DOI: 10.53477/1842-810X-22-14

OPERAŢIILE INFORMAŢIONALE – ANALIZĂ DOCTRINARĂ COMPARATIVĂ

Cosmina-Andreea NECULCEA*
Dr. Florian RĂPAN**

Scopul prezentului articol este acela de a identifica diferențele de proiecție doctrinară la nivelul Alianţei Nord-Atlantice. Articolul este conceput ca un studiu comparativ al proiecţiilor doctrinare specifice operațiilor informaționale (InfoOps) asupra cărora ne-am îndreptat atenţia: doctrinele şi manualele de luptă ale Statelor Unite ale Americii, ca inițiator al majorității acestor documente − doctrinele NATO şi doctrinele autohtone. La o primă analiză a celor trei proiecţii doctrinare, se poate observa că există diferențe în abordarea InfoOps, atât în ceea ce privește elementele de suprafață, recunoscute prin markeri identificabili, cât şi diferențele de perspectivă, care permit şi încurajează interpretarea. Este nevoie, aşadar, de clarificarea naturii InfoOps şi înţelegerea corectă a acestora din punct de vedere conceptual şi practic, precum şi de obţinerea unei coerenţe între doctrinele pentru operaţii informaţionale ale statelor membre NATO şi doctrina aliată.

Cuvinte-cheie: *operaţii informaţionale; doctrine; analiză comparativă; diferenţe; interoperabilitate doctrinară.*

*
* *

În elaborarea articolului, am pornit de la premisa identificării diferențelor de proiecție doctrinară în aparatele doctrinare american, românesc și cel al NATO, cu intenția de a contribui la un grad mai ridicat de interoperabilitate pentru acțiunile și exercițiile comune în domeniul operațiilor informaționale. În acest sens, am

**** Locotenent Cosmina-Andreea NECULCEA este asistent universitar în cadrul Academiei Forţelor Aeriene „Henri Coandă”, Braşov, şi doctorand în cadrul Şcolii Doctorale a Universităţii Naţionale de Apărare „Carol I”, Braşov, România. E-mail: saghincosmina@yahoo.com***
***** Gl.mr.(rez.) prof.univ.dr. Florian RĂPAN este cadru didactic la Universitatea Creștină „Dimitrie Cantemir”, Bucureşti, România. E-mail: rapan_florian@yahoo.com***

apelat la analiza de conținut a doctrinelor operațiilor informaționale și, ulterior, la o comparare a acestora din trei perspective: al definirii conceptului și domeniilor cheie, al identificării principiilor în baza cărora funcționează și al identificării structurii funcționale și a diferențelor de suprafață și de profunzime în aplicarea fiecăruia dintre domeniile cheie ale operațiilor informaționale, în doctrina americană, românească și NATO.

Introducere

Odată cu trecerea timpului s-a schimbat şi natura conflictelor, iar unul dintre factorii determinanţi ai războiului și cel care a condus la modelarea conceptelor a fost *tehnologia*. În trecut, diferenţele dintre capacităţile tehnologice ale adversarilor constituiau principalul element diferenţiator şi, împreună cu nivelul asimetriei din perspectiva numărului de beligeranţi implicaţi în conflict, erau esenţiale pentru câştigarea superiorităţii. În zilele noastre, fluxul de informaţii extins, scăderea numărului de militari implicaţi în operaţii (scăderea densităţii de ocupare a câmpului de luptă), precum şi influenţa exercitată de tehnologie, au făcut ca obţinerea superiorităţii informaţionale, care poate fi interpretată doar în operaţiile clasice, să devină principalul obiectiv. Pe lângă cele cinci domenii operaţionale, terestru, aerian, maritim, spaţial şi cibernetic, mintea umană poate fi considerată un nou domeniu al operaţiilor (chiar dacă nu a devenit domeniu de sine stătător, cel cognitiv este în curs de recunoaștere și în armatele occidentale; în doctrina chineză este legiferat ca atare). De exemplu, *Doctrina pentru operaţii informaţionale* a Statelor Unite ale Americii, *JP 3-13/Information Operations* subliniază importanţa influenţării omului şi conferă dimensiunii cognitive statutul de cea mai importantă dimensiune a mediului informaţional.

