de 16 zile. De asemenea, există conflicte de durată remarcabilă, cum ar fi Războiul olandez de independență (sau *Războiul de 80 de ani*), desfășurat între 1568 și 1648, sau, mai ales, cel cunoscut în istorie drept *Războiul de 100 de ani*, desfășurat între 1337 și 1453 între Anglia și Franța și durând, de fapt, 116 ani. Merită menționat faptul că în conflictele actuale, durata etapei de conflict armat propriu-zis este relativ scurtă, de circa 1-4 ani (exceptând războaiele proxy, cu o durată de circa 10 ani), mult mai lungă fiind etapa post-conflict, spre deosebire de conflictele medievale, de exemplu, în care etapa post-conflict practic nu exista și în care războiul coincidea cu o îndelungată confruntare armată propriu-zisă.

După motivație, conflictele pot fi de eliberare națională, de schimbare a unui regim politic într-un stat, de secesiune sau religioase (Chiriac *et al.*, 2007:64). În afara acestei clasificări, dar în raport cu același criteriu, Arbeitsgemeinschaft Kriegsursachenforschung (AKUF) distinge între războaiele anti-regim (care au drept scop schimbarea regimului politic sau a ordinii sociale); războaiele de autonomie/ secesiune; războaiele de eliberare de sub dominația colonială; războaiele interstatale și alte războaie (*apud* Gareis, 2012:98). După caracterul acțiunilor militare, războaiele pot fi manevriere sau poziționale (Chiriac *et al.*, 2007:65). Și această clasificare este limitată, în

afara celor două tipuri de conflicte deja amintite existând pătrunderile în adâncime (*long range penetration*, LRP), respectiv confruntările neconvenționale: insurgență/contrainsurgență, confruntări de gherilă (Applegate & Moore, *apud* McFate, 1994). Războaiele poziționale presupun angajarea frontală, distrugerea fizică a inamicului și limitarea, pe cât posibil, a accesului la resurse, caracterizând în special conflictele din antichitate și din Evul Mediu și asediile. Războaiele manevriere presupun exploatarea mișcării relative a trupelor și a gurilor de foc proprii în raport cu inamicul. Pătrunderea în adâncime vizează atacul frontal al punctelor decisive și/sau al centrului de greutate al forței inamicului, producând colapsul intern al acestuia. Confruntările de gherilă (și, implicit, toate războaiele de insurgență) au drept scop subminarea stării morale și distrugerea coeziunii forțelor inamice prin acțiuni militare de hărțuire, în spații neconvenționale, care au drept scop menținerea unui nivel ridicat de stres psihic. În cazul războaielor de insurgență, principalul scop este acela de a atrage un număr cât mai important al populației civile pentru sprijinirea cauzei: „Cea mai bună cauză pentru scopul insurgentului este una care, prin definiție, poate atrage cel mai mare număr de susținători și poate respinge un număr minim de adversari”⁴⁰ (Galula, 1964/2006:13),

Aceste tipologii conflictuale nu sunt exhaustive atâta vreme cât războaiele îmbracă forme multiple de manifestare, se adaptează condițiilor politice, sociale, economice în continuă schimbare, valorilor civilizației și tehnologiilor care produc revoluții militare. Conflictele ultimelor decenii, probabil cu atât mai puțin conflictele viitoare, nu pot fi încadrate ușor în acest

⁴⁰ The best cause for the insurgent's purpose is one that, by definition, can attract the largest number of supporters and repel the minimum of opponents. [t.n.], în engleză în original.

cadru tipologic. Cu toate acestea, pentru o înțelegere adecvată, propunem un tablou-sinteză al tipologiilor conflictuale, după cum urmează:

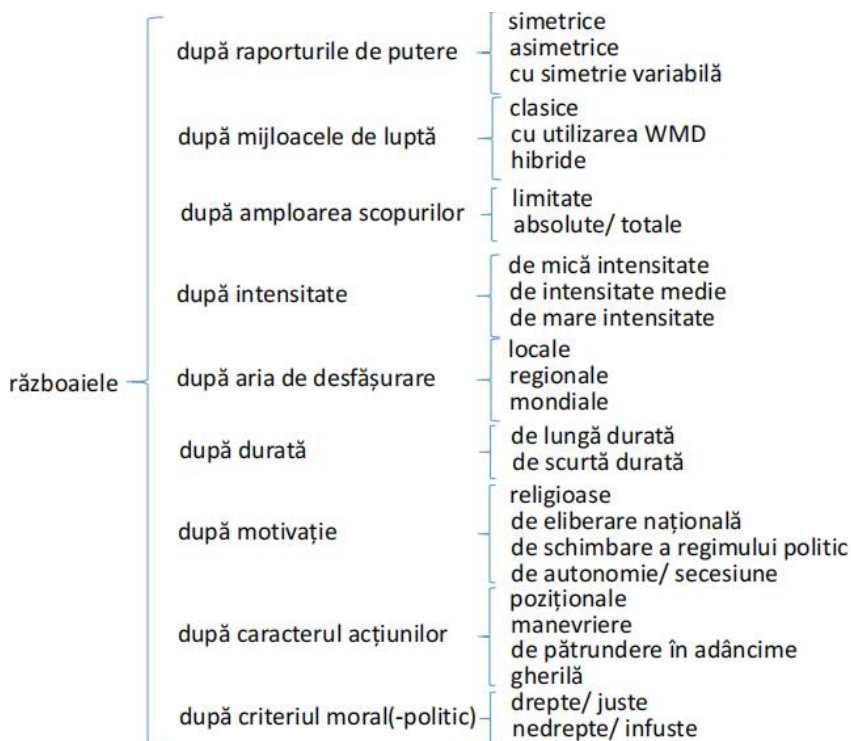


Fig.3 Un tablou-sinteză a principalelor zece tipologii conflictuale.

1.6 Ultima „revoluție militară” și efectele ei asupra conflictului contemporan

Perioada care a urmat Războiului Rece s-a caracterizat printr-o revoluție tehnologică și doctrinară importantă (una dintre multiplele revoluții în domeniul militar care au avut loc de-a lungul istoriei, dar una dintre revoluțiile majore),

cunoscută drept *Revolution in Military Affairs* (RMA), în general tradusă în lucrările românești de specialitate *mot à mot*, prin sintagma „Revoluția în afaceri militare”, uneori în traduceriile lucrărilor cu caracter politico-militar sau diplomatic, fiind utilizată și sintagma „revoluția militară”⁴¹, o sintagmă mai corectă ca aplicare în orizontul cunoașterii în școala românească de științe militare.

Termenul de „revoluție militară” nu este nou, el fiind pentru prima dată utilizat în 1956, în lucrarea lui Michael Roberts, *The Military Revolution, 1560-1660*⁴², lucrare prin intermediul căreia a fost pus în evidență rolul mobilității artileriei ca urmare a dezvoltării tunurilor mobile din bronz (și, prin urmare, a depășirii războiului pozițional al epocii), și, în subsidiar, ca urmare a dezvoltării unui nou tip de sisteme de fortificații. Revoluțiile militare ulterioare, din epoca industrializării și, mai ales, din perioada mecanizării războiului (1918-1945), au produs la rândul lor mutații profunde în arta militară, în sistemele doctrinare și în modalitățile adaptate de antrenare a trupelor și utilizare a forțelor și mijloacelor în conflictele militare:

Tancul și aeroplanul au fost introduse ca mijloace de luptă în timpul Primului Război Mondial. După război, intelectuali militari vizionari, cum ar fi J.F.C. Fuller și Giulio Douhet, le-au văzut ca mijloace de a ieși din impasul creat de puterea de foc și producția de masă. Fuller a considerat inițial tancurile ca un fel de flotă terestră, trecând peste obstacolele de pe front și capabilă să manevreze liber în spatele inamicului. Tancurile ar fi redus la neputință armatele inamicului și ar fi lovit centrele de comandă și liniile de aprovizionare. Douhet prevestea avioane

⁴¹ Spre exemplu, în traducerea lui Nicolae Năstase a lucrării lui Paul Hirst, *Război și putere în secolul 21. Statul, conflictul militar și sistemul internațional*, București: Antet, 2001.

⁴² Lucrarea a fost consultată în varianta publicată în culegerea editată de Clifford J. Rogers, *The Military Revolution Debate. Readings on the Military Transformation of Early Modern Europe* (Roberts, 1995: 13-36)

zburând peste liniile blocate ale frontului, bombardând centrele civile din spate și terorizând populația. Panica generalizată a populației ar fi răsturnat guvernele, iar astfel războiul s-ar fi încheiat. Bombardarea era un fel de versiune mai rapidă a blocadei. (Hirst, 2001:30)

După încheierea celui de-al Doilea Război Mondial, strategia nucleară, a represaliilor masive, lăsând locul ripostei flexibile, a condus la cea mai importantă schimbare strategică din istorie: înlocuirea strategiilor de acțiune cu cele de intimidare, de descurajare (*deterrence*). Efectele cumulate ale revoluțiilor militare se găsesc în strategiile și aparatele doctrinare de azi. Totuși, mobilizarea în masă și războiul total (și continuu), deși au devenit concepte inutilizabile în majoritatea lucrărilor de specialitate, dar mai ales în aparatele doctrinare occidentale, ele mai sunt încă prezente în mediul științific românesc. Noile concepte presupun angajare a unor structuri mai suplă, în rețea, în raport cu un concept relativ nou: informația, în raport cu a cărui supremație atinsă se proiectează înfrângerea sau schimbarea voinței adversarului.

Pe aceste coordonate, noile confruntări anunță noi revoluții militare (tehnologice, strategice, doctrinare, în planul instruirii și utilizării forțelor și mijloacelor pe câmpul de luptă)⁴³, dar și noi modalități de punere în dezbatere a conceptului de război. În plus, alte concepte, cum ar fi cel de „război nou”, au condus la apariția unei literaturi consistente, în care cei mai influenți autori sunt Michael Ignatieff, prin *Virtual War – Kosovo and Beyond* (2000), respectiv Mary Kaldor, prin *New and Old Wars*:

⁴³ Domeniile de aplicare a RMA sunt: tehnologic (privitor la emergența noilor tehnologii, în special a celor informaționale); doctrinar și operațional (ca transpunere a efectelor tehnologizării în concepte, principii, legi, acțiuni) și organizațional (atât în plan militar, cât și civil-militar).

Organized Violence in the Global Era (1999)⁴⁴ (apud Hirst, 2001:70). Moștenirea noilor conflicte nu trebuie înțeleasă ca fiind moștenire a conflictualității, ci ca moștenire a formelor latente ale vechilor revoluții militare, producând efecte cumulate noi. Această proiecție justifică, de fapt, cantonarea în anumite lucrări în limitele orizontului vechii paradigme, clausewitziene⁴⁵, dar nu justifică lipsa de deschidere în ceea ce privește înțelegerea cadrului actual de definire a confruntării militare și nici angajarea în conflicte de tip „război nou” cu mijloace, forțe, strategii și doctrine/ manuale moștenite de la precedentele revoluții militare. Noua revoluție sau ultima revoluție militară, *Revolution in Military Affairs* (RMA), datorată proiecției lui E.A. Cohen din articolul „A Revolution in Warfare” publicat în numărul 37 (martie-aprilie 1996) al

⁴⁴ Lucrarea lui Mary Kaldor a fost tradusă în 2001 în românește și publicată la Editura Antet, cu titlul *Războaie vechi și noi: violența organizată în era globală*.

⁴⁵ Prin paradigmă clausewitziană înțelegem proiecția paradigmatică a generalului prusac Carl von Clausewitz (1780-1831), presupunând schimbarea fundamentală a vechii perspective asupra războiului și raporturilor dintre politică și război, constând în punerea în discuție a folosirii extreme a violenței și în operaționalizarea conceptului abstract de „război absolut”. În esență, nu proiecția generalului Clausewitz privea acțiunea militară extremă, ci continuatorii ideilor sale au exagerat, producând efecte, între care cele cu adevărat extreme sunt cele desfășurate sub cupola celui de-al Doilea Război Mondial. În 2014 argumentam această poziție astfel: „(...) războiul real nu se derulează în limitele războiului absolut deoarece intervin o serie de factori externi, dintre care cel mai important este factorul politic, responsabil pentru introducerea elementelor de „raționalitate” în conflict, prin stabilirea clară a unor scopuri și prin delimitarea explicită a cadrului de aplicare. Acolo unde politica reprezintă mai degrabă un factor exprimând o patologie conflictuală decât o structură normativă, și revenim spre exemplificare la realitatea celui de-al doilea război mondial, războiul real tinde spre războiul absolut. Exterminarea (în lagăre sau pe câmpul de luptă) constituie alte orizonturi ale paradigmei clausewitziene, extinsă astfel de continuatorii unora dintre ideile generalului prusac, decupând din monumentală sa operă și nefiind în măsură să o înțeleagă în spiritul ei” (Lesenciuc, 2014:43).

revistei *Foreign Affairs*, adaptată ulterior ca proiecție doctrinară în armata americană, constă în punerea în discuție a războiului pe noi coordonate, în care cele mai importante active sunt cele informaționale. Hirst nota încă din 2001 următoarele:

[...] cele mai importante active sunt culegerea de informații, comunicațiile și armele cu ghidaj de precizie. Susținătorii cei mai proeminenți ai RMA afirmă că sistemele de comandă, control, comunicații și culegere a informațiilor sunt capabile de o dezvoltare atât de rapidă, încât vor risipi ceața de pe câmpul de luptă, permițând comandanților de rang înalt să vadă situația generală de pe teren și a celor de rang inferior să ordone lansarea unor arme complexe. Strategiile bazate pe informații necesită o aplatizare a ierarhiilor și o integrare a forțelor, perspectivă din care structurile actuale din cadrul forțelor armate sunt departe de ideal. (Hirst, 2001:75).

Totuși, o serie de concepte și implicații recente aduc în dezbatere o proiecție actualizată în raport cu perspectiva lui Hirst. Războiul hibrid (Hoffman, 2007), extinderea utilizării dronelor în războiul contemporan prin lărgirea spectrului de operațiuni de la utilizarea de către armata israeliană în 1982 a UAV-urilor Scout pentru funcțiuni de *reconnaissance* pe câmpul de luptă până la avantajul strategic al dronelor Bayraktar TB2 utilizate de azeri în războiul din Nagorno-Karabakh (2020) sau până la *gamificarea* războiului din Ucraina, utilizarea așa-numitelor tehnologii disruptive (un împrumut în terminologia operațională din vocabularul start-up-urilor) care include tehnologii informaționale și comunicaționale (*information and communication technologies*, ICT), inteligență artificială (*artificial intelligence*, AI), nano- și biotehnologii (*nano and bio technologies*) și utilizarea (cel mai adesea duală a) tehnologiilor transformative, printre care tehnologii cuantice și hipersonice, 5G, IoT (inclusiv în variantele IoB sau IoS) sau tehnologii blockchain sunt doar

câteva dintre aspectele care au produs în numeroase doctrine și manuale de luptă modificări substanțiale, stabilirea unor cerințe operaționale noi și redefinirea mediului informațional și a domeniilor în care se desfășoară acțiunea militară pe câmpul de luptă (proiectând luarea în considerare a domeniului cognitiv ca fiind esențial în acest sens). Toate aceste aspecte sunt de fapt efectele revoluției informaționale, așa cum a fost denumită încă de la început.

Colin S. Gray (2010:75-76) rezuma revoluțiile militare moderne, considerând că până la punerea în dezbatere a RMA ca revoluție informațională s-au produs cel puțin alte cinci, majoritatea având rădăcini politice, nu industriale: 1. Inventarea și afirmarea statului modern în secolul al XVII-lea; 2. Revoluția Franceză care a impus conceptul de stat-națiune; 3. Revoluția Industrială, încă în desfășurare, producând efecte în orizontul paradigmei clausewitziene; 4. Revoluția militară a Primului Război Mondial, cu importante fundamente de ordin doctrinar și în ceea ce privește proiecția nomologică a conflictualității și 5. Revoluția nucleară din anii 1940 și 1950, care a impus, în cele din urmă, strategia descurajării. În ceea ce privește revoluția informațională, ultima revoluție militară, Gray o descria astfel:

Revoluția informațională din anii 1980 până în prezent. Din nou, această revoluție este mai curând un proces, și nu un eveniment sau un episod. De asemenea, ea a avut o serie de antecedente științifice și tehnice. Am ales anii 1980 pentru că sunt un moment convenabil și plauzibil din punct de vedere strategic, precum și pentru că au fost marcați de anumite schimbări fundamentale. Acest ultim promotor al revoluției militare a fost inevitabil, asemenea tuturor celorlalte revoluții. (Gray, 2010:76)⁴⁶

⁴⁶ În lista propusă de Gray, revoluția informațională nu este ultima. El adaugă, sub semnul ipoteticului, *Revoluția culturală în derulare în lumea islamică*, pe care o descrie astfel: „Această revoluție la nivelul implicațiilor

Rezultatul efectiv al punerii în aplicare a noii perspective datorate ultimei revoluții militare a devenit vizibil în angajarea militară din Irak (2003), când s-a produs o schimbare majoră în plan strategic și doctrinar. Utilizarea în conflict de către Forțele Aeriene americane a 95 de aeronave destinate funcțiunilor C4ISR, precum și a altor numeroase aeronave destinate acțiunilor necombative, față de doar 51 destinate bombardamentului constituie cel mai important reper în ceea ce privește abandonul dezvoltării Douhet a paradigmei clausewitziene în favoarea proiecției cuceririi și menținerii supremației informaționale ca scop fundamental al operațiilor întrunite:

[...] până la războiul din Irak (2003) scopul fundamental al operațiilor întrunite era cucerirea și menținerea supremației aeriene, în timp ce începând cu acest conflict, cucerirea și menținerea supremației aeriene devin mijloace în cucerirea și menținerea supremației informaționale. (Lesenciuc, 2014:110)

Chiar dacă orizontul viitoareii revoluții militare nu poate fi previzionat, actuala revoluție, cunoscută în literatura de specialitate drept RMA, care încă nu și-a atins potențialul maxim, care nu a produs efecte decât în faza incipientă, proiectează totuși o direcție clară a evoluției conflictualității,

strategice ale credinței exploatează tehnologia industrială și a informațiilor și ar putea găsi întrebuințări pentru produsele revoluției nucleare, dar ea are loc independent de tehnologie. Caracterul dominant al războiului contemporan prezintă un grad ridicat de neregularitate fiind, așadar, asimetric” (Gray, 2010:76). Precedentele revoluții militare analizate au fundamente politice, economice sau tehnologice. Ultima revoluție luată în considerație de Colin S. Gray, presupus culturală, are fundamente ideologice, motiv pentru care, pentru a nu amesteca revoluțiile militare cu ceea ce poate fi înțeles ca fiind cauze ale conflictualității, găsim de cuviință să rămânem la proiecția revoluției informaționale ca fiind ultima, în derulare, neatingându-și încă apogeul.

presupunând o scădere accelerată a densității de ocupare a câmpului de luptă, determinată de scăderea efectivelor forțelor și de extinderea spațială (tridimensională) a limitelor câmpului de luptă. Totodată, acțiunile militare contemporane se caracterizează printr-un nou tip de „ceață” operațională, de tip ideologic. Noile tehnologii vor impune desfășurarea conflictului armat în anumite tipare acționale, prin urmare, o amprentă „post-eroică”, așa cum a numit-o Hirst (2001:77), odată cu care limitări și constrângeri provenite de la vechile revoluții militare vor fi înlocuite de limitări și constrângeri noi:

Armata „post-eroică” va elimina o constrângere, dar va impune o alta, căci războiul nu va mai fi o luptă. Informațiile perfecte și riscul scăzut de pierderi vor elimina „războiul” în sens clausewitzian; nu va mai fi o luptă morală și nu va mai implica „fricțiuni”. Folosirea forței se va asemana mai mult cu tehnicile de stopare a extinderii epidemiilor. (Hirst, 2001:77)

În acest nou context, concepte precum cel de război informațional, dar și altele din aria formelor neletale de manifestare a beligeranței: război psihologic, război mediatic, război cognitiv etc., își vor găsi maxima utilizare, chiar dacă posibila dezvoltare a unor conflicte telecomandate sau pur virtuale pare puțin probabilă.

2. Operațiile informaționale în conflictul contemporan

War is waged in three elements but there is no separate land, air, or naval war. Unless all assets in all elements are efficiently combined and coordinated against a... common objective, their maximum potential cannot be realized.

Gen. Dwight D. Eisenhower (1890-1969)

2.1 Operațiile întrunite

Succesul militar în operații este condiționat de abordarea holistică, ceea ce se traduce, în termeni militari, prin maximizarea efectelor forțelor implicate în conflict, posibil de obținut prin executarea de acțiuni în mod integrat, ceea ce asigură mai multă eficiență acțională din perspectivă sistemică. Conceptul central al aceste abordări este cel de „operație întrunită”, definind utilizarea în luptă într-o concepție unitară și sub comandă unică a forțelor, elementelor și mijloacelor de luptă aparținând a cel puțin două categorii de forțe armate. Proiecția întrunită vizează maximizarea efectelor prin utilizarea unitară a întregului potențial al forțelor și mijloacelor de luptă:

NATO recunoaște că succesul militar se bazează pe un efort întrunit, de obicei cu componente [n.a. categorie de forțe] și alte elemente ale forței reunite sub o comandă unificată. Puține operații sunt efectuate de o singură componentă. Aspectul esențial este că succesul campaniilor și operațiilor întrunite necesită o abordare cuprinzătoare pentru a maximiza eficacitatea generală a forței întrunite. Acest lucru va asigura utilizarea optimă a gamei complete de capacități.⁴⁷ (AJP-01,

⁴⁷ NATO recognizes that military success relies on a joint effort, usually with components and other force elements brought together under a unified command structure. Few operations are carried out by a single component. The essential point is that successful joint campaigns and operations require a comprehensive approach to maximize the overall effectiveness of the joint

Pentru a înțelege efectul cumulat al operațiunilor întrunite este necesară înțelegerea perspectivei sistemice proiectate de savantul Ludwig von Bertalanffy. Conceptul de sistem reprezintă un întreg organizat alcătuit din subsisteme – elemente aflate în interacțiune – incluse într-o structură distinctă (care reglementează sau prefigurează interacțiunile), evoluând într-un mediu cu care interacționează în ansamblu și prin elementele componente (von Bertalanffy, 1968). Teoria generală a sistemelor s-a impus în câmp logico-matematic, dar și ca direcție filosofică, constituindu-se ca teorie a complexității organizate, având la bază principiul că potențialul sistemului este întotdeauna mai mare decât suma potențialelor tuturor subsistemelor componente.

În ciuda faptului că războiul actual se caracterizează prin caracterul întrunit al acțiunilor de luptă, cooperarea dintre forțele aeriene, terestre și navale, în special dintre ultimele două categorii, odată ce forțele aeriene au o istorie relativ scurtă, datează de secole. Chiar dacă anterior impunerii termenului planificarea acțiunilor întrunite a fost pusă în aplicare în numeroase operațiuni militare, punerea lor în practică nu a fost tocmai facilă, motiv pentru care, de exemplu, marina și aviația naziste nu au putut produce efectul sinergic în Bătălia pentru Anglia. Operațiile întrunite își au originea într-o teorie a acțiunii militare datând de la sfârșitul secolului al XVI-lea – începutul secolului al XVII-lea, a maximizării efectelor prin acțiunile coordonate unitar ale diferitelor categorii de arme și specializări, denumită „combined arms theory”. Teoria a fost dezvoltată de Jomini în *Précis de l'art de la guerre* și pusă în aplicare în timpul războaielor napoleoniene, pentru ca ulterior, în forme apropiate de înțelesul conceptului cu care operăm în

force. This will ensure making the best use of the complete range of capabilities. [t.n.], în engleză în original.

prezent, să fie extinsă prin lucrările ofițerilor americani Jonathan House și Robert Leonhard (Angstrom & Widden, 2015:94-95). Ultimul dintre aceștia a pus la baza acțiunii combinate trei principii:

1. fiecare componentă a acțiunii combinate (specialitate, armă sau categorie de arme) are puncte forte și puncte slabe diferite, care pot fi exploatate sau suplinite prin acțiunea celorlalte;

2. prin acțiunea combinată se creează dileme inamicului și

3. acțiunea combinată îl poate forța/ determina pe inamic să acționeze pe teren nefavorabil.

În aceeași logică a teoriei generale a sistemelor, în raport cu operațiile întrunite s-a impus un concept nou, operațiile multi-domeniu (*multi-domain operations*, MDO), reprezentând un construct care presupune sincronizarea și convergența acțiunilor din diferite medii operaționale, cu scopul obținerii de avantaje operaționale în raport cu competitori similari. Spre deosebire de operațiile întrunite, în care efectul sinergic se obține prin efortul sistemic al subsistemelor în înțelesul de subsisteme ierarhice (statele majore ale categoriilor de forțe), în cazul MDO efectul sinergic se obține prin luarea în considerare ca sisteme ale mediului operațional al fiecăruia dintre mediile de acțiune: terestru, maritim, aerian, spațial și cibernetic (este luat în considerare la nivel teoretic și mediul cognitiv, fără a fi inclus încă în doctrinele americane și NATO)⁴⁸. Prin noua filosofie operațională, mediile de operare devin interdependente, structura exploatabilă în sensul obținerii efectului sinergic nemaifiind cea ierarhic militară (dublând funcțiuni operaționale), ci structura de straturi (*layere*) ale

⁴⁸ Noua Doctrină a Armatei României (D-0.1, 2025:16, art.0208), proiectând cunoașterea mediului de operare, ia în calcul domeniile operaționale anterior denumite, împreună cu spațiul de angajare (dimensiunile în care se produc efectele), mediul electromagnetic și mediul informațional, respectiv cu perspectiva sistemică PMESII.

mediului operațional. Totuși, MDO nu trebuie înțelese ca opozabile sau substituibile operațiilor întrunite, ci ca fază evolutivă a acestora:

Conceptul de operații multi-domeniu este un stadiu al evoluției operațiilor întrunite. Tranziția către operațiile multi-domeniu a început atunci când Alianța a recunoscut domeniile cibernetice și spațiale. În același fel în care introducerea puterii aeriene a transformat o concentrare pe un singur serviciu într-o abordare comună, persistența domeniului spațial, respectiv omniprezența și răspândirea domeniului cibernetic modifică modul în care Alianța operează.⁴⁹ (AJP-01, 2022:93, art.4.32)

În actualul mediu de securitate, caracterizat prin complexitate și dinamism, operațiile întrunite necesită proiectarea și luarea în considerație a unor funcții a căror menire este să reducă din efectele dinamicii mediului extern, pentru a permite o maximizare a efectelor prin intermediul acțiunilor militare desfășurate. În ediția anterioară a *Doctrinei Armatei României* (2012:art.0506), această proiecție se regăsea sub titulatura „funcții întrunite” (*joint functions*)⁵⁰, concept împrumutat din aparatul doctrinar NATO, unde este explicat astfel:

⁴⁹ The concept of multi-domain operations is an evolution of joint operations. The transition to multi-domain operations started when the Alliance recognized the cyberspace and space domains. In the same way that the introduction of air power transformed a single-service focus to a joint approach, the persistence of the space domain and the ubiquitous and pervasiveness of the cyberspace domain is changing how the Alliance operate. [t.n.], în engleză în original.

⁵⁰ În actuala doctrină (D-0.1, 2025:61, art.0423) se regăsește conceptul de acoperire strategică, subsumând descurajarea potențialilor adversari, inducerea în eroare, mascarea manevrei strategice, acțiunile de dislocare strategică, acțiuni informative, acțiuni în spațiul cibernetic, acțiuni de comunicare strategică și acțiuni de protecție și menținere funcțională a infrastructurii critice/ strategice.

Funcțiile întrunite: manevră, [putere de] foc, comandă și control, intelligence, informații, susținere, protecția forței și cooperare civili-militari (CIMIC) oferă un cadru comun pentru capacitățile și activitățile conexe reunite pentru a ajuta comandanții să integreze, să sincronizeze și să coordoneze diferite capacități și activități în cadrul operațiilor întrunite. Cadrul operaționalizează abordarea manevrieră printr-o combinație de manevră, [putere de] foc, informații și CIMIC pentru a influența atitudinea și comportamentul publicului. Printre altele, fiecare dintre aceste funcții întrunite desfășoară activități deliberate pentru a afecta direct voința, înțelegerea și capacitatea de luare a deciziilor prin impactul asupra simțurilor, stării de spirit și calculului publicului relevant.⁵¹ (AJP-10.1, 2023:10, art.1.16)

Funcțiile întrunite asigură, așadar, maximizarea efectelor, prin punerea în aplicare înainte, pe timpul și după desfășurarea operațiilor întrunite. Chiar dacă aplicabile conceptului de operații întrunite, funcțiile întrunite produc efecte și în noua filosofie acțională MDO; prin înțelegerea lor ca acțiuni și operațiuni care contribuie la obținerea efectului sinergic, doctrina aliată întrunită exemplificând în acest sens prin managementul focului, manevra, operațiile informaționale și CIMIC. (AJP-01, 2022:93, art.4.31).

⁵¹ The joint functions of manoeuvre, fires, command and control, intelligence, information, sustainment, force protection and civil-military cooperation (CIMIC) provide a framework of related capabilities and activities grouped together to help commanders integrate, synchronize and direct various capabilities and activities in joint operations. The joint functions framework operationalizes the manoeuvrist approach through a combination of manoeuvre, fires, information and CIMIC to affect the audience's attitude and behaviour. Amongst others, each of these joint functions perform deliberate activities to affect will, understanding and capability of decision-making directly by impacting a relevant audience's senses, state of mind and calculus. [t.n.], în engleză în original.

În aparatul doctrinar american (J.P. 3-13, 2014:vii), ulterior și în doctrinele NATO, instrumentele puterii naționale sunt considerate a fi de natură diplomatică, informațională, militară și economică. În mod similar, și în doctrina românească (prin intermediul aparatului doctrinar NATO, care a fost direct influențat de cel american), conceptul de instrumente ale puterii naționale, definite în conformitate cu prevederile AJP-10.1, se manifestă prin acțiuni de natură diplomatică, informațională, militară și economică (DIME). Practic, funcțiile întrunite au rolul de a se interpune între instrumentele de putere ale adversarului potențial sau actual, minimizând acțiunile acestuia îndreptate împotriva conducerii și capacităților de comandă proprii, protejând trupele proprii și influențând pe cât posibil voința sa, în special pe palierele diplomatic și informațional.

Proiectând acțiunea pe palier informațional, se poate constata că efectul sinergic al acțiunii întrunite nu se poate înregistra în absența desfășurării operațiilor informaționale, într-un mediu (în care modalitățile clasice de confruntare au devenit soluții ultime, mai puțin importante ca pondere și intenție în raport cu acțiunile pe palierul puterii *soft*) a puterii informaționale, diplomatice și economice. În doctrina NATO, informațiile ca funcție întrunită sunt considerate a fi critice în procesul decizional și necesare în înțelegerea mediului operațional:

Informația este esențială pentru luarea deciziilor, iar modul în care publicul este informat și influențat depinde de informațiile disponibile. Funcția de informare, împreună cu alte funcții, îi ajută pe comandanți și statul major să aplice sau să utilizeze informații pentru a înțelege impactul tehnologiilor emergente și disruptive, să informeze și să influențeze percepțiile, comportamentul și procesul decizional relevant al publicului. Facilitatorii cheie sunt operațiile psihologice, relațiile publice militare, războiul electromagnetic, activitățile cibernetice și

angajarea, care trebuie coordonate și integrate pe întreg parcursul procesului de planificare, pentru a sprijini toate activitățile și pentru a fi în concordanță cu narațiunile.⁵² (AJP-10.1, 2023:10, art.1.17)

Privind în ansamblu, revoluția informațională conduce, pe de o parte, la descentralizare și nivelare, pe de alta menține încă – notează Joseph Nye jr. (2005:213) –, o anumită predominanță a marilor puteri pe piața globală a informației. Din această cauză, raporturile dintre state sunt din ce în ce mai complexe, mult mai complexe decât în cazul unei simple raportări la consecințele în cascadă ale determinismului tehnologic⁵³. Decizia politico-militară este direct influențată de noul mediu global, saturat din perspectivă informațională.

În condițiile menținerii decalajelor dintre state, în ciuda rolului egalizator al revoluției informaționale, creând mai degrabă interdependență complexă, credibilitatea și susținerea publică devin resurse fundamentale în noile raporturi între puteri. Aceste noi caracteristici ale mediului global, influențate direct de revoluția informațională care este descrisă prin linii

⁵² Information is critical for decision-making and how audiences are informed and influenced is dependent on the information available to them. The information function helps commanders and staff applying or using information to understand the impact of emerging and disruptive technologies, along with other functions, to inform and influence relevant audience perceptions, behaviour and decision-making. Key enablers are psychological operations, military public affairs, electromagnetic warfare, cyber and engagement activities, which must be coordinated and integrated throughout the planning process, support all activities and be consistent with the narrative. [t.n.], în engleză în original.

