BULETINUL

UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I"

Nr. 4/ 2024

ISSN 1584-1928
eISSN 2065-8281

Publicație fondată în anul 1937

PUBLICAȚIE ȘTIINȚIFICĂ CU PRESTIGIU RECUNOSCUT
DIN DOMENIUL „ȘTIINȚE MILITARE, INFORMAȚII ȘI ORDINE
PUBLICĂ" AL CONSILIULUI NAȚIONAL DE ATESTARE A
TITLURILOR, DIPLOMELOR ȘI CERTIFICATELOR UNIVERSITARE,
INDEXATĂ ÎN BAZELE DE DATE INTERNAȚIONALE CEEOL,
GOOGLE SCHOLAR, INDEX COPERNICUS, CROSSREF

EDITURA UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I"
BUCUREȘTI, 2024

Referenți

Articolele publicate în Buletinul Universității Naționale de Apărare „Carol I”, ISSN 1584-1928, se regăsesc – titlu, autor, abstract, conținut, bibliografie – și în varianta în limba engleză a revistei, ISSN 2284-936X
L 2284-936X

Cuprins

Nr. 4/2024

BULETINUL
UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I”
https://buletinul.unap.ro

Repere esențiale ale operațiilor specifice luptei armate în mediul urban

Key Milestones in Urban Operations

Lt.col.Dr. Claudiu-Valer NISTORESCU*
*Facultatea de comandă și stat major, Universitatea Națională de Apărare „Carol I”
e-mail: nistorescu_claudiu@yahoo.com

Abstract

Noile cerințe ale mediului de operare contemporan impun ajustări la nivelul procesului de planificare a operațiilor, pregătirii și executării acestora. Mediul urban, prin specificitatea sa, generează o serie de implicații asupra operațiilor specifice luptei armate, ele devenind repere esențiale ale procesului operațional. În acest context, obiectivul acestui demers îl reprezintă identificarea și descrierea acestor repere ale procesului operațional, aferent mediului urban. Rezultatele cercetării, deși oferă soluții empirice, devin valoroase prin aportul teoretic oferit comandanților nivelului tactic în ceea ce privește abordarea acestui tip de operații.

The new demands of today's operational environment require adjustments to the planning process preparing and execution of the military operations. The urban environment, by its specificity, generates a series of implications for combat operations, which become essential benchmarks of the operational process. In this context, the objective of this paper is to identify and describe the milestones of the operational process related to urban operations. While the results of the research offer empirical solutions, their value is enhanced by the theoretical contribution they make to tactical-level commanders in terms of the approach to this type of operation.

Cuvinte-cheie:
operații specifice luptei armate; mediul urban; triada urbană;
integrarea operațiilor la nivel interarme.
Keywords:
combat operations; urban environment; urban triad; combined-arms warfare.

Info articol
Primit: 18 octombrie 2024; Evaluat: 25 noiembrie 2024; Acceptat: 4 decembrie 2024; Disponibil online: 17 ianuarie 2025

Citare: Nistorescu, C.V. 2024. „Repere esențiale ale operațiilor specifice luptei armate în mediul urban”. *Buletinul Universității Naționale de Apărare „Carol I”*, 13(4): 7-20. https://doi.org/10.53477/2065-8281-24-35

Conform estimărilor și studiilor de specialitate recente, polulația Terrei va cunoaște o creștere de 2,1 miliarde până în anul 2050, ajungând la o cifră de 9,8 miliarde. Creșterea va fi constantă, dar inegală la nivel global, având un ritm ridicat mai ales în Asia, America de Sud și Africa. În același timp, un număr din ce în ce mai mare de oameni va alege să trăiască în orașe, acest lucru ducând la o extindere a zonelor urbane, contribuind, totodată, la creșterea economiilor, dar și la presiuni asupra entităților guvernamentale, în special în țările aflate în curs de dezvoltare (UK Ministry of Defence 2024, 13). Mai mult de atât, până la mijlocul secolului se estimează că aproximativ 60,5% din populația lumii va locui în centrele urbane, o creștere semnificativă de la 48,3%, procentul estimativ al populației care își desfășoară activitatea, în prezent, în mediul urban (UK Ministry of Defence 2024, 126).

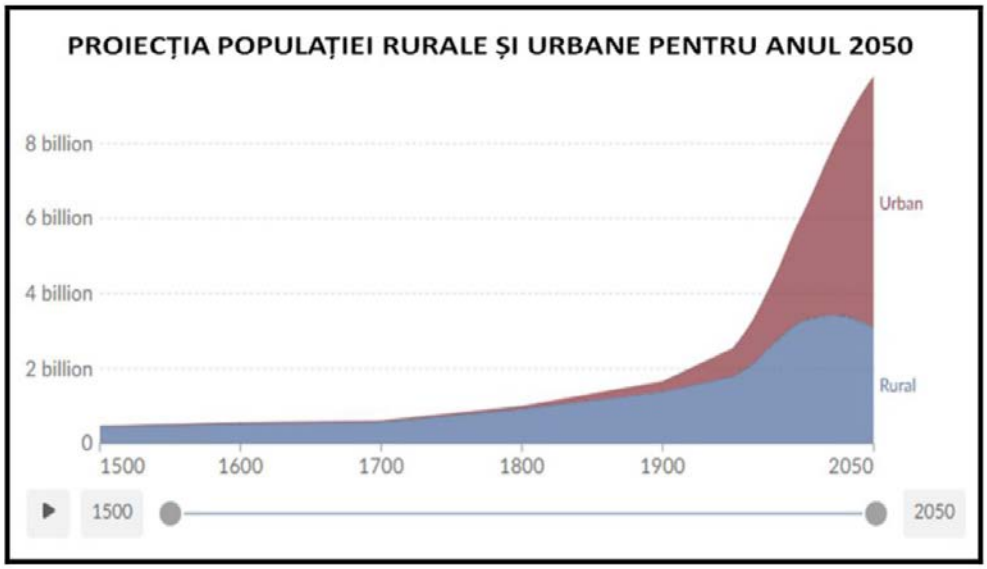


Figura 1 Evoluția comparativă a populației rurale și urbane în lume (perioada 1500-2050)
Sursa: Hannah Ritchie, Max Roser, "Urbanization", https://ourworldindata.org/urbanization, accesat la data de 12.11.2024.

În acest context, studiile realizate la nivel aliat, având la bază analiza trendului demografic, evoluția mediului geostrategic și de securitate, dezvoltarea tehnologiilor înalte și influența lor asupra societății, indică o creștere a frecvenței conflictelor armate în mediu urban (NATO 2018). Specialistul canadian în securitate Robert Muggah subliniază faptul că orașele vor deveni noua frontieră a războiului (Muggah 2015), iar Lawrence Freedman, identificând faptul că megaorașele vor deveni epicentrele activității umane de pe planetă, estimează că acestea se vor constitui în scena de desfășurare a majorității conflictelor care vor impune intervenții militare (Freedman 2019, 349).

Sensibilitatea conflictelor desfășurate în mediul urban este un rezultat al caracteristicilor unice ale acestuia. Aglomerarea fizică, deopotrivă pe orizontală și verticală, rețelele subterane, existența elementelor de infrastructură critică, congestionarea mediului electromagnetic, facilitățile media extinse și prezența factorului uman complică operațiile militare. Experiența conflictelor trecute scoate

în evidență faptul că, de multe ori, *„orașele distrug armate și armatele distrug orașe"* (Chychota 2019, 295). Ipoteza este validată de conflictele armate contemporane, mărturie fiind bătăliile din Mariupol, Bahmut, Avdiivka, Gaza sau Khan Yunis.

Având în vedere creșterea probabilității desfășurării conflictelor armate în mediul urban, se impune o evaluare atentă a procesului operațional aferent acestui tip de confruntare. Interesul teoreticienilor și liderilor militari față de acest subiect este unul ridicat, literatura de specialitate scoțând în evidență implicațiile pe care le au orașele în proiectarea operațiilor strategice (Department of the Army Headquarters, TRADOC Pamphlet 525-92-1 2020), nevoia de a realiza efecte la nivel întrunit pentru îndeplinirea condițiilor necesare atingerii stării finale dorite (US Joint Chiefs of Staff, JP 3-06 2013) și dificultatea operațiilor tactice descentralizate până la cel mai mic nivel (NATO, ATP-3.2.1.2 2022).
De aceea analiza își propune o descriere a principalelor repere care stau la baza înțelegerii mediului urban, precum și determinarea factorilor care fundamentează nevoia de schimbare a operațiilor specifice luptei armate în mediul urban. Nu în ultimul rând, din perspectiva acestor rezultate, demersul are ca principal obiectiv de cercetare identificarea implicațiilor doctrinare și operaționale, generate de noile cerințe ale mediului de operare contemporan, acestea vizând atât dimensiunea acțională, cât și cea organizațională.

Pentru canalizarea efortului de cercetare, ne-am propus să răspundem la următoarele întrebări:

- Care sunt fundamentele operațiilor specifice luptei armate desfășurate în contextul mediului urban?
- Care sunt factorii care impun reconsiderarea opererațiilor specifice luptei armate în mediul urban?
- Care sunt implicațiile generate la nivelul luptei armate în mediul urban, în contextul noilor cerințe ale mediului de operare?

Interogarea surselor deschise care fac referire la desfășurarea operațiilor de luptă din cadrul conflictelor din Ucraina și Fâșia Gaza a permis identificarea unor rezultate empirice. Subliniem, totodată, nevoia de aprofundare a acestor rezultate și validarea lor prin intermediul jocurilor de război și al exercițiilor. De asemenea, aducem în atenție faptul că există posibilitatea ca anumite date și informații să fie alterate, într-o oarecare măsură, fie din nevoi care țin de securitatea operațională, fie din dorința de a dezinforma și de a influența părțile combatante.

Înțelegerea mediului urban și a fundamentelor operațiilor specifice luptei armate desfășurate la nivelul acestuia

Complexitatea mediului urban și în mod inerent dificultatea operațiilor militare aferente rezultă din existența mai multor sisteme și subsisteme multidimensionale, care sunt, deopotrivă, interconectate și interdependente. Aceste sisteme sunt de

natură fizică și nonfizică, incluzând sistemul fizic, populația și sistemul informațional (Department of the Army Headquarters ATP 3-06, MCTP 12-10B 2017, 1-3). Toate la un loc formează ceea ce specialiștii militari numesc *triada urbană*.

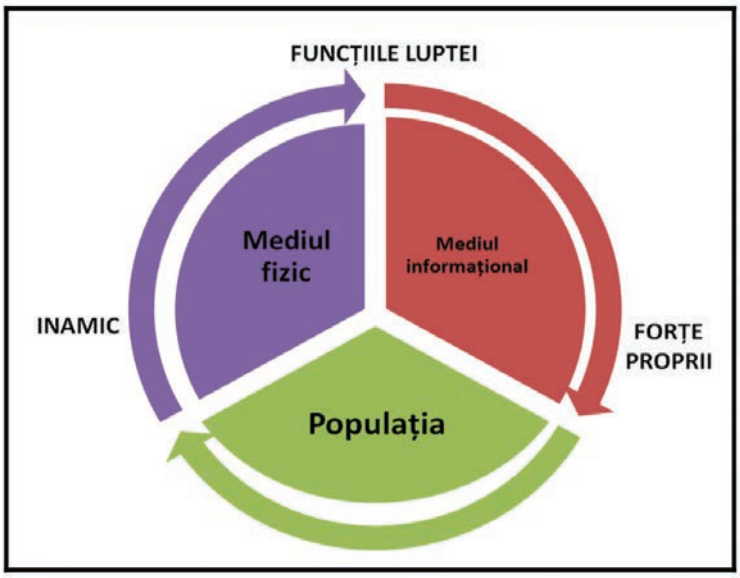


Figura 2 Triada urbană
Sursa: Department of the Army Headquarters ATP 3-06, MCTP 12-10B 2017, 1-3.