La nivelul Alianţei, *Doctrina Întrunită Aliată a NATO pentru Operaţii Informaţionale*, publicată în anul 2015, AJP-3.10/*Allied Joint Doctrine for Information Operations* subliniază influenţa tendinţelor globale asupra factorului uman şi a dinamicii puterii globale, creând instabilitate şi mărind, totodată, probabilitatea de conflict. Importanţa şi complexitatea mediului informaţional, precum şi natura schimbătoare a securităţii globale, au determinat NATO să-şi dezvolte şi să-şi adapteze în permanenţă conceptele şi doctrinele, pentru a face faţă noilor provocări.

În proiecţia doctrinară românească, **InfoOps**[1] vin în sprijinul operaţiilor întrunite, fiind considerate cel mai adecvat răspuns la ameninţările contemporane.

[1] Pentru coerența și coeziunea conținutului prezentului articol și din rațiuni de unitate conceptuală, am optat pentru abrevierea **InfoOps**, din cadrul doctrinar românesc.

1. Definiţiile InfoOps în proiecţiile doctrinare NATO, SUA şi cea românească

Schimbările rapide care au avut loc în mediul informaţional, experienţele de pe câmpul de luptă, precum şi lecţiile învăţate din conflictele recente au determinat statele membre ale Alianţei să se orienteze tot mai mult asupra conceptului *operaţii informaţionale* şi a conştientizării importanţei acestora. Preocuparea asupra politicilor şi doctrinelor InfoOps atât la nivelul Alianţei, cât şi la nivelul altor naţiuni, a început în anii 1990, când multor operaţii militare le-au fost atribuite obiective InfoOps.

SUA, ca iniţiator al majorităţii documentelor doctrinare de la nivelul Alianţei, au abordat pentru prima dată contextul operaţional al InfoOps în Manualul de luptă al armatei americane FM 100-6/ Information Operations, ce sublinia expansiunea continuă a mass-media şi aprecia că „această new era, aşa-numita Eră Informaţională, oferă oportunităţi unice, precum şi unele provocări extraordinare" (Headquarters, Department of the Army 1996, iv.). În anul 1998, a apărut prima doctrină pentru operaţii informaţionale în context întrunit, JP 3-13/ Joint Doctrine for Information Operations, iar operaţiile informaţionale au primit o definiţie foarte asemănătoare cu ce se înţelege astăzi prin operaţii în spaţiul cibernetic. De asemenea, *războiul informaţional* era descris ca fiind „operaţii informaţionale desfăşurate pe timp de criză sau conflict (inclusiv război), pentru îndeplinirea sau promovarea obiectivelor specifice asupra unui adversar sau adversari". (Joint Chiefs of Staff 1998, I-1) Apariţia unei noi doctrine, în anul 2006, a condus la renunţarea folosirii termenului de *război informaţional* în favoarea termenului *operaţii informaţionale* şi a introdus conceptul de *mediu informaţional*.

Conform doctrinei din 2006, principalul obiectiv al InfoOps era „obţinerea şi menţinerea superiorităţii informaţionale pentru SUA şi pentru aliaţi" (Joint Chiefs of Staff 2006, ix.), pentru a „creşte libertatea de acţiune a comandanţilor şi de a le permite să ia decizii şi să menţină iniţiativa, rămânând în acelaşi timp în cadrul ciclului de decizie al adversarului" (Joint Chiefs of Staff 2006, 1-5). Doctrina curentă proiectează superioritatea informaţiei doar în relaţie cu *asigurarea informaţiilor/ information assurance/ IA*[2]. În ambele doctrine, mediul informaţional este descris ca fiind „ansamblul persoanelor, organizaţiilor şi sistemelor care colectează, procesează, diseminează sau acţionează asupra informaţiilor" (Joint Chiefs of Staff 2014, ix.) şi cuprinde trei dimensiuni: fizică, informaţională şi cognitivă, care interacţionează permanent cu indivizii, organizaţiile şi sistemele.

Abordarea InfoOps din perspectiva SUA este puțin diferită față de cea NATO sau cea românească pentru că nu oferă o definiție, ci mai degrabă le consideră a fi

[2] „Asigurarea cu informații (IA) este necesară pentru obținerea și menținerea superiorității informaționale". JP 3-13/2014, p. II-9. Aici superioritatea informațională înseamnă „avantajul operațional derivat din abilitatea de a colecta, procesa și disemina un flux neîntrerupt de informații, în timp ce se exploatează sau neagă abilitatea unui adversar de a face același lucru".