⁵³ În științele sociale, determinismul tehnologic caracterizează un anumit tip de monopol mediatic, de tipul *space-biased media* (Harold Innis), fiind la rândul său caracterizat de celebra expresie a lui Marshall McLuhan, „mijlocul este mesajul” (*the medium is the message*) (McLuhan, 1994:5): „Modificând tipul de organizare socială, tehnologiile media modifică și tipul de percepere a societății, iar prin aceasta, structura internă a indivizilor, impunându-ne o grilă de referință” (Lesenciuc, 2010:133-134)

de câmp complexe, transstatale, transorganizaționale, conduce la o definiție a unui concept cu care se operează în plan strategic, acela de mediu informațional. În mediul de securitate global, mediul informațional⁵⁴ cuprinde

[...] informația în sine, indivizii, organizațiile și sistemele care recepționează, procesează și transmit informațiile, precum și spațiul cognitiv, virtual și fizic în care se petrece acest lucru. (NATO Agreed)⁵⁵ (AJP-10.1, 2023:15, art.2.7).

Mediul informațional (incluzând spațiul cibernetic) este organizat pe trei dimensiuni: fizică/ tangibilă (centrată pe platformele și elementele fizice la dispoziție: sistemele C2 și structura de sprijin); informațională (cuprinzând datele și informațiile procesate, depozitate, diseminate și protejate) și dimensiunea cognitivă (centrată pe om, cuprinzând elemente de capacitate individuală sau de grup pentru a procesa informații și pentru a lua, în baza acestora, decizii).

Față de edițiile anterioare ale doctrinei, dimensiunea informațională propriu-zisă a fost înlocuită cu cea virtuală, fiecare dintre aceste componente fiind analizată pe substraturi diferite, precum în figura 4. În noua arhitectură a mediului informațional, dimensiunea fizică include straturile geografic, fizic propriu-zis și infrastructura de rețea, dimensiunea virtuală straturile logic (software) și entitățile virtuale, iar dimensiunea cognitivă stratul social și stratul cognitiv propriu-zis.

⁵⁴ Mediul informațional este definit ca fiind spațiul virtual și fizic în care informațiile sunt recepționate, procesate și transmise. Mediul informațional conține atât informațiile propriu-zise cât și sistemele informaționale care procesează aceste informații. (MC 422/3).

⁵⁵ [...] the information itself, the individuals, organizations and systems that receive, process and convey the information, and the cognitive, virtual and physical space in which this occurs. (NATO Agreed). [t.n.], în engleză în original.

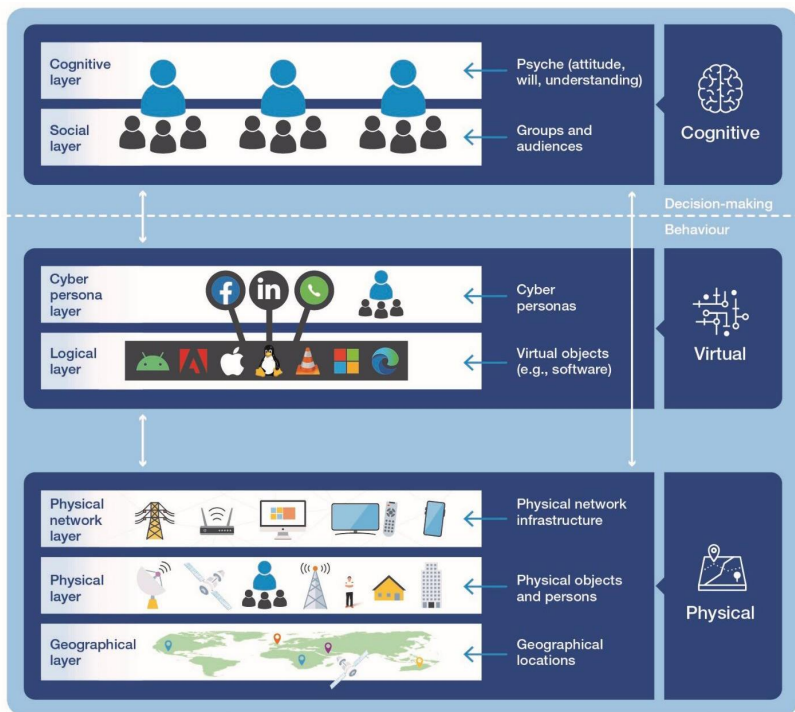


Fig.4 Mediul informațional (*apud* AJP-10.1, 2023:38)

Pentru o înțelegere adecvată a confruntării informaționale, mediul informațional trebuie privit ca entitate de sine stătătoare și ca resursă (în înțelesul de mediu informațional aplicabil în domeniul AI), similar structurii CPH (cyber-physical & human) sau structurilor similare operaționale în acest domeniu. Similaritatea devine mai evidentă în această nouă proiecție a doctrinei NATO a operațiilor informaționale, similară perspectivei americane din Joint Concept for Operating in the Information Environment (JCOIE), prin intermediul căreia este evidențiat parcursul transformării datelor în informație, cunoaștere și înțelegere comună pe parcursul construirii acestei înțelegeri comune a mediului operațional. Modelul ierarhic cognitiv utilizat în înțelegerea comună (JCOIE, 2018:12) a

mediului operațional permite înțelegerea procesului decizional în mediul informațional actual atât în condițiile apelului la inteligența umană (HI), la inteligența artificială (AI) – în mai mică măsură –, sau la varianta hibridă (AI/HI): „Deși raționarea rămâne o calitate exclusiv umană, mașinile vor ajuta din ce în ce mai mult la evaluarea informațiilor, cu intenția de a îmbunătăți viteza și calitatea procesului decizional uman”⁵⁶ (JCOIE, 2018:13).

Building Shared Understanding

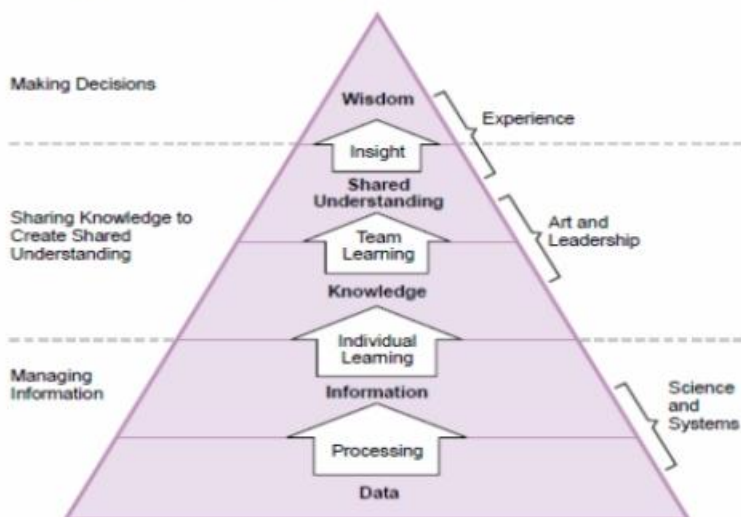


Fig.5 Modelul ierarhic cognitiv (*apud* JCOIE, 2018:12)

În înțelegerea dimensiunii cognitive a mediului informațional ca fiind fundamentală, pentru ca procesul decizional hibrid AI/HI să nu fie afectat de forme variate de alterare a adevărului, este necesară luarea în considerare a

⁵⁶ While judgment remains a uniquely human quality, machines will increasingly assist in evaluating information with the intent of improving the speed and quality of human decision-making. [t.n.], în engleză în original.

tuturor surselor de alterare, adică a tuturor dimensiunilor mediului informațional:

Dacă mediul informațional dinamic este cel care determină dinamica AI, cu siguranță motorul schimbării nu este dimensiunea fizică sau cea informațională, ci cea cognitivă, situată pe în cea mai înaltă etapă de procesare, de înțelegere partajată și de luare a deciziilor responsabile. Evident, pentru a atinge această etapă de implicare AI în luarea deciziilor, sursele de viciere a adevărului trebuie reduse sau eliminate, adică baza de exemple de antrenament (*training examples*) trebuie extinsă, iar posibilitățile de aproximare a adevărului de bază (*ground-truth*) trebuie crescute.⁵⁷ (Lesenciuc, 2024:13).

Într-o astfel de proiecție, nivelul profund de înțelegere și potențialul implicării în operațiuni militare ulterioare (JCOIE, 2018:13) nu sunt afectate de bias-urile inteligenței artificiale.

2.2 Operațiile informaționale ca funcție întrunită

Mediul operațional se caracterizează prin exercitarea puterii *hard*, iar operațiile informaționale – funcție întrunită definită de aparatele doctrinare NATO – vizează utilizarea puterilor *soft*, în special a puterii simbolice. Pe fondul complexificării raporturilor dintre state și/ sau actori non-statali, în baza modificărilor continue în ceea ce privește mediul

⁵⁷ If the dynamic information environment is the one that determines the dynamics of AI, certainly the engine of change is not the physical or informational dimension, but the cognitive one, located at the highest stage of processing, shared understanding and responsible decision-making. Obviously, in order to reach this stage of AI involvement in decision-making, the sources of corrupting the truth must be reduced or eliminated, i.e. the base of training examples must be expanded, and the possibilities of ground-truth approximation must be increased. [t.n.], în engleză în original.

informațional, pe fondul unor manifestări asimetrice extrem de violente, problematica unei coordonări corespunzătoare a acțiunilor *soft* în cadrul configurat al operațiunii militare caracterizate prin manifestarea în câmpul puterii *hard* necesită o regândire a filosofiei câmpului de luptă. În plus, date fiind continuele transformări generate de tehnologiile emergente, putem considera că aserțiunea lui Joseph Nye jr. este încă validă, adică putem lua în calcul că: „Suntem într-o asemenea etapă timpurie a revoluției informaționale, încât orice concluzie trebuie să fie provizorie/ temporară” (Nye jr., 2005:218). Din această perspectivă, proiectarea operațiilor informaționale (Info Ops) ca acțiuni realizate în scopul influențării procesului decizional (politico-militar) al adversarului și al protejării proceselor și structurilor decizionale proprii, constituie măsura prin care predictibilitatea în mediul informațional devine mult mai ridicată și prin care efectul sinergic al acțiunii întrunite nu este perturbat.

Operațiile informaționale sunt definite diferit în aparate doctrinare diferite. În precedenta doctrină românească ele erau definite în raport cu cadrul terminologic stabilit prin politicile militare NATO, în special prin documentele MC 0422/3, *NATO Military Policy on Information Operations* [study draft] și MC 0422/4, *NATO Military Policy on Information Operations*:

Info Ops este mai degrabă o funcție de stat major care are ca scop analiza, planificarea, evaluarea și integrarea activităților din mediul informațional decât o capacitate în sine (MC 0422/4, 2012:2, art.2)

Info Ops reprezintă o funcție de stat major care are ca scop analiza, planificarea, evaluarea și integrarea activităților de informare pentru a crea efectele dorite asupra voinței, înțelegerii și capacității adversarilor, potențialilor adversari și publicului

aprobat de NAC în susținerea obiectivelor misiunii Alianței.⁵⁸
(MC 0422/4, 2012:3-4, art.9)

Practic, familia de documente MC 422 (NATO Military Policy on Information Operations), promulgate de Comitetul Militar NATO de la Bruxelles, reprezintă primul cadru de definire NATO a operațiilor informaționale, începând cu luna ianuarie 1999, dar consensul privitor la conceptul „operații informaționale” a apărut mai târziu, prin intermediul MC 0422/3, care a definit pentru prima dată acest concept raportat la proiecția scopurilor în raport cu voința, înțelegerea și capacitatea acțională, așa cum subliniază cercetătorul Călin Hentea, specialist în operații psihologice, cu experiență în teatrele de operații din Albania, Kosovo și Afganistan:

Definiția din Politica NATO în domeniul operațiilor informaționale MC 422/3, din 19 martie 2007, reprezintă consensul aliat, reușit după mulți ani, asupra acestui delicat concept. (Hentea, 2008a:301)

Spre deosebire de precedentele doctrine, cele actuale nuanțează conceptul NATO din seria de documente MC 422 și îl aplică raportat la nivelurile politic și politico-militar, definiind operațiile informaționale drept funcție de stat major cu rol în analiza, planificarea, evaluarea și integrarea activităților informaționale care vizează efecte asupra voinței,

⁵⁸ Info Ops is a staff function to analyze, plan, assess and integrate activities focused on the IE rather than a capability in its own right. (MC 0422/4, 2012:2, art.2)

Info Ops is a staff function to analyze, plan, assess and integrate Information Activities to create desired effects on the will, understanding and capability of adversaries, potential adversaries and NAC approved audiences in support of Alliance mission objectives. [t.n.], în engleză în original.

înțelegerii și capacității acționale a țințelor aprobate de Consiliul Suprem de Apărare a Țării (CSAT).

În aparatul doctrinar al Statelor Unite, definiția operațiilor informaționale se axează pe tiparele acționale și pe formele de alterare a fluxurilor informaționale în raport cu tipurile de țințe:

[...] utilizarea integrată, în timpul operațiunilor militare, a IRC⁵⁹ integrate cu alte direcții de operații pentru a influența, perturba, corupe sau uzurpa procesul decizional al adversarilor și al potențialilor adversari, protejându-l pe cel propriu⁶⁰ (JP 3-13, 2014:vii),

Noua doctrină NATO a operațiilor informaționale consideră acest domeniu ca funcție de stat major și îl definește raportat la un cadru mai amplu, din care nu lipsește funcțiunea de comunicare strategică (StratCom), care asigură cadrul general de informare și influență a publicurilor în raport cu abordarea bazată pe narațiuni. Noua perspectivă schimbă fundamental filosofia operațiilor informaționale, definite în acord cu proiecția Comitetului Militar al NATO din linia de documente MC 422. Practic, elementul fundamental a fost introducerea conceptului de comunicare strategică, doar că acest concept nu a produs efecte de la început. Alinierea acțiunilor de informare și influență la filosofia StratCom, realizată prin intermediul actualei doctrine aliate a operațiilor informaționale a adus o schimbare majoră de perspectivă. În această lumină, operațiile informaționale nu se definesc substanțial diferit în raport cu precedentul cadru proiectiv, dar sunt nuanțate printr-un pachet de definiții care mai includ

⁵⁹ Information-related capabilities.

⁶⁰ [...] integrated employment, during military operations, of IRCs⁶⁰ in concert with other lines of operations to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own. [t.n.], în engleză în original.

conceptele „activități de informare”, „activități de comunicare” și „mediu informațional”, majoritatea acestora agreate la nivelul Organizației Nord-Atlantice:

a. **Operații informaționale.** O funcție de stat major care are ca scop analiza, planificarea, evaluarea și integrarea activităților informaționale pentru a crea efectele dorite asupra voinței, înțelegerii și capacității adversarilor, potențialilor adversari și publicului în sprijinul obiectivelor misiunii. (NATO Agreed).

b. **Activități informaționale.** Activități desfășurate prin orice capacitate sau mijloc, axate pe crearea de efecte cognitive. (NATO Agreed).

c. **Activități de comunicare.** În înțelesul prezentei lucrări, activitățile de comunicare sunt descrise ca activități informaționale desfășurate de structurile militare de relații publice și operații psihologice.

d. **Mediu informațional.** Un mediu alcătuit din informația propriu-zisă, indivizii, organizațiile și sistemele care recepționează, procesează și transmit informațiile, precum și spațiul cognitiv, virtual și fizic în care se întâmplă acest lucru. (NATO Agreed).⁶¹ (AJP-10.1, 2023:14-15, art. 2.7).

Practic, noul cadru doctrinar NATO nu rezumă conceptul vulgarizat de „război informațional” la „operațiile

⁶¹ a. **Information operations.** A staff function to analyze, plan, assess and integrate information activities to create desired effects on the will, understanding and capability of adversaries, potential adversaries and audiences in support of mission objectives. (NATO Agreed)

b. **Information activities.** Activities performed by any capability or means, focused on creating cognitive effects. (NATO Agreed)

c. **Communication activities.** For the purpose of this publication, communication activities are described as information activities performed by military public affairs and psychological operations capabilities.

d. **Information environment.** An environment comprised of the information itself, the individuals, organizations and systems that receive, process and convey the information, and the cognitive, virtual and physical space in which this occurs. (NATO Agreed). [t.n.], în engleză în original.

informaționale”, așa cum s-a întâmplat până în 2023, ci definește un set de activități și operațiuni și un mediu informațional care concură la configurarea unei arhitecturi informaționale a câmpului de luptă și care iau în calcul o direcție generală de informare și influență exercitată prin StratCom.

Operațiile informaționale joacă un rol important în toate fazele operațiilor întrunite, dar și înainte sau după desfășurarea acestora, presupunând o angrenare logică a fiecărei faze în tranziția de la efortul principal la efortul de sprijin (JP 3-13, 2014:xi). Operațiile informaționale nu sunt planificate și executate similar în toate armatele. În operațiile multinaționale, cadrul acțional, procedurile și instrumentele operațiilor informaționale la dispoziție se aliniază și desfășoară în conformitate cu proiecția întrunită multinațională, sub coordonarea comandantului forței multinaționale (*Multinational Force Commander*, MNFC). Ținând cont de proiecția și implementarea întrunită a operațiilor informaționale, în acord cu celelalte funcții întrunite, pentru a se obține efectul cumulat, dar și cu această proiecție unitară și executare în conformitate cu principiul comenzii unice, dar și cu celelalte principii ale războiului, operațiile informaționale pot fi definite ca funcție întrunită.

2.3 Operațiile informaționale ca operații de influențare

Doctrina românească a operațiilor informaționale izvorăște din precedentă doctrină NATO a operațiilor informaționale. Totodată, ea se aliniază parțial și filosofiei americane privitoare la arhitectura informațională a câmpului de luptă. Cel mai important aspect este cel privitor la faptul că operațiile informaționale sunt operații militare de influențare, așa cum rezultă din setul de definiții provenind din aparate doctrinare distincte și din documente politico-militare emise de Alianța Nord-Atlantică.

În conformitate cu doctrina americană, comandantul structurii de operații informaționale este responsabil de integrarea acțiunilor de influențare în cadrul procesului de planificare a operațiilor întrunite. Totodată, comandantul acestei structuri este responsabil de coordonarea și sincronizarea funcțiilor întrunite pentru îndeplinirea obiectivelor/ misiunilor stabilite de Comandantul Forțelor Întrunite (*Joint Force Commander, JFC*). Am utilizat conceptul de operații de influențare în înțelesul sintagmei *information-related capabilities* (IRC), definit în cadrul JP 3-13 (2014) din multiple motive. IRC reprezintă setul de instrumente, tehnici și activități care afectează mediul informațional. Ele pot fi puse în aplicare doar dacă sunt funcționale o serie de alte funcții sau subfuncții întrunite, cum ar fi securitatea informațiilor (INFOSEC) și a operațiilor (OPSEC), asigurarea informațiilor (IA – *information assurance*), securitatea fizică și războiul electronic (EW – *electronic warfare*). Componentele cheie ale IRC sunt datele – semnale interpretabile care pot reduce incertitudinea; informațiile – datele din context care redau scopul acțiunii; cunoștințele – informațiile din context care antrenează acțiunea directă (cunoștințe explicite și tacite) și influența – actul sau puterea de a produce efectul dorit asupra țintei vizate (TA - *target audience*) (JP 3-13, 2014:I-3).

Fiecare dintre primele trei componente cheie ale IRC constituie elemente dintr-un lanț cognitiv în baza căruia funcționează operațiile informaționale, contribuind la atingerea nivelului dorit de influențare (servind, așadar, influențării, constituind prin aceasta operații desfășurate în scopul influențării). Identificarea publicurilor țintă, înțelegerea culturii, credințelor, regulilor, normelor și convingerilor acestora, proiectarea mijloacelor disponibile pentru obținerea scopului dorit (acțiuni diplomatice, informaționale, militare, economice etc.), respectiv identificarea metodelor necesare atingerii scopului dorit, sunt etape anterioare influențării, dar care se pot realiza, în cadrul operațiilor informaționale, sub coordonarea structurilor de operații informaționale sau împreună cu acest tip de operații, nu prin deținerea capacităților și tehnicilor, ci prin aplicarea integrată a acestora pentru a obține scopul dorit: „Prin urmare, în IO⁶² nu este importantă deținerea capacităților și tehnicilor, ci mai degrabă aplicarea lor integrată pentru a atinge condițiile finale stabilite de JFC”⁶³ (JP 3-13, 2014:I-5). Prin urmare, și din acest punct de vedere, prin aplicarea integrată și prin urmărirea scopului final, de influențare a țărilor planificate, IRC pot fi înțelese drept operații de influențare.

Pe de altă parte, în 2013 utilizam, în scopul proiectării operaționalizării procesului de influențare a publicurilor țintă, conceptul de operații de influență, propus de Călin Hentea (2008b:365-366), împrumutat din aparatul doctrinar francez (unde poartă numele de *operații militare de influență/opérations militaires d'influence*⁶⁴ – OMI, v. PIA 03.253,

⁶² Operații informaționale în abrevierea din doctrinele americane.

⁶³ Therefore, in IO, it is not the ownership of the capabilities and techniques that is important, but rather their integrated application in order to achieve a JFC's end state, [t.n.], în engleză în original.

⁶⁴ Les opérations militaires d'influence (OMI) regroupent l'ensemble des activités dont l'objet est d'obtenir un effet sur les comportements d'individus, de groupes ou d'organisations (info-cibles), afin de contribuer à l'attinte des objectifs politiques et militaires. (PIA 03.253, 2008:6, 47)

2008), pentru a include în primul rând operațiile media și operațiile informaționale, mai exact

[...] pentru a reuni la nivel conceptual și, mai ales, la nivel acțional, sub comandă și planificare unică, toate domeniile de activitate cu incidență asupra comportamentelor, atitudinilor, emoțiilor, motivațiilor și percepțiilor audiențelor interne și externe, prin modalități de acțiune specifice operațiilor psihologice, relațiilor publice și operațiilor media, războiului electronic, operațiilor în rețelele de calculatoare, relațiilor civili-militari, diplomației militare etc. (Lesenciuc, 2013:34).

Actualmente, ministerul francez al apărării operează cu conceptul extins de război informațional/ război al informațiilor (*la guerre de l'information*), destinat pentru a influența adversarii, în cadrul căruia a proiectat un concept nou, *la lutte informatique d'influence* (L2I) care se referă la operațiunile militare desfășurate în spațiul virtual (cyberspațiu), contribuind împreună la comunicarea strategică (StratCom) ministerială:

Războiul cibernetic de influență (L2I) se referă la operațiuni militare desfășurate pe palierul informațional al spațiului cibernetic pentru a detecta, analiza și contracara atacuri, a sprijini StratCom, a colecta informații sau a înșela, fie independent, fie împreună cu alte operații⁶⁵. (L2I, 2021:9).

Echivalent Cyberspace Operations din doctrina NATO, conceptul L2I este mult mai amplu, pentru că el cuprinde o componentă de influențare foarte importantă, atât pentru

⁶⁵ La lutte informatique d'influence (L2I) désigne les opérations militaires conduites dans la couche informationnelle du cyberspace pour détecter, caractériser et contrer les attaques, appuyer la StratCom, renseigner ou faire de la déception, de façon autonome ou en combinaison avec d'autres opérations. [t.n.], în franceză original.

dimensiunea defensivă, *lutte informatique défensive* (LID), cât și pentru cea ofensivă, *lutte informatique offensive* (LIO) și necesită, pe lângă specialiștii în mediul virtual, și specialiști în mediul informațional și cognitiv, lingviști, psihologi sau sociologi (L2I, 2021:13). Din perspectivă doctrinară franceză, Info Ops reprezintă acronimul anglo-saxon semnificând «opération(s) d'information», adică acel set de operații militare care privesc procesul de analiză, planificare, conducere și evaluare a efectelor unor acțiuni generate de o strategie militară de influență (la stratégie militaire d'influence), așa cum sunt definite de Centre interarmées de concepts, de doctrines et d'expérimentations (CICDE, *apud* Harbulot, 2023).

Pe de o parte, conceptul de operații de influență (sau operații de influențare) se referă la un proces continuu, adică la setul de instrumente, tehnici și activități planificate și coordonate unitar care afectează mediul informațional, poate fi asociat conceptului american anterior definit, *information-related capabilities* (IRC) și poate fi utilizat, în acest sens, pentru a asigura gradul necesar de înțelegere și aplicare în mediul științific românesc. Pe de altă parte, conceptul IRC include seria de instrumente, tehnici și activități care fac obiectul unor funcții întrunite, cum ar fi: Info Ops, Media Ops, CIMIC, C2, asigurarea informațiilor.

3. Operațiile informaționale

I will tell you that a commander without the proper C2 assets commands nothing except a desk. You must have the ability to communicate with the forces under your command. You must have the ability to exchange information with them freely, frequently, and on a global basis.

Gen. Ronald R. Fogleman (n.1942)

3.1 Scop, obiective, principii

3.1.1 Scop și obiective Operațiile informaționale (Info Ops⁶⁶) fac parte din categoria operațiilor/activităților neletale desfășurate în sprijinul operațiilor întrunite, chiar dacă obiectivele lor și punerea în aplicare presupun utilizarea de mijloace letale și/ sau neletale. Info Ops presupun o foarte importantă componentă neletală. Practic, odată cu extinderea rolului mediului informațional în desfășurarea acțiunilor militare, o importanță tot mai mare a revenit operațiilor informaționale, chiar dacă acestea au putut fi puse în evidență începând de la primele lucrări de artă militară, încă din secolul VI î.Hr. Spre exemplu, în capitolul XIII din *Arta războiului*, intitulat „Folosirea agenților secreți”, generalul chinez Sun Tzu pune la baza deciziei informarea prealabilă, obținută de la oamenii care cunosc situația inamicului (în înțelesul actual de sprijin cu informații): „Or, dacă prințul luminat și generalul avizat înving inamicul de câte ori trec la acțiune, dacă realizările lor depășesc pe cele obișnuite, aceasta se datorează informării prealabile” (Sun Tzu, 1999:89-90). Informația

⁶⁶ Pentru a nu lăsa impresia că în doctrine militare diferite conceptul de „operații informaționale” acoperă arii diferite la nivel denotativ, am optat pentru utilizarea acronimului NATO, Info Ops, în detrimentul celorlalte acronime.

devine fundamentală în acțiunile militare despre care au relatat istoricii, începând din antichitate, chiar dacă proiectarea unui sistem având obiective precise în mediul informațional presupunea, de regulă, culegerea de informații de la adversar în scopul realizării surprinderii și nu neapărat acțiunea directă asupra voinței adversarului de a lupta. Sun Tzu prefigurase, de altfel, atât necesitatea unei bune cunoașteri a inamicului și a trupelor proprii:

31. (...) Cunoaște-ți inamicul și cunoaște-te pe tine însuși; într-o sută de bătălii nu te vei expune nici unei primejdii.

32. Când nu-ți cunoști inamicul, dar te cunoști pe tine însuși, șansele tale de victorie sau de înfrângere sunt egale.

33. Dacă nu-ți cunoști nici inamicul și nici pe tine însuși, ești sigur că te vei găsi în primejdie în fiecare bătălie. (Sun Tzu, 1999:29),

cât și a înfrângerii voinței de a lupta a inamicului, cucerind inamicul intact: „Scopul trebuie să fie de a cuceri intact „tot ceea ce este sub cer”. În acest mod, trupele vor rămâne neatinse și victoria va fi totală. Aceasta este arta strategiei ofensive” (Sun Tzu, 1999:18). Managementul informației a constituit, de-a lungul timpului, factorul fundamental în ceea ce privește coerența, oportunitatea și corectitudinea deciziei militare și, implicit, victoria pe câmpul de luptă. Cu timpul, informația a devenit importantă și în raport cu publicuri țintă mai extinse, cum ar fi, de pildă, populația locală din zona de operații, capabilă să influențeze, la rândul ei, voința politică de menținere a angajării în confruntare.

Pe câmpul de luptă contemporan, spre deosebire de operațiile militare propriu-zise care presupun utilizarea forței armate pentru a constrânge în scopul influențării voinței adversarului, operațiile informaționale au drept principal scop influențarea voinței adversarului și a celorlalte categorii de publicuri țintă, definită de doctrina aliată după cum urmează:

Voința este facultatea prin intermediul căreia un actor decide și inițiază un curs de acțiune. Aceasta include factori precum motivația, percepția, atitudinea, credințele și valorile și cuprinde intenția de a acționa sau de a rezista. În cadrul direcției și obiectivelor operațiunilor militare mai ample și a îndrumărilor specifice misiunii NATO, activitățile informaționale sunt destinate actorilor de la orice nivel în măsură să influențeze situația.⁶⁷ (AJP-10.1, 2023:15, art.2.7).

Prin afectarea voinței, operațiile informaționale urmăresc, după caz, întărirea sau descurajarea comportamentului diferitelor categorii de public. Această proiecție este similară în multe aparate doctrinare care definesc eficiența decizională a decidentului în raport cu voința, înțelegerea și capacitatea de aplicare. Și în precedentă doctrină aliată, în raport cu care a fost proiectată doctrina românească a operațiilor informaționale, eficiența decidentului este influențată de voința, înțelegerea și capacitatea ținutelor acestui tip de operații – am optat pentru exemplificarea din doctrina aliată din 2009 din următoarele rațiuni: pentru a ilustra continuitatea perspectivei și, implicit, pentru a permite o analiză diacronică, respectiv pentru a oferi posibilitatea înțelegerii modului în care precedentă doctrină aliată a influențat doctrine naționale aplicabile astăzi –:

⁶⁷ Will is the faculty by which an actor decides upon and initiates a course of action. It includes factors such as motivation, perception, attitude, beliefs and values and encompasses the intent to act or resist. Within the direction and goals of wider military operations, and mission-specific NATO guidance, information activities are aimed at actors at any level capable of influencing the situation. [t.n.], în engleză în original.

Eficiența unui decident (decision-maker)⁶⁸ este o funcție de *voință*⁶⁹, *înțelegere*⁷⁰ și *capacitate*. Cu alte cuvinte, un decident trebuie să aibă voința de a acționa, înțelegerea situației pentru a acționa și capacitatea de a acționa. Dacă unul dintre aceste elemente nu este prezent, capacitatea decidentului de a acționa în modul dorit va fi afectată^{71 72}(AJP-3.10, 2009:I-3 – I-4),

dar și actuala doctrină include cele trei aspecte deja menționate. Singura diferență în proiecția din cele două aparate doctrinare este cea de înțelegere a celui de-al treilea element, capacitatea, care se referă la capacitatea acțională, exemplificată în noua doctrină prin „C2S, CIS infrastructure and propaganda facilities”. *Allied Joint Doctrine for Information Operations* AJP-10.1 definește fără echivoc acest termen, în înțelesul de capacitate acțională (presupunând structura de canale și fluxuri informaționale prin intermediul cărora decidenții politici sau militari devin capabili să înțeleagă situația și să pună în aplicare voința), după cum urmează:

⁶⁸ Decision-maker is used in its broadest sense throughout this document. They include political and other leaders and military commanders, influential individuals, military personnel, armed factions and specific population groups (e.g. ethnic, cultural, religious and political). They may be adversaries, potential adversaries or other NAC approved parties.

⁶⁹ Will includes factors such as motivation, intent, attitude, beliefs and values.

⁷⁰ Will includes factors such as motivation, intent, attitude, beliefs and values.

⁷¹ The term ‘to affect’ is used throughout the document in a generic sense meaning: ‘to have an effect on’, without any implied (positive or negative) connotations.

⁷² A decision-maker’s⁷² effectiveness is a function of *will*⁷², *understanding*⁷² and *capability*. In other words, a decision-maker must have the will to act, an understanding of the situation to act and possess the capability to act. If one of these elements is not in place, the decision-maker’s ability to act in the way he wants to will be affected, [t.n.], în engleză în original.

Capacitate. Capacitatea de acțiune a unui actor depinde de capacitățile sale fizice și de utilitatea sa într-o anumită situație. Activitățile informaționale vor urmări să afecteze aceste capacități, cum ar fi infrastructura C2S și CIS și facilitățile de propagandă care permit actorilor să înțeleagă o situație și să aplice voința.

a. Activitățile informaționale urmăresc să degradeze, să perturbe, să înșele, să distrugă sau să nege acele capacități care permit factorilor de decizie adversi să își sporească înțelegerea și să își consolideze, să își impună, să aplice și să își susțină voința de a acționa eficient și (unde este cazul) să exercite [funcțiunile de] comandă și control.

b. Activitățile informaționale urmăresc, de asemenea, să atace sursa bazei de putere a unui adversar, divizând grupările și alianțele interne și externe. Scopul este de a influența procesele lor decizionale, împiedicându-i astfel să ia inițiative.

c. Activitățile informaționale urmăresc, de asemenea, protejarea capacităților, de exemplu, infrastructura C2S și CIS prietenoasă, care permite comandantului forței întrunite să exercite o comandă eficientă, să își impună voința și să preia și să mențină inițiativa.⁷³ (AJP-10.1, 2023:17, art.2.12).