Sistemul fizic al mediului urban se materializează prin caracteristicile de teren. Terenul urban include o componentă naturală (detalii ale reliefului) și una artificială (infrastructura și construcțiile umane), precum și spațiul din proximitatea așezării umane. Sistemul fizic poartă amprenta principalelor caracteristici ale componentei naturale în ceea ce privește dispunerea spațială a urbei. În același timp, componenta artificială este influențată de nivelul dezvoltării economice, de cultura societății și de împărțirea pe categorii sociale a populației.

Populația se regăsește în centrul sistemului urban și reprezintă, de asemenea, un element fundamental care modelează desfășurarea operațiilor militare. Divizarea, în funcție de apartenența populației la o anumită categorie socială, împarte orașul în zone rezidențiale bogate, zone rezidențiale ale clasei de mijloc și zone sărace de la periferie. Tipul și dispunerea clădirilor, facilitățile existente, precum și densitatea diferită a populației în respectivele zone sunt factori care pot influența abordarea operațiilor de luptă în mediul urban. Factorul economic, diversitatea etnică, culturală și religioasă sunt, de asemenea, aspecte pe care planificatorii militari trebuie să le aibă în vedere. Imposibilitatea evacuării totale a populației din centrele urbane pe timpul desfășurării ostilităților reprezintă o certitudine (Arnold și Fiore 2019). Bătăliile din Mosul, Ramadi, dar și din Mariupol sau Gaza validează acest lucru.

Sistemul informațional include totalitatea sistemelor de comunicații și a rețelelor aferente centrului urban. El este caracterizat de o mare fluiditate, fiind interconectat cu infrastructura localității și fiind influențat, totodată, de interacțiunea cu componenta umană (NATO Standard, AJP-3.2 2022, A-3). O altă caracteristică

esențială a acestui sistem este permanenta schimbare la nivelul componentelor și proceselor lui, fapt ce influențează situația operațională și modul în care comandanții și statele majore se raportează la aceasta. Gradul ridicat de permeabilitate a acestui sistem oferă oportunități tuturor actorilor. Luând în considerare sensibilitatea și impredictibilitatea acțiunilor în domeniul cibernetic și în spectrul electromagnetic, asociat cu dificultatea prevenirii și contracarării lor, avem ca rezultat o serie de amenințări asimetrice complexe. Asimetria în aceste medii rezultă din oportunitatea actorilor ostili de a executa acțiuni fără a se conforma legislației internaționale (Pamment și alții 2019, 61). În ciuda faptului că exploatarea sistemului informațional poate reprezenta un avantaj major pentru forțele proprii, în scopul influențării populației și creării unui climat care să susțină executarea operației, el oferă adversarilor un mijloc relativ facil de a influența operațiile militare.

Abordarea operațiilor militare în mediul urban presupune luarea în considerare a acestor sisteme, procesul operațional fiind influențat de modul lor de manifestare, indiferent de tema campaniei sau de natura operației. Având în vedere amploarea impactului pe care populația locală îl poate avea asupra operațiilor militare, planificatorii militari trebuie să ia în considerare nevoia de a desfășura operații care să asigure întreg spectrul de manifestare a acestora: operații specifice luptei armate, operații de securitate, operații de pace. În cadrul acestor tipuri de operații, acțiunile tactice pot include acțiuni de luptă ofensive și defensive, operații de contrainsurgență, contraterorism, asistență umanitară, evacuarea necombatanților, sprijinul autorităților locale etc. Totodată, dincolo de analiza acestor sisteme, pentru o evaluare pertinentă a mediului urban și pentru obținerea unei imagini coerente asupra unei potențiale scene de desfășurare a operațiilor militare, se impune o analiză PMESII a acestuia. De asemenea, în cadrul operațiilor tactice, pregătirea informativă a câmpului de luptă trebuie să trateze cu atenție componenta civilă, aceasta putând influența decisiv și ireversibil desfășurarea operațiilor, contribuind la succesul lor sau, dimpotrivă, negând șansele obținerii acestuia.

Factori esențiali care impun reconsiderarea operațiilor în mediul urban

În ultimele decenii, armatele occidentale și-au concentrat eforturile pentru a răspunde, cu precădere, provocărilor generate de conflictele de amploare și de intensitate mică din Orientul Mijlociu și din Africa de Nord. Cerințele operațiilor de contrainsurgență au imprimat o serie de caracteristici dominante în ceea ce privește doctrina militară, configurarea forțelor, instruirea și înzestrarea cu tehnică de luptă și sisteme de armament. Mai mult de atât, plasarea populației civile în prim plan în cadrul obiectivelor militare a impus o abordare unică a operațiilor, cu impact semnificativ în proiectarea acestora. Adversarii armatelor occidentale, prin utilizarea unor metode și capabilități asimetrice și neconvenționale, au făcut de multe ori irelevantă superioritatea cantitativă și calitativă a acestora. În consecință, mai multe capabilități convenționale au fost neglijate, la fel ca și instruirea în domeniul

războiului convențional (Scrogin 2019, 19-20). Respectiva realitate, în care succesul depindea, deopotrivă, de prezervarea securității populației și de înfrângerea unui adversar insuficient definit, a determinat adoptarea unei abordări orientate către pierderi minime în rândul forțelor proprii. Având în vedere aceste considerente și ținând cont, totodată, de creșterea probabilității materializării unor conflicte armate convenționale, se identifică *nevoia tranziției de la operațiile de contrainsurgență la operațiile specifice luptei armate*. Această tranziție trebuie realizată, deopotrivă, în plan mental și fizic. Reconsiderarea doctrinelor militare, reconfigurarea structurilor tactice și reconstituirea sau revitalizarea unor capabilități convenționale depind de acceptarea, în plan mental, de către liderii politico-militari a acestei nevoi.

Nevoia de integrare a operațiilor la nivel multidomeniu reprezintă, de asemenea, un factor care impune reabordarea operațiilor militare în mediul urban. Convergența efectelor aferente tuturor domeniilor de operare, incluzând acțiunile din spectrul electromagnetic, acțiunile cibernetice sau informaționale au determinat specialiștii militari să redefinească reperele definitorii ale operațiilor militare, în scopul păstrării superiorității militare relative. Alianța Nord-Atlantică, prin doctrina sa fundamentală, definește operațiile multidomeniu ca fiind orchestrarea tuturor acțiunilor militare și nonmilitare la nivelul tuturor domeniilor de operare astfel încât obținerea efectelor să fie oportună și elocventă (NATO Standard, AJP-1 2022, 3). Complexitatea operațiilor de luptă în mediul urban și extinderea lor dincolo de dimensiunile domeniilor clasice impun utilizarea concertată a mijloacelor specifice *„capabilităților din toate domeniile spațiului de luptă, care sunt menite să dobândească succesul în cel mai eficient mod."* (Vereș 2024, 44-59).

Noile tehnologii și sisteme de armament influețează tacticile, tehnicile și procedurile de operare. De asemenea, *creșterea letalității câmpului de luptă* reprezintă un efect direct al noilor tehnologii și sisteme de armament, extinderea razei de acțiune, îmbunătățirea preciziei și diversificarea senzorilor multispectrali susținând dezvoltarea acestora.

Un alt factor care impune reconsiderarea operațiilor specifice luptei armate în mediul urban este *transparența extinsă a câmpului de luptă*. În condițiile tehnologizării câmpului de luptă *„camuflarea forțelor și acțiunilor militare este tot mai dificil de realizat"* (Toroi 2024, 113), acest lucru forțând comandanții militari să caute noi metode inovative și creative de a-și ascunde intențiile și forțele.

Nu în ultimul rând, *algoritmul de luptă al potențialilor inamici* influențează adaptarea doctrinară și operațională a forțelor occidentale. Comportamentul operațional al forțelor rusești în Ucraina facilitează identificarea unui algoritm care scoate în evidență rolul central al artileriei, capacitatea de a accepta un număr ridicat de pierderi în rândul forțelor proprii și toleranța în ceea ce privește victimele și daunele colaterale. Modelul rusesc pare să fie bazat pe o abordare centrată pe raportul de forțe istoric, nesatisfăcând cerințele principiului dispersiei. De asemenea, el scoate în evidență ineficiența operațiilor de modelare și utilizarea excesivă a vectorilor

de lovire imprecișI. Asediul din Mariupol, bătăliile pentru Bahmut, Avdiivka scot în evidență distrugerile disproporționate, realizate de armata rusă pentru a cuceri aceste obiective tactice (Butler 2023).

Implicații generate de factorii care impun reconsiderarea operațiilor în mediul urban

Factorii generatori de implicații la nivelul operațiilor din mediul urban își regăsesc ecou la nivelul procesului operațional, având un impact direct asupra funcțiilor luptei, organizării și componenței structurilor tactice, tacticilor și procedurilor de operare.

Funcțiile luptei

Conceptual, funcțiile luptei sunt acele *„instrumente principale aflate la dispoziția comandantului, pe care acesta le integrează și coordonează în cadrul operațiilor, pentru sincronizarea efectelor în timp, spațiu și scop"* (Statul Major al Forțelor Terestre 2017, III-13). Prin integrarea lor la nivelul capacității de luptă a structurilor tactice, în contextul cerințelor impuse de mediul de operare și de acțiunile inamicului, se generează puterea de luptă a respectivelor structuri. Mediul urban, prin specificitatea sa, imprimă unicitate modului în care aceste funcții sunt integrate și de aceea este necesară o analiză a lor, în scopul înțelegerii nevoii de reconsiderare a operațiilor urbane și de identificare a soluțiilor pentru ajustarea lor. În consecință, analiza include aspecte care țin de comanda și controlul operațiilor, de realizarea sprijinului cu informații, de manevra forțelor, de sprijinul prin foc, de protecția forțelor și de realizarea sprijinului logistic.

• *Comanda și controlul*

Funcția de comandă și control este afectată în mediul urban, în primul rând, din cauza nevoii de descentralizare a operațiilor, acest lucru implicând o dezagregare a forței și măsuri suplimentare de sincronizare a acțiunilor și de coordonare a forțelor. Aglomerarea mediului electromagnetic, dezvoltarea pe verticală a terenului urban restricționează comunicațiile. Obstrucționarea câmpurilor de observare impune luarea unor măsuri de control drastice pentru evitarea fratricidului sau cauzarea de victime colaterale. De aceea actualizarea permanentă a poziției forțelor se impune pentru asigurarea progresului operației și pentru executarea oportună a sprijinului necesar. Monitorizarea poziției prin sisteme de poziționare globală/GPS reprezintă mijlocul cu cea mai mare acuratețe. De asemenea, folosirea imaginilor satelitare sau a dronelor pentru supravegherea forțelor angajate în zone dens populate îmbunătățește capacitatea de control a acestora. Totuși, eficiența acestor capabilități poate fi diminuată în mediile urbane extrem de congestionate și în condițiile contestării multidimensionale a forțelor proprii. În acest context, caracterizat de ambiguitate și incertitudine, libertatea decizională și inițiativa comandanților sunt esențiale pentru realizarea eficientă a procesului operațional.

• *Informațiile*

Integrarea informațiilor ca funcție a luptei prezintă particularități generate de specificitatea mediului de confruntare, iar dificultatea obținerii oportune a unor informații corecte este evidentă. Perisabilitatea informațiilor este ridicată, din cauza posibilităților reduse de a menține o identificare pozitivă asupra țintelor (positive identification/PID). În consecință, realizarea ciclului *căutare-detecție-identificare-supraveghere* trebuie reluată mai frecvent decât în alte condiții și presupune angajarea unor capabilități și elemente de cercetare semnificativ mai consistente. De cele mai multe ori, factorul uman este decisiv, dar diferiți senzori, produși de noile tehnologii, pot suplini resursa umană. Astfel, capabilitățile UAS, IMINT, SIGINT, dar și MASINT devin instrumente valoroase în acest mediu puternic restricționat. În timpul operațiunilor convenționale, îndeosebi pe timpul celor ofensive, comandanții ar trebui să exploateze capabilitățile HUMINT pentru a obține informații de la civilii rezidenți, de la refugiați și persoane strămutate, precum și pentru a interoga deținuții și prizonierii de război (Department of the Army, FM 2-0 2023, 1-18).