„angajarea integrată, în timpul operațiilor militare, a capabilităților informaționale (information-related capabilities/IRC) împreună cu alte linii de operare pentru a influența, perturba, corupe sau împiedica luarea deciziilor de către adversari sau potențiali adversari, protejându-le în același timp pe cele proprii" (Joint Chiefs of Staff 2014, ix). Capacităţile informaţionale sunt „instrumente, tehnici şi activităţi care afectează oricare dintre cele trei dimensiuni ale mediului informaţional" (Joint Chiefs of Staff 2014, x) și sunt puse la dispoziția comandantului pentru a afecta cele trei dimensiuni ale mediului informaţional.

În operaţiile desfăşurate de Alianţă, InfoOps au jucat un rol deosebit, rol care a fost analizat şi reflectat atât în lucrările teoretice, cât şi în doctrine şi manuale, presupunând efecte directe pe câmpul de luptă. Pentru NATO, înţelegerea comună a operaţiilor informaţionale părea să fie crucială pentru a face faţă provocărilor. În acest context, AJP-3.10/ Allied Joint Doctrine For Information Operations, publicată în 2009, definea operaţiile informaţionale astfel: „InfoOps reprezintă o funcție militară care asigură consultanță și coordonare a activităților informaționale militare pentru a crea efectele dorite asupra voinței, înțelegerii şi capacității adversarilor, potențialilor adversari și altor părți aprobate de Consiliul Nord-Atlantic (NAC) în sprijinul obiectivelor misiunii Alianței". (NATO Standardization Agency 2009, 1-3.)

Cu scopul de a defini operaţiile de influenţare, descrierea de mai sus a fost completată de o altă expresie, *activităţi informaţionale*, definite ca „acțiuni menite să producă efecte asupra informațiilor și/ sau sistemelor informaționale. Ele pot fi realizate de orice actor şi includ măsuri de protecție". (NATO Standardization Agency 2009, 1-3.) Șase ani mai târziu apare o nouă doctrină aliată AJP-3.10/ 2015, care nu aduce modificări substanţiale definiţiilor din doctrina precedentă.

La nivel naţional, conceptul *operaţii informaţionale* a fost implementat în Armata Română în anul 2006, odată cu apariţia Doctrinei Operaţiilor Informaţionale, care urmărea realizarea unui cadru general pentru planificarea, desfăşurarea şi evaluarea efectelor operaţiilor informaţionale, la nivel operativ şi tactic. Ulterior, în anul 2011 apare o nouă doctrină, Doctrina pentru operaţii informaţionale a Armatei României*,* care urmărea alinierea la documentul NATO din 2009. Apariţia noilor tipuri de ameninţări, precum cea hibridă, au determinat armatele moderne şi, implicit, Armata României să formuleze noi răspunsuri. Prin urmare, în anul 2017, apare o nouă doctrină, cea care este în vigoare şi astăzi, Doctrina Operaţiilor Informaţionale*,* doctrină ce subliniază rolul şi importanţa operaţiilor informaţionale în mediul de operare contemporan. Definiţia operaţiilor informaţionale este foarte asemănătoare cu cea din doctrina aliată: „o funcţie de stat major, destinată analizei, planificării, evaluării şi integrării tuturor activităţilor informaţionale, în vederea obţinerii efectelor dorite asupra voinţei, capacităţii de înţelegere, percepţiei şi capabilităţilor adversarilor, potenţialilor adversari şi a audienţelor ţintă aprobate de CSAT, în sprijinul îndeplinirii obiectivelor militare". (Statul Major General 2017, 13.)

Având în vedere analiza comparativă a definiţiilor InfoOps din perspectivă diacronică, putem afirma că InfoOps rămân un subiect complex, care are nevoie de o înţelegere clară şi concisă. De exemplu, în timp ce definiția InfoOps din doctrina americană limitează coordonarea și sincronizarea InfoOps doar pe timpul operațiilor militare, definițiile celorlalte două proiecții analizate nu specifică acest lucru. În concepția americană, InfoOps se bazează pe alte capacități informaționale pentru a crea efecte la un moment specific, în și prin mediul informațional, oferindu-i comandantului capacitatea de a obține un avantaj operațional. În timp ce aceste IRC creează propriile efecte, InfoOps reprezintă agregarea acestor efecte, acțiune văzută ca fiind esențială pentru atingerea obiectivelor.

În vreme ce doctrinele NATO și cea românească menționează, într-o manieră generală, că scopul InfoOps este acela de a crea efectele dorite, definiția americană este mult mai specifică, scopul InfoOps fiind acela de a influența, perturba, corupe sau împiedica (influence, disrupt, corrupt, usurp) luarea deciziilor adversarilor sau a potențialilor adversari. Ținând cont de cele trei dimensiuni ale mediului informațional, efectele cognitive manifestate prin modificarea comportamentului sunt cele mai importante pentru obținerea unor rezultate decisive, dar au nevoie de timp pentru a se manifesta, comparativ cu efectele în dimensiunea fizică și informațională, care pot fi imediate.