⁷³ **Capability.** An actor's capacity for action is dependent upon their physical capabilities and their utility in a particular situation. Information activities will seek to affect those capabilities, such as C2S, CIS infrastructure and propaganda facilities that enable actors to understand a situation and apply their will.

a. Information activities seek to: degrade, disrupt, deceive, destroy or deny those capabilities that allow adversary decision-makers to increase their understanding and bolster, impose, apply and sustain their will to act effectively and (where appropriate) exercise command and control.

b. Information activities also seek to attack the source of an adversary's power base, splitting internal and external groupings and alliances. The aim is to influence their decision-making processes, thereby preventing them from taking the initiative.

c. Information activities also aim to protect capabilities. For example, friendly C2S and CIS infrastructure that allow the joint force commander to exercise effective command, impose their will and seize and maintain the initiative. [t.n.], în engleză în original.

Din această structură ternară a proiecției scopului operațiilor informaționale: voință – înțelegere – capacitate acțională derivă direct obiectivele Info Ops. Pentru o punere în evidență a proiecției obiectivelor pe cele trei dimensiuni pe care se desfășoară operațiile informaționale în funcție de tipul de ținte ale influenței planificate: adversari și potențiali adversari, aliați și trupe proprii, respectiv alte entități aprobate (fără definire explicită în doctrina românească, în timp ce doctrina NATO le proiectează la cel mai înalt nivel de coordonare), am ales soluția prezentării lor în formă tabelară (Tabelul 3), ca rezultat al analizei diferitelor doctrine pentru operații informaționale:

Tabelul 3 Obiectivele operațiilor informaționale

	La adversari și potențiali adversari	La aliați și trupele proprii	La celelalte entități aprobate
Influențarea voinței	O1.1 subminarea coeziunii, a sprijinului moral și diminuarea hotărârii de a-și continua acțiunile	O1.2 protecția și întărirea voinței prin menținerea coeziunii și creșterea libertății de acțiune, precum și contracararea eforturilor adversarilor de a-i influența	O1.3 promovarea intereselor naționale sau ale NATO/UE, influențarea în favoarea aliaților și trupelor proprii, precum și contracararea eforturilor adversarilor de a-i influența
Influențarea înțelegerii	O2.1 blocarea/întârzierea accesului la informații, degradarea și	O2.2 asigurarea informațiilor în timp util/real, a acurateței, securității și	O2.3 furnizarea de informații concrete, în scopul obținerii sprijinului

	alterarea informațiilor destinate factorilor de decizie	protecției acestora și contracararea eforturilor adversarilor de a degrada, altera sau bloca accesul la informații	acestora și contracarării eforturilor adversarilor de a-i atrage de partea lor, de a degrada, altera sau bloca accesul la informații
Influențarea capacității acționale	O3.1 împiedicarea luării inițiativei, prin degradarea, alterarea, interzicerea accesului sau distrugerea infrastructurii sistemelor de comandă, control, comunicații, calculatoare și informații, a celor ce permit exercitarea efectivă a conducerii, a celor de propagandă și a surselor care generează puterea fizică	O3.2 protejarea dezvoltarea sistemelor de comandă, control, comunicații, calculatoare și informații care permit exercitarea conducerii și menținerea inițiativei	O3.3 protejarea sistemelor de comandă, control, comunicații, calculatoare și informații, direct, prin furnizarea de consultații și sprijin material, sau indirect, prin acțiuni asupra acelor capacități acționale ale adversarului care le-ar amenința pe ale acestora

Doctrinile actuale proiectează obiectivele ca efecte așteptate ale activităților informaționale pe două tipuri de ținte, mai exact adversari sau potențial adversari și audiențe țintă aprobate. Cele două categorii de ținte sunt cele definite aproape

similar în precedentele doctrine – ultima categorie privind alte entități aprobate –, eliminându-se luarea în calcul la nivel doctrinar a acțiunilor de protecție privitoare la voința, înțelegerea și capacitatea acțională a trupelor proprii și aliaților ca efecte proiectate sau ca obiective ale Info Ops. Privitor la efectele urmărite la forțele proprii și la aliați, cele trei paliere privesc protecția și întărirea voinței având drept efecte creșterea libertății de acțiune, menținerea coeziunii și contracararea acțiunilor sau operațiilor informaționale ale adversarilor, dar și asigurarea cu informații în timp real și în mod oportun, în cantitatea și la calitatea optimale, contracarându-se eforturile adversarilor de a interveni în fluxul transmiterii de informații, precum și protejarea sistemelor C4ISR pentru a se putea menține inițiativa și pentru a se putea exercita comanda în condiții optime.

Prin această luare în considerare ulterioară a aliaților și forțelor proprii, fără definirea precisă ca fiind categorie de public-țintă și fără considerarea proiecției ca fiind obiective al Info Ops sau efecte urmărite (adică tot obiective), doctrina actuală nu limpezește perspectiva teleologică. În plus, categoria „audiențe țintă aprobate de CSAT” acoperă în intensiunea termenului și conceptul de „adversari sau potențial adversari”, pentru că activitățile informaționale presupun continuitate în cazul celor care vizează obiective de protecție (pe toate cele trei paliere, privind voința, înțelegerea și capacitatea acțională), respectiv aprobarea țăntelor de către CSAT în cazul celor exploratorii sau ofensive. Din acest punct de vedere privind, prezentarea obiectivelor Info Ops în proiecția tabelară este utilă în scopuri didactice și permite o înțelegere mai clară a palierelor de acțiune și a tipurilor de activități informaționale desfășurate.

3.1.2 Principiile operațiilor informaționale. Principiile operațiilor informaționale stau la baza planificării și conducerii

acestora în scopul integrării în procesul de planificare și execuție a operațiilor întrunită și influențării voinței, înțelegerii și capacității acționale a părților implicate în conflict. O parte a acestor principii derivă, prin urmare, din setul general de principii ale pregătirii și ducerii acțiunilor de luptă, așa cum rezultă din cadrul nomologic proiectat și dezvoltat în timp de personalități militare precum Thomas Robert Bugeaud, Antoine Henry de Jomini sau Ferdinand Foch, în timp ce altele sunt particulare managementului informației pe câmpul de luptă. Practic, într-un cadru nomologic care nu a cunoscut modificări majore în ciuda succedării a numeroase revoluții militare, legile generale ale războiului, legile care guvernează lupta armată și principiile generale ale pregătirii și desfășurării acestora au rămas neschimbate. În acest cadru nomologic ierarhizat în raport cu generalitatea aplicării, principiile care stau la baza planificării și desfășurării operațiilor informaționale se încadrează în categoria principiilor specifice de întrebuințare a categoriilor de forțe armate, a armelor și specializărilor. Aceste principii, așa cum sunt ele descrise în diferite aparate doctrinare, majoritatea proiectate în conformitate cu precedentele doctrine aliate *Allied Joint Doctrine for Information Operations* (AJP-3.10, 2009 și 2015), cu nuanțe în traducerea lor (inclusiv în ceea ce privește neînțelegerea adecvată a unor concepte), sunt diferite în noua filosofie NATO privitoare la operațiile informaționale.

Printr-o analiză diacronică a principiilor în doctrina NATO (edițiile 2009, 2015 și 2023) se poate observa că doctrina românească a continuat să se raporteze la setul de principii Info Ops din doctrina NATO din 2009, în timp ce edițiile noi ale proiecției aliate aduc o modificare consistentă a perspectivei. O analiză similară a fost realizată anterior apariției doctrinei NATO AJP-10.1 din 2023 de Cosmina-Andreea Neculcea și Florian Răpan (2022:74).

Tabelul 4 Principiile operațiilor informaționale izvorâte din
aparatul doctrinar NATO

AJP 3.10 (2009)	AJP 3.10 (2015)	AJP 10.1 (2023)
Abordarea operațiilor în baza efectelor	Concentrarea și integrarea	Înțelegerea cuprinzătoare
Îndrumările date de comandant și implicarea personală a acestuia	Coerența și consistența	Coordonarea prin narațiuni
Strânsa coordonare și sincronizarea permanentă	Înțelegerea cuprinzătoare	Concentrarea pe efecte
Acuratețea intelligence-ului și a informațiilor	Planificarea centralizată și execuția descentralizată	Integrarea
Planificarea centralizată și execuția descentralizată	Continuitatea	Agilitatea
Contribuție la managementul întrunit al țințelor	Monitorizarea și evaluarea	Planificarea centralizată și execuția descentralizată
Implicarea timpurie și pregătirea la timp	Agilitatea	Evaluarea
Monitorizarea și evaluarea		
Adaptabilitatea		

Există câteva aspecte care trebuie subliniate în urma analizei comparate a direcțiilor doctrinare majore. În primul rând, este vorba o schimbare a filosofiei de proiecție a principiilor operațiilor informaționale. Înțelese ca funcție întrunită, operațiile informaționale presupun o particularizare a unor principii de luptă la specificul tipului de operații, ceea ce

înseamnă fie definirea lor ca principii de sine stătătoare, aplicabile doar în cadrul Info Ops (perspectiva doctrinei aliate din 2009), fie menținerea în cadrul general de definire, cu aplicabilitate distinctă descrisă în cadrul doctrinei (versiunile doctrinei aliate din 2015 și 2023). Diferența majoră între aceste versiuni este dată de faptul că noua doctrină abordează arhitectura informațională a câmpului de luptă într-un context mai amplu, plecând de la conceptul de comunicare strategică (StratCom), de unde derivă și principiul distinctiv în raport cu celelalte aparate doctrinare și cu celelalte versiuni ale doctrinei, „coordonarea prin narațiuni” (*narrative-led*)⁷⁴. Doctrina proiectează principiile pentru a fi utile în procesul de planificare și stabilire a ȋntelilor comune și pentru coordonarea tuturor activităȋilor care au efecte asupra mediului informaȋional, aplicându-se așadar tuturor temelor operaȋionale în cadrul confruntării. Din această nouă perspectivă asupra operaȋiilor informaȋionale derivă principiile Info Ops la nivelul alianȋei, care presupun înȋelegerea cuprinzătoare a fluxurilor de comandă, proiecȋiei StratCom, a mediului informaȋional și a publicurilor (*comprehensive understanding*), coerenȋa fluxurilor comunicaȋionale (*narrative-led*), centrarea pe efecte

⁷⁴ În limba română a pătruns în forma unui substantiv neutru, *narativ* (uneori sub forma unui substantiv feminin, *narativă*) un termen englezesc, *narrative*, care avea deja corespondent românesc, *naraȋiune*. Probabil încercând să acopere un anumit înȋeles al cuvântului englezesc, „mod particular de a explica și a înȋelegere evenimentele”, termenul a devenit frecvent utilizat în limbajul mediatic. Acad. Rodica Zafiu (2021) consideră că această accepȋie nu este una specială și că „Din acest punct de vedere, termenul englezesc ar trebui tradus în română pur și simplu prin naraȋiune, cu toate accepȋiile sale. [...] Nu știu de ce ar trebui să recurgem la o formă oscilantă cu sens alunecos, când avem la îndemână termenul pe care se puteau cu ușurinȋă grefa noile accepȋii și conotaȋii. Naraȋiune mi se pare net preferabil narativului și narativei.” În acest sens am optat pentru utilizarea în toate contextele doctrinare a termenului românesc „naraȋiune” în detrimentul celui de „narativ”, iar aceasta în ciuda faptului că în practică sunt utilizaȋi termenii „narativ(ă)” și „coordonare în baza narativei”.

și, implicit, înțelegerea efectelor acțiunii militare pe câmpul de luptă (*effects focused*), conștientizarea efectului cognitiv (*integrated*), flexibilitatea și răspunsul activ la mediul informațional în continuă evoluție (*agility*), integrarea activităților Info Ops pentru obținerea efectului sinergic și execuția descentralizată pentru creșterea flexibilității și realizarea surprinderii (*centralized planning and decentralized execution*), respectiv continua evaluare a efectelor în raport cu obiectivele vizate (*assessment*).

În ceea ce privește doctrina americană a operațiilor informaționale, aceasta nu definește principiile Info Ops deoarece Statele Unite susține și aplică aspectele doctrinare NATO în raport cu care propriile aspecte sunt aliniate și armonizate, dar pune în aplicare concepte și perspective diferite. Privitor la principii, în cadrul Info Ops sunt puse în aplicare principiile operațiilor întrunite, doctrina operațiilor informaționale izvorând din doctrina pentru operații. Abordarea fiind diferită, nu a fost utilă punerea în dezbatere a principiilor operațiilor informaționale în doctrina românească și în cea aliată cu principiile operațiilor întrunite din doctrina americană.

Revenind la perspectiva românească asupra operațiilor informaționale, diferențele majore între principiile Info Ops în înțelesul celor două ediții ale doctrinei românești a operațiilor informaționale nu presupun numai alinierea la vechea filosofie NATO, ci și existența unor concepte ale doctrinei aliate pentru operații care nu au aplicabilitate în aparatul doctrinar românesc, care nu au fost ratificate și care au fost denunțate în anumite doctrine, precum cea germană, britanică sau americană. Unul dintre aceste concepte este cel numit *Effect-Based Approach to Operations*, devenit principiu în ediția 2009 a doctrinei aliate, denunțat de doctrina germană, nededunțat de cea română și acceptat în ambele versiuni autohtone prin traducerea aproximativă de „abordare cuprinzătoare a operației”. În prima ediție a lucrării *Războiul informațional* (Lesenciuc, 2016) am

insistat asupra acestor diferențe, dar odată cu schimbarea filosofiei în baza căreia a fost proiectată versiunea 2023 a doctrinei aliate pentru operații informaționale această analiză este inoportună. Din același motiv nu este necesară analiza comparată a fiecăruia dintre principiile operațiilor informaționale în cele două doctrine în uz. Merită în schimb să aprofundăm analiza principiilor operațiilor informaționale în raport cu doi poli de interes: 1. integrare și 2. continuitate. Față de acești poli, doctrina aliată propune principiul director de coordonare prin narațiuni, care privește două aspecte: unul care tinde spre polul integrare (unitate, conducere unitară), iar celălalt care privește un principiu aplicabil în management, branding și comunicare organizațională (în special în situații de criză), rezumat la formula „One Single Voice”, având drept scop impunerea unei strategii de comunicare (proiecția StratCom, consolidarea încrederii și întărirea identității). Privind din această perspectivă putem constata că operațiile informaționale nu se pot planifica și coordona în afara unui cadru general de proiecție (operațiile întrunite), fapt ce reclamă, pe de o parte, o ierarhie doctrinară corespunzătoare (doctrina operațiilor informaționale izvorând din doctrina operațiilor întrunite și din doctrina StratCom⁷⁵ și situându-se pe palierul imediat superior doctrinelor operațiilor derivate: operații psihologice, inducere în eroare etc.), respectiv o ierarhie structurală aferentă (structurile de operații informaționale aflate în subordinea Statului Major al Apărării și subordonând la rândul lor structurile aferente). În ceea ce privește continuitatea, Info Ops se pot executa atât în timpul războiului (cu condiția aprobării țințelor de către CSAT la nivel național, de către NAC la nivelul alianței), cât și pe timp de pace sau în perioada post-conflict, în special în ceea ce

⁷⁵ Actuala doctrină NATO pentru InfoOps (AJP 10.1) derivă din doctrina NATO pentru StratCom (AJP 10), la fel precum și doctrina pentru relații publice (AJP 10.3) sau cea PsyOps - în curs de aprobare (AJP 10.2).

privește acțiunile de protecție în planul voinței, înțelegerii și capacității acționale a trupelor proprii și structurilor aliate.

3.2 Relații de coordonare și cooperare

3.2.1 Filosofia StratCom. Polul integrării, prezentat anterior, în ciuda execuției descentralizate și specializate, presupune o abordare unitară la nivelul structurilor întrunite, în așa fel încât operațiile informaționale să devină multiplicator de forță și să creeze efectul dorit. Această proiecție integrativă rezultă atât din doctrina de specialitate NATO: AJP-10.1 (2023:12, art.1.22, b), cât și din cea a Statelor Unite: JP 3-13 (2014:II-5). Doctrina NATO a fost în timp cea mai explicită din acest punct de vedere: pentru atingerea obiectivelor de natură informațională, au fost proiectate o serie de capacități, instrumente și tehnici, constituind baza majorității activităților de operații informaționale care, coordonate planificat și sincronizate (prin apel inclusiv la utilizarea forței pentru coerciție sau distrugere), le subordonează⁷⁶. Actualmente, filosofia de organizare a

⁷⁶ În vechea filozofie privitoare la operațiile informaționale ca funcție întrunită, raporturile de subordonare erau definite prin enumerarea și descrierea domeniilor cheie coordonate (sintagmă în uz în doctrina națională a operațiilor informaționale). Pentru a nu exista interpretări de natura înțelegerii exacte a raportului de subordonare, redăm textul din *Allied Joint Doctrine for Information Operations* (AJP-3.10, 2009:I-8, art.0120): „Clearly, many of these tools and techniques have a much wider application than Info Ops (and when not used to support Info Ops the potential unintended information effects of such activity must be considered), but can be drawn upon by Info Ops.” În noua filozofie de organizare a conținuturilor, operațiile informaționale sunt considerate funcție de stat major aflată în relații de coordonare cu comunicarea strategică (StratCom), care proiectează o abordare presupunând „coordonarea prin narativă” (*narrative-led*), principiu dezvoltat în subcapitolul anterior, respectiv subordonarea unor câmpuri de activitate privitoare la capacitățile

fluxurilor informaționale la nivel NATO (și implicit a doctrinei operațiilor informaționale) s-a modificat considerabil, motiv pentru care este necesară o prezentare a noii proiecții. Info Ops, precum celelalte tipuri de operații definite de AJP-3, *Allied Joint Doctrine for the Conduct of Operations* (2025) sunt coordonate unitar (AJP-3, 2025:B-6, art. B.14), dar această coordonare se realizează în baza direcțiilor și îndrumărilor StratCom oferite de Strategic communications coordination board (SSCB) (AJP-3, 2025:B-14, art. B.28). Prin urmare, StratCom, definit în cadrul NATO drept:

[...] integrarea capacităților de comunicare și a funcțiunii personalului din domeniul informații cu alte activități militare, pentru a înțelege și modela mediul informațional, în sprijinul scopurilor și obiectivelor strategice ale NATO.⁷⁷ (AJP-10, 2023:3, art.1.1; AJP-10.1, 2023:13-14, art.2.4),

reprezintă o funcție de stat major responsabilă pentru înțelegerea mediului informațional în ansamblu și pentru utilizarea adecvată a mijloacelor de comunicare de masă „pentru a informa și influența în mod corespunzător atitudinile și comportamentele unui public printr-o abordare bazată pe narațiuni în urmărirea stării finale dorite”⁷⁸ (AJP-10, 2023:3, art.1.1). Cu alte cuvinte, StratCom oferă o imagine de ansamblu, o concepție unitară și concentrată în raport cu toate tipurile de activități informaționale și de comunicare, o

comunicaționale și la alte capacități și tehnici în măsură să integreze activitățile informaționale.

⁷⁷ [...] the integration of communication capabilities and information staff function with other military activities, in order to understand and shape the information environment, in support of NATO strategic aims and objectives. [t.n.], în engleză în original.

⁷⁸ [...] to appropriately inform and influence an audience's attitudes and behaviours through a narrative-led approach in pursuit of the desired end state. [t.n.], în engleză în original.

înțelegere cuprinzătoare a publicurilor și, evident, căi, mesaje și explicații adecvate de comunicare. În proiecția NATO, StratCom răspunde în mod unitar la trei întrebări fundamentale, precum în tabelul de mai jos, definindu-și astfel scopurile :

Tabelul nr. 5 Proiecția StratCom la nivel NATO (*apud* AJP-10, 2023:5, fig.1.1)

Ce?	Cum	De ce?
Mentținerea relevanței strategice a tuturor activităților la toate nivelurile de comandă, pe tot parcursul confruntării	Alinierea forței la o narațiune comună folosind acțiuni, imagini și cuvinte	Pentru asigurarea că toate activitățile Alianței sunt coerente cu narațiunea și susțin rezultatele strategice scontate

La nivel național comunicarea strategică (StratCom) are aceleași roluri, promovând comunicațional coordonat și coerent interesele naționale. Ilustrativă scopului nostru de a deveni expliciti în ceea ce privește noua filozofie NATO privitoare la operațiile informaționale este înțelegerea StratCom nu doar ca proces sau funcție întrunită, ci mai ales ca filozofie – așa cum propune doctrina britanică pentru operații întrunite, *UK Joint Operations Doctrine* (JDP-01) –, adică în înțelesul de totalitate a concepțiilor și principiilor metodologice în măsură să articuleze o cale de acțiune la toate nivelurile:

Comunicarea strategică este definită ca fiind promovarea intereselor naționale prin utilizarea tuturor mijloacelor de comunicare din domeniul apărării pentru a influența atitudinile și comportamentele oamenilor. Este în primul rând o filozofie, parțial o capacitate și parțial un proces. Filosofia este elementul cheie, deoarece stă la baza corelării cuvintelor, imaginilor și acțiunilor pentru a realiza influența.⁷⁹ (JDP-01, 2014:20, art.1.35).

⁷⁹ Strategic communication is defined as: advancing national interests by using all Defence means of communication to influence the attitudes and behaviours of people. It is primarily a philosophy, partly a capability and

Doctrina aliată a operațiilor informaționale proiectează StratCom ca funcție aplicabilă la toate nivelurile de comandă, vizând obiective informaționale unice și scontate, atinse prin intermediul narațiunilor construite în scopul sprijinirii obiectivelor militare și politice ale NATO, așadar într-o concepție bazată pe „coordonarea prin narațiuni”, asigurând concepția, planificarea, executarea și evaluarea activităților informaționale și sprijin pentru activități mai ample, „facilitată de o înțelegere cuprinzătoare a publicului și a modului în care acesta există într-un mediu informațional contestat.”⁸⁰ (AJP-10.1, 2023:13, art.2.2).

Conceptul de StratCom este mai amplu și aplicabil în primul rând în câmp politic, de unde a migrat în zona puterii *hard*, contribuind la integrarea comunicării strategice în misiuni militare prin alinierea unor linii de acțiune/ operaționale în scopul susținerii obiectivelor naționale (ale marii strategii, în termenii lui B.H. Liddell Hart, 1967:335) cu direcții în procesul construirii de înțeles necesar punerii în aplicare a anterior menționatei linii de acțiune. Teoretizarea și instituționalizarea termenului sunt consecințe ale procesului de extindere și îmbogățire a conceptului de mediu informațional, dar mai ales de dezvoltare a tehnologiilor informaționale și de integrare în acțiunile militare, iar filosofia StratCom este rezultatul încercării de coordonare a fluxurilor informaționale nu întotdeauna convergente ale câmpului de luptă. Totuși, odată cu modificarea filosofiei NATO rezultă și o serie de recalibrări privitoare la înțelegerea relațiilor de coordonare în cadrul Info Ops, respectiv de cooperare cu Info Ops în cadrul StratCom.

partly a process. Philosophy is the key element since it underpins aligning words, images and actions to realise influence. [t.n.], în engleză în original.

⁸⁰ enabled by a comprehensive understanding of audiences and how they exist in a contested information environment, [t.n.], în engleză în original.

3.2.2 Relații de coordonare în cadrul Info Ops. Doctrinile operațiilor informaționale proiectate în acord cu anterioara filosofie NATO definesc explicit domeniile coordonate în cadrul Info Ops, după cum urmează (din rațiuni didactice am optat pentru expunerea *in extenso* a termenilor și cu echivalentul lor din aparatul doctrinar NATO): operațiile psihologice/ Psychological Operations (PsyOps); prezența, postura și profilul/ Presence, Posture & Profile (PPP); securitatea operațiilor/ Operations Security (OPSEC); securitatea informațiilor/ Information Security (INFOSEC), subsumând domeniile securitatea comunicațiilor/ Communications Security (COMSEC), securitatea calculatoarelor/ Computer Security (COMPUSEC) și protejarea rețelelor de calculatoare/ Computer Network Defense (CND), element funcțional al operațiilor în rețelele de calculatoare/ Computer Network Operations (CNO), subordonat Info Ops și asigurând, totodată, Computer Network Attack (CNA) și Computer Network Exploitation (CNE); inducerea în eroare/ Deception sau Military Deception (MilDec); războiul electronic/ Electronic Warfare (EW); distrugerea fizică / Physical Destruction, angajarea liderilor cheie/ Key Leader Engagement (KLE) și cooperarea civili-militari/ Civil-Military Cooperation (CIMIC).

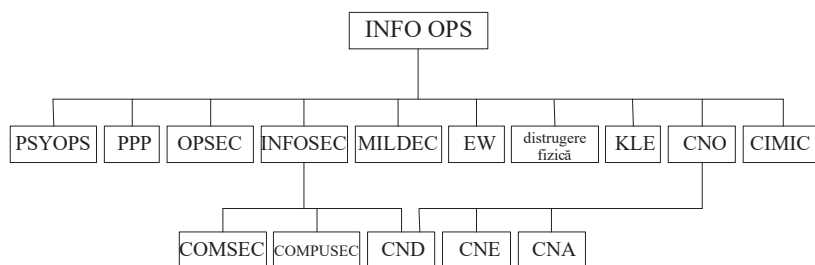


Fig.6 Domeniile cheie ale operațiilor informaționale în precedenta doctrină NATO *Allied Joint Doctrine for Information Operations* (AJP-3.10, 2009:I-8 – I-10, art.0121-0128)

Actuala doctrină aliată redefineste domeniile coordonate de Info Ops, dar înțelegând fluxurile informaționale în baza principiului „coordonarea prin narațiuni” derivat din filosofia StratCom, așază împreună domeniile Info Ops și cele presupunând în anterioara doctrină relații de cooperare cu Info Ops. Practic, doctrina aliată în vigoare definește două tipuri de activități după altă logică decât cea în baza căreia s-a constituit doctrina anterioară, astfel: capacități comunicaționale (*communication capabilities*)⁸¹; capacități și tehnici suplimentare care pot fi integrate ca activități informaționale, respectiv angajarea, prezența, postura și profilul. Prima categorie include operațiile psihologice/ Psychological operations (PsyOps) și relațiile publice, definite după model american drept Military Public Affairs (Mil PA).

Cea de-a doua include operații cibernetice/ Cyberspace Operations; război electromagnetic/ Electromagnetic warfare;

⁸¹ În doctrinele românești a fost introdus după aderarea României la NATO un termen nou, „capabilitate”, preluat din termenul englezesc *capability*. „Capabilitate” există în limba române desemnând însușirea de a fi capabil, dar sensul în care este utilizat în aparatul doctrinar românesc este diferit și derivat dintr-o accepție particulară în limba engleză (în dicționarele generale, nu în cele de specialitate), însemnând „cantitatea de armament și de trupe de care are nevoie o țară pentru a lupta într-un război”. În înțeles doctrinar european, conceptul *capability* este definit ca fiind „The ability to create an effect through employment of an integrated set of aspects categorized as doctrine, organization, training, materiel, leadership development, personnel, facilities, and interoperability” (EP, 2020:4), adică o capacitate specifică, de a crea efect sinergice prin utilizarea integrată a doctrinei, organizării, instruirii, tehnologiilor, personalului, cu alte cuvinte a tuturor tipuri de resurse. Doctrina românească definește conceptul de „capabilitate” ca fiind (1) abilitate de a acționa/ executa acțiuni și (2) ansamblu de măsuri și acțiuni definite similar ca în anterior menționatul document (EP, 2020), ambele reducibile la termenul „capacitate” (1) latentă și (2) explicită. În acest sens, diferit de termenul utilizat în aparatul doctrinar românesc, am optat pentru a traduce *communication capabilities* prin capacități comunicaționale.

cooperarea civili militari și interacțiunea civili-militari/ Civil-military cooperation (CIMIC) and civil-military interaction (CMI); distrugere fizică/ Physical destruction; securitatea operațiilor și inducerea în eroare/ Operations security (OPSEC) și Deception; sprijinul cu informații/ Information assurance, deși înțelesul doctrinei aliate este diferit⁸²; tehnologiile emergente și disruptive/ Emerging and disruptive technologies (EDTs).

Ultima categorie include angajarea/ Engagement, realizată la niveluri diferite, astfel: angajare strategică/ Strategic engagement; angajarea liderilor cheie/ Key leader engagement (KLE) și angajarea la nivel de soldat/ Soldier-level engagement, ultimele două categorii putând fi deliberate („O angajare deliberată este o interacțiune personală planificată și anticipată, menită să creeze un anumit rezultat”⁸³) sau dinamice („Angajările dinamice sunt întâlniri neprevăzute sau improvizate pentru care nu a fost realizată o anumită planificare”⁸⁴) (AJP-10.1, 2023:23, art.2.23); înțelegere culturală și angajare/ Cultural understanding and engagement; prezența, postura și profilul/ Presence, posture and profile (PPP), respectiv conduita și

⁸² Și în cazul acestui termen există câteva surse de erori în interpretare. „Information assurance” se traduce prin „asigurarea informațiilor”, presupunând securitatea fizică și securitatea informațiilor (INFOSEC), în timp ce „sprijinul cu informații” se referă la acțiunea de culegere și furnizare de date/ informații/ cunoaștere pentru a facilita înțelegerea și pentru a coordona diferite acțiuni/ operații. Sprijinul cu informații privește procesul de intelligence, care presupune colectarea, analiza, interpretarea și transmiterea de informații și cunoaștere în scopul luării deciziilor în domeniul apărării (în înțeles restrâns) sau în domeniul securității naționale (în înțeles extins). Pentru acuratețea analizei, vom utiliza pentru „Information assurance” doar conceptul de „asigurare a informațiilor”, ca extensie a INFOSEC, și nu cel de „sprijin cu informații”.

⁸³ A deliberate engagement is a planned and anticipated personal interaction designed to create a specific outcome, [t.n.], în engleză în original.

⁸⁴ Dynamic engagements are unanticipated or impromptu encounters for which specific planning has not been conducted, [t.n.], în engleză în original.

standardele de comportament/ Conduct and standards of behaviour (AJP-10.1, 2023:17-24, art.2.13-2.26).

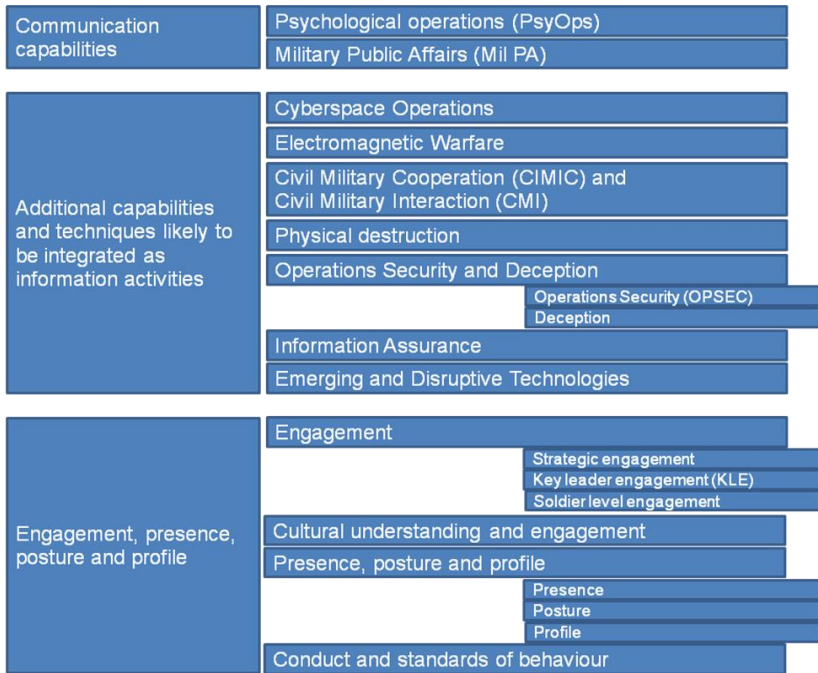


Fig.7 Domeniile cheie ale operațiilor „coordonate prin narațiuni” (AJP-10.1, 2023:17-24, art.2.13-2.26)

Noua arhitectură a domeniilor informaționale cheie „coordonate prin narațiuni” (*narrative-led*) derivată din filosofia StratCom diferă considerabil de precedenta și împrumută o parte din perspectiva americană, fără ca între aceasta și perspectiva NATO să existe similaritate.