• *Manevra*

Posibilitățile de manevră ale forțelor convenționale sunt restricționate semnificativ în mediul urban, acțiunile forțelor îmbarcate fiind canalizate de-a lungul străzilor. Fragmentarea terenului implică o abordare compartimentată și metodică a operațiilor de luptă, acest lucru generând nevoia de a împărți orașul în zone de operații rectangulare, clar delimitate de străzi și în conformitate cu posibilitatea de acțiune a subunității/unității căreia îi este atribuită. Clădirile, canalele și alte infrastructuri constituie obstacole pentru atacator, favorizând, în același timp, apărătorul. De cele mai multe ori, cucerirea și securizarea unui obiectiv presupun cucerirea și securizarea fiecărei clădiri, complex de clădiri și de aceea manevra forțelor are un ritm redus în mediul urban. Experiența acumulată de forțele israeliene în Gaza indică faptul că nu se recomandă alocarea unor zone de operații noncontigue forțelor angajate pe direcțiile principale de ofensivă (Watling și Reynolds 2024, 1). Angajarea forțelor blindate în mediul urban trebuie realizată după o atentă evaluare a amenințării, de cele mai multe ori binomul infanterie-tancuri reprezentând soluția adecvată pentru realizarea manevrei în mediu urban. Succesul operațiilor manevriere depinde în mare măsură de asigurarea unor forțe de acoperire care să neutralizeze elementele antitanc, ambuscadele și lunetiștii inamicului, dar și a unor elemente de infanterie ușoară care să realizeze siguranța apropiată a blindatelor. De aceea comandanții trebuie să urmărească obținerea unui echilibru optim între forțele îmbarcate și forțele debarcate. Manevra forțelor blindate poate fi facilitată de operațiile de modelare, executate de detașamentele de desant aerian tactic. Totuși, aceste structuri tactice dispun de o putere de luptă relativ redusă, ele fiind limitate temporal, din perspectiva capacității de susținere a operațiilor. Nu în ultimul rând succesul forțelor de manevră depinde de eficiența sprijinului prin foc și de posibilitățile de a asigura mobilitatea forțelor. Conform lecțiilor învățate, loviturile artileriei pot produce un efect benefic, raportat la situația tactică imediată, dar provoacă distrugeri care, ulterior, reduc posibilitățile de manevră. În consecință capabilitățile de geniu trebuie integrate elementelor

de manevră pentru a asigura curățarea și deschiderea culoarelor de mobilitate (Department of the Army Headquarters, TRADOC Pamphlet 525-92-1 2020, 19).

• *Sprijinul prin foc*

Sprijinul prin foc se realizează mai dificil în mediul urban, pe de o parte, din cauza fragmentării terenului și dificultății în a repera și identifica țintele, și, pe de altă parte, din cauza riscului de a produce pagube și victime colaterale. Deși conflictele recente din Ucraina și Fâșia Gaza scot în evidență predispoziția forțelor de a-și utiliza capabilitățile de sprijin prin foc, ele păstrează doar un rol de modelare, acțiunea forțelor de manevră fiind necesară pentru înfrângerea inamicului (Mirea 2024, 126-136). De asemenea, riscul fratricidului este ridicat, în condițiile obstrucționării sectoarelor de observare și de tragere. În acest sens, măsurile de control al sprijinului prin foc sunt cruciale la fel ca realizarea estimărilor privind producerea de pagube și victime colaterale (Collateral Damage Estimation/CDE). În consecință, posibilitățile capabilităților de sprijin prin foc trebuie adaptate efectelor urmărite. Munițiile inteligente pot fi de folos, dar trebuie ținut cont de riscul mare ca acestea să fie bruiate. Mijloacele antitanc cele mai pretabile sunt sistemele portabile de rachete antitanc dirijate. Aceste capabilități, prin funcțiile lor *fire and forget*, *top attack* sau *flying top-attack*, devin extrem de utile în luptele din mediul urban, bătălia pentru Kiev, din faza inițială a conflictului din Ucraina, fiind o dovadă elocventă a acestui fapt (Johnson 2022).

• *Protecția*

Luând în considerare ritmul redus al operațiilor și limitarea posibilităților de a manevra, în mediul urban se resimte o nevoie acută de protecție multidimensională atât pentru forțele îmbarcate, cât și pentru cele debarcate. Vulnerabilitatea specifică elementelor debarcate și a celor îmbarcate poate fi redusă doar prin coordonarea unor acțiuni manevriere și de sprijin reciproc care să se realizeze atât la nivelul capabilităților amintite, cât și între structurile tactice vecine (NATO, ATP-3.2.1.2 2022). De asemenea, se simte o nevoie accentuată de protejare a forțelor împotriva ambuscadelor, lunetiștilor, dronelor și dispozitivelor explozive improvizate, elementele de acoperire și siguranță jucând un rol important în acest sens.

• *Sprijinul logistic*

Mediul urban pune o presiune ridicată asupra sistemului logistic, îndeosebi în condițiile operațiilor specifice luptei armate. Se înregistrează consumuri mari de muniții, rutele de aprovizionare pot fi interceptate cu ușurință de inamic, iar evacuarea medicală se face de cele mai multe ori pe cale terestră. Totuși, mediul urban oferă o serie de facilități combatanților, chiar dacă acestea pot fi temporare și nu ar trebui luate în calcul în ecuația procesului operațional: surse de electricitate, hrană și apă, facilități medicale civile, spații de cazare și cartiruire etc.

Organizarea și compoziția forței

Faza inițială a invaziei Federației Ruse în Ucraina a scos în evidență ineficiența și deficiențele grupurilor tactice de luptă de nivel batalion angajate de aceasta în

operațiile ofensive, inclusiv în centrele urbane (Jones 2022). Acestea, deși construite pentru a opera independent, inclusiv în mediul urban, nu au putut fi integrate unitar în cadrul operațiilor ofensive la scară largă și nu au beneficiat de efectele operațiilor de modelare pe care eșalonul superior trebuia să le realizeze în sprijinul lor (Kofman și Lee 2022). În consecință, Federația Rusă a renunțat la aceste structuri de tip *battle group*, revenind la configurarea clasică a structurilor tactice – pe regimente și divizii –, iar pentru operațiile în mediul urban, ele au fost înlocuite de *detașamentele de asalt*, niște structuri mai suple și adaptate condițiilor de mediu (Nistorescu 2024).

Nu există o formulă unică privind organizarea structurilor tactice destinate luptei în mediul urban. Totuși, în contextul operațiilor specifice luptei armate împotriva unui inamic cu capabilități convenționale și relativ egale, se impune realizarea unui mix al forțelor principale care să includă blindate grele (tancuri sau mașini de luptă ale infanteriei), infanterie medie (transportoare blindate de trupe) și infanterie ușoară, îmbarcată pe blindate ușoare, și infanterie debarcată. La acestea, se adaugă structuri de artilerie, elemente de artilerie și rachete antiaeriene, geniu luptă și cercetare blindată, dar și capabilități aeropurtate. În luptele din Fâșia Gaza, armata israeliană a angajat cu preponderență structuri de nivel brigadă, acestea având în compunere 1 batalion de blindate grele (tancuri), 1 batalion mecanizat, 1 batalion de infanterie ușoară, 1 batalion de geniu, 1 batalion de artilerie, 1 detașament de forțe pentru operații speciale și elemente de sprijin de luptă descentralizate până la nivelul subunităților (Watling și Reynolds 2024).

Tactici, tehnici și proceduri

Tacticile, tehnicile și procedurile au în plan central nevoia de a menține o superioritate relativă asupra inamicului, în condițiile desfășurării simultane a mai multor ciocniri și angajamente tactice. Descentralizarea operațiilor presupune și o descentralizare a forțelor și capabilităților, îndeosebi a celor de sprijin. Succesul tactic la nivelul operațiilor de luptă depinde de o serie de măsuri, precum înțelegerea mediului operațional și a relației *forțe proprii-inamic-populație*, conștientizarea faptului că forțele proprii sunt permanent monitorizate, crearea și exploatarea unor poziții de avantaj – fizice, informaționale sau din perspectiva populației –, realizarea inițială a contactului cu inamicul cu elemente cât mai mici, anticiparea provocărilor, identificarea opțiunilor și a criteriilor pentru tranziție, consolidarea câștigurilor și menținerea moralului.

Tacticile în mediul urban se bazează pe elementul surpriză, pe ritmul ridicat al operațiilor și pe agilitatea forței. Raidurile pot avea efecte devastatoare asupra inamicului, afectându-i acestuia, deopotrivă, componenta fizică și psihologică a puterii de luptă. Forțele de desant aerian sau cele aeromobile pot contribui la succesul operației, dar trebuie ținut cont de vulnerabilitatea acestora, posibilitățile de luptă fiind limitate în spațiu și timp. Este de notorietate eșecul operației de desant aerian al forțelor rusești, executate pentru a cuceri aeroportul Hostomel, din apropierea capitalei ucrainene, Kiev (Collins, Kofman și Spencer 2023).

Nevoia realizării unei abordări tridimensionale a terenului rămâne pregnantă,

experiența conflictului din Fâșia Gaza arătând importanța blocării canalelor și tunelurilor subterane, a controlului demisolurilor și parterului clădirilor, precum și a etajelor intermediare. Totuși, s-a observat scăderea tendinței de a ocupa ultimul nivel al clădirilor sau acoperișul acestora, ceea ce reduce semnificativ libertatea de manevră, oportunitățile de observare de la înălțime fiind suplinite de drone (Watling și Reynolds 2024, 6).

În conflictul de mare intensitate din Ucraina, tancurile au fost folosite rar ca element principal de asalt în lupta urbană. Totuși, acestea au fost alocate detașamentelor de asalt și au îndeplinit misiuni de sprijin prin foc al infanteriei, dar și pentru a penetra barajele neexplozive sau pentru a crea culoare prin dărâmăturile aflate pe căile de comunicații (Watling și Reynolds 2023, 16).

Concluzii

Analiza realizată oferă un răspuns întrebărilor de cercetare și scoate în evidență, deopotrivă, nevoia de adaptare a forțelor și operațiilor executate de către acestea. Mai mult de atât, demersul realizat atrage atenția asupra faptului că, doar printr-o explorare și studiere atentă și susținută a evoluției mediului de operare, sunt create premisele pentru inovare și adaptare. Lecțiile conflictelor militare recente demonstrează că desfășurarea operațiilor militare în mediul urban impune realizarea unor transformări constante și o adaptare continuă, deopotrivă, la nivel doctrinar și operațional a acestora. Aceste transformări includ reconsiderarea abordărilor conceptuale, ajustarea tacticilor, tehnicilor și procedurilor, recalibrarea din punct de vedere organizatoric și compozițional a structurilor tactice de forțe, înzestrarea cu noi sisteme de armament și echipamente militare, instruirea forțelor și dezvoltarea liderilor. Adaptarea operațiilor se transpune într-o serie de implicații care vizează: formarea și angajarea în luptă a unor structuri tactice interarme, adaptate specificității mediului de operare; controlul punctelor cheie și al infrastructurii critice din oraș, în scopul valorificării sistemului urban; gestionarea populației locale; izolarea amenințărilor; minimizarea daunelor și victimelor colaterale și menținerea integrității sistemelor urbane; crearea unui mediu colaborativ propice pentru încetarea ostilităților și tranziția către operații de stabilitate.