Evoluția continuă a domeniului informațional impune mai mult ca niciodată necesitatea actualizării permanente a acestor definiţii pentru garantarea unei viziuni clare asupra a ceea ce înseamnă complexitatea InfoOps. Totodată, definițiile diferite în cele trei proiecții doctrinare vor conduce la interpretări diferite, iar aceste interpretări pot duce la eșecuri strategice.

2. Principiile InfoOps în proiecţiile doctrinare NATO, SUA şi cea românească

La baza planificării şi desfăşurării operaţiilor informaţionale se află un set de principii, ce au rolul de a direcţiona activităţile cu impact asupra mediului informaţional în sprijinul întregii game de operaţii militare, precum şi integrarea în procesul de selectare a ţintelor.

Doctrina operaţiilor informaţionale prezintă un număr de zece principii care stau la baza planificării şi desfăşurării operaţiilor informaţionale, principii ce sunt preluate, în mare măsură, din doctrina NATO, din 2009, cu unele modificări sau completări.

O primă diferenţă identificată este aceea că doctrina întrunită aliată cuprinde un set de nouă principii, în timp ce, la nivel naţional, setul iniţial de nouă principii a fost completat cu al zecelea, *adaptabilitatea*. De asemenea, se observă că principiile nu sunt enumerate identic, principiile 7 şi 8 schimbându-şi locurile.

În altă ordine de idei, doctrina aliată pentru operaţii informaţionale, din 2015, se remarcă printr-un set diferit de principii, faţă de doctrina precedentă, după cum se poate observa în tabelul următor:

Tabelul nr. 1: Principiile InfoOps conform doctrinei româneşti şi cea a NATO

Nr. crt.	Doctrina operațiilor informaționale/ 2017	AJP-3.10/ Allied Joint Doctrine for Information Operations/ 2009	AJP-3.10/ Allied Joint Doctrine for Information Operations/ 2015
1.	Abordarea cuprinzătoare a operației	Abordarea operaţiilor pe baza efectelor	Concentrarea și integrarea
2.	Precizările comandantului şi implicarea personală a acestuia	Precizările comandantului şi implicarea personală a acestuia	Coerența și consistența
3.	Coordonarea şi sincronizarea permanentă	Coordonarea şi sincronizarea permanentă	Înțelegere cuprinzătoare
4.	Acurateţea informaţiilor pe care se fundamentează deciziile	Acurateţea informaţiilor	Planificarea centralizată şi execuţia descentralizată
5.	Planificarea centralizată şi execuţia descentralizată	Planificarea centralizată şi execuţia descentralizată	Continuitatea
6.	Contribuţia la procesul de management întrunit al ţintelor	Contribuţia la procesul de management întrunit al ţintelor	Monitorizarea şi evaluarea
7.	Continuitatea	Implicarea timpurie şi pregătirea oportună	Agilitatea
8.	Implicarea timpurie şi pregătirea oportună	Continuitatea	-
9.	Monitorizarea şi evaluarea efectelor	Monitorizarea şi evaluarea	-
10.	Adaptabilitatea	-	-

Una dintre componentele durabile ale doctrinei este reprezentată de principii, pentru că acestea reprezintă baza conducerii operaţiilor militare şi trebuie să fie aplicate la scară largă, indiferent de contextul operaţional. Am putea afirma că, odată ce în doctrine regăsim principii diferite, acest lucru poate fi văzut şi ca simplu decalaj conceptual. Această analiză a diferențelor în proiecția principiilor operațiilor informaționale sunt markeri identificabili sau elemente de suprafață în analiza doctrinară comparativă.