Pentru a evidenția suprapunerile parțiale cu domeniile cheie ale operațiilor informaționale din aparatul doctrinar american, vom enumera aspectele de interes din perspectiva doctrinei operațiilor informaționale a Statelor Unite. Doctrina americană *Joint Publication 3-13 Information Operations* este mai puțin

explicită, analizând o serie de structuri militare care contribuie la atingerea obiectivelor operațiilor informaționale, necesitând a fi luate în considerație în ceea ce privește procesul de planificare (JP 3-13, 2014:II-5 – II-13): comunicarea strategică/ Strategic Communication (SC); coordonarea interagenției/ Joint Interagency Coordination Group (JIACG); relațiile publice/ Public Affairs (PA), fosta structură Public Relations (PR); operațiile civil-militare/ Civil-Military Operations (CMO); operațiile cibernetice/ Cyberspace Operations (CO); sprijinul cu informații/ Information Assurance (IA); operațiile spațiale/ Space Operations (SO); operațiile militare de susținere informațională/ Military Information Support Operations (MISO); intelligence/ Intelligence (INTEL), prin utilizarea integrării acestora în operațiile informaționale/ information operations intelligence integration (IOII); inducerea în eroare/ Military Deception (MILDEC); securitatea operațiilor/ Operations Security (OPSEC); operațiile tehnice speciale/ Special Technical Operations (STO); operațiile în spectru electromagnetic integrat/ Joint Electromagnetic Spectrum Operations (JEMSO), constând în război electronic/ Electronic Warfare (EW) și în managementul spectrului electromagnetic/ Electromagnetic Spectrum Management (EMS) și angajarea liderilor cheie/ Key Leader Engagement (KLE).

Doctrina românească este în mică măsură explicită proiectând o serie de relații de coordonare, respectiv o serie de domenii cheie coordonate în cadrul operațiilor informaționale, care coincid în mare măsură. Astfel sunt determinate structurile cu care relaționează/ cooperează operațiile informaționale, urmărindu-se armonizarea, sincronizarea și obținerea efectelor sinergice proiectate precum și evitarea efectelor colaterale nedorite, mai precis cu cele în a căror responsabilitate se află domeniile: operații psihologice; informare și relații publice; informații militare; cooperare civili-militari; război electronic; inducere în eroare/ mascare; protecția/ securitatea operației; protecția/ securitatea informațiilor; operații speciale; operații

întrunite; managementul întrunit al țințelor; operații în spațiul cibernetic și alte domenii cu un posibil impact direct sau indirect asupra audiențelor țintă. Dintre aceste treisprezece domenii menționate, șapte sunt domenii cheie ale operațiilor informaționale, majoritatea celorlalte fiind încadrate în categoria de funcții întrunite în care sunt incluse și operațiile informaționale. Această includere a unei serii de domenii care fac obiectul coordonării sau cooperării produce confuzii și ar fi necesare atât o clarificare doctrinară, cât și o actualizare a filosofiei doctrinare în raport cu perspectiva StratCom care guvernează doctrina aliată a Info Ops. Analizând doctrine diferite, confuzia persistă atâta vreme cât unele dintre domeniile cheie coordonate de Info Ops se regăsesc în categoria de domenii cu care se realizează relații de cooperare. Exemplul la îndemână este cel al cooperării civili-militari, care pe de o parte în vechea doctrină aliată era inclus în domeniile cheie coordonate de Info Ops, iar în actuala doctrină este menținută în categorii funcții întrunite (*joint functions*) (AJP-10.1, 2023:10, art.1.16), pe același palier cu operațiile informaționale, iar pe de altă parte sunt incluse în categoria de domenii „coordonate prin narațiuni” în sintagma cooperare civili-militari (CIMIC) și interacțiune civili-militari (CMI) (AJP-10.1, 2023:19, art.2.17). Noua perspectivă NATO nu creează confuzii dacă domeniile „coordonate prin narrative” nu sunt considerate domenii coordonate de Info Ops, ci elemente care configurează arhitectura informațională a câmpului de luptă. Asupra acestui aspect și asupra filosofiei StratCom vom reveni pentru a evita posibile confuzii interpretative. Vechea doctrină NATO, în schimb, nu era suficient de clară atâta vreme cât domeniul CIMIC era considerat a fi coordonat Info Ops și, prin urmare, această confuzie persistă în toate aparatele doctrinare care mențin vechea filozofie privitoare la operațiile informaționale.

Activitățile CIMIC fac cu siguranță obiectul funcțiilor întrunite, având efecte directe în ceea ce privește desfășurarea operațiilor întrunite. Rolul activităților CIMIC este cât se poate de clar și explicit formulat: structurile CIMIC colaborează cu structurile Info Ops, iar activitățile CIMIC nu sunt coordonate în cadrul activităților Info Ops. Din acest punct de vedere, considerăm mai adecvată perspectiva americană în ceea ce privește raporturile CIMIC – Info Ops, date fiind coordonatele reale în care acestea sunt puse în evidență în cadrul teatrelor de operații, dar și argumentele americane pe marginea unei doctrine aliate anterioare a operațiilor informaționale⁸⁵. Noua doctrină NATO rezolvă această problemă și elimină confuziile în chiar corpul articolului privitor la CIMIC și CMI ca domeniu în infrastructura informațională „coordonată prin narațiuni”:

Personalul Info Ops și CIMIC lucrează conjugat într-un cartier general pentru a planifica și integra activitățile CMI și pentru a oferi înțelegere având la bază interacțiunile cu publicul. Rezultatul interacțiunii cu publicul non-militar poate servi obiectivelor StratCom stabilite pentru o operațiune prin executarea de activități civil-militare colective, vizibile publicului, în favoarea armatei, subliniind astfel unitatea eforturilor. Personalul CIMIC trebuie să fie reprezentat în Grupul de lucru pentru activități informaționale (Information Activities Working Group) la toate nivelurile de comandă, nu numai pentru a

⁸⁵ Diferențele de perspectivă dintre doctrinele americană și NATO sunt evidente, fiind explicit marcate în textul doctinar al AJP-3.10 (2009:xii), în secțiunea „Record of specific reservations”, de exemplu: „The US does not subscribe to the idea that Civil-Military Cooperation (CIMIC) as discussed in paragraphs 0130-1031, Section V, *Capabilities, Tools, and Techniques Used in Support of Information Objectives*, is a capability. Rationale. The United States believes the current placement of paragraphs 0130-0131 could mislead readers as to the actual doctrinal relationship between information activities and CIMIC. These paragraphs would be better served if placed into a separate section entitled *Relationship to Civil-Military Cooperation* which describes how information activities support CIMIC operations”.

identifica oportunitățile de activități informaționale, ci și pentru a aborda potențialele efecte negative pe care activitățile și operațiunile militare sau civil-militare le pot avea asupra percepției publicului.⁸⁶ (AJP-10.1, 2023:19, art.2.13-2.17).

Practic, coordonarea activităților informaționale nu mai este apanajul operațiilor informaționale, ci este coordonat în cadrul unor entități care integrează activitatea informațională la toate nivelurile de comandă și care asigură „coordonarea prin narațiuni”.

3.2.3 Relațiile de cooperare cu structurile PR/ PA/ Mil PA/ Media Ops. În ceea ce privește relațiile de cooperare, perspectiva doctrinei românești a operațiilor informaționale nu poate fi luată în considerație atâta timp cât există o suprapunere importantă între domeniile coordonate Info Ops și și cele situate pe același palier, al funcțiilor întrunite. De referință rămân funcțiile întrunite, operațiile informaționale situându-se pe același palier cu manevra, aplicarea puterii de foc, comanda și controlul, sprijinul cu informații, susținerea, protecția forței și cooperarea civili-militari.

Totuși, noua doctrină aliată și doctrina americană a operațiilor informaționale includ în arhitectura comunicațională/informațională și alte domenii decât cele analizate în cadrul raporturilor de coordonare, printre care comunicarea strategică (StratCom) în doctrina americană sau relațiile publice/ Public

⁸⁶ Info Ops and CIMIC staff are closely aligned in a headquarters to plan and integrate CMI activities, and to provide understanding based on interactions with audiences. The outcome of interacting with non-military audiences may well serve the StratCom goals set for an operation by executing collective civil-military activities, visible to the public, in favour of the military, thereby underlining unity of effort. CIMIC staff must be represented in the Information Activities Working Group at all levels of command, not only to identify information activity opportunities but also to address potential negative effects military or civil-military activities and operations may have on the perception of the public. [t.n.], în engleză în original.

Affairs în doctrina S.U.A., Military Public Affairs (Mil PA) în doctrina NATO, în afara acelor relații deja analizate din perspectiva raporturilor de coordonare în doctrina românească. Dar, pentru a evidenția raporturile de coordonare sau cooperare, atâta vreme cât doctrina americană nu distinge explicit în textul său, analiza ierarhiei doctrinare este elocventă și oferă o perspectivă realistă asupra raporturilor proiectate.

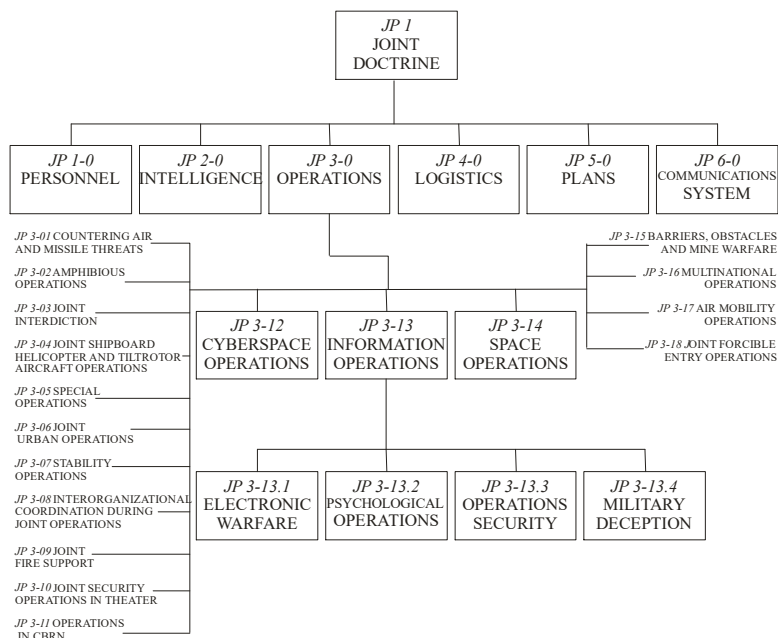


Fig.8 Ierarhia doctrinară americană

Prin urmare, războiul electronic (EW), operațiile psihologice (PsyOps), securitatea operațiilor (OPSEC) și inducerea în eroare (MILDEC), chiar dacă sunt prezentate în JP 3-13 ca fiind domenii aflate în relații de cooperare cu operațiile informaționale, reprezintă domenii cheie coordonate de acestea, în timp ce operațiile cibernetice (echivalente CNO în doctrina românească și Cyberspace Operations în doctrina NATO) sau operațiile spațiale se găsesc pe același palier ierarhic. Dat fiind

faptul că doctrina românească optează, în conformitate cu vechea proiecție NATO, la subordonarea funcțiunilor CIMIC celor Info Ops (Roman, 2020a:31), singura posibilă relație de cooperare la nivel de structuri este cea cu relațiile publice/ Public Affairs (PA).

Relațiile publice sau Public Affairs în doctrina americană fac obiectul unei alte confuzii, pe care am analizat-o detaliat în *Operațiile mass-media* (Lesenciuc, 2013). Astfel, structurile de relații publice, sub directa coordonare a Direcției Informare și Relații Publice, aflată în subordinea secretarului de stat pentru relația cu parlamentul, informare publică și creșterea vieții personalului din cadrul Ministerului Apărării Naționale, au fost proiectate în conformitate cu experiența din teatrele de operații și în acord cu modelele american și NATO. Oficial, activitatea de relații publice în Armata României a fost introdusă în anul 1991, odată cu înființarea Secției de Informare și Relații Publice a Armatei (SIRPA). Ulterior, secția s-a transformat în direcție (1993), a primit denumirea de Direcția Relații Publice/ DRP (1997) și, în cele din urmă, de Direcția Informare și Relații Publice/ DIRP (2007). Sistemul de informare și relații publice este format din secțiile informare publică, relații publice, comunicare internă și centrul de monitorizare media, precum și din structurile de relații publice din unitățile militare și are misiunea de a

[...] sprijini comandanții/ șefii prin comunicarea/ transmiterea informațiilor de interes public, cu acuratețe, în timp util, personalului propriu, cetățenilor, instituțiilor și organizațiilor legal constituite, pentru a îmbunătăți gradul de conștientizare și înțelegere a publicului față de problematica militară, rolul, obiectivele, misiunile, operațiile și activitățile desfășurare, contribuind astfel la consolidarea credibilității instituției militare (M 103, 2020:2 art.2)

Relațiile publice reprezintă efortul planificat de stabilire și menținere a bunăvoinței publicurilor (intern și extern) ale unei organizații, având rolul de a evalua percepțiile publicului, de a dezvolta politicile care necesită aprobare, de a proiecta succesul asupra reputației organizației și de a genera susținere în cadrul publicurilor cheie (Haywood, 2002:5). Din această perspectivă, odată ce relațiile publice urmăresc informarea corectă a audiențelor, și DIRP urmărește o informare corectă, completă și oportună a publicurilor M.Ap.N.:

Activitatea de informare și relații publice din M.Ap.N este de a stabili, menține și dezvolta relații de încredere între instituția militară și societatea românească, pentru promovarea scopurilor și obiectivelor militare și creșterea gradului de informare și a nivelului de înțelegere a problematicii asociate domeniului apărării. (M 103, 2020:2 art.1, alin.2).

Pe de altă parte, preluând un termen din doctrina britanică⁸⁷, una dintre anterioarele *Doctrine ale Armatei României* (2007) a introdus un concept nou în categoria „capabilităților suport” pentru desfășurarea operațiilor întrunite (actualele funcții întrunite): operațiile mass-media. Acest concept încorporează relațiile publice și, implicit, informarea publică și vizează activitățile de promovare a bunăvoinței și înțelegerii publicurilor pentru operațiile desfășurate, presupunând punerea în aplicare la nivelurile optime și în condițiile adecvate, promovând înțelegerea pentru toate categoriile de public țintă.

Conceptul de operații mass-media nu este exclus din aparatul doctrinar românesc, chiar dacă acesta nu este cuprins explicit în categoria funcțiilor întrunite. Precizările doctrinare vin să lămurească faptul că operațiile mass-media presupun activități de relații publice și fac obiectul Direcției Informare și

⁸⁷ În doctrina britanică, termenul „operații mass-media” (MEDIA OPS) a fost introdus în urma acțiunii militare în Balcanii de Vest, la fel cum conceptul de relații publice a fost introdus în armata americană în urma războiului din Vietnam. Iată, pe scurt, cum s-a produs acest fapt, pentru a suplini nevoia de susținere publică: „Înțelegând rolul media în conflictul contemporan ca fiind element de legătură între palierele politic și militar, chiar mediator între acestea, teatrul de operații Kosovo a fost cadrul în care, în raport cu armata britanică, media au mobilizat opinia publică, au conștientizat guvernul și au atras atenția asupra rolului media (în triumghiul decizional politici-media-public, de la care nu se poate sustrage armata). Rezumând rolul lecțiilor învățate din Kosovo, Roberts (2004:77) a subliniat fundamentul operațiilor mass-media redus la nivelul unui principiu acțional de referință în raport cu publicul contribuabil/ națiunea care susține eforturile de război. (...). În urma acestor operații întreprinse în Kosovo, armata Marii Britanii a înțeles, așadar, înființarea structurii de operații mass-media, a cărei filosofie poate fi ușor rezumată la îndemnul cu care generalul de brigadă S.J.L. Roberts își încheie studiul: „*Tell the Truth!*” sau, mai nuanțat, la expunerea „adevărului demonstrabil, spus simplu și interesant” (Roberts, 2004:76), în consens cu principiul fundamental al relațiilor (sau afacerilor) publice, al obligativității spunerii adevărului. De aici rezultă și echivalența dintre structura MEDIA OPS și cele de relații publice, devenite Public Affairs, atât în doctrina SUA, cât și în cea a NATO.

Relații Publice. Cu toate acestea, aparatul doctrinar românesc nu este suficient de clar și nu proiectează adecvat coordonarea operațiilor mass-media de către structura de relații publice (ci doar, în particular, în ceea ce privește sprijinul pe care centrele de operații mass-media/ COMM din zonele de operații întrunite trebuie să îl primească din partea Grupului Mobil de Informare Publică/ GMIP al DIRP). În ceea ce privește coordonarea Info Ops – PR, doctrina autohtonă se aliniază anterioarei proiecții doctrinare NATO (AJP-3.10, 2009).

Precedenta doctrină NATO este mai limpede: obiectivele relațiilor publice/ Public Affairs (PA) și ale operațiilor informaționale sunt diferite, primele vizând o informare corectă, completă și oportună, celelalte o influențare a publicurilor țintă, prin urmare structurile PA nu vor îndeplini sub nicio formă funcțiunile Info Ops. Palierul comun de acțiune privește susținerea obiectivelor militare (a operațiilor întrunite), în descurajarea acțiunilor informaționale ale adversarului, pe căi diferite și cu mijloace diferite, în susținerea consistenței mesajelor transmise de militari și în promovarea eficienței și credibilității operațiilor desfășurate (AJP-3.10, 2009:I-13, art.0133). Doctrina operațiilor informaționale din Armata României este din anumite puncte de vedere mai explicită decât precedenta doctrină NATO, mai ales în ceea ce privește cooperarea cu alte structuri militare, și este la fel de explicită precum doctrina aliată și în ceea ce privește activitatea din cadrul Comitetului de Coordonare a Activităților Informaționale/ Information Activities Coordination Board (IACB).

3.2.4 Relațiile de cooperare cu CIMIC. Relațiile civili-militari (CIMIC) constituie o funcțiune militară necesară creării, armonizării și dezvoltării relațiilor dintre militari și instituțiile militare din zona de operații. CIMIC constituie un domeniu cu

aplicabilitate în special (dar nu exclusiv)⁸⁸ după încheierea perioadei de conflict armat propriu-zis, apărând în urma evoluției dezvoltării practicilor post-conflict și având, din punct de vedere politic și imagologic, rolul de a lăsa în conștiința publicului mai degrabă imaginea de *peacekeeper* decât de combatant: „Într-o oarecare măsură, (...) CIMIC a funcționat, cel puțin în ceea ce privește introducerea imaginii de ‘peacekeeper’ mai degrabă decât de ‘soldat’ în conștiința publică a multor țări occidentale”⁸⁹ (Ankersen, 2008:5). Din punct de vedere operațional, structurile CIMIC au rolul de a oferi sprijin în protecția forței, de a menține un nivel ridicat al moralului trupelor și, în special, de a funcționa ca domeniu militar cu rol informațional:

Într-un sens mai larg, CIMIC este conceput ca parte a unui efort mai amplu de a desfășura operații informaționale. Această perspectivă concepe activitățile CIMIC ca parte a unei campanii – alături de operații psihologice și relații publice – care își propune să ajute comandanții să „își modeleze mediul” și să-și îndeplinească misiunile prin valorificarea unei game diverse de abordări. În acest sens, CIMIC este o cale de transmitere a informațiilor: permite forțelor militare să colecteze informații de la populație, dar facilitează și răspândirea informațiilor în societate. Armata poate coordona mesajele cu activitățile CIMIC pe care le desfășoară, fie direct către cei care participă la acestea, fie către comunitatea mai largă.⁹⁰ (Ankersen, 2008:5).

⁸⁸ CIMIC-ul are un rol activ pe timpul războiului în ceea ce privește non-interferența populației civile cu acțiunile militare, coordonarea convoaielor cu ajutoare, dialogul lucrul cu organizațiile non-guvernamentale s.a.

⁸⁹ To some extent, (...) CIMIC has worked, at least as far as putting the image of ‘peacekeeper’ rather than ‘soldier’ into the public consciousness of many Western countries, [t.n.], în engleză în original.

⁹⁰ Looking more broadly, CIMIC is conceived of as a part of a larger effort to conduct Information Operations. This perspective sees CIMIC activities as a part of a campaign – along with psychological operations and public/media affairs – that aims at helping commanders ‘shape their environment’ and fulfil

Această perspectivă complexă asupra relațiilor civili-militari (CIMIC) permite o înțelegere a acestui domeniu ca fiind mult mai amplu decât un domeniu cu rol pur informațional. Așa cum am menționat, structurile CIMIC sunt destinate să asigure accesul către populația civilă, și, prin intermediul acesteia, către resursele locale, facilitând totodată tranziția dinspre autoritatea multinațională militară către guvernarea civilă națională. Din acest punct de vedere, dar și din punctul de vedere anterior subliniat, conform căruia CIMIC îndeplinesc roluri multiple, politice și operaționale, cel mai important fiind rolul informațional, activitățile CIMIC pot fi cel mai bine privite ca făcând obiectul funcțiilor întrunite, cu rol, alături de alte funcțiuni, de intelligence, sprijin cu informații, C2, Info Ops, dar și de relații publice/ Media Ops, în managementul informațiilor pe câmpul de luptă. Cel mai important argument în înțelegerea CIMIC ca funcție întrunită reprezintă obiecția Statelor Unite privitoare la includerea CIMIC sub umbrela conceptuală și procedurală/ operațională a Info Ops în doctrina aliată din 2023: „Statele Unite consideră că amplasarea actuală a paragrafelor 0130-1031 ar putea induce în eroare cititorii în ceea ce privește relația doctrinară reală dintre activitățile de informare și CIMIC.”⁹¹ (AJP-3.10, 2009:xii). În plus, în respectiva doctrină NATO, perspectiva asupra acceptării CIMIC drept funcție întrunită (cu rol în managementul informațiilor) mai degrabă decât drept funcție informațională, este mai explicită, în timp ce

their missions by harnessing a wide variety of approaches. In this sense, CIMIC is a conduit for information: it allows military forces to gather information from the population, but it also facilitates the spreading of information into the society. Militaries can tie messages to the CIMIC activities they conduct, either directly to those participating in them or to the wider community. [t.n.], în engleză în original.

⁹¹ The United States believes the current placement of paragraphs 0130-0131 could mislead readers as to the actual doctrinal relationship between information activities and CIMIC. [t.n.], în engleză în original.

doctrina din 2023 a rezolvat problema, definind CIMIC „funcția întrunită a capacităților care permit interacțiunea civili-militari (CMI) între publicul militar și cel non-militar în cadrul spațiului de angajare”⁹² (AJP-10.1, 2023:19, art.2.17), ceea ce nu a mai atras obiecția Statelor Unite.

În doctrina NATO a relațiilor civili-militari, rolul CIMIC este definit în sens lărgit astfel:

CIMIC sprijină, facilitează sau desfășoară direct CMI prin activități precum legătura civil-militară angajarea liderilor cheie (KLE), evaluări ale mediului civil, precum și planificarea și coordonarea cu publicul non-militar relevant din zona de operații întrunite pentru a contribui la înțelegerea cuprinzătoare a mediului informațional⁹³ (AJP-10.1, 2023:19, art.2.17),

de unde rezultă și modalitățile de cooperare cu Info Ops sub umbrela „coordonării prin narațiuni”. Totuși a existat și încă mai persistă confuzia privitoare la faptul că CIMIC sunt înțelese ca operând în scopul atingerii obiectivelor operațiilor întrunite, multinaționale și multidimensionale, presupunând susținerea reciprocă a militarilor și civililor din teatrul de operații, așa cum rezultă din doctrina aliată de specialitate din 2013 (AJP 3.4.9, 2013:xi), pentru ca în cadrul capitolului 4 al aceleiași doctrine, *CIMIC planning and execution*, relațiile civili-militari să fie văzute drept funcție întrunită (*joint function*), similar perspectivei aliate actuale, având rol în susținerea operațiilor și a altor funcții întrunite, cum ar fi

⁹² [...] the joint function of capabilities that enables civil-military interaction (CMI) between the military and non-military audiences within the engagement space, [t.n.], în engleză în original.

⁹³ CIMIC supports, facilitates or directly conducts CMI through activities such as civil-military liaison, key leader engagement (KLE), assessments of the civil environment, as well as planning and coordination with relevant non-military audiences within the joint operations area to inform the comprehensive understanding of the operating environment. [t.n.], în engleză în original.

planificarea, coordonarea, evaluarea întrunite, continuitatea informațională, operațiile informaționale și relațiile publice:

CIMIC ca Funcție Întrunită. CIMIC este o parte integrantă a misiunilor, de la urgențe umanitare la conflicte armate. Prin intermediul CIMIC, comandantul se va baza pe legături cu actorii civili. Este puțin probabil ca forța să obțină libertate deplină de acțiune și mișcare fără interacțiune, dar stabilirea unor relații bune ar putea, de asemenea, să priveze de aceleași avantaje forțele ostile sau potențial ostile. Contribuția CIMIC la alte funcții întrunite este crucială, deoarece maximizează impactul oricărei operațiuni militare. Exemplele includ, dar nu se limitează la:

- a. Stabilirea țintelor la nivel întrunit, deoarece CIMIC ajută la identificarea infrastructurii critice
- b. Planificarea întrunită, deoarece CIMIC ajută la identificarea celor mai benefice acțiuni
- c. Operațiile informaționale, deoarece CIMIC contribuie la concentrarea asupra publicului țintă adecvat
- d. Evaluarea întrunită, deoarece CIMIC ajută la includerea opiniei partenerilor civili
- e. Informarea continuă și dobândirea de cunoștințe în legătură alții
- f. Relațiile publice susținute de contactele CIMIC.⁹⁴ (AJP 3.4.9, 2013:4-1 – 4.2, art.0402).

⁹⁴ **CIMIC as a Joint Function.** CIMIC is an integral part of missions, spanning from humanitarian emergency to armed conflict. Through CIMIC the commander will rely on links with the civil actors. The force is unlikely to gain full freedom of action and movement without interaction but establishing good relations might also deny the same advantages to hostile or potentially hostile forces. CIMIC's contribution to other joint functions is crucial, as it maximizes any military operations impact. Examples include but are not limited to:

- a. Joint Targeting as CIMIC helps identifying critical infrastructure
- b. Joint Planning as CIMIC helps identifying most beneficial actions
- c. Information Operations as CIMIC helps focus on the right target audience
- d. Joint Assessment as CIMIC helps including the opinion of civil partners
- e. Continuous information – and knowledge acquisition by liaison with others
- f. Public Affairs supported by CIMIC contacts. [t.n.], în engleză în original.

Aceste argumente ale transformării perspectivei asupra rolului CIMIC în cadrul operațiilor întrunite în ansamblu, în cadrul operațiilor informaționale în particular, ar putea să ne determine să înțelegem activitățile CIMIC în aria activităților de influențare, atâta vreme cât acestea contribuie la punerea în valoare a informațiilor culese din mediul civil, dar proiecția doctrinară aliată a lămurit multe aspecte, separând conceptul CIMIC de cel american de operații civil-militare (CMO). Odată făcută distincția dintre modalitățile de operare cu informațiile în scopul influențării prin intermediul Info Ops (vizând persuadarea publicurilor țintă și presupunând acțiuni cu caracter persuasiv) și prin intermediul altor funcțiuni cu rol în managementul informațiilor, cum ar fi relațiile publice/ Media Ops, de exemplu (vizând informarea corectă, completă și oportună a publicurilor țintă), CIMIC pot fi înțelese în proximitatea ultimelor, în relații de cooperare cu Info Ops. Această perspectivă se nuanțează și mai mult dacă luăm în calcul principiile CIMIC: înțelegerea contextului, înțelegerea scopurilor și obiectivelor actorilor militari și civili din zona de operații, acțiune în limitele legale (internaționale), câștigarea respectului și încrederii, primatul civil și al proprietății, planificarea integrată și comunicarea eficientă (AJP 3.4.9, 2013:3-1 – 3-6, art.0302), sau dacă plecăm de la proiecția empirică funcțională numită *paradigma bunei intenții*, „care constă în convingerea partenerilor de comunicare asupra bunei intenții a forțelor proprii” (Roman, 2020a:8). Această paradigmă a bunei intenții sau a încrederii reciproce (Roman, 2020a:8-9; 2020b:35-36) contribuie la consolidarea încrederii, prin urmare servește funcțiunii de informare în proiecția StratCom, și nu celei de influențare.

3.2.5 Alte relații de cooperare. Noua doctrină NATO include în seria de capacități, operații și acțiuni „coordonate prin narațiuni” și asigurarea informațiilor/ Information assurance

(care nu trebuie confundată cu funcția întrunită sprijin cu informații), dar și tehnologiile emergente și disruptive/ Emerging and disruptive technologies (EDTs), ambele putând fi luate în considerare nu ca domenii cheie ale operațiilor informaționale, ci în categoria de domenii aflate în relații de cooperare cu Info Ops. Totuși, asigurarea cu informații, include și componenta de securitate a informațiilor (INFOSEC), așa cum se regăsește în anterioarele doctrine aliate ale Info Ops în categoria de domenii cheie coordonate prin operațiile informaționale. Doctrina aliată definește asigurarea informațiilor ca fiind:

Asigurarea informațiilor reprezintă protecția și apărarea informațiilor și a sistemelor informatice prin asigurarea disponibilității, integrității și confidențialității acestora. Asigurarea informațiilor necesită procese de management pentru a se asigura că sistemele și rețelele utilizate de o organizație sunt fiabile și sigure și că există procese pentru a detecta și contracara activitățile rău intenționate. Asigurarea informațiilor include elemente de securitate fizică (de exemplu, securitatea personalului și a documentelor) și securitatea informațiilor.⁹⁵ (AJP-10.1, 2023:22, art.2.20).

Pentru acuratețea analizei, vom considera asigurarea informațiilor în egală măsură domeniu aflat în coordonarea Info Ops (în acord cu cadrul doctrinar aliat în ansamblu), dar și domeniu aflat în relații de cooperare cu operațiile informaționale.

⁹⁵ Information assurance is the protection and defence of information and information systems by ensuring their availability, integrity and confidentiality. Information assurance requires management processes to ensure the systems and networks employed to manage the critical information used by an organization are reliable and secure, and processes are in place to detect and counter malicious activity. Information assurance includes elements of physical security (for example, personnel and document security) and information security. [t.n.], în engleză în original.

În ceea ce privește tehnologiile emergente și disruptive/ Emerging and disruptive technologies (EDT), domeniu inclus în categoria capacităților și tehnicilor adiționale care ar putea fi considerate/ integrate ca activități informaționale (doctrina aliată nu este foarte precisă din acest punct de vedere), acestea nu sunt definite drept capacități, tehnici, acțiuni sau instrumente ale operațiilor informaționale, ci ca elemente cu impact asupra rezilienței, atât în plan militar, cât și asupra pregătirii civile, „prin afectarea infrastructurii critice și a informațiilor publice (inclusiv Info Ops) oriunde în cadrul Alianței.”⁹⁶ (AJP-10.1, 2023:22, art.2.20). Nefiind coordonate de Info Ops, le putem include în categoria de domenii aflate în relații de cooperare, atâta vreme cât EDT schimbă modul de operare al NATO și al adversarilor alianței pe timp de pace, criză și conflict. Sectorul privat și mediul academic sunt considerate forțele motrice ale EDT, iar viteza lor de dezvoltare, caracterul dual și impactul societal, analizate în ansamblu, permite înțelegerea lor ca elemente aparținând mai degrabă mediului extern, cu impact asupra operațiilor informaționale, atât pozitiv (ca oportunități), cât și negativ (ca amenințări).

3.2.6 Fluxuri informaționale de informare și influență. Odată cu introducerea în noua doctrină aliată a conceptului de Military Public Affairs (Mil PA) echivalent conceptului Public Affairs (PA) din doctrina Statelor Unite, perspectiva se schimbă substanțial. Pentru a înțelege necesitatea Mil PA și a tipurilor de raporturi dintre Info Ops și această structură și capacitate responsabilă de promovarea scopurilor și obiectivelor NATO este necesară o redesenare a infrastructurii comunicaționale/ informaționale din care fac parte operațiile informaționale, dar care operații nu subordonează, precum în precedentă doctrină, toate domeniile care privesc direct mediul informațional în

⁹⁶ [...] by affecting critical infrastructure and public information (including Info Ops) anywhere across the Alliance, [t.n.], în engleză în original.

ansamblu. Pentru o abordare corespunzătoare a problematicii și pentru înțelegerea noii filosofii a doctrinei informaționale aliate este necesară parcurgerea unor pași în înțelegerea procesului comunicațional și a finalităților sale. În mediul competitiv militar este aplicabil ceea ce este aplicabil la modul general, mai precis faptul că raporturile de putere se definesc și se realizează prin intermediul comunicării, ale cărei scopuri fundamentale sunt de informare și de influență:

Raporturile cu celălalt, de cooperare sau de competiție, de înfrățire/ consolidare a relațiilor sau de putere/ construire sau consolidare a poziției, se realizează prin intermediul comunicării. Dar comunicarea servește deopotrivă informării și influenței. (Lesenciuc, 2017:84).