Operațiile specifice luptei armate își păstrează întâietatea în ceea ce privește dificultatea și intensitatea, transpuse în amploarea numărului de victime și în distrugeri disproporționate. Deși extrem de costisitoare, materializarea luptelor în mediul urban rămâne o certitudine, principala cauză fiind tendința părții mai slabe de a exploata avantajele mediului urban. Operațiile defensive sunt avantajate, iar rezultatele cercetării indică faptul că inițiativa atacatorului este pierdută, odată ce forțele pătrund în oraș. Ritmul ofensivei scade, forțele aflate în ofensivă fiind nevoite să reia ciclul *identificare-fixare-lovire* mult mai des. Orașele de dimensiuni mari nu pot fi izolate complet, iar infrastructura urbană permite forțelor aflate în apărare să reziste mult timp, îndeosebi în zonele industriale. La fel de adevărat este și faptul că

o evacuare completă a populației este puțin probabilă, în consecință forțele armate trebuie să gestioneze problemele cauzate de prezența civililor în zona de operație. Probabil, provocarea cea mai mare rămâne realizarea tranziției de la operațiile specifice luptei armate la cele de stabilitate și invers. În acest sens, structurile tactice de forțe terestre trebuie să fie instruite și echipate corespunzător, dar mai ales pregătite mental să realizeze această tranziție într-un mod eficient. Riscurile inerente perioadei de schimbare rezultă din dificultatea de a evalua corect nivelul amenințării, dar și din sensibilitatea procesului de transfer al autorității între forțele armate și instituțiile guvernamentale.

Luând în considerare factorul tehnologic, putem concluziona că evoluția operațiilor militare în mediul urban va depinde direct de dezvoltarea tehnologiilor de vârf, emergente și disruptive. Acestea vor determina, în viitor, apariția și dezvoltarea unor noi sisteme de armament care vor genera un impact semnificativ asupra tacticilor, tehnicilor și procedurilor de luptă. Tendințele generale în ceea ce privește evoluția armamentului vor rămâne extinderea razei de acțiune și îmbunătățirea preciziei, la acestea adăugându-se îmbunătățirea algoritmilor de identificare a țintelor și delimitarea civililor de elementele ostile. Frecvența utilizării capabilităților fără pilot/echipaj, inclusiv a celor autonome, reprezintă un alt aspect modelator al operațiilor urbane, chiar dacă acestea vor fi folosite, inițial, pe direcții secundare, misiuni de acoperire, recunoaștere și supraveghere sau în cadrul unor operații de inducere în eroare. Totuși, în ciuda tehnologizării fără precedent a câmpului de luptă și a transparenței accentuate a acestuia, versatilitatea adversarilor și complexitatea mediului urban creează premisele exploatării avantajelor acestuia din urmă.

În final, subliniem faptul că omul va rămâne elementul central în ecuația operațiilor militare din mediul urban. Prin capacitatea lor unică de a interacționa cu populația civilă, dar și cu autoritățile guvernamentale și locale, forțele terestre vor reprezenta pionul principal în conflictele viitorului, atributele lor conferindu-le capacitatea de a neutraliza amenințările, de a soluționa diferendele existente și de a atinge starea finală dorită.

Referințe

Allied Joint Publication, AJP-3. 2019. *Allied Joint Doctrine for the Conduct of Operations*. Edition C Version 1. Bruxel: NATO Standardization Office (NSO).

Arnold, Thomas D. și Nicolas Fiore. 2019. ”Five Operational Lessons from the Battle for Mosul.” *Military Review*. https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/JF-19/Arnold-Fiore-Lessons-Mosul.pdf.

Butler, Marcus. 2023. ”Russia’s Response to the Challenges of Urban Warfare in the Russo-Ukrainian War.” *Towson University Journal of International Affairs*. https://wp.towson.edu/iajournal/2023/01/13/russias-response-to-the-challenges-of-urban-warfare-in-the-russo-ukrainian-war/.

Chychota, Michael T. 2019. ”Large-Scale Combat Operations in Urban Terrain”. Vol. *Large-Scale Combat Operations - The Division Fight*. Editor US Army Command and General Staff College Press Book. Army University Press.

Collins, Liam, Michael Kofman și John Spencer. 2023. ”The Battle of Hostomel Airport: A Key Moment in Russia's Defeat in Kyiv”. https://warontherocks.com/2023/08/the-battle-of-hostomel-airport-a-key-moment-in-russias-defeat-in-kyiv/.

Department of the Army Headquarters ATP 3-06, MCTP 12-10B. 2017. *Urban Operations.* United States Marine Corps.

Department of the Army Headquarters, TRADOC Pamphlet 525-92-1. 2020. ”The Changing Character of Warfare: The Urban Operational Environment”. https://adminpubs.tradoc.army.mil/pamphlets/TP525-92-1.pdf.

Department of the Army, FM 2-0. 2023. *Intelligence.* Headquarters, Department of the Army.

Freedman, Lawrence. 2019. *Viitorul războiului.* București: Editura Litera.

Johnson, David. 2022. ”The Tank Is Dead: Long Live the Javelin, the Switchblade, the… ?” https://warontherocks.com/2022/04/the-tank-is-dead-long-live-the-javelin-the-switchblade-the/.

Jones, Seth G. 2022. ”Russia's Ill-Fated Invasion of Ukraine: Lessons in Modern Warfare”. https://www.csis.org/analysis/russias-ill-fated-invasion-ukraine-lessons-modern-warfare.

Kofman, M. și R. Lee. 2022. ”Not Built For Purpose: The Russian Military's Ill-Fated Force Design.” https://warontherocks.com/2022/06/not-built-for-purpose-the-russian-militarys-ill-fated-force-design/.

Mirea, Adrian. 2024. „Pregătirea de foc a ofensivei – necesitatea actualizării algoritmului de planificare”. *Buletinul Universității Naționale de Apărare „Carol I”* 13 (3): 126-136.

Muggah, Robert. 2015. ”Fixing Fragile Cities.” https://www.foreignaffairs.com/articles/africa/2015-01-15/fixing-fragile-cities.

NATO. 2018. *Framework for Future Alliance Operations.* Bruxel: NATO Standardisation Office.

NATO Standard, AJP-1. 2022. *Allied Joint Doctrine.* Vols. Edition F, Version 1. Bruxel: NATO Standardization Office (NSO).

NATO Standard, AJP-3.2. 2022. *Allied Joint Doctrine for Land Operations.* Vol. Edition B Version 1. Bruxel: NATO Standardization Office (NSO).

NATO, ATP-3.2.1.2. 2022. *Conduct of Land Tactical Operations in Urban Environments.* Vols. Edition A, Version 1. Bruxel: NATO Standardization Office (NSO).

Nistorescu, Claudiu-Valer. 2024. *Forțele Terestre ale Federației Ruse.* București: Editura Centrului Tehnic-Editorial al Armatei.

Pamment, James, Vladimir Sazonov, Francesca Granelli, Sean Aday, Māris Andžāns, Una Bērziņa-Čerenkova, John-Paul Gravelines și alții. 2019. ”Hybrid Threats: 2007 cyber attacks on Estonia”. 52-69. https://stratcomcoe.org/publications/hybrid-threats-2007-cyber-attacks-on-estonia/86.

Scrogin, James D. 2019. ”*Large-Scale Combat Operations: Relearning an Old Concept”. Vol. Large-Scale Combat Operations – The Division Fight*. Editor US Army Command and General Staff College Press Book. Army University Press.

Statul Major al Forțelor Trerestre, F.T.-1. 2017. *Doctrina operațiilor forțelor terestre.* București: Statul Major al Forțelor Terestre.

Toroi, George. 2024. „Reziliența – multiplicator al efectelor în pregătirea contracarării inducerii în eroare." *Buletinul Universității Naționale de Apărare „Carol I"* 13 (3): 111-125.

UK Ministry of Defence. 2024. *Global Strategic Trends.* Seventh Edition. https://assets.publishing.service.gov.uk/media/673602412469c5b71dbc7b6f/Global_Strategic_Trends_Out_to_2055.pdf.

US Joint Chiefs of Staff, JP 3-06. 2013. "Joint Urban Operations". https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_06.pdf.

Vereș, Petru-Marian. 2024. „Integrarea capabilităților multidomeniu în operațiile unităților interarme din forțele terestre." *Buletinul Universității Naționale de Apărare „Carol I"* 13 (1): 44-59.

Watling, Jack și Nick Reynolds. 2023. *Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine.* Londra: Royal United Services Institute for Defence and Security Studies/RUSI.

—. 2024. *Tactical Lessons from Israel Defense Forces Operations in Gaza, 2023.* Londra: Royal United Services Institute for Defence and Security Studies.

BULETINUL
UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I"
https://buletinul.unap.ro

Evoluția navelor de luptă în era digitală

Evolution of warships in the digital age

Cpt.cdor.Dr. Alexandru-Lucian CUCINSCHI*
*Universitatea Națională de Apărare „Carol I", București, România
e-mail: cucinschi.alexandru@gmail.com

Abstract

În contextul evoluției istorice a conflictelor maritime, navele de luptă au fost întotdeauna pilonii centrali ai puterii navale, determinând cursul unor imperii și influențând rezultatul războaielor. De la triremele grecești și galerele romane, care au dominat lumea antică, până la portavioanele epocii moderne, aceste nave au fost esențiale atât în apărarea națională, cât și în explorarea și colonizarea noilor teritorii. În era contemporană, rolul navelor de luptă s-a extins și mai mult, integrând misiuni umanitare și de menținere a păcii, menținându-și însă funcțiile fundamentale de protejare a căilor maritime de comunicații, de control al spațiilor maritime și de proiecție a forței. Pe măsură ce tehnologia continuă să avanseze, era digitală redefinește capabilitățile navale, propulsând navele de luptă într-o nouă eră de inovație și complexitate strategică. În acest articol se prezintă un scurt istoric al navelor de luptă, evidențiindu-se elementele esențiale care au contribuit la dezvoltarea și relevanța lor continuă, analizându-se impactul erei digitale asupra acestor platforme esențiale pentru securitatea globală.

In the context of historical developments in maritime conflicts, warships have always been the central pillars of naval power, determining the course of empires and influencing the outcomes of wars. From ancient Greek triremes and Roman galleys to modern aircraft carriers, these vessels have been essential in both national defence and the exploration and colonization of new territories. In contemporary times, the role of warships has further expanded to include humanitarian and peacekeeping missions while maintaining their fundamental functions of protecting maritime communication routes, controlling maritime spaces, and projecting force. As technology continues to advance, the digital age redefines naval capabilities, propelling warships into a new era of innovation and strategic complexity. This article provides a brief history of warships, highlighting the essential elements that have contributed to their development and ongoing relevance, and explores the future impact of the digital age on these crucial platforms for global security.

Cuvinte-cheie:
putere maritimă; securitate maritimă; eră digitală; nave de luptă;
tehnologie digitală; inteligență artificială.

Keywords:
maritime power; maritime security; digital age; warships; digital technology; artificial intelligence.

Info articol
Primit: 20 septembrie 2024; Evaluat: 17 octombrie 2024; Acceptat: 11 noiembrie 2024; Disponibil online: 17 ianuarie 2025
Citare: Cucinschi, A.L. 2024. „Evoluția navelor de luptă în era digitală".
Buletinul Universității Naționale de Apărare „Carol I", 13(4): 21-29. https://doi.org/10.53477/2065-8281-24-36

Acest articol explorează principalele repere istorice care au definit funcțiile și importanța navelor de luptă de-a lungul timpului, evidențiind modul în care acestea și-au păstrat misiunile esențiale, în pofida transformărilor aduse de progresul tehnologic. De asemenea, analizează implicațiile modernizării și digitalizării asupra operațiunilor navale contemporane, subliniind provocările și oportunitățile emergente în cadrul securității maritime globale. Această analiză critică urmărește să ofere o înțelegere aprofundată a dinamicii istorice și tehnologice a navelor de luptă, evidențiind relevanța lor continuă în contextul geopolitic actual.
Din această perspectivă istorică și contemporană, studiul navelor de luptă relevă nu doar o poveste de adaptare și inovare, ci și o manifestare continuă a influenței lor durabile asupra geopoliticii și securității internaționale. Într-o lume în continuă schimbare, Forțele Navale vor continua să joace un rol central, adaptându-se noilor realități tehnologice și strategice.

Metodologia cercetării pentru elaborarea acestui articol cuprinde:

- o abordare cronologică, pentru a examina tranzițiile cheie în designul și funcția navelor de luptă, identificând factorii tehnologici și geopolitici care au determinat aceste schimbări;
- selectarea și analiza unor studii de caz ale națiunilor care au avut o contribuție semnificativă la inovațiile navale, cum ar fi Anglia în epoca modernă timpurie sau Statele Unite în era contemporană, pentru a înțelege variațiile în strategii și tehnologii;
- analizarea modului în care aceste evoluții tehnologice și istorice influențează strategiile de apărare națională și internațională, folosind modele strategice și scenarii de conflict actuale.