3. Domeniile cheie coordonate în cadrul InfoOps, conform proiecţiilor doctrinare NATO, SUA şi cea românească

Încadrabile în aceeași categorie a elementelor de suprafață, domeniile cheie diferă în măsură mai mare între aparatele conceptuale analizate. Prima diferenţă vizează tocmai denumirea/încadrarea listei de activităţi sub umbrela InfoOps. Doctrina românească a operaţiilor informaţionale proiectează o serie de 12 **domenii**

cheie: operaţii psihologice (PSYOPS), prezenţa, profilul şi postura trupelor (PPP), securitatea operaţiilor (OPSEC), securitatea informaţiilor (INFOSEC), inducerea în eroare, războiul electronic (EW), distrugerea fizică, angajarea liderilor cheie (KLE), angajarea la nivelul militarului, operaţii în spaţiul cibernetic, apărarea cibernetică şi relaţiile civil-militare (CIMIC), subordonate şi coordonate în cadrul InfoOps, cu menţiunea că „ele pot fi considerate activităţi în cadrul InfoOps numai atunci când sunt îndreptate direct asupra capacităţii de înţelegere şi percepţie, voinţei şi capabilităţilor sau mijloacelor adversarului, potenţialului adversar sau altor entităţi aprobate”. (Statul Major General 2017, 22)

Doctrina NATO, AJP-3.10/ 2015, include domeniile cheie InfoOps într-o categorie distinctă, intitulată Capabilități și Tehnici integrate prin InfoOps/ Capabilities and Techniques Integrated Through Information Operations. Cu toate că lista nu este una exhaustivă, capabilităţile şi tehnicile enumerate reprezintă baza majorităţii activităţilor InfoOps. De asemenea, actuala doctrină a completat lista de capabilități din doctrina precedentă cu alte trei capabilităţi, precum Capabilități speciale, Afaceri Publice Militare, Înțelegerea Culturală și angajarea/Special capabilities, Military Public Affairs şi Cultural understanding and engagement şi a exclus securitatea informaţională/INFOSEC (NATO Standardization Office 2015, 1-10).

În SUA, doctrina pentru operaţii informaţionale JP 3-13/ Information Operations, din 2014, enumeră o serie de capacităţi care contribuie la InfoOps, pe care le încadrează la rubrica Relationship and Integration, după cum urmează: comunicarea strategică, grupul de coordonare întrunită interagenții, afacerile publice, operaţiile civil-militare, operaţiile în spaţiul cibernetic, asigurarea informaţională, operaţiile în spaţiul cosmic, operaţiile de sprijin al informaţiilor militare/MISO (în ediţiile anterioare ale doctrinelor, operaţii psihologice sau PSYOP), intelligence, inducerea în eroare, securitatea operaţiilor, operațiile tehnice speciale, operațiile întrunite privitoare la spectrul electromagnetic, angajarea liderilor cheie. (Joint Chiefs of Staff, 2014, II-5)

A doua diferenţă izvorăşte din diferenţele de terminologie. Aceasta include și elemente de suprafață, markeri direct identificabili în ceea ce privește strict denumirea, dar și aspecte de profunzime sau diferențe de perspectivă în ceea ce privește filozofia și fizionomia domeniilor cheie implicate. În ceea ce priveşte operaţiile psihologice, cu acronimul PSYOPS, utilizat de majoritatea statelor NATO, în anul 2011, la nivelul SUA s-a produs o schimbare terminologică, prin înlocuirea acronimului PSYOP cu **MISO** (Operaţii de Sprijin al Informaţiilor Militare/Military Information Support Operations), dar această schimbare nu a produs efecte considerabile. Conform locotenent-colonelului Robert Bockholt, purtător de cuvânt al Comandamentului pentru Operaţii Speciale al SUA, „Forțele Operațiilor Psihologice conduc Operațiile de Sprijin a Informațiilor Militare”, iar „operațiile psihologice fac referire la numele unităților, în vreme ce MISO fac referire la funcția pe care o îndeplinesc militarii din unitățile PSYOPS”. (Myers 2017)

De asemenea, în comparaţie cu operaţiile mass-media şi activităţile de informare şi relaţii publice, activităţile PSYOPS deţin controlul asupra conţinutului şi a mijloacelor de diseminare a informaţiilor şi, implicit, presupun focalizarea pe activitatea de influenţare prin intermediul acestora, adică pe atingerea anumitor efecte scontate ale conţinuturilor transmise. Spre exemplu, abordarea rusă a InfoOps privind securitatea informaţiilor urmăreşte nu doar garantarea integrităţii tehnice a informaţiilor, ci şi producerea efectului cognitiv scontat. De asemenea, Rusia se concentrează pe influenţarea percepţiilor audienţei ţintă, în timp ce Occidentul este constrâns mai degrabă de obiectivitatea informaţiilor. (Prats i Amorós 2019, 16) Aceste exemple permit o înțelegere a problematicii ca urmare a diferenței de perspectivă în mai mare măsură decât ca urmare a simplei diferențe de suprafață, adică a numirii.