Cele două tipuri de raporturi comunicaționale, cu scopul transmiterii de informații sau cu scopul influențării, presupun trasee comunicaționale și mecanisme distincte. Primul tip de comunicare este coeziv, cultivă încrederea ca liant social și se bazează pe transmiterea adevărului care poate fi probat. Cel de-al doilea tip de relație presupune modificarea acțiunilor și manifestărilor celuilalt, nu se bazează pe transmiterea adevărului, ci pe influențarea voinței, înțelegerii și capacității acționale a acestuia. Practic, influența este rezultatul unor raporturi manifeste de putere. Privitor la mediul informațional militar, fluxurile comunicaționale se pot defini pe cele două direcții prezentate anterior. Există un flux al comunicării bazat pe principiul spunerii adevărului – principiul „Tell the Truth!” – și al menținerii încrederii în instituție, respectiv un flux al comunicării bazat pe principiul obținerii de avantaje competitive prin influențarea voinței, înțelegerii și capacității acționale. Cele două fluxuri comunicaționale sunt contrare și, în cazul interacțiunii, ar conduce la contaminarea primului de către celălalt, adică a scăderii încrederii publicurilor țintă în raport cu instituția militară emitentă. Cu alte cuvinte, cele două

fluxuri informaționale ar trebui realizate pe căi distincte, utilizându-se elemente ale infrastructurii informaționale care servesc unui singur scop. Principiul doctrinei aliate de „coordonare prin narațiuni” este un principiu derivat din filosofia StratCom și din nevoia menținerii vocii unice. Analizând în ansamblu cele două fluxuri informaționale și filosofia StratCom, putem constata că:

a) există un flux comunicațional bazat pe consolidarea încrederii și pe spunerea adevărului, funcțional în cazul relațiilor publice (indiferent dacă poartă această denumire sau dacă se numesc PA, Mil PA sau Media Ops), în care se încadrează și conceptul CIMIC, iar planificarea activităților din cadrul acestui flux comunicațional nu trebuie întreruptă sau subminată de activitățile de influențare, așa cum este stabilit în cadrul doctrinei aliate a operațiilor informaționale:

Utilizarea capacităților CIMIC și desfășurarea activităților CMI se bazează pe principiile fundamentale: respect, încredere, transparență, credibilitate și fiabilitate, pe care activitățile informaționale nu ar trebui să le submineze.⁹⁷ (AJP-10.1, 2023:19, art.2.13-2.17).

CIMIC este văzută în noua doctrină ca fiind o funcție întrunită care asigură interacțiunile civil-militare (CMI), dar nici aceste interacțiuni nu presupun angajare în înțelesul doctrinar, adică nu sunt activități încadrate în cea de-a treia categorie, care cuprinde și prezența, postura și profilul trupelor. Spre deosebire de CIMIC, operațiile civil-militare/ Civil-Military Operations (CMO) din doctrina americană nu sunt o funcție întrunită, ci reprezintă un instrument de sincronizare civil-militară, în special în perioada post-conflict, dar și în

⁹⁷ The use of CIMIC capabilities and the conduct of CMI activities are based on the core interacting principles of: respect, trust, transparency, credibility and reliability, which information activities should not undermine. [t.n.], în engleză în original.

cazul acțiunilor de contrainsurgență sau în alte forme de confruntare asimetrică: „în special în sprijinul stabilității, contrainsurgenței și altor operațiuni care se ocupă de amenințări asimetrice și neregulate”⁹⁸ (JP 3-57, 2008:vii). În înțelesul convenit prin intermediul cadrului doctrinar NATO, CIMIC și CMI se încadrează în fluxul de activități comunicaționale având la bază consolidarea încrederii și pe punerea adevărului.

b) există un flux comunicațional bazat pe influență, funcțional în cazul operațiilor informaționale (Info Ops), definite precis în vechea doctrină aliată, dar puse sub aceeași cupolă a informațiilor coordonate prin narațiuni în doctrina actuală. Luând în considerare operațiile de influență din categoria de competențe, operații și acțiuni descrise de doctrina aliată, putem considera că există două moduri distincte de realizare a influenței: prin structuri specializate și prin angajarea, prezența, postura și profilul trupelor, realizate în acord cu însușirea unei filosofii acționale și cu punerea ei adecvată în practică. În prima categorie a acțiunilor de influență se încadrează operațiile psihologice/ Psychological operations (PsyOps), operațiile cibernetice/ Cyberspace Operations; războiul electromagnetic/ Electromagnetic warfare; distrugere fizică/ Physical destruction; securitatea operațiilor și inducerea în eroare/ Operations security (OPSEC) and Deception (în doctrina românească a rămas inclusă și componenta INFOSEC, o parte acoperită în doctrina NATO prin componenta Cyberspace Operations, dar în cea mai mare măsură prin asigurarea informațiilor, cu care se realizează și relații de cooperare); asigurarea informațiilor și angajarea coordonată/ Engagement, realizată la nivelurile angajare strategică/ Strategic engagement și angajare a liderilor cheie/

⁹⁸ particularly in support of stability, counterinsurgency and other operations dealing with asymmetric and irregular threats, [t.n.], în engleză în original.

Key leader engagement (KLE). În cea de-a doua categorie se înscriu angajarea, în special cea deliberată, la nivel de soldat/ Soldier-level engagement; înțelegerea culturală și angajarea/ Cultural understanding and engagement; prezența, postura și profilul/ Presence, posture and profile (PPP), respectiv conduita și standardele de comportament/ Conduct and standards of behaviour.

c) în afara celor două fluxuri informaționale, există o proiecție unitară care presupune transmiterea unidirecțională (fără a permite contaminarea fluxurilor informaționale între ele) a narațiunilor derivate din proiecția StratCom.



Fig.9 Fluxurile comunicaționale și principiul „coordonării prin narațiuni”

Această reprezentare schematică simplifică perspectiva asupra celor două fluxuri comunicaționale coordonate unitar prin intermediul principiului *narrative-led* și permite o înțelegere mai ușoară a proiecției doctrinare aliate.

4. Activități desfășurate în cadrul operațiilor informaționale

Public sentiment is everything. With public sentiment, nothing can fail; without it, nothing can succeed.

Abraham Lincoln (1809-1865)

4.1 Tipuri de activități desfășurate în cadrul operațiilor informaționale

Analizând diacronic și comparat doctrinele operațiilor informaționale, rezultă că operațiile (direcțiile) coordonate de Info Ops sunt operațiile psihologice (PsyOps), operațiile cibernetice, războiul electromagnetic, distrugerea fizică, securitatea operațiilor și inducerea în eroare, asigurarea informațiilor (incluzând INFOSEC) și angajarea coordonată; asigurarea informațiilor și angajarea coordonată, la nivel

strategic și la nivelul liderilor cheie (KLE), la care se adaugă funcțiuni coordonate în cadrul Info Ops, dar realizate prin intermediul trupelor, incluzând angajarea deliberată, la nivel de soldat, înțelegerea culturală și angajarea, prezența, postura și profilul și conduita/ standardele de comportament. Celelalte domenii incluse în diferite aparate doctrinare fie fac obiectul relațiilor de colaborare, majoritatea lor constituind funcții întrunite, fie sunt domenii de interes în ceea ce privește arhitectura informațională a câmpului de luptă, dar care au caracter dual și influențează reziliența societală în ansamblu. Totuși, această clasificare a operațiilor informaționale nu este singura aplicabilă, iar înțelegerea domeniului necesită luarea în considerare a categoriilor de operații informaționale în raport cu ariile de activitate, așa cum au fost stabilite prin *NATO Military Policy for Information Operations* (MC 0422/4, 2012), de unde au fost preluate în doctrina aliată a operațiilor informaționale.

Doctrina autohtonă păstrează linia stabilită la nivelul politicii militate aliate privitoare la Info Ops, presupune ca activitățile planificate în cadrul operațiilor informaționale să fie concentrate preponderent pe voința, capacitatea de înțelegere și percepție și capacitățile acționale ale publicurilor-țintă, iar din acest punct de vedere aceste activități pot fi de influențare, de protecție informațională sau îndreptate împotriva conducerii și capacităților acționale ale inamicului sau potențialului inamic. Această clasificare a activităților a făcut obiectul anterioarelor doctrine NATO, în cadrul cărora, în secțiunea IV *Information Operations Activity Areas* (spre exemplu, AJP-3.10, 2009:I-7, art.0119), unde ariile de activitate informațională au fost descrise într-o manieră mai nuanțată. Prima dintre arii, cea privitoare la influențare, a fost înțeleasă în doctrina aliată ca fiind categoria de activități focalizată pe schimbare, influențare sau întărire a percepțiilor sau atitudinilor adversarilor, potențialilor adversari sau publicurilor-țintă neutre. Activitățile

de protecție informațională au fost descrise ca fiind focalizate pe menținerea libertății de acțiune în mediul informațional și prin protejarea datelor și informațiilor necesare factorilor decizionali, precum și a canalelor și fluxurilor informaționale proprii. Activitățile îndreptate împotriva conducerii și capacităților acționale ale inamicului vizau afectarea fluxurilor informaționale ale acestuia utilizate în procesele de comandă-control, culegere de informații, supraveghere etc. Pe scurt, aceste arii de activități erau prezentate după cum urmează:

- a. Activități informaționale care se concentrează pe schimbarea, influențarea sau consolidarea percepțiilor și atitudinilor adversarilor și ale altor părți aprobate de NAC.
- b. Activități informaționale care se concentrează pe păstrarea și protejarea libertății de manevră a Alianței în mediul informațional prin apărarea datelor și informațiilor care sprijină factorii de decizie și procesele decizionale din Alianță.
- c. Activități informaționale care se concentrează pe contracararea funcțiilor și capacităților de comandă, prin afectarea datelor și informațiilor care sprijină adversarii și alte părți aprobate de NAC și sunt utilizate în comandă și control, informații, supraveghere și management al țintelor, precum și în sisteme de armament.⁹⁹ (AJP-3.10, 2009:I-7, art.0119)¹⁰⁰

⁹⁹ a. Information activities that focus on changing, influencing, or reinforcing perceptions and attitudes of adversaries and other NAC approved parties.

b. Information activities that focus on preserving and protecting Alliance freedom of manoeuvre in the information environment by defending the data and information that supports Alliance decision-makers and decision-making processes.

c. Information activities that focus on countering command functions and capabilities, by affecting the data and information that support adversaries and other NAC approved parties, and are used in command and control, intelligence, surveillance and target acquisition, and weapon systems. [t.n.], în engleză în original.

¹⁰⁰ Noua doctrină aliată a operațiilor informaționale nu definește diferit aceste, ci doar rezumă perspectiva MC 0422 într-o viziune coerentă cu

Analizând doctrina aliată și alte doctrine ale operațiilor informaționale, constatăm că sunt definite trei categorii de activități informaționale: (i) activitățile de influențare, adică acele activități care afectează în mod negativ cursul acțiunilor adversarului sau potențialului adversar și încurajează atitudini defavorabile în raport cu entitățile neutre – doctrina proiectează concretizarea acestor acțiuni prin intermediul operațiilor psihologice, cooperării civili-militari, angajării liderilor cheie și războiului electronic, ba chiar și relațiilor publice, dar asupra acestui punct de vedere vom reveni –, (ii) activitățile de protecție informațională ca activități care contribuie la păstrarea libertății de manevră în mediul informațional, realizate în principal prin securitatea operațiilor și securitatea informațiilor, dar și prin componente defensive ale operațiilor psihologice, războiului electronic și operațiilor cibernetice, respectiv prin alte funcții întrunite și (iii) activitățile îndreptate împotriva conducerii și capacităților acționale ale adversarilor ca activități care se realizează cu scopul alterării fluxurilor informaționale și procesului decizional în ansamblu, mai precis materializându-se prin atacarea infrastructurii informaționale a inamicului, a sistemelor C4ISR și a tuturor celorlalte instrumente și capacități acționale care permit luarea deciziei și punerea ei în practică, prin distrugere fizică, respectiv prin

întreg conținutul doctrinar, astfel: „a. Information activities focused on always preserving and protecting the Alliance freedom of action in the information environment. This is achieved by defending the data, networks and information that supports Alliance decision-makers and decision-making processes. b. Information activities focused on behaviours, perceptions and attitudes of audiences as part of Alliance military operations to induce, reinforce, convince or encourage them in support of NATO objectives. c. Information activities focused on countering an adversary's information activities, as well as their command and control functions and capabilities that support opinion forming and decision-making processes.” (AJP-10.1, 2023:14, art.2.6).

componentele ofensive ale războiului electronic și operațiilor cibernetice.

Această proiecție a acțiunilor informaționale și, implicit, clasificarea Info Ops în raport cu domeniile care definesc scopul operațiilor informaționale: voința, capacitatea de înțelegere și percepție și capacitatea acțională nu sunt foarte precise, deoarece, pentru exemplificare, activitățile de influențare vizează deopotrivă voința și capacitatea de înțelegere și percepție a inamicului și a altor entități aprobate (v. obiectivele O1.1, O1.3, O2.1 și O2.3 din Tabelul 2 Obiectivele operațiilor informaționale), activitățile de protecție informațională privesc deopotrivă protecția instrumentelor și capacităților acționale proprii și a altor entități aprobate, neutre (O3.2, O3.3), cât și a voinței și capacității de înțelegere și percepție prin protecția psihologică a acțiunilor de luptă ale trupelor proprii și a factorilor de decizie (O1.2, O2.2), în timp ce activitățile îndreptate împotriva capacității acționale privesc acțiunea directă împotriva capacităților inamicului sau a altor entități aprobate (O3.1, O3.3), dar urmăresc și realizarea impactului asupra voinței, capacității de înțelegere și percepției factorilor de decizie, adică atingerea obiectivelor O1.1 și O2.1.

Privind din perspectiva preponderenței unor anumite tipuri de acțiuni informaționale în cadrul domeniilor cheie coordonate în cadrul Info Ops, distribuția acestora este următoarea:

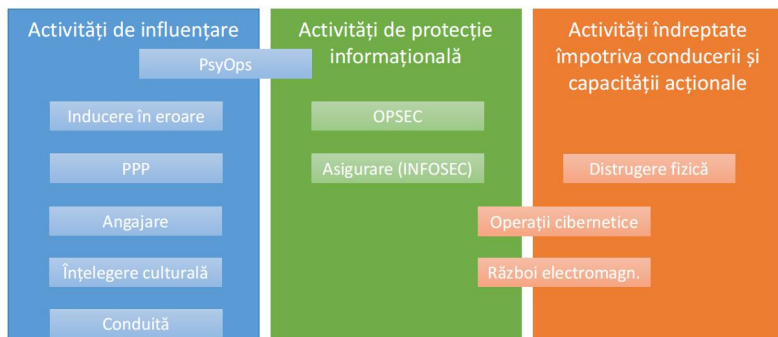


Fig.10 Domeniile cheie coordonate în cadrul operațiilor informaționale în raport cu tipurile de activități informaționale predominante

Practic, influențarea se realizează prin intermediul operațiilor psihologice, angajării deliberate strategice și a liderilor cheie, inducerii în eroare și tuturor categoriilor de funcțiuni coordonate în cadrul Info Ops, dar realizate prin intermediul trupelor: angajarea deliberată la nivel de soldat, înțelegerea culturală și angajarea, prezența, postura și profilul și conduita/ standardele de comportament. Dintre aceste categorii de domenii, singurul care acoperă și alte arii, mai exact protecția informațională, este cel al operațiilor psihologice. Protecția informațională este asigurată prin securitate operațiilor și asigurarea informațiilor, respectiv prin componentele pasive/ defensive ale operațiilor psihologice, operațiilor cibernetice și războiului electromagnetic. Activitățile îndreptate împotriva conducerii și capacităților acționale sunt realizate prin intermediul componentelor active/ ofensive ale operațiilor cibernetice și războiului electromagnetic și prin distrugerea fizică.

4.2 Activități de influențare

Activitățile de influențare se desfășoară doar ca parte a unui plan de operații și în urma aprobării țintelor și definirea adversarilor sau potențialilor adversari. În conformitate cu proiecția doctrinară americană, acțiunile informaționale de influențare se desfășoară începând cu faza a doua, a cuceririi inițiativei acționale, până în faza a cincea, de transfer de autoritate către civili¹⁰¹. În cadrul acestor activități, cel mai

¹⁰¹ Conform doctrinei americane JP 3-13, fazele planului operațional sunt: faza 0 (*Shape*), de proiecție acțională, cuprinsă între aprobarea planului de operații (OPLAN) și activarea ordinului de operații (OPORD); faza I (*Deter*), de descurajare a activităților inamice; faza a II-a (*Seize Initiative*),

important domeniu cheie este cel al operațiilor psihologice (PsyOps), care se desfășoară continuu, ca urmare a rolului pe care îl au în protejarea trupelor proprii.

4.2.1 Operațiile psihologice (PsyOps). Operațiile psihologice au drept principal scop influențarea voinței, percepțiilor, atitudinilor și comportamentului țărilor aprobate, fiind definite în drept activități psihologice realizate cu scopul de a influența percepții, atitudini și comportamente ale audiențelor țintă aprobate, realizate sub coordonarea Info Ops, aliniate liniilor directorare, obiectivelor și efectelor Info Ops, diferențiindu-se de relațiile publice/ Media Ops prin faptul că dețin controlul asupra conținutului și mijloacelor de difuzare a produselor proprii. În doctrina aliată, PsyOps sunt definite drept:

[...] activități planificate care utilizează metode de comunicare și alte mijloace direcționate către publicuri aprobate pentru a influența percepțiile, atitudinile și comportamentul, afectând realizarea obiectivelor politice și militare¹⁰² (AJP-10.1, 2023:17, art.2.13)

Data fiind prevalența acestei dimensiuni direcționate spre ținte adverse sau spre entități neutre aprobate în raport cu protecția psihologică a trupelor proprii, operațiile psihologice reprezintă setul de acțiuni cu influență socială majoră, însemnând acțiunea exercitată de organismul militar prin structuri specializate de PsyOps orientate spre modificarea

de cucerire a inițiativei; faza a III-a (*Dominate*), de dominare; faza a IV-a (*Stabilize*), de stabilizare și ultima fază, a V-a (*Enable Civil Authority*), încheiată odată cu încetarea OPORD și presupunând transferul de autoritate către instituțiile civile.

¹⁰² [...] planned activities using methods of communication and other means directed at approved audiences in order to influence perceptions, attitudes and behaviour, affecting the achievement of political and military objectives, [t.n.], în engleză în original.

acțiunilor și manifestărilor adversarului, presupunând, treptat, modificarea capacității de înțelegere și percepție, ulterior a voinței și prin excepție a capacității acționale a inamicului sau potențialului inamic. PsyOps contribuie la reconfigurarea balanței de putere și control impus prin influențare, nu prin constrângere. Din acest punct de vedere, deși vizează aceleași obiective, acțiunile PsyOps se diferențiază de cele Media Ops deoarece presupun modificarea comportamentelor prin acțiuni persuasive¹⁰³ sau manipulatorii¹⁰⁴, în timp ce Media Ops asigură informarea corectă și oportună.

Doctrina NATO distinge operațiile psihologice între scopul influenței directe asupra înțelegerii și voinței, și scopul efectelor directe asupra capacității acționale a țărilor aprobate. Termenul operații psihologice și acronimul PsyOps sunt specifice doctrinei NATO, în timp ce în doctrina americană este utilizat conceptul Military Information Support Operations (MISO), planificate în scopul influențării emoțiilor, motivelor, rațiunilor obiective și, nu în cele din urmă, a comportamentului guvernelor străine, a organizațiilor, grupurilor și chiar indivizilor, focalizându-se preponderent pe acțiuni cognitive (JP 3-13, 2014:II-9 – II10), fără a fi omise acțiunile manipulatorii, presupunând distorsionarea adevărului. Diferența de nuanță între PsyOps și MISO a fost explicată de Meghann Myers: Forțele Operațiilor Psihologice conduc Operațiile de Sprijin a Informațiilor Militare, iar „operațiile

¹⁰³ Persuasiunea reprezintă activitatea de influențare a percepțiilor, atitudinilor și comportamentelor țintei în vederea producerii unor schimbări concordante atât cu scopurile agenților inițiatori, cât și cele ale țintelor. Spre exemplu, acțiunile de educare a persoanelor aparținând grupurilor extremiste constituie acțiuni persuasive.

¹⁰⁴ Manipularea constituie activitatea de influență îndreptată împotriva unei ținte care este determinată să acționeze în concordanță cu scopurile agentului inițiator, dar în discordanță cu scopurile sale. Manipularea se produce prin distorsionarea adevărului și prin crearea falsei impresii a libertății decizionale și acționale.

psihologice fac referire la numele unităților, în vreme ce MISO fac referire la funcția pe care o îndeplinesc militarii din unitățile PSYOPS.” (Myers 2017, *apud* Neculcea & Răpan, 2022:75)¹⁰⁵. În aparatul doctrinar NATO există o doctrină a operațiilor psihologice, care utilizează drept cadru de referință în definire Allied Administrative Publication (AAP)-06¹⁰⁶. În acest cadru doctrinar, operațiile psihologice presupun coordonare atât în cadrul conceptului mai larg de comunicare strategică/ Strategic Communication (StratCom), care mai coordonează și activitățile de diplomatie publică/ public diplomacy (PD), relații publice/ public affairs (PA), relații publice militare/ military public affairs (Military PA) și operații informaționale/ information operations (Info Ops), precum și în cadrul acestora din urmă, în manieră integrată, cu menținerea proiecției stabilite prin intermediul StratCom. În vechile doctrine aliate, care nu includeau filosofia StratCom, această coordonare era explicit formulată astfel: „PSYOPS, împreună cu alte structuri, vor fi coordonate prin procese Info Ops, ghidate de strategia informațională din cadrul abordării StratCom a NATO”¹⁰⁷ (AJP-3.10.1, 2015:1-3, art.0107).

Operațiile psihologice necesită suport informațional din partea structurilor de intelligence și din partea structurilor C2/ C4ISR, sunt planificate unitar în cadrul proiecției informaționale generale (prin Info Ops), în limitele cadrului

¹⁰⁵ Din perspectiva aparatului doctrinar american, PSYOP reprezintă o specialitate militară (military occupational specialty), pe când MISO activitatea în sine.

¹⁰⁶ În baza AAP-06, doctrina NATO a operațiilor psihologice definește PSYOPS ca fiind „planned activities using methods of communication and other means directed at approved audiences in order to influence perceptions, attitudes and behaviour, affecting the achievement of political and military objectives” (AJP-3.10.1, 2015:1-1, art.0102).

¹⁰⁷ PSYOPS, along with other capabilities, will be coordinated through Info Ops processes guided by the information strategy within NATO’s StratCom approach, [t.n.], în engleză în original.

StratCom în doctrina NATO. În ceea ce privește coordonarea sub umbrela Info Ops, doctrina operațiilor psihologice AJP-3.10.1 (2015:1-10, art.0126) o proiectează astfel:

În sprijinul Info Ops, PSYOPS urmăresc să influențeze percepțiile, atitudinile și comportamentul; pot afecta o gamă largă de public, de la populații la factori de decizie la toate nivelurile.

Planificatorii Info Ops se vor asigura că PSYOPS sunt strâns coordonate cu alte activități militare la toate nivelurile pentru a se asigura că efectul dorit asupra unei ținte nu este compromis de nicio inconsistență în planul de campanie al comandanților.¹⁰⁸

De asemenea, structurile PsyOps cooperează cu structuri de protecție a forței, cu structuri CIMIC și relațiile publice, fiind complementare, în ciuda faptului că utilizează instrumente și tehnici complet diferite.

4.2.2 Inducerea în eroare (MILDEC). Chiar dacă doctrina aliată operează cu un câmp unic de operațiuni, denumit securitatea operațiilor și inducerea în eroare, odată definite ariile/ tipurile de activități informaționale, cele două direcții servesc influențării, respectiv protecției informaționale, deci trebuie luate în considerare separat, cel puțin din punct de vedere didactic și analitic. Punerea lor împreună se datorează faptului că există o doctrină aliată unitară pentru securitatea operațiilor și inducere în eroare, dar și faptului că cele două direcții definesc „activități militare discrete care pot fi utilizate ca

¹⁰⁸ In support of Info Ops, PSYOPS seeks to affect perceptions, attitudes and behaviour; it can affect a broad range of audiences from populations to decision-makers at all levels.

Info Ops planners will ensure that PSYOPS are closely coordinated with other military activities at all levels to ensure that the desired effect on a target is not compromised by any inconsistency in the commanders' campaign plan. [t.n.], în engleză în original.

activități de informare”¹⁰⁹ (AJP-10.1, 2023:20, art.2.19). Activitățile informaționale OPSEC și planurile de inducere în eroare trebuie coordonate cu operațiile informaționale, iar narațiunile utilizate în cadrul inducerii în eroare, adică a unor acțiuni de influențare nu vor fi contrazise de funcțiile întrunite asigurate prin Mil PA și CIMIC.

Inducerea în eroare (uneori acestui concept i se alătură și cel de mascare) sau *deception*, abreviată MILDEC (de la *Military Deception*) constituie o categorie de activități destinate înșelării adversarului și, implicit, influențării capacității sale de percepție și înțelegere (principalul palier acțional), dar și voinței acestuia de a lupta. Doctrina aliată a operațiilor informaționale definește inducerea în eroare astfel:

Inducerea în eroare este un proces psihologic care urmărește un răspuns comportamental, fie că este vorba de acțiune sau inacțiune. Scopul inducerii în eroare este de a exploata avantajul obținut prin înșelarea decidentului advers vizat; accentul se pune pe influențarea comportamentului prin modelarea atitudinilor și percepției. Baza acestui răspuns implică diverse aspecte ale învățării, motivațiile pentru învățare și gândirea umană, aceasta din urmă cunoscută și sub numele de cogniție. Inducerea în eroare vizează în mod explicit decidentul critic, evaluat ca fiind cel mai probabil să reacționeze în modul comportamental dorit. Decidentul se poate afla la orice nivel, în orice mediu și poate fi vizat indirect de grupurile de influență sau de senzori. Acest lucru necesită o analiză aprofundată a preconcepțiilor țintei, a răspunsurilor probabile și a preferințelor informaționale. Înșelăciunea eficientă vizează un decident identificat și procesul său decizional. Dacă inducerea în eroare nu vizează decidenții în baza unei analize aprofundate, este puțin probabil să existe rezultate în beneficiul forțelor aliate. Inducerea în eroare creează și dezvăluie falsul și maschează intențiile, punctele forte, vulnerabilitățile și dispozițiile prietenoase reale pentru a crește

¹⁰⁹ [...] discrete military activities which may be used as information activities, [t.n.], în engleză în original.

sau reduce ambiguitatea forțelor adversarului.¹¹⁰ (AJP-10.1, 2023:20, art.2.19).

Inducerea în eroare este una dintre cele mai vechi forme de influențare în mediul militar. În condițiile actuale în care se desfășoară confruntările militare, caracterizate prin transparență a câmpului de luptă, MILDEC constituie unul dintre cele mai puțin eficiente mijloace de influențare a percepției adversarului. MILDEC necesită cunoașterea în ansamblu a potențialului adversarului, a capacităților acționale ale acestuia și este direct focalizat asupra comportamentului dorit prin înșelare. Prin intermediul MILDEC nu se urmărește simpla înșelare cu privire la posibilitățile proprii, ci se urmărește și obținerea comportamentului avantajos al adversarului pentru acțiunile trupelor proprii sau ale coaliției (JP 3-13, 2014:II-10). Principiile MILDEC, așa cum rezultă din doctrina americană specifică (JP 3-13.4, 2006:viii), sunt concentrarea, obiectivitatea, planificarea centralizată și controlul, securitatea, acțiunea la și în timp, respectiv integrarea. Și în doctrina NATO, la fel ca în cea americană, inducerea în eroare este considerată o funcțiune mai

¹¹⁰ Deception is a psychological process that seeks a behavioural response, be it action or inaction. The aim of deception is to exploit the advantage gained from misleading the targeted adversary decision-maker; the focus is on influencing behaviour through shaping attitudes and perception. The basis of this response involves various aspects of learning, motivations for learning and human thinking, the latter otherwise known as cognition. Deception explicitly targets the critical decision-maker assessed as most likely to respond in the desired behavioural manner. The decision-maker may be at any level in any environment and may be indirectly targeted by influencing groups or sensors. This requires in-depth analysis of target preconceptions, likely responses and information preferences. Effective deception targets an identified decision-maker and their decision-making process. If deception does not target decision-makers, supported by in-depth analysis, it is unlikely to result in outcomes that benefit friendly forces. Deception creates and reveals the false, and masks real friendly intentions, strengths, vulnerabilities and dispositions to increase or reduce ambiguity in the adversary forces. [t.n.], în engleză în original.

amplă decât cea restrânsă la nivelul Info Ops, fiind necesară coordonarea în cadrul acestei funcții întrunite.

4.2.3 Prezența, postura și profilul trupelor (PPP). Conduita și standardele de comportament. Prezența, postura și profilul trupelor (PPP) nu constituie o funcțiune distinct planificată, căreia să îi corespundă o structură militară al cărei principal scop să privească direct și explicit imaginea publică a forței prin impresia directă pe care o imprimă trupele în teatrul de operații. De exemplu, în armata canadiană, în care operațiile informaționale sunt distinct proiectate în domeniile Counter Command Activities, Information Protection Activities și Influence Activities (IA), similare proiecției doctrinare NATO și românești, domeniul IA include structurile și funcțiunile de operații psihologice/ Psychological Operations (PsyOps), relații civili-militari/ Civil-Military Cooperation (CIMIC) și relații publice/ Public Affairs (PA), dar și „facilitatori” (*enablers*) în domeniile Military Deception, Presence, Posture, and Profile (PPP) și Key Leader Engagement (KLE) (Sullivan, 2011:iii). PPP constituie un domeniu cheie coordonat în cadrul operațiilor informaționale și reprezintă imaginea publică a forței și comandantului construită prin prezența, atitudinea și comportamentul trupelor/ comandamentului având ca scop influențarea percepției și atitudinii țintelor aprobate.

PPP trebuie înțeleasă ca funcțiune imagologică a trupelor, atât prin efectul direct asupra publicului local, cât și prin efectul indirect asupra publicului global. Evaluarea, controlul și indicațiile privitoare la impactul PPP asupra publicului sunt de realizate prin intermediul structurilor Info Ops. Imaginea publică a organismului militar este asociată în mentalul colectiv cu forța, iar în anumite contexte cu stabilitatea. Efectul imagologic al prezenței, posturii și profilului trupelor este variabil, depinzând de o serie de factori. Organismul militar este văzut ca un continuum, ca un bastion al modernității târzii,

bazat pe o raționalitate aparte și pe eficiență. Doctrina aliată a operațiilor informaționale proiectează distinct cele trei componente ale PPP. Prezența (sau amenințarea) are impact asupra percepțiilor și este în măsură, în condițiile dislocării oportune, să adauge „credibilitate substanțială a mesajelor transmise prin alte canale”¹¹¹ și să aibă o importantă contribuție la descurajare. Postura (și conduita) contribuie la percepția diferită în cazul tuturor categoriilor de public de interes, iar profilul comandanților și structurilor de comandament are rol important în setarea și transmiterea mesajelor-cheie AJP-10.1, 2023:23-24, art.2.25). În teatrele de operații, prezența, postura și profilul trupelor produc efecte imagologice importante, de la cele de încredere din partea unor grupuri etnice sau sociale, până la reacții adverse, de respingere sau teamă. Simpla prezență a trupelor constituie un important catalizator în plan imagologic și produce efecte directe asupra percepției și înțelegerii, chiar și asupra voinței adversarului.

Noua doctrină aliată include un domeniu care nu fusese definit în precedentele ediții, care are legătură directă cu postura trupelor. Acest domeniu se numește conduită și standarde de comportament/ Conduct and standards of behaviour și țintește imaginea pozitivă a trupelor dislocate obținută prin comportamentul personal și profesional, pentru a evita astfel subminarea credibilității și eficacității. Conduita și standardele de comportament nu au fost incluse încă în toate aparatele doctrinare europene.