Limitele cercetării sunt reprezentate de lipsa accesului la informații clasificate, referitoare la cele mai recente tehnologii implementate de Forțele Navale aparținând statelor care posedă o industrie de apărare foarte dezvoltată, în care instituțiile militare au institute de cercetare și inovare. În cele mai multe state, în prezent, Forțele Armate nu mai sunt cele care inovează, acestea rezumându-se la selectarea tehnologiilor civile care prezintă interes militar și la dezvoltarea lor.

Articolul este structurat în patru părți, în prima parte voi prezenta câteva repere istorice relevante pentru evoluția navelor de luptă, apoi voi prezenta un posibil model de construire a capabilităților navale, pentru a înțelege, în principal, limitările platformelor navale, iar în a treia și a patra parte voi prezenta caracteristicile principale ale erei digitale și impactul asupra navelor de luptă.

Scurt istoric al navelor de luptă

Pe parcursul istoriei, navele de luptă au fost instrumente esențiale ale puterii maritime, influențând desfășurarea conflictelor și formarea imperiilor. În era modernă, misiunile navelor de luptă sunt, în principal, cele consolidate de-a lungul

istoriei, ele jucând un rol crucial în securitatea maritimă globală, în protejarea liniilor de comunicații și proiecția forței în conflicte regionale și internaționale.
Pentru a evidenția faptul că misiunile navelor de luptă nu s-au schimbat în esență și pentru a construi un tipar al evoluției și relevanței acestora, voi prezenta principalele repere istorice care au definit navele de luptă și importanța acestora.

Primele nave de luptă, precum triremele grecești și galerele romane, erau propulsate cu rame și erau folosite în confruntările maritime. Aceste nave erau construite pentru a manevra rapid și a provoca daune prin abordaj, folosindu-se de arcașii și de catapultele de la bord (Strauss 2004).
În Evul Mediu, vikingii au dezvoltat nave lungi, rapide și manevrabile, folosite pentru raiduri și comerț (Magnusson 1980). Aceste nave au influențat designul ulterior al navelor de luptă din Europa.
Progresul în construcția navelor a condus la apariția navelor de linie, mari și cu mult armament, care dominau mările. Acestea aveau punți multiple pe care erau instalate tunuri, fiind folosite în marile bătălii navale, precum cele din timpul războaielor napoleoniene.

Navele de luptă au permis explorarea și colonizarea noilor teritorii. În perioada descoperirilor maritime, națiuni precum Portugalia, Spania, Olanda și Anglia au folosit nave de luptă pentru a explora teritorii necunoscute, pentru a stabili colonii și a revendica noi pământuri. Această expansiune a contribuit la crearea imperiilor globale și la răspândirea influențelor culturale și economice.
Controlul mărilor și oceanelor a fost esențial pentru prosperitatea economică a imperiilor. Navele de luptă protejau rutele comerciale împotriva pirateriei și atacurilor inamice, asigurând fluxul liber de bunuri și resurse. De exemplu, pe măsură ce Imperiul Britanic s-a extins, Marina Regală a protejat rutele comerciale globale, contribuind la dominația economică a Marii Britanii în secolele XVII-XIX.
Revoluția industrială a marcat trecerea de la navigația cu vele la propulsia cu abur. Această eră a introdus navele de luptă blindate, cum ar fi celebrul HMS Warrior.

Cele două războaie mondiale au determinat o dezvoltare rapidă a navelor de luptă. Cuirasatele, precum HMS Dreadnought, au redefinit lupta navală la începutul secolului XX (Edwards 2024). După Cel de-Al Doilea Război Mondial, portavioanele au devenit esențiale, datorită capacității lor de a lansa avioane și de a proiecta putere la distanțe mari.

Prezența unei flote puternice poate acționa ca un factor de descurajare împotriva adversarilor și poate fi folosită pentru a proiecta puterea unei națiuni la scară internațională. Navele de luptă permit desfășurarea rapidă și strategică a forțelor militare, oferind națiunilor capacitatea de a interveni în conflicte la mare distanță de granițele lor. Aceste capacități sunt evidente în exemplele moderne de utilizare a portavioanelor și a grupurilor de luptă maritimă de către marile puteri ale lumii. Bătălii navale celebre, precum Bătălia de la Midway, au dovedit că superioritatea navală poate decide soarta războaielor și poate schimba echilibrul de putere

internațională (history.com 2024). Victoria în aceste confruntări a oferit puterilor maritime controlul asupra mărilor, subminând capacitatea inamicilor de a apăra sau extinde teritoriile.

În epoca contemporană, navele de luptă nu sunt doar instrumente de război, ci și platforme pentru misiuni umanitare, de menținere a păcii și de cooperare internațională. Participarea la exerciții maritime internaționale și la misiuni comune ajută la întărirea relațiilor dintre națiuni, promovând stabilitatea și securitatea globală.
În continuare, apreciez că o detaliere a modului în care sunt construite capabilitățile navale este necesară, având în vedere diversitatea și specificitatea acestora, în funcție de factorii determinanți pentru caracteristicile principale ale unei platforme navale.

Factorii care influențează construcția navelor – tipuri de nave

Pentru a înțelege elementele care concură la construirea capabilităților Forțelor Navale, consider că elementele reieșite din studiul pe care l-am întocmit cu privire la lupta la litoral pot reprezenta un model simplist, pe baza căruia se construiesc platforme navale, adecvate diferitelor situații strategice.
Astfel, principala concluzie a studiului, bazat pe analiza unor cazuri istorice de acțiuni militare, desfășurate în zona litoralului, este că particularitățile mediului influențează modul în care este construită platforma navală, care, la rândul său, influențează armamentul și tehnica instalate pe platformă, toate acestea având implicații directe asupra tacticii utilizate în luptă (Cucinschi 2020).

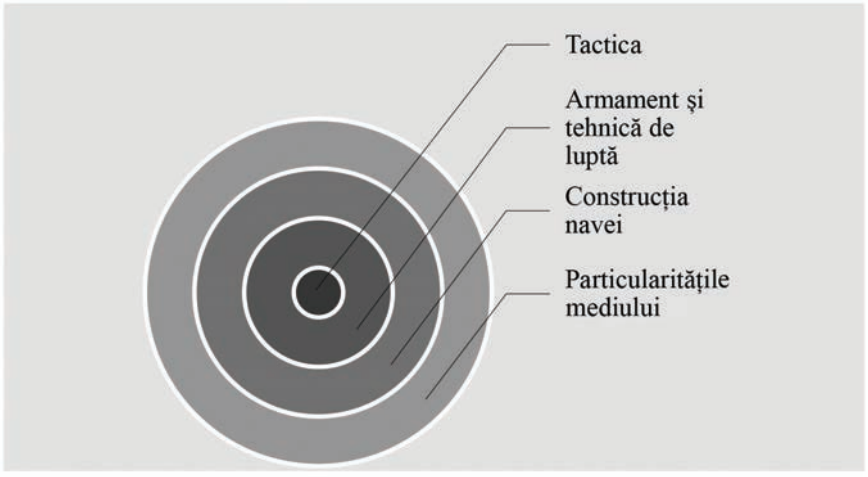


Figura 1 Interdependența dintre elementele principale ale luptei la litoral (Cucinschi 2020)

Ulterior, prin studii de caz, având ca subiect statele care au dezvoltat capabilități eficiente pentru lupta la litoral, am ajuns la concluzia că, pe lângă cele menționate anterior, trebuie să se mai țină cont de adversar, de forma acțiunii (ofensivă sau defensivă și mai puțin, în cazul operațiilor de stabilitate) și de experiența în construcția de platforme navale (Cucinschi 2020).

Plecând de la acest studiu, se poate înțelege modul în care sunt construite, în prezent, capabilitățile navale, în funcție de mediul fizic – acesta poate permite construirea de platforme mari (pentru oceane și mări de dimensiuni mari) sau mici, pentru mări de dimensiuni mici, închise sau semiînchise.

Ulterior, platformele, în funcție de dimensiunile lor, pot fi echipate cu diferite tipuri de armament. Având în vedere faptul că Forțele Navale abordează lupta pe medii: la suprafață, antisubmarin, antiaerian (mai nou, lupta pe fundul mării), armamentul este grupat în aceste trei categorii.
De regulă, navele de dimensiuni relativ mici, de tipul corvetelor, permit echiparea cu armament și cu senzori, pentru lupta într-un singur mediu și limitat, în celelalte medii. Fregatele, care sunt nave de dimensiuni medii, permit echiparea cu senzor și armament pentru lupta în două medii și limitat, în al treilea mediu. Distrugătoarele, fiind nave de dimensiuni mari, permit montarea de echipament și senzori care să fie în măsură să lupte în toate cele trei medii.

Pe lângă misiunile specifice doar Forțelor Navale, navele militare pot executa și acțiuni în sprijinul Forțelor Terestre, Forțelor Aeriene și Forțelor pentru Operații Speciale, de regulă cu nave de dimensiuni mari (distrugătoare, crucișătoare, portavioane) sau cu nave specializate (nave de desant). Lupta pe fundul mării, până în prezent, nu a fost asociată cu un anumit tip de navă, neexistând deocamdată elemente concrete privind modul de abordare a acestui nou mediu.

Consider că este important să înțelegem modul în care sunt construite principalele tipuri de nave de luptă, pentru că, în multe cazuri, așteptările celorlalte categorii de forțe sau al comandanților forțelor întrunite depășesc sfera posibilului pentru platformele navale. De asemenea, pentru a înțelege modul în care era digitală impactează transformarea navelor militare, este necesar să înțelegem reperele care stau la baza specificității tipurilor de nave utilizate în conflictele actuale, acesta fiind motivul pentru care am desfășurat această scurtă analiză.
În continuare, voi face o analiză cu privire la ceea ce reprezintă intrarea în era digitală și la modul în care aceasta poate conduce la transformări în ceea ce privește construirea de capabilități pentru platformele Forțelor Navale.

Era digitală – caracteristici definitorii

Era digitală, numită adesea și era informațională, este o perioadă din istoria umanității, caracterizată de revoluții tehnologice majore și de tranziția de la economia bazată pe resurse materiale la una bazată pe informație și cunoaștere. Această eră are câteva caracteristici definitorii care au transformat profund societatea, economia, cultura și modul în care interacționăm unii cu ceilalți.

1. *Tehnologia digitală și accesibilitatea informației:* Una dintre cele mai emblematice trăsături ale erei digitale este abundența și accesibilitatea informației prin intermediul tehnologiei. Internetul, calculatoarele personale,

smartphone-urile și alte dispozitive digitale ne permit să accesăm și să distribuim informații la scară globală într-un mod rapid și eficient. Acest acces nelimitat la informație a democratizat cunoașterea, permițând indivizilor să învețe și să se dezvolte în mod autonom (Katz și Ronald 2002).

2. Comunicațiile globale: Era digitală a transformat radical modul în care comunicăm. Rețelele sociale, e-mailurile, mesajele instantanee și platformele de videoconferință ne permit să rămânem conectați cu ceilalți, indiferent de distanțele geografice. Această globalizare a comunicațiilor a favorizat schimburile culturale și economice, dar a condus și la fenomene precum dependența de tehnologie și difuzarea rapidă a dezinformărilor (Castells 1996).

3. Economia digitală: Inovațiile tehnologice au dus la apariția unei economii digitale, în care bunurile și serviciile sunt create, gestionate și tranzacționate în mediul online. Platformele de comerț electronic, activele digitale și criptomonedele sunt manifestări ale acestei tranziții. Economia digitală a creat oportunități de afaceri noi și a schimbat paradigmele de angajare, permițând lucrul la distanță și dezvoltarea de cariere în domenii emergente (Brynjolfsson și McAfee 2014).