Două domenii cheie care înglobează aspectele ofensive şi defensive ale InfoOps în spaţiul cibernetic sunt *operaţiile în spaţiul cibernetic* şi *apărarea cibernetică.* Termenul *cibernetic* este folosit şi în proiecţia doctrinară americană, prin denumirea *cyberspace operations.* În schimb, la nivel NATO, doctrina din 2009 a rămas la formularea *operaţii în reţele de calculatoare/computer network operations (atac, exploatare şi apărare/*atack, exploitation and defence*),* iar cea din 2015 se rezumă doar la *computer network attack* şi *computer network exploitation.*

Prin intermediul războiului electronic/EW, armatele încearcă să domine spectrul electromagnetic, prin cele trei tipuri de acțiuni EW: protecţie electronică, atac electronic şi sprijin electronic. Echivalentul EW la nivelul SUA constă în *operații întrunite de management al spectrului electromagnetic/JEMSO*, care presupune atât acţiuni de război electronic, cât şi operaţii de management întrunit al spectrului electromagnetic (Joint Chiefs of Staff 2014, II-12)**.**

În timp ce doctrina Alianţei, AJP-3.10/ 2015 şi doctrina românească folosesc termenul *Cooperare Civili-Militari/Civil-Military Cooperation/CIMIC*, SUA folosesc termenul *Operaţii civil-militare/Civil-military operations/CMO* şi nu admit ideea ca această dimensiune acțională, cooperarea civili-militari, să fie considerată o capacitate.

În ceea ce priveşte angajarea liderilor cheie/key leader engagement/KLE, această capacitate apare în toate cele trei proiecţii doctrinare analizate, iar în proiecţia NATO şi cea românească apare şi angajarea la nivelul militarului. În îndeplinirea misiunii, fiecare militar interacţionează cu populaţia locală, fapt ceea ce impune nevoia de pregătire a fiecăruia privind modul de interacţiune, precum şi mesajele ce urmează a fi diseminate. Legătura dintre *comunicarea strategică/strategic communications/* StratCom şi KLE este aceea că angajarea StratCom necesită „un program robust de KLE" (Gage 2014, 54). Acest concept beneficiază de o documentaţie destul de săracă şi nici nu sunt stabilite standarde despre ce ar însemna un KLE finalizat cu succes.

Un alt aspect important al activităţilor informaţionale este reprezentat de prezenţa, postura şi profilul/PPP. Unitatea sau unităţile dislocate trebuie să fie

conştiente de imaginea publică pe care o afişează, indiferent de zona de dislocare sau misiunea încredinţată. În proiecţia americană această capacitate nu este inclusă în listă, dar aspecte referitoare la aceasta regăsim în încercările de definire a StratCom, o capacitate care nu înseamnă doar „comunicare verbală, este prezența, postura și profilul activităților noastre, în special disponibilitatea noastră de a ne susține cuvintele cu acțiuni, arătându-ne astfel puterea de la nivel politic până la cel foarte tactic". (TŪTINS 2015)

În doctrina românească, PPP ocupă locul secund în setul de domenii cheie coordonate în cadrul InfoOps. Percepția și atitudinea audienței țintă pot fi influențate de prezența, atitudinea și comportamentul trupelor și a conducerii acestora. De asemenea, descrierea PPP subliniază nevoia de sincronizare a acestor aspecte cu operațiile mass-media, având în vedere rolul comandanților în transmiterea mesajelor, precum și cerințele de protecție a forțelor desfășurate în teren. Doctrina aliată încadrează PPP în setul de capacități și tehnici integrate prin InfoOps, evidențiind totodată efectul individual pe care această capacitate îl poate crea, deoarece „simpla prezență a unei forțe poate avea un impact semnificativ asupra percepțiilor", dar și asupra mediului informațional. (NATO Standardization Office 2015, 1-12)