4.2.4 Angajarea. Înțelegerea culturală. Angajarea liderilor cheie (KLE) reprezintă domeniul inclus și în aproape toate doctrinele operațiilor informaționale, dar doctrina aliată operează cu un termen mai complex, de angajare, deși KLE constituie în mod tradițional elementul tradițional și de

¹¹¹ [...] substantial credibility to messages delivered through other channels, [t.n.], în engleză în original.

referință în această direcție. Implicarea la toate nivelurile poate produce efecte mai importante, motiv pentru care este necesară conștientizarea faptului că percepțiile, atitudinile și comportamentele publicurilor-țintă aprobate depinde de modul în care structurile Info Ops planifică angajarea. Cele trei niveluri de angajare proiectate de doctrina aliată sunt:

(i) angajarea strategică, realizată cu scopul influențării elementelor de putere *soft* – doctrina le denumește ca elemente de putere non-militară – ;

(ii) angajarea liderilor cheie, asupra căreia vom reveni, reprezentând direcția de maxim efort și

(iii) angajarea la nivel de soldat, care privește cel mai important ca pondere a interacțiunilor dintre cele trei niveluri, realizată deliberat sau ca oportunitate, motiv pentru care structurile Info Ops trebuie să instruiască militarii asupra efectelor pe care le poate avea comportamentul lor, asupra modului în care narațiunile instituționale, exprimate în varianta simplă, ușor de înțeles și transmis, pot produce efecte cumulate foarte mari.

Revenind la angajarea liderilor cheie, acesta este unul dintre domeniile coordonate în cadrul operațiilor informaționale. Activitățile specifice acestui domeniu constau în identificarea liderilor cu influență din zona de operații și a relațiilor dintre aceștia și în stabilirea de contacte în baza unor planuri dinainte stabilite la nivel Info Ops. Stabilirea de contacte trebuie să aibă la bază, obligatoriu, o pregătire anterioară, utilizarea cumulului de informații despre liderii-cheie (religioși, tribali, personalități academice etc.), atât privitoare la biografiile acestora, cât și la personalitate, motivații, interese, dorințe, ambiții, stiluri de conducere, obiective, scopuri explicite și ascunse. Un rol important îl are cunoașterea profilului psihologic al acestor lideri, a istoricului raporturilor cu ceilalți lideri, a influenței lor, a relațiilor de interdependență cu instituții și lideri, dar această cunoaștere

este insuficientă în lipsa unei cunoașteri adecvate a mediului cultural, a implicațiilor sociale, religioase, politice etc., a contextului general în care acești lideri produc influență asupra populației civile și structurilor militare sau paramilitare implicate în conflict. Doctrina aliată a operațiilor informaționale prevede existența unui plan KLE, care conține informații despre contextul situațional, evenimentele critice, contactele planificate cu actorii relevanți, obiectivele, temele majore de abordat, efectele dorite și mijloacele aferente (MOE) (AJP-10.1, 2023:21-22, art.2.22).

Angajarea liderilor cheie (KLE) se realizează în conformitate cu o serie de proceduri descrise pentru prima dată de Kitzen (2012) și amendată ulterior de diverși cercetători în domeniul științelor militare, mai exact: definirea condițiilor de îndeplinire a misiunilor și a obiectivelor; identificarea surselor de putere; evaluarea liderilor cheie; proiecția profilului; luarea deciziei și evaluarea (Duchaine, 2015:216). În cazul în care angajarea liderilor cheie nu este eficientă, structurile militare de operații informaționale pot „crea” lideri cheie, prin intermediul cărora să se realizeze influența dorită asupra publicurilor-țintă, dar efortul este mai mare, fiind necesară implicarea în crearea influenței, adunarea aderenților/suporților, generarea influenței și asistarea ei.

Noua doctrină NATO a operațiilor informaționale include un domeniu nou, înțelegere culturală și angajare/ Cultural understanding and engagement, prezentat ca direcție distinctă în raport cu nivelurile angajării prezentate anterior, vizând pe de o parte înțelegerea culturii-gazdă și a sensibilităților culturale, iar pe de altă exploatarea ca angajare a oportunităților oferite de calendarul cultural local. Acest tipar al angajării este unul predominant deliberat. În ceea ce privește înțelegerea culturală, pentru prima dată în cadrul operațiilor informaționale se pune problema competențelor lingvistice și interculturale, deși problematica înțelegerii sau cunoașterii culturale în cadrul

teatrului de operații nu este una nouă. Înțelegerea culturală reprezintă un stadiu intermediar între conștientizarea culturală (*cultural awareness*) care presupune înțelegerea aspectelor privitoare la parcursul unei națiuni/ culturi și inteligență culturală, care privește abilitatea angajării într-un set de comportamente corespunzătoare unor valori și atitudini specifice națiunii/ culturii. Doctrina operațiilor informaționale nu definește precis nivelul înțelegerii culturale, ci doar proiectează angajarea în raport cu un calendar cultural și cu anumite habitusuri care pot fi exploatate favorabil în interacțiuni.

4.3 Activități de protecție informațională

Activitățile de protecție informațională sunt cele care conferă caracterul de continuitate operațiilor informaționale. Doctrinile aliate anterioare prevedeau explicit această continuitate a protecției informaționale: „operațiile informaționale axate pe păstrarea și protejarea libertății de manevră a Alianței în mediul informațional ar trebui să aibă loc în permanență”¹¹² (AJP-3.10, 2009:1-7, art.0119), în timp ce doctrina actuală o proiectează implicit. Aceste activități se realizează prin măsuri de protecție aplicate informațiilor critice prin apel la metode pasive de protecție a echipamentelor, procedurilor și personalului pe de o parte, a informațiilor pe de alta, respectiv metode active îndreptate împotriva ISR și ISTAR inamice. Metodele pasive conduc la structurarea a două domenii cheie coordonate în cadrul operațiilor informaționale, securitatea operației (OPSEC) și securitatea informațiilor (INFOSEC). În doctrina aliată INFOSEC este inclus în domeniul asigurarea informațiilor.

¹¹² [...] information operations focussing on preserving and protecting Alliance freedom of manoeuvre in the information environment should take place at all times, [t.n.], în engleză în original.

4.3.1 Securitatea operației (OPSEC). Securitatea operației (OPSEC), proiectată pentru prima dată în doctrina americană și utilizată în principal pentru funcțiunile sale defensive, de protecție a echipamentelor, procedurilor și personalului, este utilizată pentru asigurarea unui grad suplimentar de securitate în desfășurarea operațiilor militare întrunit. OPSEC poate apela la mijloace pasive sau active de protecție, având rolul de a limita accesul adversarilor sau potențialilor adversari la informațiile care pot vulnerabiliza sistemele proprii. Securitatea operației presupune identificarea vulnerabilităților și împiedicarea exercitării de acțiuni ostile care să interfereze în acest sens, precum și asigurarea constantă a protecției informaționale critice.

Doctrina NATO operează cu conceptul de Essential Elements of Friendly Information (EEFI) pentru a descrie informația critică pentru succesul operației, necesară a fi protejată pe durata întregii campanii, concept definit în precedenta doctrină: „EEFI vor trebui protejate pe tot parcursul ciclului de viață și pe întreaga gamă de operațiuni militare”¹¹³ (AJP-3.10, 2009:1-9, art.0123), dar operațional în actuala. Practic, OPSEC are rolul, din perspectivă informațională, de a utiliza tehnici pasive sau active de protecție a EEFI, astfel încât voința, înțelegerea și capacitățile acționale ale inamicului să fie orientate în afara acestor informații critice. Și în doctrina americană, OPSEC este proiectată procesual ca o funcțiune standardizată de interdicere a adversarului să ajungă la informațiile critice și indicatorii observabili ai trupelor proprii. Securitatea operației are, așadar, rolul de a interzice accesul inamicului la informația critică, impunând precauție suplimentară și activarea posibilităților de răspuns în ceea ce privește acțiunile adversarului de culegere a informațiilor:

¹¹³ EEFI will need to be protected throughout their lifecycle and throughout the range of military operations, [t.n.], în engleză în original.

Acestea se adoptă în scopul de a asigura operației un grad complementar de securitate, utilizând mijloace active sau pasive, pentru interzicerea cunoașterii de către inamic a dispozitivelor, posibilităților, intențiilor și punctelor vulnerabile proprii, chiar dacă aceasta necesită un interval mai mare de timp. Aplicarea corectă a măsurilor de securitate a operațiilor nu permite transmiterea către inamic a informațiilor despre pregătirile defensive ale forțelor proprii. (Nițu, 2010:388)

OPSEC, odată identificând riscurile externe și vulnerabilitățile interne privitoare la informația critică, apelează la sprijinul altor structuri/domenii informaționale cheie, cu rol preponderent activ (MILDEC¹¹⁴, distrugere fizică etc.) pentru a nu permite adversarului sau potențialului adversar să aibă acces la informație. Coordonarea și sincronizarea sunt cerințe fundamentale pentru punerea în aplicare a funcțiunii numite securitatea operațiilor, în cadrul căreia conștientizarea situației în ansamblu este absolut necesară. Doctrina americană a operațiilor informaționale este însă foarte categorică în ceea ce privește protejarea exclusivă a informațiilor critice. Protejarea altor informații sub scuza rolului major pe care îl au acestea în cadrul operației planificate constituie, de fapt, o încălcare a principiului comunicării corecte, complete și oportune prin intermediul structurilor de relații publice / Public Affairs (PA): „Necesitatea de a practica OPSEC nu ar trebui folosită ca o scuză pentru a refuza publicului informații necritice”¹¹⁵ (JP 3-13, 2014:II-12).

4.3.2 Asigurarea informațiilor. În doctrina aliată, asigurarea informațiilor vizează protecția informațiilor și sistemelor

¹¹⁴ Acesta este un argument suplimentar pentru care actuala doctrină NATO a operațiilor informaționale operează cu binomul „Operation security and deception”.

¹¹⁵ The need to practice OPSEC should not be used as an excuse to deny noncritical information to the public, [t.n.], în engleză în original.

informatică „prin asigurarea disponibilității, integrității și confidențialității acestora”¹¹⁶ (AJP-10.1, 2023:21, art.2.20), presupunând asigurarea că sistemele sunt fiabile și sigure și că procedurile sunt corect implementate, astfel încât să fie împiedicate, contracarate sau dejucate acțiunile rău intenționate îndreptate împotriva fluxurilor informaționale proprii. Asigurarea informațiilor presupune securitate fizică, a personalului și documentelor, și securitate a informațiilor, realizate în mod continuu.

Securitatea informațiilor (INFOSEC) a fost înțeleasă, inițial ca parte a securității operațiilor. Spre deosebire de OPSEC, focalizată pe protecția echipamentelor, procedurilor și personalului, INFOSEC se focalizează pe protecția informațiilor (înregistrate, protejate sau transmise) în raport cu posibilele pierderi sau deteriorări în ceea ce privește confidențialitatea, integritatea și disponibilitatea lor. Scopul securității informațiilor este de a proteja confidențialitatea, integritatea și disponibilitatea informațiilor, iar măsurile care se iau în acest sens presupun acțiuni coordonate Info Ops și având drept scop blocarea acțiunilor Info Ops ostile care pot altera informațiile sau exploata vulnerabilitățile sistemului informațional propriu.

Măsurile INFOSEC, pentru a deveni curențe ca practică și pentru a asigura continuitatea în ceea ce privește protecția informațională (practic, continuitatea operațiilor informaționale), sunt măsuri cu caracter rutinier, procedural, presupunând o clasificare generală a datelor, nu în raport cu caracterul critic privitor la o acțiune sau activitate militară în parte. Practic, scopul fundamental al INFOSEC este de a proteja trupele proprii și, în principal, factorii de decizie de acțiunile adversarului în domeniul operațiilor informaționale (acțiunile adversarului îndreptate

¹¹⁶ [...] by ensuring their availability, integrity and confidentiality, [t.n.], în engleză în original.

împotriva conducerii și capacității de comandă a trupelor proprii), de a interzice accesul la EEFI și de a contracara influența și inducerea în eroare. Din această perspectivă, structurile INFOSEC au fost proiectate în doctrina aliată din 2009 ca structuri integrative care conțin domeniile securitatea comunicațiilor/ Communications Security (COMSEC), securitatea calculatoarelor/ Computer Security (COMPUSEC) și protejarea rețelelor de calculatoare / Computer Network Defense (CND) (AJP-3.10, 2009:1-9, art.0124). Prin Hotărârea nr.585 din 13 iunie 2002 pentru aprobarea Standardelor naționale de protecție a informațiilor clasificate în România, și la noi structurile INFOSEC cuprind elemente COMSEC și COMPUSEC, în termenii Oficiului Registrului Național al Informațiilor Secrete de Stat (ORNISS) acești termeni fiind definiți după cum urmează:

INFOSEC - ansamblul măsurilor și structurilor de protecție a informațiilor clasificate care sunt prelucrate, stocate sau transmise prin intermediul sistemelor informatice de comunicații și al altor sisteme electronice, împotriva amenințărilor și a oricăror acțiuni care pot aduce atingere confidențialității, integrității, disponibilității autenticității și nerepudierii informațiilor clasificate precum și afectarea funcționării sistemelor informatice, indiferent dacă acestea apar accidental sau intenționat. Măsurile INFOSEC acoperă securitatea calculatoarelor, a transmisiilor, a emisiilor, securitatea criptografică, precum și depistarea și prevenirea amenințărilor la care sunt expuse informațiile și sistemele;

securitatea calculatoarelor - COMPUSEC - aplicarea la nivelul fiecărui calculator a facilităților de securitate hardware, software și firmware, pentru a preveni divulgarea, manevrarea, modificarea sau ștergerea neautorizată a informațiilor clasificate ori invalidarea neautorizată a unor funcții;

securitatea comunicațiilor - COMSEC - aplicarea măsurilor de securitate în telecomunicații, cu scopul de a proteja mesajele dintr-un sistem de telecomunicații, care ar putea fi interceptate, studiate, analizate și, prin reconstituire, pot conduce la dezvăluiri de informații clasificate. (H.G. 585, 2002:art.237).

Această perspectivă este dublată și de lucrările de specialitate publicate în domeniul protecției informațiilor și tehnologiilor informatice, cum ar fi, de exemplu, Cantaragiu (2001:13), care definește securitatea informațiilor ca suma măsurilor de protecție și apărare a informațiilor și sistemelor informatice împotriva accesului neautorizat, împotriva modificării conținuturilor în informațiile aflate în faza de stocare, prelucrare sau transport și asigurarea accesului utilizatorilor autorizați: „INFOSEC cuprinde acele măsuri destinate pentru descoperirea, informarea și contracararea acestor tipuri de acțiuni”.

Reformulând, structurile componente INFOSEC sunt securitatea hard, a echipamentelor de calcul (COMPUSEC) și soft, a comunicațiilor (COMSEC și TRANSEC¹¹⁷). Practic, securitatea informațiilor (INFOSEC), deși înțeleasă drept domeniu cheie al operațiilor informaționale în vechea doctrină aliată și subdomeniu al asigurării informațiilor în noua doctrină, constituie în esență un domeniu mult mai amplu, care privește managementul securității informațiilor, în accepțiunea lor de instrumente organizaționale (inclusiv militare). Securitatea informațiilor militare se aliniază cadrului general, atât în limitele sale normative, cât și în limitele sale etice, luând în calcul elementele de echilibru ale unei strategii a securității informaționale organizaționale, mai exact: nivelul de protecție asigurat, costul securității informațiilor și gradul de accesibilitate pentru persoanele autorizate (Baskerville & Dhillon, 2008:18). Ca funcțiune informațională INFOSEC constituie un pilon de bază în proiectarea activităților de protecție informațională, protejând fluxurile informaționale atât pe timpul desfășurării operațiilor întrunite, cât și în afara acestora.

¹¹⁷ TRANSEC sau *Transmission Security* constituie o componentă a COMSEC și privește securitatea comunicațiilor în procesul efectiv de transmitere prin alte mijloace decât cele criptate.

4.4 Activități îndreptate împotriva conducerii adversarului și capacității sale acționale

La fel ca în cazul activităților de influențare, cele îndreptate împotriva conducerii adversarului și capacității sale acționale se desfășoară doar ca parte a unui plan de operații, odată ce țintele au fost aprobate. Acestea sunt acțiuni ofensive desfășurate în scopul cuceririi inițiativei și dominării în ceea ce privește spectrul electromagnetic și rețelele de calculatoare, în scopul afectării fluxurilor informaționale destinate luării deciziilor de către adversari sau transmiterii deciziilor pentru executare. Activitățile îndreptate împotriva conducerii adversarului și capacității sale acționale constau în atacul fizic (la nivel *hard*) al sistemelor C2 și a tuturor fluxurilor informaționale care asigură funcționalitatea în planul deciziei și execuției, precum și împotriva sistemelor și funcțiilor Info Ops ale adversarului, urmărind efecte atât asupra voinței, cât și asupra capacității de înțelegere sau percepție, respectiv asupra capacităților acționale ale acestuia. În cadrul acestor activități, cele mai importante domenii cheie sunt cele ale operațiilor cibernetice și al războiului electromagnetic, la care se adaugă distrugerea fizică.

4.4.1 Operațiile cibernetice. Doctrina aliată definește operațiunile în rețele și dispozitive conectate wireless sau cu fir

și în dispozitivele accesibile prin intermediul spațiului cibernetic care se pot constitui în ținte potențiale sau care pot face obiectul unor amenințări potențiale operații cibernetic/Cyberspace operations, înlocuind vechiul termen de operații în rețele de calculatoare sau Cyber Network Operations (CNO) Domeniul cibernetic este în continuă dezvoltare și el începe să înglobeze nu doar rețele informatice standard, ci și rețele de tipul Internet of Things (IoT), Internet of Bodies (IoB) sau Internet of Senses (IoS), ultimele două categorii presupunând, printre altele, și controlul de la distanță asupra luptătorilor dislocați în teatrul de operații. În doctrina românească a fost funcțional conceptul de operații în rețele de calculatoare, ulterior fiind înlocuit prin alte două concepte, operații în spațiul cibernetic, care se referă la protecția, controlul și utilizarea sistemelor C2 și a rețelelor de calculatoare vizând obținerea și menținerea supremației informațională, respectiv apărarea cibernetică „în scopul protejării, monitorizării, analizării, detectării, contracarării agresiunilor și asigurarea răspunsului oportun împotriva amenințărilor asupra infrastructurilor cibernetic” (S.M.G.-66. 2017:22). Cele două direcții reprezintă de fapt domeniile activ și pasiv ale conceptului de operații cibernetic sau, cu vechea denumire, al conceptului CNO, care în doctrina aliată actuală sunt definite prin două tipuri de operații cibernetic: ofensive/ offensive cyberspace operations (OCO) și defensive/ defensive cyberspace operations (DCOs). În doctrina aliată, cele două componente necesită aprobare în procesul de direcționare comună, diferența dintre ele fiind dată de modul în care se manifestă:

Tehnicile și capacitățile operațiile cibernetic ofensive (OCO) pot fi utilizate pentru a desfășura activități informaționale pentru a crea un efect multiplicator asupra altor activități informaționale desfășurate. Operațiile cibernetic defensive (DCO) constau în măsuri de păstrare a capacității de a utiliza

spațiul cibernetic cu scopul de a permite propria libertate de acțiune și protecția forței.¹¹⁸ (AJP-10.1, 2023:19, art.2.15).

Ținând cont că doctrina românească operează cu conceptele de OPSEC și INFOSEC, iar cea aliată cu OPSEC și asigurarea informațiilor, respectiv că nu niciuna nu propune o discriminare precisă între aceste concepte și respectiv apărarea cibernetică și DCOs, sunt necesare câteva clarificări prin apel la analiza diacronică. Conceptul de INFOSEC cuprinde și componenta defensivă, denumită Cyber Network Defence în doctrinele aliate anterioare (care nu diferă de DCO), la rândul său inclusă în structura Cyber Network Operations (CNO). Probabil echivalente OCOs ar fi componentele active CNO numite Cyber Network Exploitation (CNE) și Cyber Network Arrack (CNA). CNO, în formularea consacrată în doctrina NATO presupuneau utilizarea spațiului cibernetic în interes propriu și limitarea, pe cât posibil, a acțiunilor adversarului în acest nou mediu operațional. Spre deosebire de războiul electromagnetic care presupune utilizarea spectrului electromagnetic pentru transmiterea informațiilor, mai exact utilizarea undelor radio, a microundelor, a radiațiilor infraroșii, a emisiilor în spectru vizibil, a radiațiilor ultraviolete, a radiațiilor X și a undelor γ , spațiul cibernetic presupune transfer de informații între sisteme de informații atât prin fir cât și fără (*wireless*)¹¹⁹. Măsurile sunt în mare măsură similare

¹¹⁸ OCOs techniques and capabilities can be used to conduct information activities to create a multiplier effect to other information activities put in place. DCOs consist of measures to preserve the ability to use cyberspace with the purpose of enabling own freedom of action and force protection, [t.n.], în engleză în original.

¹¹⁹ În manualul american FM 3-13 (2013), activitățile desfășurate în spațiul cibernetic și în spectrul electromagnetice sunt descrise de un termen comun, „cyber electromagnetic activities”. Acestea includ războiul electronic, operațiile în spațiul cibernetic și managementul spectrului electromagnetic (FM 3-13, 2013:3-1, art.3-3) și sunt definite drept „activities leveraged to seize, retain, and exploit an advantage over

războiului electromagnetic, de atac, de protecție și de exploatare, contribuind la susținerea altor tipuri de acțiuni. Precedenta doctrină aliată a descris explicit elementele componente ale sistemului CNO (atac, exploatare, protejare/acțiuni defensive) după cum urmează:

a. **Atacul în rețelele de calculatoare.** Vulnerabilitățile software și hardware permit atacarea computerelor, dispozitivelor de stocare și echipamentelor de rețea prin inserarea de software rău intenționat, cum ar fi virusii, sau prin manipularea mai subtilă a datelor, modificând caracteristicile și performanța dispozitivelor sau exprimarea și afișarea informațiilor conținute în acestea. Această capacitate este îmbunătățită de utilizarea tot mai mare a software-ului comercial disponibil în sistemele militare.

b. **Exploatarea rețelor de calculatoare.** CNE susține Info Ops prin capacitatea de a obține informații despre computere și rețele de calculatoare, prin obținerea accesului la informațiile găzduite pe acestea și prin capacitatea de a utiliza informațiile și computerele/rețelele de calculatoare.

c. **Apărarea rețelor de calculatoare.** Scopul CND este de a proteja împotriva CNA și CNE. CND reprezintă acțiuni întreprinse pentru a proteja împotriva perturbării, refuzării, degradării sau distrugerii informațiilor rezidente în computere și rețele de calculatoare sau a computerelor și rețelor în sine. CND este esențială pentru menținerea capacității decizionale; pe lângă menținerea unei posturi defensive, aceasta va utiliza tehnici de monitorizare și protecție împotriva penetrării pentru a detecta, caracteriza și răspunde la un atac, inițiind acțiuni de izolare și recuperare, după cum este necesar.¹²⁰ (AJP-3.10, 2009:1-11–1-12, art.0129)

adversaries and enemies in both cyberspace and the electromagnetic spectrum, while simultaneously denying and degrading adversary and enemy use of the same and protecting the mission command system” (FM 3-13, 2013:3-5, art.3-29).

¹²⁰ a. **Computer Network Attack.** Software and hardware vulnerabilities allow computers, storage devices and networking equipments to be attacked through insertion of malicious code, such as viruses, or through more subtle manipulation of data, changing the characteristics and performance of the

Doar ultima dintre componentele sistemului CNO în doctrina aliată, Computer Network Defence (CND), constituind un set de acțiuni incluse și în INFOSEC, contribuie la protecția informațiilor. În mod similar, DCOs (în denumirea actuală) contribuie la protecția informațiilor. Celelalte două componente ale CNO, respectiv OCOs, constituie acțiuni preponderent îndreptate împotriva conducerii adversarului și capacității sale acționale. Totuși, efectele urmărite asupra spațiului cibernetic privesc o gamă mai largă de acțiuni decât cele definite prin CNO, motiv pentru care doctrina actuală a optat pentru operații cibernetice/ Cyberspace operation, după modelul doctrinar american, unde se operează cu același concept care îl include și pe cel de operații în rețele de calculatoare/ Computer Network Operations (CNO). Acest domeniu larg al operațiilor cibernetice privește atingerea obiectivelor de natură ofensivă și defensivă în spațiul cibernetic (*cyberspace*), definit drept domeniu în cadrul mediului informațional, constând în rețele de infrastructuri tehnologice informaționale și date incluse, cum ar fi Internetul, rețelele de telecomunicații, sistemele de calculatoare, precum și procesoarele aferente (JP 3-13, 2014:II-

devices or the expression and display of the information contained therein. This capability is enhanced by the increasing use of commercial off-the-shelf software in military systems.

b. **Computer Network Exploitation.** CNE supports Info Ops by the ability to get information about computers and computer networks, by gaining access to information hosted on those and the ability to make use of the information and the computers/computer networks.

c. **Computer Network Defence.** The purpose of CND is to protect against CNA and CNE. CND is action taken to protect against disruption, denial, degradation or destruction of information resident in computers and computer networks or the computers and networks themselves. CND is essential to maintain decision-making capability; as well as maintaining a defensive posture, it will use monitoring and penetration protection techniques to detect, characterise, and respond to an attack, instigating containment and recovery action as required. [t.n.], în engleză în original.

9). În sprijinul operațiilor informaționale, CO interzic sau influențează deciziile adversarilor sau potențialilor adversari, mesajele propriu-zise sau actorii virtuali (cyber-persona¹²¹).

4.4.2 Războiul electromagnetic. Războiul electromagnetic este un concept al doctrinei aliate a operațiilor informaționale, influențat de conceptul american, care a luat locul vechiului concept de război electronic. Modificarea este firească și presupune acoperirea unui câmp mai larg de activități care privesc managementul spectrului electromagnetic/ electromagnetic spectrum (EMS) în scopul operării libere în mediul electromagnetic/ electromagnetic environment (EME). Doctrina aliată definește războiul electromagnetic în raport cu operațiunile electromagnetice:

Războiul electromagnetic este un segment cheie al operațiunilor electromagnetice și poate oferi comandantului la nivel operațional un mijloc de a modela EME pentru a sprijini operațiunile NATO, negând în același timp același lucru adversarului sau inamicului.¹²² (AJP-10.1, 2023:19, art.2.16)

În ansamblul Info Ops, războiul electromagnetic asigură desfășurarea altor activități, precum operațiile cibernetice, inducerea în eroare sau operațiile psihologice. Războiul electromagnetic constituie un domeniu cu aplicare largă în operațiile militare, care contribuie la diminuarea potențialului adversarului, a capacității sale de a utiliza forța, prin acțiuni active

¹²¹ Cyber-persona constituie „an online identity that facilitates communication, decision making, and the influencing of audiences in the cognitive dimension” (JP 3-13, 2014:II-9).

¹²² Electromagnetic warfare is a key segment of electromagnetic operations and can provide the operational-level commander with a means to shape the EME to support NATO operations, whilst denying the same to the adversary or enemy. [t.n.], în engleză în original.

și pasive îndreptate împotriva sistemului de comandă și sistemului informatic al acestuia prin utilizarea spectrului electromagnetic și interzicerea utilizării acestuia de către adversari.

În doctrina românească, unde a rămas operațional conceptul de război electronic/ Electronic Warfare (EW) ca domeniu cheie în cadrul operațiilor informaționale, acesta este definit prin efectele temporare sau permanente ale activităților desfășurate în spectrul electromagnetic, contribuind la protecția informațională, pe de o parte, respectiv la desfășurarea de acțiuni îndreptate împotriva capacității acționale a adversarului. Practic, conceptul de război electronic a înlocuit conceptul de război electronic, fără să aducă o perspectivă nouă asupra domeniului, cu excepția încorporării conceptului de management al EMS. Războiul electromagnetic este un concept aliat preluat din doctrina americană, unde anterior a funcționat conceptul de război electronic (EW) definit de Departamentul American de Apărare (Department of Defence, DoD) drept categoria de acțiuni militare presupunând utilizarea spectrului electromagnetic și a energiei direcționate în scopul controlului acestui spectru și al atacării adversarilor, scopul fundamental fiind acela de a asigura și menține libertatea de acțiune în spectrul electromagnetic pentru forțele proprii și aliate și de a nu o permite pentru adversari: „Scopul războiului electronic este de a asigura și menține libertatea de acțiune în spectrul electromagnetic pentru forțele aliate și de a interzice aceași libertate pentru adversar”¹²³ (Boyd & Chapman, 2013:7). În cadrul acestei perspective doctrinare, în funcție de tipul de măsuri pe care le impune, putem aduce în discuție trei tipologii acționale ale războiului electronic, astfel:

- atacul electronic (*electronic attack*), constând în utilizarea energiei electromagnetice direcționate sau a

¹²³ The purpose of electronic warfare is to secure and maintain freedom of action in the electromagnetic spectrum for friendly forces and to deny the same for the adversary, [t.n.], în engleză în original.

armamentului antiradiație împotriva forțelor și mijloacelor adversarului, în scopul degradării, neutralizării sau distrugerii capacităților acționale ale acestuia, în special pentru distrugerea capacităților informaționale, prin acțiuni în principal ofensive, dar și defensive¹²⁴;

- protecția electronică (*electronic protection*), constând în acțiuni de protecție a forțelor și mijloacelor proprii față de acțiunile adversarului în spectrul electromagnetic pentru degradarea, neutralizarea sau distrugerea capacității acționale proprii sau a aliaților;

- sprijin electronic (*electronic warfare support*), constând în interceptarea, identificarea și localizarea surselor de radiație electromagnetică în scopul desfășurării de acțiuni ofensive împotriva acestora, cu mijloace care fac obiectul altor tipuri de operații militare, respectiv în coordonarea (inclusiv conducerea focului) în diferite acțiuni întrunite (Boyd & Chapman, 2013:7).

Cele trei categorii de acțiuni desfășurate în cadrul EW au fost descrise explicit și în anterioara doctrină a NATO, care le definea drept *electronic attack*, *electronic protective measures* și *electronic support measures*, dar nu și în doctrina românească.

Diferența de proiecție doctrinară constă în faptul că în doctrina americană EW și INFO OPS sunt funcții informaționale situate pe același palier și incluse în conceptul-umbrelă IRC (*information-related capabilities*), pe când în anterioara doctrină NATO EW constituia o funcțiune a Info Ops, chiar dacă aplicațiile militare ale războiului electronic sunt multiple și excedează cerințele operațiilor informaționale¹²⁵. Mai mult,

¹²⁴ Mason Boyd și Pierce T. Chapman (2013:70) exemplifică aceste tipuri diferite de acțiune astfel: „Electronic attack can be used offensively, such as jamming enemy communication or jamming enemy radar to suppress its air defenses, and defensively, such as deploying flares”.

¹²⁵ Doctrina aliată a operațiilor informaționale admite această poziție: „Electronic Warfare (EW) has wide application in military operations.” (AJP-3.10, 2009:1-9, art.0126)

doctrina americană proiectează războiul electronic în baza unei concepții organizatorice diferite, incluzându-l într-un domeniu mai amplu, operații în spectru electromagnetic integrat / Joint Electromagnetic Spectrum Operations (JEMSO). JEMSO cuprind războiul electronic/ Electronic Warfare (EW) și managementul spectrului electromagnetic / Electromagnetic Spectrum management operations. În acest cadru, războiul electronic are rolul de asigura și menține libertatea de acțiune și de a interzice acțiunile adversarului în spectrul electromagnetic, în timp ce funcțiunea întrunită, JEMSO, sprijină operațiile informaționale. Această cooperare EW – Info Ops (IO în abrevierea americană) este cel mai bine descrisă în doctrina americană a războiului electronic, JP 3-13.1, după cum urmează:

EW contribuie la succesul operațiilor informaționale (IO) prin utilizarea tacticilor și tehnicilor ofensive și defensive într-o varietate de combinații pentru a modela, perturba și exploata utilizarea adversă a spectrului EM, protejând în același timp libertatea de acțiune prietenoasă în acest spectru. Extinderea dependenței de spectrul EM crește atât potențialul, cât și provocările EW în IO. Toate capacitățile IO de bază, de sprijin și conexe utilizează fie direct EW, fie beneficiază de pe urma EW.¹²⁶ (JP 3-13.1, 2007:vi),

respectiv detaliată în subcapitolul 7, *Electronic Warfare's Relationship to Information Operations*, din primul capitol al doctrinei, *Overview of Electronic Warfare* (JP 3-13.1, 2007:I-7 – I-8). Prin introducerea conceptului de război electromagnetic,

¹²⁶ EW contributes to the success of information operations (IO) by using offensive and defensive tactics and techniques in a variety of combinations to shape, disrupt, and exploit adversarial use of the EM spectrum while protecting friendly freedom of action in that spectrum. Expanding reliance on the EM spectrum increases both the potential and the challenges of EW in IO. All of the core, supporting, and related IO capabilities either directly use EW or indirectly benefit from EW. [t.n.], în engleză în original.

doctrina aliată armonizează dezvoltările în domeniu, fără a continua să diferențieze între tipurile de acțiuni pasive/ active sau defensiv/ ofensive.