4. Automatizarea și inteligența artificială: Progresele în inteligența artificială și în automatizare au avut un impact profund asupra locurilor de muncă și eficienței industriale. Deși aceste tehnologii au îmbunătățit productivitatea și au redus costurile, ele au generat și îngrijorări legate de pierderea locurilor de muncă și de etica în utilizarea IA (Tapscott 1995).

5. Impactul social și cultural: Era digitală a modelat profund și aspectele sociale și culturale ale vieții noastre. Persoanele își construiesc identități hibride atât fizice, cât și virtuale, având posibilitatea de a se exprima și organiza în comunități digitale. Totuși, acest mediu a contribuit și la fenomenul de izolare socială și a ridicat întrebări privind intimitatea și securitatea datelor personale (Turkle 2012).

6. Provocările de securitate: Cu beneficiile conectivității digitale vin și provocările legate de securitatea cibernetică. Amenințările, precum hackingul, frauda online și atacurile cibernetice, sunt în creștere, impunând nevoia de soluții sofisticate de securitate și educație în domeniul protecției datelor (Van Dijk 2012).

În concluzie, era digitală se caracterizează printr-o interconectivitate sporită, inovații economice și tehnologice și provocări sociale și etice. Aceste transformări au dus la o reconfigurare a societății globale, oferind numeroase oportunități, dar, în același timp, solicitând responsabilitate în gestionarea efectelor tehnologice asupra umanității.

Impactul erei digitale asupra platformelor navale

Era digitală a adus transformări majore în multiple domenii de activitate, inclusiv în cel al conflictelor maritime. Navele de luptă, considerate esențiale în strategiile de apărare ale oricărei națiuni maritime, nu au rămas insensibile la aceste schimbări.

În primul rând, tehnologia digitală a revoluționat echipamentele și sistemele de

bord ale navelor de luptă. Sistemele de gestionare a informațiilor la bordul navelor au devenit mai avansate și mai interconectate. Integrarea tehnologiilor digitale a dus la dezvoltarea sistemelor de senzori mai eficienți, a sistemelor de comunicație securizate și la îmbunătățirea capacității de reacție rapidă. De exemplu, utilizarea inteligenței artificiale a permis automatizarea unor procese complexe, astfel încât multe dintre operațiunile de rutină pot fi acum gestionate cu un impact minim din partea echipajului uman, ceea ce reduce erorile și crește eficiența operațională.

În al doilea rând, era digitală a deschis noi orizonturi în ceea ce privește strategiile navale. Conceptul de război cibernetic a devenit o componentă crucială a conflictelor moderne. Navele de luptă trebuie acum să fie pregătite pentru amenințări cibernetice, dezvoltând capacități de apărare și de atac digital. Acest lucru presupune implementarea unor sisteme avansate de securitate cibernetică și instruirea personalului în domeniul războiului cibernetic, asigurând protecția informațiilor critice și a infrastructurii de comunicare.

În plus, proiectarea asistată de calculator și simulările virtuale au revoluționat modul în care navele de luptă sunt concepute și testate. Aceste tehnologii permit inginerilor să creeze modele 3D extrem de detaliate și să simuleze diverse scenarii operaționale, înainte de a începe construcția efectivă. Astfel, se reduc erorile de design și se optimizează performanța navei pentru diferite condiții de luptă, economisind timp și resurse semnificative.

De asemenea, sistemele moderne de armament, integrate cu tehnologie digitală reprezintă un progres semnificativ atât în apărare, cât și în atac. Tehnologiile ghidate digital, cum ar fi torpilele inteligente și rachetele teleghidate, oferă precizie și putere de foc superioare. Sistemele de apărare antiaeriană și antinavă au fost și ele mult optimizate prin senzori și radare avansate, permițând detectarea și neutralizarea amenințărilor cu mult înainte de a deveni critice.

Totodată, tehnologia digitală a dus la îmbunătățiri în ceea ce privește durabilitatea și sustenabilitatea navelor de luptă. Proiectele moderne se concentrează pe reducerea semnăturii radar și acustice, utilizând materiale avansate și design inovator care le fac mai greu de detectat de către inamici și mai eficiente din punct de vedere energetic. Mai mult decât atât, era digitală a promovat integrarea și interoperabilitatea dintre diferite tipuri de forțe armate și națiuni. Navele de luptă sunt acum capabile să participe la exerciții multinaționale și la operațiuni de menținere a păcii, datorită sistemelor standardizate de comunicație și partajare a informațiilor. Aceste capacități sunt cruciale pentru cooperarea internațională și pentru reactualizarea rapidă a informațiilor strategice în situații de criză.

Pe lângă avantajele tehnice și strategice, transformările din era digitală au provocat și unele dileme etice și sociale. Automatizarea și folosirea inteligenței artificiale în deciziile de luptă ridică probleme de responsabilitate și moralitate, mai ales când vine vorba de acțiuni letale. În plus, dependența crescută de sistemele digitale

expune navele de luptă la riscuri de manipulare sau disfuncționalități, cauzate de atacuri cibernetice.

Astfel, consider că se poate afirma faptul că era digitală a influențat profund evoluția navelor de luptă, modul în care acestea operau fiind radical redefinit. Inovațiile tehnologice au dus la îmbunătățirea eficienței și a capacităților operaționale ale navelor, în timp ce noi provocări strategice și etice au apărut, în contextul integrării digitale. Este esențial ca forțele navale să continue să se adapteze la aceste schimbări, dezvoltând soluții inovatoare pentru a răspunde cerințelor moderne de apărare și securitate.

Concluzii

Pe parcursul istoriei, navele de luptă au rămas esențiale în proiecția puterii maritime și protejarea securității internaționale. Deși misiunile fundamentale ale acestor nave au evoluat, esența lor a rămas aceeași: asigurarea controlului spațiului maritim și protecția liniilor de comunicație.
Din epoca triremelor și galerelor până la navele moderne, dotate cu tehnologii avansate, evoluția navelor de luptă reflectă progresele în construcția navală și armament. Aceste nave au fost instrumentale nu doar în războaie, ci și în explorare și colonizare, definind contururile marilor imperii istorice.

Revoluția industrială și, mai recent, era digitală au transformat în mod fundamental platformele navale. Propulsia modernă, armamentul sofisticat și automatizarea au sporit eficiența, dar au introdus și noi provocări, cum ar fi necesitatea protecției cibernetice și gestionarea etică a inteligenței artificiale.
Era digitală a facilitat promovarea cooperării maritime internaționale. Navele de luptă moderne sunt echipate pentru interoperabilitate, permițând participarea la exerciții și misiuni multinaționale, ceea ce întărește relațiile diplomatice și contribuie la securitatea globală.

În contextul erei digitale, Forțele Navale trebuie să continue să se adapteze, dezvoltând soluții inovatoare pentru a răspunde provocărilor contemporane. Integrarea de noi tehnologii trebuie echilibrată cu responsabilitățile etice și cu protecția împotriva amenințărilor cibernetice.

Referințe

Brynjolfsson, E. și A. McAfee. 2014. "The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies". W. W. Norton & Company, Inc. https://edisciplinas.usp.br/pluginfile.php/4312922/mod_resource/content/2/Erik%20-%20The%20Second%20Machine%20Age.pdf.

Castells, M. 1996. *The Rise of the Network Society.* Malden: Blackwell Publishers. https://onlinelibrary.wiley.com/doi/book/10.1002/9781444319514.

Cucinschi, Alexandru-Lucian. 2020. *Lupta la litoral pentru Forțele Navale.*

Edwards, Giles. 2024. ”How the Dreadnought sparked the 20th Century’s first arms race”. https://www.bbc.com/news/magazine-27641717.

history.com. 2024. ”Battle of Midway”. https://www.history.com/topics/world-war-ii/battle-of-midway.

Katz, J. și R. Ronald. 2002. *Social Consequences of Internet Use: Access, Involvement, and Interaction.* MIT Press Ltd. https://direct.mit.edu/books/monograph/3803/Social-Consequences-of-Internet-UseAccess.

Magnusson, Magnus. 1980. *Vikings.* E.P. Duton. https://www.abebooks.co.uk/9780370302720/Vikings-Magnusson-Magnus-0370302729/plp.

Strauss, Barry. 2004. *The Battle of Salamis The Naval Encounter That Saved Greece - and Western Civilisation.* Simon and Schuster. https://books.google.ro/books/about/The_Battle_of_Salamis.html?id=gcJ34dOcA3MC&redir_esc=y.

Tapscott, D. 1995. *The Digital Economy: Promise and Peril in the Age of Networked Intelligence.* McGraw-Hill. https://books.google.ro/books/about/The_Digital_Economy.html?id=Nzi8QgAACAAJ&redir_esc=y.

Turkle, S. 2012. ”Alone Together: Why We Expect More from Technology and Less from Each Other”. https://www.academia.edu/3129910/Alone_together_Why_we_expect_more_from_technology_and_less_from_each_other.

Van Dijk, J. 2012. *The Network Society.* SAGE Publications Ltd.

BULETINUL
UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I"
https://buletinul.unap.ro

Date noi privind amploarea dezertărilor din Armata Roșie (Sovietică) – expresie a rezistenței antisovietice a populației RSS Moldovenești în anii 1944-1954

New data on the practice of desertions from the Red (Soviet) Army as an expression of the anti-Soviet resistance of the Moldavian SSR population in the years 1944-1954

Conf.univ.Dr.habil. Anatolie LEȘCU*
*Academia Militară a Forțelor Armate „Alexandru cel Bun", Chișinău, Republica Moldova
e-mail: lescuanatol@yahoo.com

Abstract

Istoria părții de est a ceea ce a fost pe timpuri Țara Moldovei sau a arealului estic al spațiului românesc, situat în interfluviul pruto-nistrean, teritoriu, care, ulterior, a primit denumirea de Basarabia, este una tragică și zbuciumată. Numai în ultimii 200 de ani acest teritoriu a trecut prin trei ocupații și anexări, toate săvârșite de statul rus, în diferite forme ale existenței sale – 1812, 1940, 1944. Sovietizarea Moldovei după a doua ocupație a Basarabiei, din vara anului 1944, a decurs cu mari greutăți, populația din artificial creata RSS Moldovenească opunându-se prin diferite metode autorităților sovietice. Printre diversele forme de rezistență, se regăsea și dezertarea din rândurile Armatei Sovietice. În condițiile sovietizării forțate a RSSM, în perioada anilor 1944-1953, această practică a căpătat unele trăsături cu un pronunțat caracter antisovietic, făcând parte din arsenalul luptei populației împotriva ocupanților.

The history of the eastern part of what used to be Moldova, or the eastern area of Romanian territory located in the Pruto-Nistrean interfluve, which later became known as Bessarabia, is a tragic and turbulent one. In the last 200 years alone, this territory has undergone three occupations and annexations, all carried out by the Russian state in different forms: 1812, 1940, and 1944. The Sovietization of Moldova after the subsequent occupation of Bessarabia in the summer of 1944 proceeded with great difficulties, as the artificially created population of the Moldavian SSR resisted Soviet authorities in various ways. One of the forms of resistance was desertion from the Soviet Army. Desertion, a phenomenon characteristic of all armies worldwide, is a criminal offence that involves evading military service through various methods, such as fleeing from a unit or avoiding enlistment altogether. Under the conditions of forced Sovietization in the SSR between 1944 and 1953, this practice took on distinctly anti-Soviet characteristics, becoming a part of the population's struggle against the occupiers.

Cuvinte-cheie:
URSS; RSS Moldovenească; Armata Roșie (Sovietică); mobilizare; populație; dezertare; servicii de securitate; soldat; ofițer; crimă; fugă de sub escortă; arest.

Keywords:
USSR; Moldavian SSR; Red Army (Soviet); mobilization; population; desertion; security services; soldier; officer; murder; escape; arrest.