Chiar dacă conceptul OPSEC a apărut relativ târziu, conţinutul semantic este unul foarte vechi, fiind un mijloc de protecţie a cărui provocare „nu este transmiterea de informaţii clasificate, ci mai degrabă a unor piese ale unui puzzle, care oferă adversarilor o imagine a operaţiei, în ansamblu" (Dominique 2009, 17). Toate cele trei proiecții doctrinare analizate subliniază importanța OPSEC în prevenirea scurgerii accidentale de informații, precum și rolul acestei capacități în protecția informațiilor proprii. OPSEC necesită o atenție constantă, iar această capacitate trebuie integrată în toate aspectele operațiilor militare, încă din faza de planificare. Totodată, OPSEC se dovedește foarte importantă când vine vorba de inducerea în eroare. Cele două domenii se dovedesc a fi esențiale în realizarea surprinderii, precum și obținerea și menținerea inițiativei. Deși OPSEC și MILDEC sunt procese distincte și discrete, cele două domenii se sprijină reciproc. Acest aspect este evidențiat în toate cele trei proiecții analizate, fiecare dintre acestea evidențiind distinct în textul doctrinei această relație. Legătura dintre cele două domenii izvorăște tocmai din finalitatea acestora, respectiv afectarea procesului decizional al adversarului. Cu toate că istoria oferă multe exemple privind inducerea în eroare, succesul militar nu depinde întru totul de inducerea în eroare. Aceasta servește, mai degrabă, ca un multiplicator de forță. Schimbările recente din peisajul socio-politic nu au mărit doar importanţa inducerii în eroare, ci impun ţărilor occidentale să-şi intensifice jocul înşelăciunii. Spre exemplu, armata rusă privește inducerea în eroare ca pe o activitate distinctă, conturată prin termenul Maskirovka (Vowel 2016) o formă mult mai complexă de înşelare a inamicului.

Singura pârghie cinetică, aşa cum menţiona Călin Hentea, a rămas *distrugerea fizică*, o pârghie folosită „nu doar pentru eliminarea sau anihilarea unor puncte sau

reţele de comandă sau comunicaţii adverse, ci şi pentru obţinerea unui anumit impact psihologic asupra populaţiei sau liderilor vizaţi". (Hentea 2008, 303)

Definiţia IA/Information Assurance/asigurării informaţionale surprinde rolul acestei capacităţi pentru obţinerea şi menţinerea superiorităţii informaţionale, precum şi interdependenţa dintre IA şi operaţiile cibernetice. De asemenea, multe caracteristici ale IA sunt atribuite INFOSEC/securităţii informaţionale.

Odată cu recunoaşterea spaţiului cosmic şi cibernetic ca fiind două noi domenii operaţionale, s-a schimbat şi fizionomia războiului. Spaţiul poate fi folosit atât în scopuri paşnice, cât şi pentru agresiune, iar potenţialul unui conflict în spaţiu nu a fost niciodată mai evident.

În ceea ce priveşte legătura *operaţiilor spaţiale* cu operațiile informaționale, văzută ca funcție întrunită, doctrina americană precizează că cele două se sprijină reciproc. Spaţiul cosmic sprijină fluxul de informaţii, sprijină și procesul de luare a deciziilor, dar poate asigura şi livrarea informaţiilor în mediul informaţional. Pe de altă parte, informaţiile pot genera efecte care sprijină atingerea superiorităţii informaţionale, definită ca „gradul de control în spațiu al unei forțe asupra oricărei alte forțe care permite desfășurarea operațiilor sale la un moment și un loc dat, fără interferențe prohibitive din partea amenințărilor terestre și spațiale". (Joint Chiefs of Staff 2020, I-4)

Concluzii

Pentru atingerea obiectivelor încredinţate, o condiţie esenţială este reprezentată de capacitatea armatelor de a se intrui şi de a opera împreună, într-o manieră integrată şi coordonată. Acest lucru contribuie la garantarea eficienţei operaţionale, care poate fi obţinută doar printr-o abordare controlată a interoperabilităţii. În acest context, doctrinele reprezintă pilonul de bază ce cuprinde atât conceptele (*ce?*), cât şi toate regulile de angajare şi aspectele care caracterizează acţiunea militară (*cum?*). Cu alte cuvinte, doctrinele descriu metodele, organizarea, precum şi ansamblul de proceduri care fac posibilă desfăşurarea acţiunilor în cadru întrunit. Prin urmare, compararea diferitelor abordări InfoOps reprezintă un proces esenţial în efortul de asigurare a coerenţei doctrinare.

Natura InfoOps trebuie clarificată în permanenţă, pentru ca operațiile informaționale să fie bine înțelese din punct de vedere conceptual şi practic şi pentru a fi în concordanţă cu evoluţia şi tendinţele de pe câmpul de luptă modern. De asemenea, este nevoie de obţinerea unei coerenţe între doctrinele pentru operaţii informaţionale ale NATO şi ale statelor aliate. Spre exemplu, atâta vreme cât gradul de corespondență doctrinară între doctrinele NATO și românească în domeniul operațiilor informaționale este destul de ridicat, interoperabilitatea se poate realiza fără sincope. În schimb, prezența românească în operațiuni informaționale sub