4.4.3 Distrugerea fizică. Distrugerea fizică este subdomeniul care corespunde strictamente acțiunii ofensive, reprezentând domeniul cu cea mai largă aplicabilitate în acțiunile militare constând în atacarea sistemelor C2 ale adversarului și a tuturor palierelor mediului informațional în ansamblu. Prin intermediul acestui atac, acțiunea vizează, în subsidiar, afectarea voinței și capacității de înțelegere și percepție a adversarului. Practic, prin distrugere fizică se înțelege atât distrugerea rețelei de senzori a adversarului, cât și a nodurilor critice din rețeaua C2, a rețelelor de calculatoare și a centrelor de comandă. Distrugerea fizică, înțeleasă ca domeniu al Info Ops în diferite aparate doctrinare, presupune în doctrina aliată coordonare la nivelul Info Ops prin identificarea și selecția țintelor trimise spre aprobare în procesul comun de direcționare.

5. Războiul informațional

Information dominance would be of only academic interest, if we could not turn this information dominance into battlefield dominance.

David S. Alberts (n.1942)

5.1 Conceptul actual de război informațional

Conceptul de război informațional (information warfare, IW sau INFO WAR) a devenit popular odată cu modificările cantitative și calitative ale mediului informațional, în special în ceea ce privește utilizarea spațiului cibernetic și a spectrului electromagnetic. Războiul informațional poate fi înțeles în raport cu două posibile abordări: (i) ca mutație din zona de manifestare a puterii *hard* înspre cea a puterii *soft*, adică de schimbare a accentului confruntării având centrul de greutate în domeniul fizic înspre confruntarea având centrul de greutate în domeniul informațional¹²⁷, pe de o parte, respectiv (ii) ca o continuare a

¹²⁷ Alberts *et al.* (2001:11-14) definesc domeniile fizic, informațional și cognitiv în raport cu operațiile militare după cum urmează: „The physical domain is the place where the situation the military seeks to influence exists. It is the domain where strike, protect, and manoeuvre take place across the environments of ground, sea, air, and space. It is the domain where physical

proiecției Info Ops de pe palier operativ pe palier strategic.

În literatura română de specialitate, conceptul de război informațional a pătruns cu semnificația asociată mutației centrului de greutate de pe domeniul fizic pe cel informațional. În fapt, acest concept este golit de conținut în acest înțeles, deoarece nu a fost încă identificată și clar definită o categorie distinctă de conflicte armate sau o formă de continuare a războiului care să poarte numele de războaie informaționale. Martin C. Libicki a construit încă din 1995 acest concept golit de semnificație directă, ca sumă a unor forme conflictuale particulare, cum ar fi: (i) războiul de comandă și control/ command-and-control warfare (C2W), îndreptat împotriva structurilor C2 ale adversarului; (ii) războiul bazat pe culegerea informațiilor/ intelligence-based warfare, ulterior devenit information-based warfare¹²⁸ (IBW), constând, după caz, în proiectarea și protejarea structurilor informaționale proprii, respectiv contracararea sistemelor care încearcă să domine din punct de vedere informațional spațiul de conflict; (iii) războiul electronic (EW), o proiecție a funcțiunilor complete a operațiilor

platforms and the communications networks that connect them reside. (...) The information domain is where information lives. It is the domain where information is created, manipulated, and shared. It is the domain that facilitates the communication of information among warfighters. It is the domain where the command and control of modern military forces is communicated, where commander's intent is conveyed. (...) The cognitive domain is in the minds of the participants. This is the place where perceptions, awareness, understanding, beliefs, and values reside and where, as a result of sensemaking, decisions are made."

¹²⁸ Acest termen, uneori confundat cu „information warfare”, desemnează conflictul având la bază nevoia de control al informațiilor în scopul obținerii de avantaje decisive, mai exact „Information-based warfare is an approach to armed conflict focusing on the management and use of information in all its forms and at all levels to achieve a decisive military advantage especially in the joint and combined environment” (definiție propusă de School of Information Warfare and Strategy, National Defense University, în 1993, *apud* Aldrich, 1996:3)

omonime, pentru Libicki o proiecție a utilizării tehnologiilor radioelectronice și criptografice, având ca scop obținerea supremației în spectrul electromagnetic; (iv) războiul psihologic/ psychological warfare (PSYWAR sau ΨW), o proiecție la nivel strategic a operațiilor psihologice, vizând utilizarea informațiilor pentru obținerea efectelor dorite în ceea ce privește modificările de natură atitudinală și comportamentală asupra trupelor proprii și comenzii acestora, asupra aliaților, adversarilor sau părților neutre; (v) războiul „hacker”-ilor/ „hacker” warfare (HW), ca extensie a operațiilor în cibernetice, presupunând obținerea supremației în acest mediu; (vi) războiul informațiilor economice/ economic information warfare (EIW), privind controlul informațional în scopul obținerii și menținerii de efecte în plan economic, până chiar a supremației în acest domeniu și (vii) războiul cibernetic/ cyberwarfare¹²⁹, ulterior devenit cybernetic warfare (CW sau CybW), constituind totalitatea acțiunilor în plan virtual în scopul obținerii de rezultate în plan fizic (Libicki, 1995:x).

Cea de-a doua perspectivă de definire a războiului informațional (Info War) este mult mai clară. Info War poate fi

¹²⁹ Libicki (1995:x) consideră această ultimă formă de război informațional un amalgam de scenarii futuriste, „a grab bag of futuristic scenarios”. În capitolul special destinat acestui domeniu, Libicki (1995:75-83) identifică un set de forme particulare de manifestare, cum ar fi terorismul informațional (*information terrorism*), atacul semantic (*semantic attack*): „The difference between a semantic attack and hacker warfare is that the latter produces random, or even systematic, failures in systems, and they cease to operate. A system under semantic attack operates and will be perceived as operating correctly (otherwise the semantic attack is a failure), but it will generate answers at variance with reality.”, războiul simulat (*simula-warfare*) și războiul Gibson (*Gibson-warfare*), definit după numele autorului romanului SF *Neuromancer*, constând în disputa dintre personaje virtuale echivalente. Concluzia autorului american privitoare la posibilitatea și relevanța unor asemenea forme de confruntări este limpede și justifică argumentul său din introducere: „Possible? Actually, yes. Relevant to national security? Not soon.”

înțeles ca un ansamblu unitar de operații, pentru a se opera distincția război – operație în sensul discriminării realizate de Carl von Clausewitz¹³⁰, care concură la atingerea unor obiective de ordin superior, strategic, constituind o formă distinctă de beligeranță, nonviolentă, neletală, având caracteristicile și limitele de aplicare ale termenului englez „warfare”, traducibil prin „confruntare” (v. subcapitolul 1.4 *Război vs. confruntare*). Confruntarea informațională, așadar, reprezintă forma corectă de utilizare a conținutului semnificativ pentru desemnarea ansamblului operațiilor informaționale desfășurate la nivel strategic, dar pentru a nu produce o mutație terminologică importantă (și nejustificată de alte rațiuni decât de natură lingvistică), am ales să utilizăm termenul de război informațional în sensul anterior menționat. Înțelesul asociat conceptului de război informațional din această perspectivă, presupunând stare de conflictualitate manifestată prin competiția în planul obținerii supremației informaționale, a făcut obiectul unor lucrări din literatura românească de specialitate, dar nu s-a impus ca atare.

În sens larg, războiul informațional vizează controlul asupra sistemului informațional în ansamblu (asupra informației, fluxurilor informaționale, canalelor necesare acestora, precum și altor capacități acționale), pentru obținerea supremației informaționale, a unei forme de dominație bazate pe puterea *soft*. În viziuni restrânse, acest tip de confruntare neletală a fost definită inclusiv în documentele oficiale ale unor

¹³⁰ Contrariat de perspectiva generalului Heinrich Dietrich von Bülow dintr-o lucrare din 1799, în care tactica era definită drept știința mișcărilor trupe în limitele câmpului vizual, în timp ce strategia se ocupa cu mișcarea trupelor în afara acestuia, tânărul căpitan de 25 de ani, Carl von Clausewitz, pune în 1805 bazele unei noi perspective a raporturilor dintre cele domenii ale artei militare: „La fel cum tactica este întrebuințarea forțelor armate în luptă, strategia este întrebuințarea luptei – adică legarea luptelor singulare într-un ansamblu – în vederea scopului final al războiului” (*apud* Soare, 1993:31).

națiuni și alianțe începând cu anul 1995, după utilizarea primelor concluzii desprinse în urma desfășurării conflictului din Golf, când Departamentul pentru apărare al Statelor Unite / Department of Defense (DoD) a publicat primele definiții și primele studii dedicate Info War (spre exemplu, *Information Warfare / Information Operations Study*), deși termenul a fost lansat anterior. O strategie a operațiilor informatice în Armata Stelelor Unite a existat încă din 1988, ea constituind nucleul actualei perspective asupra operațiilor informaționale.

În primele definiții, dar și în limitele primului cadru de definire a Info War ca structură de forme particulare de beligeranță, a fost luată în considerație superioritatea informațională și nu supremația informațională, ca urmare a unor convingeri din acea perioadă privitoare la imposibilitatea controlului total și interdicției în plan militar a acțiunilor adversarului. În acest context, mediul informațional era înțeles ca fiind un mediu care nu prezintă caracteristici esențialmente specifice câmpului de luptă. Cu excepția câtorva subdomenii relativ restrânse și a unor tipuri de activități sau activități aferente, care fac obiectul unui mediu așa-zis al conflictualității (cum ar fi bruiajul electronic sau alte măsuri active sau pasive din spectrul electromagnetic), acest mediu informațional, odată excedând limitele cadrului confruntării, se transformă și se redefineste. Din această perspectivă, supremația informațională nu devine un concept tocmai simplu de înțeles și utilizat, dat fiind faptul că superioritatea informațională a unei părți implicate în conflict nu poate asigura, implicit, și interdicția informațională. Libicki (1995:xi) este primul dintre cercetătorii în domeniul științelor securității care pune problema sub această lumină:

Informația nu este în sine un mediu al confruntării, cu excepția anumitor aspecte restrânse (cum ar fi bruiajul electronic). Superioritatea informațională poate avea sens, dar supremația informațională (în care o parte poate împiedica cealaltă să intre

pe câmpul de luptă) nu are mai mult sens decât supremația logistică.¹³¹

Interdicția în mediul cibernetic și în spectrul electromagnetic este posibilă, fapt ce conduce la posibilitatea proiecției unei supremații informaționale puse în practică începând cu Războiul din Irak (2003).

Războiul informațional, spre deosebire de celelalte forme ale conflictualității explicite, bazate pe violență fizică deschisă, având așadar centrul de greutate în domeniul fizic, se sprijină pe un set diferit de principii ale planificării și ducerii conflictului, dat fiind faptul că se situează în mare măsură în afara spectrului acțiunilor militare propriu-zise, respectiv datorită faptului că se fundamentează pe alte logici în ceea ce privește funcționalitatea, pe alte modalități de aplicare și pe alte posibilități de acțiune decât cele specifice mediului militar în ansamblu. Putem vorbi, astfel, de o determinare nomologică bazată pe alte logici ale angajării directe, asupra cărora influența logicii de piață, respectiv proiecțiile politică, socială, religioasă, culturală au un anumit tip de efect și determină o abordare diferențiată. Nicolaescu și Simileanu (2004:35) pun la baza războiului informațional principiile: (1) „decapitării”, presupunând separarea informațională a țintelor primare (factorii decizionali) de rețeaua decizională și de execuție; (2) intuiției, ținând distrugerea sau scoaterea din operativitate a senzorilor adversarilor; (3) interoperabilității, vizând impunerea unor rețele de comunicare optimă între structurile de diferite funcțiuni sau aparținând diferitelor națiuni, care colaborează în cadrul unor coaliții sau alianțe; (4) cunoașterii, presupunând asimilarea și gestionarea unei cantități cât mai mari de informații privitoare la

¹³¹ Information is not in and of itself a medium of warfare, except in certain narrow aspects (such as electronic jamming). Information superiority may make sense, but information supremacy (where one side can keep the other from entering the battlefield) makes little more sense than logistics supremacy. [t.n.], în engleză în original.

sistemele proprii și aliate; (5) supraviețuirii, presupunând conectarea la sistemul nomologic al acțiunii militare propriu-zise, realizându-se prin planificarea acțiunilor informaționale, conducerea centralizată a acestora, realizarea comunicării eficiente între subsisteme și execuția descentralizată a acțiunilor informaționale proprii, respectiv principiile (6) ierarhiei și (7) intensității. Aceste principii acționale sunt cele care privesc, din perspectiva cercetătorilor români, punerea în aplicare a acțiunii informaționale ofensive și defensive în condițiile conflictualității deschise, după aprobarea țințelor, presupunând utilizarea deopotrivă a tuturor celor trei tipuri de acțiuni. Per ansamblu, principiile operațiilor informaționale, așa cum au fost ele prezentate și descrise anterior, rămân valabile și produc efecte în acțiunea informațională continuă.

5.2 De la conceptul de război la necesitatea de redefinire a conceptului de război informațional

Mediul informațional actual și, implicit, operațiile informaționale, au influențat major redefinirea termenului de război și particularizarea celui de război în Era Informațională, modificând radical suportul proiectiv la nivelurile operativ și strategic, tipul de acțiuni de luptă planificate, efectele acestora, introducând concepte noi, funcționale, la rândul lor descriind structuri sau arhitecturi funcționale, operând cu informațiile gestionate integrat și continuu. Astfel, concepte precum cel de comandă, control, comunicații, calculatoare și informații / command, control, communications, computers & information (C4I), având la bază funcția întrunită de comandă-control (C2), operând integrat cu conceptul și arhitectura aferentă de informații, supraveghere și recunoaștere/ intelligence, surveillance & reconnaissance (ISR) și conducând la proiecția C4ISR sau a Dominant Battlespace Knowledge (DBK),

respectiv împreună cu conceptul și arhitectura loviturilor ghidate cu precizie/ precision guided munition (PGM), așa numitele, în studiile românești, „lovituri chirurgicale”, au permis construirea unor metasisteme acționale, complexe, având la bază un sistem informațional și tehnologic care poate asigura supremația informațională¹³². Ulterior, metasistemul C4I – ISR – PGM a fost suplimentat cu funcțiunile derivate din abordarea operațiilor bazate pe efecte (EBAO), rezultând o metodă de analiză a eficienței structurilor de comandă și control (C2) denumită Command and Control Measures of Effectiveness (C2MOE)¹³³, în sine aplicabilă metasistemului extins numit Război Bazat pe Rețea (RBR)/ Network Centric Warfare (NCW).

¹³² Această structură, intitulată *System-of-Systems*, element fundamental al proiecției ultimei revoluții militare (RMA), se datorează lui William Owens (1996). *System-of-Systems* a fost conceput ținându-se cont de două cerințe ale actualei Ere Informaționale, informație și caracter înrunit. Iată cum este descrisă proiecția metasistemului de Michael Raska (2016): „The system-of-systems concept focused on two elements: information and jointness. It envisioned integrating existing (and in some ways overlapping) inter-service platforms and components – particularly, advanced C4I systems with ISR systems into a coherent, interoperable joint framework. Connecting diverse C4I architectures and ISR information systems would be enable unprecedented situational awareness capabilities – so-called ”Dominant Battlespace Knowledge” (DBK) – envisioned by Owens accross a large area of operations (200-by-200-mile boxes). In conjugation with PGMs and their platforms, the system-of systems approach would exploit DBK that would accelerate decision-making processes and result in a „precision force in action and results” (Owens, 1996, 37) and essentially enable the U.S. military to locate, track, and destroy enemy forces with virtual impunity”.

¹³³ Funcțiunile metodei analitice C2MOE sunt multiple, dar rolul care o face aplicabilă metastructurilor NCW este cel de măsurare a eficienței directe atât a funcționalității structurilor C2, cât și a sistemelor de lovire: „through C2MOE is represented by direct effectiveness like engagement success rate, hit probability, enemy damage probability, they are reflected by the items of indirect effectiveness of C2 such as information fusion processing time, decision times, information fusion accuracy etc.” (Cha *et al.*, 2012:395)

Funcția întrunită C2, moștenire a erei industriale, proiectată în primele doctrine aliate la nivelul domeniilor fizic (senzori, sisteme, platforme etc.), informațional (date, informații, fluxuri informaționale etc.) și cognitiv (percepție, înțelegere, voință, decizie), a fost, așadar, suplimentată cu funcțiuni complexe pe toate nivelurile anterior amintite, în special pe nivel informațional. Rezultatul a fost proiecția ternară a sistemului de sisteme (*System-of-Systems*) și punerea sa în aplicare efectivă în cadrul conceptului de Război Bazat pe Rețea, având la bază exploatarea în condiții optime a mediului informațional pentru a se putea crea o rețea informațional-acțională alcătuită din senzori, elemente decizionale și sisteme de foc. Această arhitectură permite configurarea unei imagini unitare a câmpului de luptă, culegerea de informații și transmiterea la centrele decizionale, actul decizional cvasiinstantaneu și acțiunea imediată în plan fizic prin aplicarea puterii de foc, indiferent cât de dispersate geografic sunt elementele rețelei. Nu întâmplător, principiile RBR sunt superpozabile principiilor operațiilor informaționale: divizarea, specializarea, ierarhizarea, optimizarea, planificarea centralizată și execuția descentralizată (Alberts, 2005, *apud* Gherman 2014:37).

RBR reprezintă o formă de conflictualitate letală, presupunând un număr mult mai redus de victime decât în cazul confruntării clasice, care se fundamentează pe proiectarea acțiunilor militare în acord cu exploatarea riguroasă și oportună a resursei informaționale. RBR depinde de dezvoltarea de infrastructură tehnologică adecvată (domeniu fizic), de existența unor fluxuri informaționale de transmitere de date și comenzi (domeniu informațional) și a unor competențe decizionale bazate pe cunoaștere și, mai ales, pe distribuirea oportună a informației¹³⁴ (domeniu cognitiv). Acest principiu,

¹³⁴ Pe palier cognitiv, Gherman (2014:45) ridică problema exploatării prin distribuire, mai exact: „este necesar ca oamenii care exploatează aceste

al distribuirii informației, devine fundamental și singura garanție a funcționalității metasisemului militar în cadrul proiecției strategice a RBR. Privind distribuirea informației în concordanță cu creșterea nivelului de delegare a autorității de conducere către structurile funcționale subordonate (descentralizare în planul execuției) și de creștere a nivelului de interrelaționare între structurile funcționale subordonate, principiul anterior menționat conduce la un efect cumulat de interacțiune. Analizând aceste efecte cumulate în sistemul NATO Network-Enabled Capability C2 Maturity System (N2M2C2) elaborat de cercetătorii americani David S. Alberts, R.K. Huber, și J. Moffat (2010, *apud* Gherman, 2014:50) în cadrul grupului de analiză 065 (NATO System and Analysis Studies group 065), presupunând luarea în considerație a acțiunii izolate, separate, coordonate, colaborative și ideale (cu subsistemele capabile de autosincronizare), poate fi ușor de evidențiat potențialul nivelului ideal în raport cu celelalte:

informații să-și schimbe abordarea de la conceptul „necesitatea de a cunoaște” la conceptul „necesitatea de a distribui”.

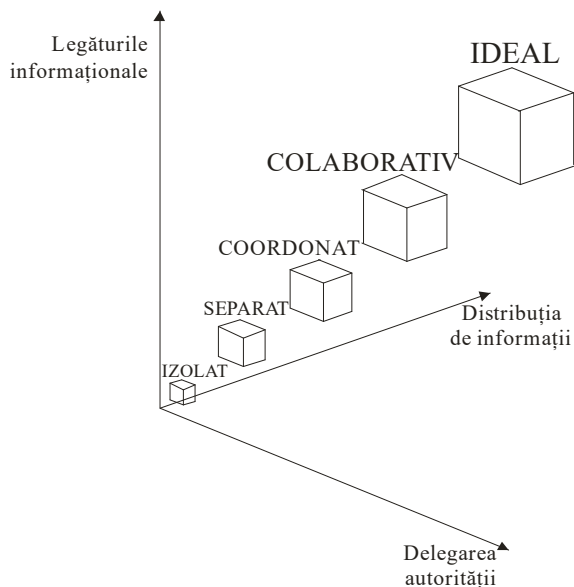


Fig.11 Nivelurile de interacțiune dintre substructuri în cadrul conceptului N2M2C2 (*apud* Gherman, 2014:57)

În acest context, al acțiunii coordonate, colaborative sau autosincronizate (ideale), efectul cumulat, coroborat cu pierderile reduse, presupunând exploatarea corespunzătoare a mediului informațional, conduce la necesitatea de re proiectare a rețelelor informaționale, de distribuție a informațiilor, capabile să facă față cerințelor de oportunitate din noul mediu.

Din acest punct de vedere, se impune o regândire a conceptului de război informațional, o reconfigurare, o redimensionare, o continuă ajustare la nevoile războiului specific erei informaționale.

5.3 Măștile războiului informațional

Războiul informațional nu este, așadar, război în înțelesul clasic al termenului, ci o formă de confruntare informațională, o

formă de beligeranță neletală în natura ei, desemnând ansamblul operațiilor informaționale și a altor tipuri de operații și activități militare, desfășurate în acord cu proiecția comunicării strategice (StratCom). Ar trebui să admitem că limba română, săracă în expresii privitoare la violența militară, utilizează termenul război și în sensul de confruntare (divergență, disensiune, competiție), ceea ce produce foarte multe confuzii, în special în discursul mediat. Conceptul de război informațional trebuie înțeles ca reprezentând mai degrabă confruntarea informațională care incumbă și palierul puterilor *soft* decât extensia operațiilor informaționale la nivel strategic. Dacă s-ar impune un asemenea termen în detrimentul celui de război (fie el informațional, psihologic, cognitiv sau de orice altă natură neletală), probabil că s-ar reduce panica, s-ar dezamorsa starea de încordare a publicului. Înțelesul de război informațional și-ar putea extinde aria de cuprindere ca *whole-of-society approach* doar în condițiile unui război real (*war*), ca anvelopă informațională a acestuia. În esență conceptul de război informațional se referă la utilizarea adecvată a informației, a mediului informațional, a arhitecturii informaționale a câmpului de luptă. Confruntarea informațională caracterizează acele războaie în care acțiunile forțelor armate își îndreaptă atenția către informare și influențare mai degrabă decât către distrugere. În condițiile diversificării actorilor participanți la conflict se produce o hibridizare a acțiunilor militare prin creșterea rolului acțiunilor militare *soft*, neletale sau non-kinetice, categorie din care operațiile informaționale sunt cele mai importante, un factor multiplicator de forță, cu rol hotărâtor în influențarea deciziilor politice, a opiniei publice și, implicit, în evoluția evenimentelor la nivel strategic. Confruntarea intensificată pe palier informațional caracterizând războiul contemporan nu se mai rezumă la obținerea și transmiterea informațiilor, ci mai ales la manipularea și modelarea percepțiilor pentru a influența opinia publică, deciziile politice și, în măsura în care este posibil, chiar

la evoluția conflictelor. Totuși, conflictualitatea contemporană presupune manifestarea unor tendințe contrare, pe de o parte amintita reducere a manifestării kinetice generată de evoluția tehnologică, pe de alta masificarea trupelor impulsionată de regimurile iliberale, manifestându-se în alternanță sau chiar suprapunându-se.

Foarte important de menționat este faptul că, deși suficient de incert, impunerea termenului război informațional este o victorie occidentală în „războiul definițiilor” în raport cu școala rusă, deoarece provine din studiile și doctrinele occidentale și are la bază un concept operaționalizat, cu foarte mici variațiuni în ceea ce privește aplicarea: conceptul de „operații informaționale”. În terminologia militară rusă, care a reușit să impună un înțeles diferit în cazul preluării altor termeni occidentali, conceptul de război informațional excedează, evident, aria de aplicare din doctrinele occidentale.

Conceptul rusesc de operații informaționale presupune, după schema clasică, o extindere a aplicării conceptului de la aria de manifestare a puterii *hard* la puterile *soft*, prin contaminare, ca în cazul războiului hibrid (Lesenciuc, 2023). Ceea ce caracterizează războiul informațional rus și îl diferențiază de școala occidentală este tradiția sovietică – o radiografie a acestei perioade de dezvoltare a domeniului a fost realizată de Allen & Moore (2018:61-62) –, din cadrul căreia provine conceptul de „control reflexiv” (*reflexivnoe upravlenie*), atipic gândirii militare occidentale, cu rădăcini care se găsesc în anii 1960, testat împreună cu conceptele *maskirovka* (tradus în majoritatea lucrărilor occidentale prin indecere în eroare, dar excedând acest cadru interpretativ) și dezinformare (Thomas, 2004:239). Din perspectivă sovietică și ulterior rusă, exploatarea morală și psihologică a adversarului sunt esențiale în conflict. Acest tip de acțiune este caracterizată astfel de T.L. Thomas:

Într-un război în care se folosește controlul reflexiv, partea cu cel mai mare grad de reflectare (partea cea mai capabilă să imite gândurile celeilalte părți sau să aibă predicții asupra comportamentului acesteia) va avea cele mai mari șanse de câștig. Gradul de reflectare depinde de mulți factori, dintre care cei mai importanți sunt capacitatea analitică, cultura generală și experiența, precum și a domeniului de aplicare a cunoașterii despre inamic.¹³⁵ (Thomas, 2004: 242)

Teoria controlului reflexiv privește o gamă variată de acțiuni militare, majoritatea încadrabile în conceptul occidental de operații informaționale, vizând influențarea sau alterarea procesului decizional al adversarului, dar aceste acțiuni realizate pe palierul puterii *hard* sunt dublate de cele provenind de pe palierul *soft*, în special de acțiuni politice și simbolice, care să construiască o realitate alternativă și convenabilă, bazată pe narațiuni rusești, rezumate în gama de manifestări care include următorul repertoriu:

[...] utilizarea forței superioare, demonstrațiile de forță, atacurile psihologice, ultimatumurile, amenințările cu sancțiuni, amenințările riscurilor (dezvoltate din concentrarea atenției asupra unui comportament sau a unei conduite iraționale, ori din delegarea puterii către o persoană iresponsabilă), acțiuni de recunoaștere, manevre provocatoare, testarea armamentului, refuzul accesului inamicului în anumite zone, creșterea stării de alertă a forțelor, formarea de coaliții, declararea oficială a războiului, sprijinirea forțelor interne care destabilizează situația din spatele inamicului, lovituri limitate pentru a scoate din luptă

¹³⁵ In a war in which reflexive control is being employed, the side with the highest degree of reflex (the side best able to imitate the other side's thoughts or predict its behavior) will have the best chances of winning. The degree of reflex depends on many factors, the most important of which are analytical capability, general erudition and experience, and the scope of knowledge about the enemy. [t.n.], în engleză în original.

unele forțe, exploatarea și exagerarea victoriei, demonstrarea de acțiuni nemiloase și manifestarea de compasiune față de un aliat inamic care a încetat să lupte.¹³⁶ (Ionov, 1994:47, *apud* Thomas, 2004:244-245)

În timp, în acord cu perspectiva teoreticianului militar rus S.A. Komov (1997:18-22, *apud* Thomas, 2004: 248-249), conceptul de „control reflexiv” a fost înlocuit cu cel de „control intelectual”, asimilat termenului occidental de război informațional, incluzând în timp acțiuni care privesc distragerea atenției, supraîncărcarea cu informații a canalelor informaționale, înșelăciunea, producerea discordiei, descurajarea, provocarea, presiunea. Conceptul este unul important pentru Federația Rusă, utilizat în prezent și promovat prin fluxurile de narațiuni plecând de la convingerea că victoria occidentală în Războiul Rece s-a datorat inițiativelor de control reflexiv (intelectual). Totuși, odată ce conceptul occidental de operații informaționale a devenit tot mai important, el nu a rămas indiferent în Federația Rusă și, la fel cum s-a întâmplat în cazul conceptului de război hibrid, el a fost preluat ca atare și folosit cu o arie de acoperire diferită de Igor Panarin, începând cu 2006. Invocând necesitatea apărării ca urmare a acțiunilor statelor occidentale în Ucraina, Kârgâzstan, Georgia, dar și în Primăvara Arabă, șeful Statului Major General al Federației Ruse, Valerii Gherasimov, a construit ceea ce poartă numele de „doctrina Gherasimov” (2013), implicit conceptul

¹³⁶ [...] the use of superior force, force demonstrations, psychological attacks, ultimatums, threats of sanctions, threats of risk (developed by focusing attention on irrational behavior or conduct, or delegating powers to an irresponsible person), combat reconnaissance, provocative maneuvers, weapons tests, denying enemy access to or isolating certain areas, increasing the alert status of forces, forming coalitions, officially declaring war, support for internal forces destabilizing the situation in the enemy rear, limited strikes to put some forces out of action, exploiting and playing up victory, demonstrating ruthless actions, and showing mercy toward an enemy ally that has stopped fighting. [t.n.], în engleză în original.

de război hibrid (*ghibridnaia voina*) plecând de la conceptul propus în 2006 de Panarin. Perspectiva lui Igor Panarin, absolvent al școlii militare de comunicații a KGB, preia evident conținutul conceptului de „control reflexiv” sovietic și îl include în anvelopa celui de „război informațional”. În ceea ce privește viziunea oficială a Federației Ruse, elementele de „control reflexiv” erau deja acceptate și incluse în definirea războiului informațional, înțeles:

[...] ca abilitate de a... sublima sistemele politic, economic și social, de a desfășura campanii psihologice în masă împotriva populației unui stat pentru a destabiliza societatea și guvernul și de a forța un stat să ia decizii în interesul oponentilor lui.¹³⁷ (*Conceptual Views regarding the Activities of the Armed Forces of the Russian Federation in Information Space*, 2011, *apud* Thomas, 2015:12, *apud* Allen & Moore, 2018:60),

în condițiile în care un concept mai apropiat de cel occidental de operații informaționale, cel de „confruntare informațională” (*informaionnoe protivoborstvo*) încorporând efectele tehnice și psihologice asupra câmpului de luptă fusese deja definit cu copul de „a modela percepțiile și de a manipula comportamentul publicului țintă”¹³⁸ (Allen & Moore, 2018:60) și devenise operațional în mediul științific de la Moscova. Practic, în Federația Rusă au ajuns în uz trei concepte.

Elementul de referință în operarea celor trei concepte: control reflexiv/ informațional, la nivel teoretic, război informațional la nivel politic și confruntare informațională la nivel militar, este informațional, dar bulversează capacitatea de

¹³⁷ [...] as the ability to . . . undermine political, economic, and social systems; carry out mass psychological campaigns against the population of a state in order to destabilize society and the government; and force a state to make decisions in the interest of their opponents. [t.n.], în engleză în original.

¹³⁸ [...] shape perceptions and manipulate the behavior of target audiences, [t.n.], în engleză în original.

înțelegere a unui tipar acțional asupra mediului informațional. Cele trei concepte sunt aplicabile direct sau indirect atât pe timp de război, cât și pe timp de pace, fără o diferențiere precisă, așa cum este făcută în doctrinele occidentale ale operațiilor informaționale. Cele trei concepte asigură construirea unei realități alterate, convenabile Federației Ruse, în acord cu narațiunile proprii, producând neîncredere, dezordine și disensiuni în exterior (Lesenciuc *et al.*, 2025:35-44) și presupunând punerea în aplicare prin intermediul capacităților informaționale proprii în diferite conflicte contemporane. Conceptul de bază a rămas cel de război informațional propus de Igor Panarin (2006:146), conform căruia informația este văzută ca fiind armă flexibilă utilizată nu doar în domeniul militar, ci și în câmp politic, diplomatic, economic și militar. De fapt, școala de gândire rusă se bazează pe disimularea prin crearea confuziei terminologice, presupunând ca înțelesul de „război informațional” rus să fie acceptat în termenii restrictivi ai doctrinelor occidentale, cum se bazează, în conformitate cu proiecția realismului politic, și pe ideea că războiul nu se rezumă la confruntarea la nivelul puterii *hard*. Prin urmare, propaganda, instrument eminamente al puterii politice, este inclusă în războiul informațional, cum de altfel și activitatea de intelligence servește aceluiași scop. Această perspectivă are la bază ideea tributară paradigmei realiste privitoare la războiul continuu, adică la continua și constanta confruntare informațională dintre actorii statali.