Info articol
Primit: 26 iunie 2024; Evaluat: 25 august 2024; Acceptat: 6 noiembrie 2024; Disponibil online: 17 ianuarie 2025
Citare: Leșcu, A. 2024. „Date noi privind amploarea dezertărilor din Armata Roșie (Sovietică) – expresie a rezistenței antisovietice a populației RSS Moldovenești în anii 1944 - 1954". *Buletinul Universității Naționale de Apărare „Carol I"*, 13(4): 30-37. https://doi.org/10.53477/2065-8281-24-37

Odată cu înaintarea trupelor Armatei Roșii (din **februarie** 1946 – Armata Sovietică) pe teritoriul Basarabiei, ca urmare a operației Uman-Botoșani, iar ulterior, Iași-Chișinău, autoritățile sovietice intensifică procesul sovietizării și comunizării RSSM, proces început încă din iunie 1940, manifestat prin colectivizarea forțată, foametea **provocată**, deportări în masă **ale elitei autohtone**. **Din primele zile ale ocupației,** populația românească locală, dar și cea alolingvă, s-a arătat reticentă față de noii stăpâni, manifestându-și nesupunerea prin diferite forme de **rezistență**. Printre multiple forme de rezistență antisovietică din această perioadă, **se observă și numărul mare de** dezertări ale tinerilor încorporați în Armata Sovietică din unitățile militare sau **neprezentarea la încorporare** în armată. Dosarele organelor de partid și ale celor sovietice, cât și ale comisariatelor militare din RSSM din perioada 1944 - 1955, păstrate în depozitele Arhivei Naționale a Republicii Moldova și Arhivei Organizațiilor Social-Politice a Republicii Moldova, aruncă o lumină nouă asupra acestui aspect din istoria rezistenței instaurării regimului comunist din perioada respectivă. Noțiunii generale de dezertare, autoritățile militare sovietice îi atribuiau mai multe înțelesuri, printre care se regăseau: dezertarea propriu-zisă din unitatea militară, **neprezentarea la încorporare în armată** și la citațiile comisariatului militar, fuga din transport pe timpul deplasării către locul **prestării** serviciului militar până la depunerea jurământului, **nerevenirea** la unitatea militară din concediu sau tratament medical și altele. Sub incidența dezertării, intrau și tinerii premilitari, recrutați în mod obligatoriu pentru studii la școli profesional-tehnice (FZU – **transliterarea din limba rusă a termenilor respectivi**) de pe teritoriul URSS.

Mobilizarea masivă a populației din RSSM a început odată cu înaintarea trupelor sovietice pe teritoriul țării. RSSM era privită de comandamentul militar sovietic ca o importantă **resursă** demografică de suplinire a pierderilor Armatei Roșii, suferite în timpul campaniei din anul 1944 de pe toate teatrele de operații. Numai în perioada martie - 25 decembrie 1944 au fost mobilizați în armată sute de mii de oameni, după cum urmează:

- în unitățile Regiunii militare Odessa – 115.504 de oameni;
- în unitățile Fronturilor 1 și 2 Ucrainean – 123.776 de oameni;
- mobilizați **premilitari** – 2.658 de oameni;
- mobilizați în calitate de rezervă a Regiunii militare Odessa – 21.343 de oameni;
- în TOTAL – 263.281 de oameni.

Totodată, în economie au fost mobilizați 23.334 de oameni (AOSPRM, Fond 51, inventar 3, dosar 438, f. 4). Dar începând mobilizarea în masă a populației, autoritățile sovietice și militare s-au ciocnit cu un fenomen nou pentru ei, cel a dezertărilor în masă a populației mobilizate din unitățile militare sau **neprezentarea** la mobilizare. Din start acest fenomen a **vădit** un pronunțat caracter antisovietic. Astfel, în iunie 1944, numai din Regimentul 52 pușcași de rezervă, cu dispunerea permanentă în orașul Moghilău (Mohîliv-Podilskîi) din stânga Nistrului, au dezertat peste 300 de ostași nou mobilizați din județul Soroca, toți moldoveni, în frunte cu Gumenâi Venedict (AOSPRM, Fond 51, inventar 3, dosar 431, f. 21). În iunie 1944,

în pădurea de la Otaci acționa un grup de dezertori din Armata Roșie, compus din **șapte** persoane, în frunte cu Ruga Ion, originar din comuna Rudi, înarmați cu **două** puști și un pistol automat, iar în pădurea de la Țeplenești, județul Bălți, un alt grup, în frunte cu Chicu Grigorie, originar din satul respectiv (AOSPRM, Fond 51, inventar 3, dosar 431, f. 22). Cel mai periculos pentru autorități era totuși un grup înarmat de dezertori, compus din șapte persoane, care activa în comuna Șeptelici și care își avea ca scop lupta armată împotriva puterii sovietice (AOSPRM, Fond 51, inventar 3, dosar 431, f. 24).

Amploarea fenomenului **a fost** atât de mare, **încât a alarmat autoritățile militare,** care, în nota informativă, adresată, la 25 iulie 1944, pe numele lui Nikita Salogor, Prim-secretarului Partidului Comunist din RSS Moldovenească, comunicau că „în rândurile moldovenilor mobilizați în Armata Roșie se manifestă tendința de a dezerta din unitățile armatei agravată de spiritul antisovietic." (AOSPRM, Fond 51, inventar 3, dosar 45, f. 48). Astfel, numai din Divizia 35 de Instrucție a **Pușcașilor**, în iulie 1944, au dezertat 32 de cursanți, toți moldoveni, din raioanele recent „eliberate" de Armata Roșie. Simptomatic **este faptul** că organizatorii fugarilor, printre care se evidenția N. Spinei, condamnat, ulterior, de justiția sovietică la moarte, au făcut parte în trecut din armata română (AOSPRM, Fond 51, inventar 3, dosar 45, f. 48 verso). Alarmați de creșterea fenomenului și pentru a curma tendința tot mai mare a moldovenilor de a fugi din rândurile Armatei Roșii**,** în cadrul organelor centrale de partid și a celor sovietice a fost creată o comisie specială, însărcinată cu elaborarea măsurilor concrete de luptă împotriva dezertărilor, compusă din nouă persoane, după cum urmează:

1. tovarășul Proletarschi, șef secția militară a comitetului județean de partid Bender (Tighina);
2. căpitanul Mulița, adjunct șef secția 1, Comisariatul Militar RSSM;
3. locotenent-major Ivliev, adjunct șef secție 1, lupta contra banditismului, Comisariatul Poporului de Interne (NKVD) RSSM;
4. căpitan Cuceruc, adjunct șef secție 1, lupta contra banditismului, Comisariatul Poporului de Interne (NKVD) RSSM;
5. tovarășul Haidalov, șef secția militară a comitetului raional de partid Chișinău;
6. locotenent-major Corniuhin, adjunct șef secție 2, Comisariatul raional Strășeni;
7. tovarășul Minin, instructor în cadrul Departamentului militar CC PC(b) Moldova;
8. căpitan Gologalov, secretarul organizației de partid a Comisariatului Militar RSSM;
9. căpitan Kocetkov, șef secția 2, lupta contra banditismului, Comisariatul Poporului de Interne (NKVD) **al** RSSM (AOSPRM, Fond 51, inventar 3, dosar 431, f. 16).

În pofida „entuziasmului" bolșevic și eforturilor depuse, lucrările comisiei s-au arătat a fi ineficiente, **activitatea ei soldându-se** cu un eșec total. Din lună în lună,

numărul fugarilor creștea, **încurajați** și de rudele rămase acasă, care, în scrisori trimise **celor luați** în armată, **îi** îndemnau să fugă. În cunoștință de cauză privind cenzurarea scrisorilor trimise, chiar și scrise în limba română, mulți foloseau cuvinte cifrate sau fraze și cuvinte scrise în limba țigănească (**rromani**), de neînțeles pentru ruși (AOSPRM, Fond 51, inventar 3, dosar 45, f. 1). Mult mai grav era faptul că dezertorii și cei care **nu se prezentau** la mobilizare se adunau în grupuri și începeau a duce o luptă armată împotriva puterii sovietice. Astfel, în comuna Comratul Nou, la 5 ianuarie 1945, **doi bărbați pe nume** Slavovici – **tată și fiu – l-au ucis pe** funcționarul F. Gherasimov, responsabil cu rechizițiile agricole, care intimida populația **amenințând-o** cu mobilizări în masă în armată. Aceeași soartă a avut și succesorul său, abia intrat în funcție, ucis la 11 ianuarie 1945. În aceeași zi a fost ucis și secretarul sovietului sătesc din Chirsova, V. Tafratov.

Tot în Bugeac activa și un grup de persoane **care refuzau să se prezinte la** serviciul militar, punând la cale asasinarea președinților sovietelor sătești din Taraclia și Căinari (AOSPRM, Fond 51, inventar 3, dosar 89, f. 12). În pădurea de lângă localitatea Olănești, se ascundea de mobilizare un grup, compus din 85 de persoane. Numai în primele două luni ale anului 1945, în județul Bender (Tighina) au fost reținuți 3.226 de dezertori și persoane care **nu se prezentau** la serviciul **militar** în Armata Roșie și 980 de dezertori **din rândul celor** mobilizați la munci în cadrul complexului industrial URSS, fapt ce nu putea să nu pericliteze planurile anunțate privind mobilizarea la război a populației republicii (AOSPRM, Fond 51, inventar 3, dosar 89, f. 13).

Documentele analizate demonstrează un fapt surprinzător pentru situația **de atunci** din Republica Moldova, dar explicabil din punct de vedere istoric, anume ostilitatea populației Bugeacului, majoritar găgăuză și bulgară, față de puterea sovietică și Armata Roșie, și simpatiile sincere **pentru** România. **Astfel**, în martie 1945, cetățeana Baradja Maria, **de naționalitate** bulgară, din comuna Taraclia, îndemna localnicii la puțină răbdare, deoarece „în primăvara 1945, în Basarabia vor veni eliberatorii noștri – români”, iar locuitorul localității Cazaclia, Stefoglo Mihail, găgăuz de naționalitate, îndemna populația să nu cedeze pământurile **ei** colhozurilor, deoarece „în curând, în Basarabia vor veni românii și trebuie ajutați ai noștri […] trebuie să ne ascundem de mobilizare și să întâmpinăm armata română”. De aceeași părere era și locuitorul comunei Tătar Copceac, Anghelcev Tudor, găgăuz de naționalitate, care declara sus și tare că „este necesar cu orice preț să nu nimerim în Armata Roșie […] deoarece **Basarabia a fost și va fi românească**”. Merită tot respectul generației actuale președintele sovietului sătesc din Cazaclia, Dobrova Xenia, care, în pofida funcției ocupate, nu numai că susținea deschis în fața consătenilor că „viața în URSS este nocivă pentru țărani, iar comuniștii sunt impostori, pe când românii în perioada interbelică se **arătau** cu respect față de găgăuzi și nu aveau loc represalii politice”, dar **îi și avertiza** pe bărbați asupra datei mobilizării ca ei să aibă timp să se ascundă în păduri (AOSPRM, Fond 51, inventar 3, dosar 89, f. 20).