comandă americană ar crea probleme privitoare, de exemplu, la integrarea INTEL în cadrul acestei funcții întrunite. Putem afirma că interoperabilitatea la nivel operaţional şi tactic depinde şi de această chestiune, de diferenţele doctrinare, atât la nivel de suprafață (principii și domenii cheie), cât și la nivel de profunzime, ca mod de aplicare şi subordonare în raport cu comanda întrunită. În ceea ce priveşte cele trei proiecţii doctrinare, există diferenţe semnificative atât la nivelul termenului umbrelă „operaţii informaţionale", cât şi la nivelul domeniilor cheie. Prin urmare, subliniem nevoia de revizuire a terminologiilor aferente, pentru a putea ţine pasul cu caracteristicile mediului de operare contemporan, sau completarea aparatului doctrinar cu documente necesare obținerii unui grad ridicat de interoperabilitate în exerciții comune româno-americane. Nu este necesară schimbarea terminologiei utilizate, fiind compatibilă cu terminologia NATO, ci doar identificarea acestor forme de coordonare în scopul obținerii unui coeficient mai înalt de interoperabilitate doctrinară, respectiv introducerea în aparatul doctrinar românesc a altor concepte necesare pentru înțelegerea funcționalității și dinamicii câmpului de luptă, precum acela de abordare a operațiilor pe baza efectelor. Nu în ultimul rând, o actualizare a Doctrinei Armatei României ar permite o adaptare mai facilă la realitățile câmpului de luptă.

BIBLIOGRAFIE:

Dominique, Michael. 2009. *Information operations: the military's role in gaining information superiority*, U.S. Army War College. https://apps.dtic.mil/sti/pdfs/ADA498020.pdf

Gage, Daniel. 2014. *The continuing evolution of Strategic Communication within NATO,* The Three Swords Magazine, 27/ 2014 https://www.jwc.nato.int/images/stories/threeswords/NOV_STRATCOM_evolution.pdf.

Headquarters, Department of the Army. 1996. FM 100-6 *Information Operations*, https://www.hsdl.org/?view&did=437397

Hentea, Călin. 2008. *Noi dimensiuni ale războiului contemporan,* „Revista Română de Sociologie", serie nouă, anul XIX, nr. 3–4, p. 289–306, Bucureşti. https://www.revistadesociologie.ro/pdf-uri/nr.3-4-2008/Art%206-Hentea.pdf

Joint Chiefs of Staff. 1998. "Joint Pub 3-13 *Joint Doctrine for Information Operations*". https://www.c4i.org/jp3_13.pdf.

–. 2006. "Joint Publication 3-13 *Information Operations*". https://www.globalsecurity.org/intell/library/policy/dod/joint/jp3_13_2006.pdf

–. 2014. "Joint Publication 3-13 *Information Operations*". https://irp.fas.org/doddir/dod/jp3_13.pdf.

–. 2020. "Joint Publication 3-14 *Space operations*". https://irp.fas.org/doddir/dod/jp3_14.pdf

Lesenciuc, Adrian. 2016. *Războiul informațional.* Editura Academiei Forțelor Aeriene „Henri Coandă", Brașov.

Myesr, Meghan. 2017. *The Army's psychological operations community is getting its name back*. https://www.armytimes.com/news/your-army/2017/11/06/the-armys-psychological-operations-community-is-getting-its-name-back/

NATO Standardization Agency. 2009. *Allied Joint Doctrine for Information Operations* 3.10.

NATO Standardization Office. 2015. *Allied Joint Doctrine for Information Operations* 3.10. Edition A Version 1.

Prats I Amorós, Joam, Guillaume-Barry, Augustin. 2019. *Not Only Blood. The Need to Integrate Psychological Operations in the West's Military Culture*, Instituto Español de Estudios Estratégicos, Opinion Paper IEEE 81/2019.

Statul Major General. 2006. *Doctrina Operaţiilor Informaţionale*.

–. 2011. *Doctrina pentru operaţii informaţionale a Armatei României*.

–. 2017. *Doctrina Operaţiilor Informaţionale*, Ediţia a 2-a.

TŪTINS, Māris. 2015. *Strategic Communication and Protecting Environment in Military Training Areas.* NATO StratCom COE. http://putniadazos.lv/sites/default/files/kcfinder/files/2015-05-05_StratCom_environment.pdf

Vowel, JB. 2016. *Maskirovka: From Russia, With Deception.* https://www.realcleardefense.com/articles/2016/10/31/maskirovka_from_russia_with_deception_110282.html