Federația Rusă a aplicat războiul informațional (în varianta sa dezvoltată pe scheletul „controlului reflexiv” sovietic) pentru prima dată în conflictul din Georgia (2008), unde a optat pentru prima dată la derularea acțiunilor pe două paliere, informațional-tehnic, axat pe confruntarea cibernetică, și informațional-psihologic, axat pe confruntarea psihologică, în înțelesul occidental, completată de ample acțiuni de propagandă, cu efecte în planul relațiilor internaționale (Iasiello,

52-53). Ulterior acest război informațional în înțeles rusesc a fost purtat în timpul anexării Crimeei unde, deși existau o serie de premise similare celor care au dus la războiul georgian, efectele nu au fost similare, deoarece pe palier informațional-psihologic rușii nu au putut justifica o amenințare directă, motiv pentru care propaganda, dezinformarea și inducerea în eroare au fost extinse în special prin intermediul rețelelor sociale și au produs efecte în special pe palier politic și social, doar în subsidiar producând și argumente de ordin militar. Disimularea a atins cote stranii, în primul rând prin mimarea exercițiului democratic:

Poate că cel mai grăitor aspect al succesului a fost acela că Rusia i-a împiedicat pe cei mai mari adversari – Statele Unite și NATO – să intervină, permițând astfel organizarea unui referendum în care parlamentul Crimeei a votat pentru aderarea la Rusia. În timp ce Occidentul refuză să recunoască separarea Crimeei, Rusia cere respectarea deplină a procedurilor democratice, un fapt greu de contestat pe scena internațională¹³⁹ (Iasiello, 2017:58)

Aplicarea celor două paliere ale războiului informațional rus în conflictul din Ucraina, începând din 2014 și intensificându-se ulterior, cu un an înaintea izbucnirii războiului, a produs efecte – nu cele scontate –, dar a continuat să fie înțeles în țările democratice în limitele interpretative ale conceptului definit doctrinar, cel de operații informaționale. Practic, dezinformarea prin disimularea doctrinară a continuat

¹³⁹ Perhaps the most telling aspect of success, Russia kept its biggest adversaries—the United States and NATO—from intervening thereby enabling a referendum in which the Crimean parliament voted to join Russia. While the West refuses to acknowledge Crimea's secession, Russia attests full compliance with democratic procedures, a fact difficult to argue against on an international stage. [t.n.], în engleză în original.

și continuă, extinzând războiul informațional pe palierul puterilor *soft* și îndreptându-l și împotriva statelor care nu sunt parte la conflict.

În operarea conceptului de „război informațional” sunt esențiale înțelegerea sa contextualizată în raport cu tipul de confruntare, cu adversarul sau potențialul adversar, dar și înțelegerea altor condiții care pot conduce la redimensionarea și reconsiderarea terminologică necesare evitării inducerii în eroare prin banala utilizare a unui concept relativ clar în doctrinele occidentale.

Abrevieri

AAP-6	Allied Administrative Publication-06/ NATO Glossary of Terms and Definitions
AC	Asymetric cost
ACC	Air Combat Command
AI	Inteligență artificială/ Artificial intelligence
AJP	Allied Joint Publication
AKUF	Arbeitsgemeinschaft Krissursachenforschung
ALSA	The Air Land Sea Application
AO	Asymmetric operations
AT	Asymmetric threats
AW	Asymmetric warfare
CA	Cultural asymmetry

CAN	Computer Network Attack
CICDE	Centre interarmées de concepts et d'expérimentations
CIMIC (CMO)	Cooperarea civili-militari/ Civil-Military Co-operation
CIS	Communication and Information Systems
CMI	Interacțiune civili-militari/ Civil-Military Interactions
CMO	Operații civil-militare/ Civil-Military Operations
CND	Computer Network Defense
CNE	Computer Network Exploitation
CNO	Operații în rețele de calculatoare/ Computer Network Operations
CO	Cyberspace Operations
COMM	Centrul de Operații Mass-Media
COMSEC	Securitatea comunicațiilor/ Communications Security
COMPUSEC	Securitatea calculatoarelor/ Computer Security
CPH/ CPHS	Cyber-Physical & Human (Systems)
CSAT	Consiliul Suprem de Apărare a Țării
CW (CybW)	Război cibernetic/ Cyber Warfare
C2	Comandă-control/ Command and Control
C2S	Command and Control Systems
C2MOE	Command and Control Measures of Effectiveness
C2W	Război pentru comandă și control/ Command-and-Control Warfare
C4I	Comandă, control, comunicații, calculatoare și informații/ Command, Control, Communications, Computers & Information
C4ISR	Comandă, control, comunicații, calculatoare, informații, supraveghere și recunoaștere/ Command, Control, Communications, Computers, Intelligence, Surveillance, & Reconnaissance
DAR	Doctrina Armatei României (2012)
DBK	Dominant Battlespace Knowledge

DCO	Operații cibernetice defensive/ Defensive Cyberspace Operations
DIME	Diplomatic, informațional, military și economic (instrumentele puterii)
DIRP	Direcția Informare și Relații Publice
DoD	Department of Defense
DRDC CORA	Defence R&D Canada/ Centre for Operational Research & Analysis
DRP	Direcția Relații Publice
EBAO	Effects-Based Approach Operations
EDT	Emerging and disruptive technologies
EEFI	Essential Element of Friendly Information
EM	Electromagnetic
EMS	Managementul spectrului electromagnetic / Electromagnetic Spectrum Management
EME	Mediu electromagnetic/ Electromagnetic environment
EW	Război electronic / Electronic Warfare
FM 3-13	Inform and Influence Activities. Field Manual
GMIP	Grupul Mobil de Informare Publică
HI	Inteligență umană/ Human intelligence
HW	Războiul hackerilor/ Hacker Warfare
IA	Sprijin cu informații/ Information Assurance
IACB	Information Activities Coordination Board
IBW	Război bazat pe informații/ Intelligence-Based Warfare
ICRC	Comitetul Internațional al Crucii Roșii/ International Committee of the Red Cross
IEW	Războiul informațiilor economice/ Information Economic Warfare
ILA	International Law Association
Info Ops (INFO OPS, IO)	Operații informaționale/ Information operations
INFOSEC	Securitatea informațiilor/ Information Security
INTEL	Intelligence
IoB	Internet of Bodies
IOII	Information Operations Intelligence Integration

IoS	Internet of Senses
IoT	Internet of Things
IRC	Information-Related Capabilities
ISR	Informații, supraveghere și recunoaștere/ Intelligence, Surveillance & Reconnaissance
ISTAR	Informații, supraveghere, descoperire, identificare, localizare și cercetare a țintelor/ Intelligence, Surveillance, Target Acquisition & Reconnaissance
IW (INFO WAR)	Information Warfare
JCOIE	Joint Concept for Operating in the Information Environment
JEMSO	Operații în spectrul electromagnetic integrat/ Joint Electromagnetic Spectrum Operations
JIACG	Coordonare interagenții / Joint Interagency Coordination Group
JFC	Comandantul forței întrunite / Joint Force Commander
JP	Joint Publication
KLE	Angajarea liderilor cheie/ Key Leader Engagement
LID	Lutte informatique défensive
LIO	Lutte informatique offensive
LORANOW	Long-Range Analysis of War
LRP	Long-range penetration
L2I	Lutte informatique d'influence
MApN	Ministerul Apărării Naționale
MC	Military Committee
MEDIA OPS (Media Ops)	Operații mass-media/ Media Operations
MILDEC	Inducere în eroare/mascare/ Military Deception
Military PA (Mil PA)	Relații publice militare/ Military Public Affairs
MISO, v. PsyOps	Operații militare de susținere informațională (operații psihologice)/ Military Information Support Operations
MNFC	Comandantul forței multinaționale/

	Multinational Force Commander
MOE	Measurement of Effect
NAC	Consiliul Nord-Atlantic/ The North Atlantic Council
NATO	Organizația Tratatului Atlanticului de Nord/ North Atlantic Treaty Organization
NCW	Război Bazat pe Rețea/ Network Centric Warfare
NSA	NATO Standardization Agency
NSO	NATO Standardization Office
N2M2C2	NATO Network Enabled Capacity C2 Maturity System
OCO	Operații cibernetice ofensive/ Offensive Cyberspace Operations
OMI	Operații militare de influență/ Opérations militaires d'influence
OPLAN	Plan de operații/ Operation Plan
OPORD	Ordin de operații / Operation Order
OPSEC (Opsec)	Securitatea operațiilor / Operations Security
ORNISS	Oficiul Registrului Național al Informațiilor Secrete de Stat
PA	Relații publice/ Public Affairs
PD	Diplomație publică/ Public Diplomacy
PGM	Lovituri ghidate cu precizie / Precision guided ammunition
PIA	Publications interarmées françaises
PMESII	Politic, militar, economic, informațional, infrastructură
PPP	Prezența, postura și profilul trupelor/ Presence, Posture & Profile
PSYOPS (Psyops, PsyOp)	Operații psihologice/ Psychological operations
PSYWAR (ΨW)	Războiul psihologic/ Psychological Warfare
RBR, v. NCW	Război Bazat pe Rețea
RMA	Revoluția militară/ Revolution in Military Affairs
SIRPA	Secția de Informare și Relații Publice a Armatei

SIRPI	The Stockholm International Peace Research Institute
SMAp	Statul Major al Apărării
SMG	Statul Major General
SNap	Strategia Națională de Apărare
SO	Operații spațiale/ Space Operations
SSCB	Strategic Communication Coordination Board
STO	Operații tehnice speciale/ Special Technical Operations
StratCom (SC)	Comunicare strategică / Strategic Communication
TA	Target Audience
TRANSEC	Securitatea transmisiunilor/ Transmission Security
UCDP	Uppsala Conflict Date Program
WMD	Arme de distrugere în masă/ Weapons of mass destruction

Bibliografie

- Alberts, David S.; Garstka, John J.; Hayes, Richard E.; Signori, David A. (2001). *Understanding Information Age Warfare*. Washington, DC: CCRP Publication Series.
- Aldrich, Richard W. (1996). *The Interantional Legal Implications of Information Warfare*. INSS Occasional Paper 9. Colorado Springs, CO: USAF Institute for National Security Studies / US Air Force Academy.
- Allen, T.S. & Moore, A.J. (2018). Victory without Casualties: Russia's Information Operations. *The U.S. Army War College Quarterly: Parameters*. Vol.48, no.1. 59-71. doi:10.55540/0031-1723.2851

- Angstrom, Jan. (2005). Introduction. Debating the nature of modern war. În Isabelle Duyvesteyn & Jan Angstrom (eds.), *Rethinking the Nature of War*. Londra, New York: Frank Cass. 1-25.
- Angstrom, Jan; Widdén, J.J. (2015). *Contemporary Military Theory. The Dynamics of War*. Londra, New York: Routledge.
- Ankersen, Christopher. (2008). Introduction: interrogating civil-military cooperation. În Christopher Ankersen (ed.), *Civil-Military Cooperation in Post-Conflict Operations. Emerging Theory and Practice*. Londra, New York: Routledge. 1-12.
- Badiou, Alain. (2006). Pour une politique illimitée. In *De la limite*. Marseille: Editions Parenthèses. 146-166.
- Baskerville, Richard; Dhillon, Gurpreet. (2008). Information systems security strategy: A process view. În Detmar W. Straubb, Seymour Goodman & Richard L. Baskerville (eds.), *Information Security. Policy, Processes, and Practices*. Armonk, NY, Londra: M.E. Shape. 15-45.
- Bazargan, Saba. (2013). The permissibility of aiding and abetting unjust wars. În Thom Brooks (ed.), *Just War Theory*. Leiden: Brill. 11-28.
- Booth, Ken. (1991). Security in Anarchy: Utopian Realism in Theory and Practice. *International Affairs*. Vol. 67, no.3. 527-545.
- Booth, Ken. (2011) Realism redux: contexts, concepts, contests. În Ken Booth (ed.), *Realism and World Politics*. Londra: Routledge. 1-14.
- Bouthoul, Gaston. (1951). *Traité de sociologie. Les guerres, elements de polémologie*. Paris: Payot.
- Bouthoul, Gaston. (1978). *Războiul*. Traducere, prefață și note de Simion Pitea. București: Editura Militară.
- Boyd, Mason; Chapman, Pierce T. (eds.) (2013). *Electronic Warfare. Select Assessments of Military Capabilities and Strategies*. New York: Nova Science Publishers, Inc.
- Brennan, Brian W. (2002). Limited vs. total war. *Armor*. Sep/ Oct, 111. 5. 8-11.
- Brooks, Thom (ed.). (2013). *Just War Theory*. Leiden: Brill.
- Buffaloe, David L. (2006, September). *Defining Asymmetric Warfare*. The Land Warfare Papers, no.58. Arlington, Virginia: The

- Institute of Land Warfare, Association of the United States Army.
- Cable, James. (1993). Limited War. *International Relations*. Vol.11, issue 6. 555-569.
- Cantaragiu, Ștefan. (2001). e-Defence și societatea informațională, societatea cunoașterii [online]. *Academia Română*. URL: http://www.academiaromana.ro/pro_pri/pag_com01socinf_te_m.htm. [consultat în ianuarie 2016].
- Cha Seung-Hun; Lee Dong-Jun; Na Jae-Ho; Cho Byung-In; Jin Jong-Hyeon; Ryu Dong-Kuk; Kim Hyung-Gyoon. (2012). The Analysis Method of Command and Control Measures of Effectiveness (C2MOE). În Jong-Hyun Kim, Kansun Lee, Satoshi Tanaka & Soo-Hyun Park (eds.), *Advanced Methods, Techniques, and Applications in Modeling and Simulation. Proceedings in Information and Communications Technology* (PICT), Asia Simulation Conference, 2011, Seoul, Korea. Tokyo, Heidelberg, New York, Dordrecht, Londra: Springer. 394-402.
- Chiriac, Mircea-Dănuț; Ion, Emil; Manta, Dănuț. (2007). *Conflictul militar în epoca contemporană*. București: Editura Universității Naționale de Apărare „Carol I”.
- Cioffi-Revilla, Claudio. (2000). War and warfare. Scales of conflict in Long-Range Analysis. În R.A. Denemark, J. Friedman, B.K. Gills & G. Modelski (eds.). Londra: Routledge. 253-272.
- Clausewitz, Carl von. (1982). *Despre război*. Operă postumă a generalului Carl von Clausewitz. Studiu introductiv, note și verificarea științifică a textului de general-maior dr. Corneliu Soare. București: Editura Militară.
- Cusack, Jeremy J.; Bradfer-Lawrence, Tom; Bradham-Herd, Zachary; Castelló y Tickell, Sofia; Duporge, Isla; Hegre, Håvard; Moreno Zárate, Lara; Naude, Vincent; Nujhawan, Sahil; Wilson, John; Zambrano Cortes, Dario Gerardo & Bunnefeld, Nils. (2021). Measuring the intensity of conflicts in conservation. *Conservation Letters*. Vol.14, issue 3. <https://doi.org/10.1111/conl.12783>
- Danylyuk, Olga. (2025). Combat at Gamer's Pace. No Pause nor Reset Button. *Body, Space & Technology*, 24(1). DOI: <https://doi.org/10.16995/bst.18480>

- Dianzenza, Diaku. (2013). War or armed conflict? Thinking on ways the world view the difference between these notions [online]. *Peace & Collaborative Development Network*. URL: <http://www.internationalpeaceandconflict.org/profiles/blogs/war-or-armed-conflict-thinking-on-ways-the-world-view-the#.VmEN3cuhfMo>. [accesat în decembrie 2015].
- Ducheine, Paul A.L. (2015). Non-Kinetic Capabilities: Complementing the Kinetic Prevalence tot Targeting. În Paul A.L. Ducheine, Michael N. Schmidt & Frans P.B. Osinga (eds.), *Targeting: The Challenges of Modern Warfare*. Haga: T.M.C. ASSER PRESS / Springer Verlag. 201-230.
- European Parliament. (2020, ianuarie). *CSDP defense capabilities development*. In-depth analysis requestd by the Sub-Committee on Security and Defence. Bruxelles: Policy Department for External Relations, Directorate for External Policies of the Union.
- Freedman, Lawrence. (1994). The Theory of Limited War. În Alex Danchev & Dan Keohane (eds.), *International Perspectives on the Gulf Conflict, 1990-1991*. Londra: Palgrave Macmillan. 201-223.
- Fridman, Ofer. (2019). A War of Definitions: Hybridity in Russia and the West. În Ofer Fridman, Vitaly Kabernik & James C. Pearce, *Hybrid Conflicts and Information Warfare. New Labels, Old Politics*. Londra & Boulder, Colorado: Lynne Rienner Publishers, Inc. 67-84.
- Galula, David. [1964] (2006). *Counterinsurgency Warfare: Theory and Practice*. Foreword by John A. Nagl. Westpost, CT/ Londra: Praeger Security International.
- Gareis, Sven Bernhard. (2005) [2012]. *The United Nations. An Introduction*. Second Edition. Traducere de Lindsay P. Cohn. New York: Palgrave Macmillan.
- Garnett, John. (1970). Introduction. În John Garnett (ed.), *Theories pf Peace and Security. A Reader in Contemporary Strategic Thought*. Londra: Macmillan. St Martin's Press. 13-40.
- Garnett, John. (2007). The Causes of War and the Conditions of Peace. În John Baylis, James Wirtz, Colin S. Gray, & Eliot Cohen, *Strategy in the Contemporary World*. Oxford: Oxford University Press.

- Gherasimov, Valerii [Герасимов Валерий]. (2013, 27 februarie). Ценность науки в предвидении Новые вызовы требуют переосмыслить формы и способы ведения боевых действий (Țennosti nauki v predvidenii). Военно-Промышленный Курьер/ Voennno-Promîşlennîi Kurier. 8 (476).
- Gherman, Laurian. (2014). *Războiul electronic în era informațională*. Brașov: Editura Academiei Forțelor Aeriene „Henri Coandă”.
- Goldstein, J.H. (1989). Beliefs about human aggression. În Jo Groebel & Robert A. Hinde (eds.), *Aggression and War: Their Biological and Social Bases*. Cambridge: Cambridge University Press. 10-24.
- Gray, Colin S. [2007] (2010). *Războiul, pacea și relațiile internaționale. O introducere în istoria strategică*. Traducere de Ramona Lupu. Iași: Polirom.
- Gusti, Dimitrie. (1970). *Opere*, vol. IV. București: Editura Academiei R.S.R.
- Guvernul României. (2002, 5 iulie). Hotărâre nr. 585 din 13 iunie 2002 pentru aprobarea Standardelor naționale de protecție a informațiilor clasificate în România (HG 585). *Monitorul Oficial al României*, Partea I, nr.485.
- Harbulot, Christian. (2023) La guerre de l'information. *Centre de Recherche Appliquée de l'École de Guerre Économique* [online]. URL: <https://cr451.fr/guerre-de-information/> [Accesat în 28 decembrie 2025]
- Haywood, Roger. [1994] (2002). *Manage your Reputation. How to Plan Public Relations to Build & Protect the Organization's Most Powerful Asset*. 2nd Edition. Milford, CT: Kogan Page.
- Hentea, Călin. (2008a). Noi dimensiuni ale războiului contemporan. *Revista Română de Sociologie*, serie nou. Anul XIX, nr.2-4. 289-306.
- Hentea, Călin. (2008b). *Noile haine ale propagandei*, Pitești: Editura Paralela 45.
- Hirst, Paul. (2001). *Război și putere în secolul 21. Statul, conflictul militar și sistemul internațional*. Traducere de Nicolae Năstase. București: Antet XX Press.

- Hoffman, Frank. (2007). *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington, VA: Potomac Institute for Policy Studies.
- Iasiello, E.J. (2017). Russia's Improved Information Operations: From Georgia to Crimea. *The US Army War College Quarterly: Parameters*. Vol. 47, doi:10.55540/0031-1723.2931
- International Law Association (ILA)/ Committee on the Use of Force. (2008). Report. Initial Report on the Meaning of Armed Conflict in International Law. *The 73rd Conference of the International Law Association*. Brazilia: Rio de Janeiro, 17-21 august.
- Kaurin, Pauline M. (2014). *The Warrior, Military Ethics and Contemporary Warfare. Achilles Goes Asymmetrical*. Farnham, Surrey/ Burlington, VT: Ashgate.
- Kitzen, Martijn. (2012). Close Encounters on the Tribal Kind: the Implementation of Co-Operation as a Tool for De-escalation of Conflict – The case of Netherlands in Afganisthan's Uruzgan Province. *Journal of Strategic Studies*, vol. 35, issue 5 (Special Issue: The Escalation and De-escalation of Irregular War). 713-734.
- Kuru, Husseyin. (2018). Evolution of war and cyber=attacks in the concept of conventional warfare. *Journal of Learning and Teaching in Digital Age*. 3(1), 12-20
- Lesenciuc, Adrian. (2010). *Teoria comunicării*. Braşov: Editura Academiei Forţelor Aeriene „Henri Coandă”.
- Lesenciuc, Adrian. (2013). *Operaţiile mass-media. Echilibrul instabil dintre logica militară şi logica media*. Braşov: Editura Academiei Forţelor Aeriene „Henri Coandă”.
- Lesenciuc, Adrian. (2014). *Introducere în arta militară*. Braşov: Editura Academiei Forţelor Aeriene „Henri Coandă”.
- Lesenciuc, Adrian. (2016). *Războiul informaţional*. Ediţia I. Braşov: Editura Academiei Forţelor Aeriene „Henri Coandă”.
- Lesenciuc, Adrian. (2023). *Războiul hibrid sau întoarcerea din disimulare la războiul absolut*. Bucureşti: Centrul Tehnic-Editorial al Armatei (CTEA).
- Lesenciuc, Adrian. (2024). Defective truth. Ai or HI ideological imprints and political biases? *Romanian Journal of*

- Information Technology and Automatic Control*. Vol. 34, No. 3. 9-22. <https://doi.org/10.33436/v34i3y202401>
- Lesenciuc, Adrian; Sauciuc, Iasmina-Georgian & Jagiełło-Tondera, Agata. (2025). *Nobody: The name behind informational blindness. The Russian information warfare in Ukraine. Redefining Community in Intercultural Context*. Vol.12, nr.1. 35-44.
- Libicki, Martin C. (1995). *What is Information Warfare?* Washington, DC: Center for Advanced Concepts and Technology Institute for National Strategic Studies/ National Defense University.
- Liddell Hart, B.H. (1967) *Strategy*. Second revised edition. New York, NY: Fredrick A. Praeger Publishers
- Marshall, Monty G. (2002). Measuring the Societal Impact of War. În Osler Hampton & David M. Malone, *From Reaction to Conflict Prevention. Opportunities for the UN System*. A Project of the International Peace Academy. Londra: Lynne Rienner Publishers/ Boulder. 63-104.
- Mattis, James N. & Hoffman, Frank. (2005). Future Warfare: The Rise of Hybrid Wars. *US Naval Institute Proceedings*. Vol. 131 no.11.
- McFate, Montgomery. (1994). *Pax Britannica. British Counterinsurgency in Northern Ireland 1969-1982*. A Dissertation Presented to the Faculty of the graduate School of Yale University in Candidacy for the Degree of Doctor of Philosophy. [Electronic edition]. New York: Wilberforce Codex.
- McLuhan, Marshall. (1994). *Understanding Media: The Extensions Of Man*. Cambridge, MA: MIT Press.
- McMahan, Jeff. (2006). Război și pace. În Peter Singer (ed.), *Tratat de etică*. Traducere de prof.univ.dr. Vasile Boari și Raluca Mărincean. Cuvânt înainte de Vasile Boari. Iași: Polirom.
- Meron, Theodor. (1999). Classification of Armed Conflict in the former Yugoslavia: *Nicaragua's* Fallout. În *War Crimes Law Comes of Age: Essays*. Oxford: Oxford Academic. 286-295. <https://doi.org/10.1093/acprof:oso/9780198268567.003.0016>
- Ministère des Armées. (2021). *Éléments publiques de doctrine militaire de lutte informatique d'influence (L2I)*. Paris: COMCYBER.

- Ministerul Apărării Naționale. (2020). Ordin pentru aprobarea Instrucțiunilor privind activitatea de Informare și Realții Publice în Ministerul Apărării Naționale (M.103). *Monitorul Oficial al României*. nr. 474/ 4 iunie.
- Morgenthau, Hans J. (1949). *Politics among Nations. The Struggle for Power and Peace*. New York: Alfred A. Knopf.
- Neculcea, Cosmina-Andreea & Răpan, Florian. (2022). Operațiunile informaționale – analiză doctrinară comparativă. *Impact strategic*. Nr. 2-3-4. 69-80. doi: 10.53477/1842-810X-22-14
- Nicolaescu, Gheorghe; Simileanu, Vasile. (2004). *Informație, management, putere. Vol.2. Război informațional*. Cuvânt introductiv de Eugen Bădălan. București: Editura Top Form.
- Nițu, Costinel. (2010). Contramăsuri specifice CCD în operații ofensive. *Buletinul Universității Naționale de Apărare „Carol I”*. Nr.1. 386-392.
- Nye jr., Joseph S. (2005). *Descifrarea conflictelor internaționale. Teorie și istorie*. Traducere de Ion Vlădoiu. București: Antet XX Press.
- Orzeață, Mihail. (2011). *Războiul continuu*. București: Editura Militară.
- Palathra, Aakash. (2024). Drones and the Gamification of War. *Journal of Foreign Affairs at Carolina* [online]. URL: <https://jfacunc.org/blog/drones-and-the-gamification-of-war> [Accesat în 22 decembrie 2025]
- Panarin, Igor. (2006). *Informatsionnaya voyna i geopolitika*. Moscova: Pokolenie.
- Paulus, Andreas; Vashakmadze, Mindia. (2009). Asymmetrical war and the notion of armed conflict – a tentative conceptualization. *International Review of the Red Cross*. Vol. 91, no.873. 95-125.
- Psarros, Nikolaos. (2023) The Nature of War. *Conatus* 8, no. 2 (2023): 457-475 doi: <https://doi.org/10.12681/cjp.35271>
- Raska, Michael. (2016). *Military Innovation in Small States. Creating a Reverse Asymmetry*. Abingdon, OX, New York, NY: Routledge.
- Regehr, Ernie. (2011). Armed Conflict: Trends and Drivers. *The Simons Foundation Canada* [online]. URL:

- <https://www.thesimonsfoundation.ca/resources/armed-conflict-trends-and-drivers> [Accesat în 22 decembrie 2025]
- Roberts, Michael. [1956] (1995). *The Military Revolution, 1560-1660*. În Clifford J. Rogers (ed.), *The Military Revolution Debate. Readings on the Military Transformation of Early Modern Europe*. Boulder, Colorado, Oxford: Westview Press. 13-36.
- Roberts, S.J.L. (2004). Media Operations: Lessons from Kosovo. In Stephen Badsey, Paul Latawski (eds.), *Britain, NATO and the Lessons of the Balkan Conflicts 1991-1999*. Introducere de Geoffroy Hoon. Londra, New York: Frank Cass. 67-78.
- Roman, Cosmina-Oana. (2020a). *Introducere în CIMIC*. Braşov: Editura Academiei Forţelor Aeriene „Henri Coandă”.
- Roman, Cosmina-Oana. (2020b). *CIMIC în coordonarea Forţelor Aeriene Române. Baltica 2007*. Braşov: Editura Academiei Forţelor Aeriene „Henri Coandă”.
- Ryan, Klem. (2012). *Fair and Unfair Wars*. Oxford: Oxford University Press.
- Sezal, Mustafa. (2019). *Origins of Differentiation in Critical Security Schools: A philosophic-genealogical search for emancipatory roots*. Unpublished PhD Thesis. Groningen: University of Groningen..
- Singer, J. David. (1989). The political origins of international war: a multifactorial review. În Jo Groebel & Robert A. Hinde (eds.), *Aggression and War: Their Biological and Social Bases*. Cambridge: Cambridge University Press. 202-229.
- Soare, Corneliu. (1993). *Recitindu-l pe Clausewitz*. Bucureşti: Editura Militară.
- Sullivan, Andrew. (2011). *Some Considerations in Developing Effective Messaging. The SUCCEsS Framework and Military Influence Activities*. DRDC CORA CR 2011-004. Kingston, ON: Defence R&D Canada/ Centre for Operational Research & Analysis / Strategic Analysis Section.
- Sun Tzu. (1999). *Arta războiului*. Traducere din limba franceză de Raluca Pârvu. Bucureşti: Antet XX Press.
- Taylor, Maxwell D. (1960). *The Uncertain Trumpet*. New York: Harper and Brothers.

- Thomas, T.L. (2004). Russia's Reflexive Control Theory and the Military. *The Journal of Slavic Military Studies*. 17. 237-256.
- Thomas, T.L. (2007). Dialectical versus empirical thinking: Ten key elements of the Russian understanding of information operations. *The Journal of Slavic Military Studies*. 11(1). 40-62. <https://doi.org/10.1080/13518049808430328>
- Uppsala Conflict Data Program (UCDP). (2025). UCDP Definitions. *Uppsala Universitet* [online]. URL: <https://www.uu.se/en/departament/peace-and-conflict-research/research/ucdp/ucdp-definitions> [Accesat în 22 decembrie 2025]
- von Bertalanffy, Ludwig. (1968). *General System Theory. Foundations, Development, Applications*. New York: George Braziller.
- Walzer, Michael. (1977). *Just and Unjust Wars. A Moral Argument with Historical Illustrations*. New York: Basic Books.
- Wolfendale, Jessica. (2017). Defining War. În Michael L. Gross & Tamar Meisels (eds.) *Soft Wars. The Ethics of Unarmed Conflicts*. Cambridge: Cambridge University Press. 16-32.
- Zafiu, Rodica. (2021). „Narativul” și „narativa”. *Dilema Veche*. nr.916/ 28 oct. – 3 nov.
- ***. (1977). Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (protocol I), 8 June 1977 [online]. *International Committee of the Red Cross (ICRC). Treaties, states parties and commentaries*. URL: <https://www.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?action=openDocument&documentId=D9E6B6264D7723C3C12563CD002D6CE4>. [consultat în decembrie, 2015].
- ***. (2006). *Military Deception. Joint Publication 3-13.4 (Formerly JP 3-58)*. (JP 3-13.4). Washington, DC: Joint Staff.
- ***. (2007). *Electronic Warfare. Joint Publication 3-13.1*. (JP 3-13.1). Washington, DC: Joint Staff.
- ***. (2007, Septembrie). *Media Operations. Joint Doctrine Publication 3-45.1*. (JDP 3-45.1). Shrivenham, Swindon: The Development, Concepts and Doctrine Centre, Ministry of Defence.

- ***. (2007, 19 martie). *NATO Military Policy on Information Operations* (MC 0422/3) [study draft]. Bruxelles: NATO Military Committee.
- ***. (2008). *Doctrine Interarmées des Opérations Militaires d'Influence*, PIA 03.253. Paris: Ministère de la Défense / État-Major des Armées/CICDE. N°069 DEF/CICDE/NP.
- ***. (2008, 8 iulie). *Civil-Military Operations* (JP 3-57). Washington, DC: Joint Staff.
- ***. (2009). *Allied Joint Doctrine for Information Operations*. (AJP-3.10). Bruxelles: NATO Standardization Agency (NSA).
- ***. (2012, 20 iulie). *NATO Military Policy on Information Operations* (MC 0422/4). Bruxelles: NATO Military Committee.
- ***. (2013). *Allied Joint Doctrine for Civil-Military Cooperation. Allied Joint Publication-3.4.9* (AJP 3.4.9). Edition A Version 1. Bruxelles: NATO Standardization Agency (NSA).
- ***. (2013). *Field Manual No.3-13. Inform and Influence Activities* (FM 3-13). Washington, DC: Department of the Army.
- ***. (2014). *Joint Publication 3-13. Information Operations*. (JP 3-13). Washington, DC: Joint Staff.
- ***. (2014). *Joint Doctrine Publication 01. UK Joint Operations Doctrine* (JDP-01). Swindon, Wiltshire: The Development, Concepts and Doctrine Center.
- ***. (2015). *Allied Joint Doctrine for Information Operations* (AJP-3.10). Edition A Version 1. Bruxelles: NATO Standardization Office (NSO).
- ***. (2015). *Allied Joint Doctrine for Psychological Operations. Allied Joint Publication-3.10.1* (AJP-3.10.1). Edition B Version 1, with UK National Elements. Bruxelles: NATO Standardization Office (NSO).
- ***. (2018, 25 iulie). *Joint Concept for Operating in the Information Environment (JCOIE)*. Washington, DC: Joint Chiefs of Staff.
- ***. (2022). *Allied Joint Doctrine* (AJP-01). Edition F Version 1. Bruxelles: NATO Standardization Office (NSO).

- ***. (2023, ianuarie). *Allied Joint Doctrine for Information Operations* (AJP-3.10). Edition A Version 1. Bruxelles: NATO Standardization Office (NSO).
- ***. (2023, martie). *Allied Joint Doctrine for Strategic Communications* (AJP-10). Edition A, Version 1. Bruxelles: NATO Standardization Office (NSO).
- ***. (2025, august). *Allied Joint Doctrine for the Conduct of Operations*. Edition D, Version 1. Bruxelles: NATO Standardization Office (NSO).