În pofida măsurilor întreprinse, situația se agrava cu fiecare zi. Amploarea fenomenului poate fi demonstrată prin numărul dezertorilor și al celor care **nu se**

prezentau la încorporare, reținuți în perioada aprilie 1944 - aprilie 1945, fără a ține cont de cei care nu au fost prinși, date prezentate în tabelul următor:

TABEL NR. 1

Numărul dezertorilor și neprezentaților, reținuți în aprilie 1944-aprilie 1945
(AOSPRM, Fond 51, inventar 3, dosar 89, f. 19)

Județ	Numărul neprezentaților reținuți	Numărul dezertorilor reținuți
Chișinău	1 113	1 480
Soroca	1 894	4 091
Bălți	2 082	3 478
Orhei	1 614	1 312
Bender (Tighina)	3 114	2 013
Cahul	2 315	1 905
Stânga Nistrului	810	901
TOTAL	**12 942**	**15 180**

Procesul a continuat cu **aceeași** amploare și în anii următori. În anii 1947-1948 erau înregistrate 162 de persoane dezertate din armată (AOSPRM, Fond 51, inventar 7, dosar 60, f. 113). Pe întreg anul 1948 și **în primele** patru luni **ale** anului 1949, în RSSM au fost înregistrate 240 de cazuri de **neprezentare la încorporare în** Armata Sovietică, 208 cazuri de dezertare, iar 30 de persoane nu s-au prezentat la **centrele** de mobilizare (AOSPRM, Fond 51, inventar 8, dosar 76, f. 71). Procesarea tuturor documentelor existente ne permite să constatăm că, în perioada anilor 1946-1954, au fost raportate 228 de cazuri de dezertare din rândurile Armatei Sovietice. Fapt, că, printre dezertori, au fost numai **trei** ruși, un evreu și un buriat[1], restul fiind moldoveni, inclusiv patru moldoveni din **raionul** Chilia (RSS Ucraineană), denotă încă o dată că fenomenul dezertării avea un pronunțat caracter național de rezistență antisovietică. Situația poate fi prezentată în tabelul următor:

TABEL NR. 2

Numărul dezertorilor din Armata Sovietică (pe ani)

Raion	Anul					
	1948-1949	1950	1951	1952	1953	1954
Bravicea						
Călărași				6	2	
Lipcani						1
Edineț					3	
Drochia		1		3		
Strășeni						
Otaci						
Ocnița					4	
Soroca						
Zgurița						
Olănești						
Vulcănești						
Chipirceni						
Total - 84	**228**	**1**		**9**	**9**	**1**

[1] Buriații sunt un grup etnic mongol, orginar din sud-estul Siberiei care vorbesc o limbă proprie.

Analiza tabelului demonstrează că numărul maxim de cazuri **de dezertare se înregistrează în** anii 1948-1949, cei mai grei ani din istoria contemporană a Moldovei, când a avut loc procesul de colectivizare forțată, soldat cu foamete provocată și deportări în masă ale populației republicii, ceea ce este un argument în plus că dezertările din Armata Sovietică, în condițiile concrete ale RSSM din acești ani, au devenit o formă de manifestare antisovietică. Raioanele cele mai afectate de acest fenomen erau Soroca, inclusiv raionul Zgurița, care făceau parte din județul Soroca și din raionul Bravicea.

Majoritatea dezertorilor erau prinși de organele de miliție sau de autoritățile militare și **readuși** în unitățile **lor**, cum ar fi cazul ostașilor Jardan Diomid, Moroșan Ștefan și Brașovean Nicolae, care, la 11 iunie 1950, fugiseră din unitatea militară nr. 53609, dar au fost prinși la 15 iunie 1950 în localitatea Kamîșovka, regiunea Vladimir (ANMR, Fond 2862, inventar 3, dosar 5, f. 2). Un caz asemănător a avut loc la 30 ianuarie 1952, când Călin Ștefan, originar din **satul** Buda, **raionul** Călărași, ostaș în unitatea militară nr. 02151, aflată în localitatea Pereiaslavovka, regiunea Kaliningrad, profitând de lipsa electricității, la ora 22.00, a fugit din unitate, sub pretextul deplasării sale la **toaletă**. După o lună de căutări fără succes, s-a întors de bunăvoie, în februarie 1952, la unitate, negăsind posibilitatea de a părăsi regiunea (ANRM, Fond 2859, inventar 3, dosar 4, f. 8). O singură zi a durat dispariția soldatului Grec Dumitru, care a părăsit unitatea militară nr. 86716 la data de 06.01.1954, fiind prins și adus la unitate la data de 07.01.1954 (ANRM, Fond 2859, inventar 3, dosar 10, f. 1).

Erau și cazuri când căutările durau mai mult timp, fugarii reușind să se ascundă de autoritățile sovietice, parcurgând mii de kilometri, ca să ajungă cu bine acasă. Astfel, în noaptea de 11 spre 12 decembrie 1947, din Batalionul 492 Independent de Construcții, dispus în Novo-Fominsk, au dezertat soldații Popescu Vasile și Coptari Timofei, iar în noaptea următoare, tot din aceiași unitate, soldații Negruță Ion, Gorman P. și Gulea I, toți originari din raionul Zgurița, care au ajuns în **localitățile lor de domiciliu** (ANRM, Fond 2875, inventar 3c, dosar 1, f. 7-8). Prinderea lor era îngreunată din cauză că fugarii, ajungând în țară, cunoșteau **prea bine** toate locurile unde se puteau ascunde, din cauză că **autoritățile locale de miliție și cele militare nu dispuneau de informații referitoare la acești tineri,** în cea mai mare parte veniți din interiorul URSS. Nu a fost încununată de succes nici căutarea, din vara anului 1948, a dezertorilor Guțu Vasile și Ceban Gheorghe, care au evitat toate raziile și ambuscadele, organizate de organele militare, în colaborare cu miliția locală, ei reușind să se ascundă în pădure și în lanurile de porumb (ANRM, Fond 2875, inventar 3c, dosar 3, f. 25). Norocos s-a dovedit a fi fost și soldatul companiei 7 pază a Grupului Operativ Sud (România), Șandra Vasile, originar din comuna Ciuciuleni, raionul Strășeni, care a dezertat din unitate în decembrie 1946, **a fost** căutat până în octombrie 1949 **și nu a fost** găsit (ANRM, Fond 2873, inventar 4, dosar 8, f. 5). Putem doar să presupunem că el a rămas în România, fiind ascuns de populația locală.

Printre cazurile de dezertare, erau și **unele** absolut excepționale. Dacă succesul evadării lui V. Șandra din unitatea militară poate fi explicat **prin** eventualul ajutor

acordat acestui moldovean de către populația românească, unde el își putea ascunde cetățenia sovietică, atunci **dezertarea soldatului** Cozubenco Ion pare parcă desprinsă dintr-un roman de ficțiune. La 27 martie 1950, **soldatul din** Batalionul 459 Independent de asigurare tehnică de aerodrom, din cadrul Grupului militar sovietic de ocupație din Germania, Ion Cozubenco, originar din localitatea Palanca, raionul Călărași, profitând de faptul că, în perioada respectivă, zona de ocupație sovietică din Germania nu era încă total separată de zonele occidentale de ocupație, a părăsit unitatea și a fugit în zona americană de ocupație, devenind de neatins de justiția sovietică (ANRM, Fond 2859, inventar 3, dosar 4, f. 14).

Caracterul antisovietic al fenomenului dezertării poate fi lesne demonstrat prin existența unor grupe înarmate, formate din dezertori care activau pe teritoriul RSSM. Reprezentativ din acest punct de vedere este cazul lui Ștefan Ion Batrîncea, care, fiind încorporat în Armata Sovietică de către Comisariatul militar Călărași, la 11 decembrie 1950 fuge **de la** punctul de adunare a recruților și înființează un grup armat care, pe parcursul a doi ani, **a terorizat** autoritățile sovietice locale. Numai după prinderea sa de către trupele speciale ale securității, el **a fost** arestat și deferit justiției la 14 iulie 1952 (ANRM, Fond 2859, inventar 3, dosar 4, f. 4). Un grup de dezertori, compus din șase persoane, activa în vara anului 1948 și în localitatea Sudarca, raionul Otaci (ANRM, Fond 2891, inventar 2, dosar 2, f. 70). Un grup **terorist** antisovietic s-a format în vara anului 1949 și în satul Recea, raionul Strășeni, și **a activat** în raza raionului respectiv. În 1949, acest grup l-a ucis pe președintele sovietului sătesc din comuna Pănășeni, iar în 1950 l-a rănit grav pe secretarul organizației UTCL (Komsomol) din localitatea Zubrești. În vara anului 1950, membrii grupului au fost arestați de organele de securitate (ANRM, Fond 2879, inventar 3, dosar 4, f. 4).

În concluzie, putem afirma că, în perioada 1944-1954, dezertările din rândul populației din RSS Moldovenească **erau numeroase și aveau un caracter** vădit antisovietic, devenind o formă a luptei moldovenilor împotriva ocupației sovietice. Cu timpul, din cauza represaliilor, dar și „îmblânzirii" regimului sovietic în perioada „dezghețului" hrușciovist, acest fenomen a dispărut ca manifestare **cu caracter** antisovietic.

Referințe

Arhiva Națională a Republicii Moldova (ANMR). Fond 2862, inventar 3, dosar 5.

__. Fond 2859, inventar 3, dosar 4.

__. Fond 2859, inventar 3, dosar 10.

__. Fond 2873, inventar 4, dosar 8.

__. Fond 2875, inventar 3c, dosar 1.

__. Fond 2875, inventar 3c, dosar 3.

__. Fond 2891, inventar 2, dosar 2.

__. Fond 2879, inventar 3, dosar 4.

Arhiva Organizațiilor Social-politice a Republicii Moldova (AOSPRM). Fond 51, inventar 3, dosar 45.

__. Fond 51, inventar 3, dosar 89.

__. Fond 51, inventar 3, dosar 431.

__. Fond 51, inventar 3, dosar 438.

__. Fond 51, inventar 7, dosar 60.

__. Fond 51, inventar 8, dosar 76.

BULETINUL
UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I"
https://buletinul.unap.ro

Contribuții la elucidarea unui episod controversat. Cazul Ciulei (2)

Contributions to the elucidation of a controversial episode.The Ciulei Case (2)

Col.Dr. Liviu CORCIU*
*Arhivele Militare Naționale Române, București, România
e-mail: liviu.corciu@yahoo.com

Abstract

În baza unei documentări anterioare, nu neapărat pentru subiectul acestui articol, se poate afirma că administrarea justiției militare în Războiul de Întregire nu a fost un proces perfect, printre cele mai importante critici aduse acesteia fiind erorile judiciare, înregistrate, pe de-o parte, și imixtiunile comandanților în actul de justiție, pe de altă parte. Faptul că membrii completelor curților marțiale erau numiți de către comandanții marilor unități pe lângă care acestea funcționau, de la nivelul diviziilor în sus, reprezenta o procedură care facilita, în mod firesc, existența relațiilor de subordonare, cu efect direct asupra actului de justiție. O altă explicație pentru calitatea scăzută a actului de justiție este lipsa pregătirii de specialitate a membrilor consiliilor de război și ai curților marțiale, pregătirea ofițerilor chemați să înfăptuiască actul de justiție militară fiind grevată de tarele sistemului educațional al acelor vremuri. În acest context, trebuie analizat și modul în care a decurs procesul sublocotenentului Constantin Ciulei, care dobândește astfel noi sensuri și semnificații. Situația disciplinară a trupelor cerea o pedeapsă exemplară, aplicată rapid și care să fi impresionat audiența, iar faptul că Ciulei era ofițer reprezenta un atu, care asigura notorietatea evenimentului.

Based on previous documentation, not necessarily the subject of this article, we can state that the administration of military justice in the War of the Integration was not a perfect process, among the most important criticisms being the judicial errors recorded, on the one hand, and the interference of commanders in the act of justice, on the other. The fact that the members of court martial panels were appointed by the commanders of the major units with which they operated, from the divisional level upwards, was a procedure that naturally facilitated the existence of subordination relationships, with a direct effect on the administration of justice. Another explanation for the low quality of justice is the lack of specialized training of the members of the councils of war and courts-martial, the training of the officers called upon to carry out military justice being encumbered by the educational system of the time. It is in this context that the trial of Second Lieutenant Constantin Ciulei should also be analyzed, which thus takes on new meanings and significance. The disciplinary situation of the troops called for an exemplary punishment, which was swiftly carried out and significantly impressed the audience, and the fact that Ciulei was an officer was an asset that ensured the notoriety of the event.

Cuvinte-cheie:
curte marțială; execuție sumară; dezertor; justiție militară; eroare judiciară.

Keywords:
court-martial; summary execution; deserter; military justice; miscarriage of justice.

Info articol
Primit: 26 iunie 2024; Evaluat: 22 august 2024; Acceptat: 7 noiembrie 2024; Disponibil online: 17 ianuarie 2025
Citare: Corciu, L. 2024. „Contribuții la elucidarea unui episod controversat. Cazul Ciulei (2)"
Buletinul Universității Naționale de Apărare „Carol I", 13(4): 38-60. https://doi.org/10.53477/2065-8281-24-38

Validarea

După cum am promis la începutul acestui articol, vom aborda, pe rând, toate ipotezele vehiculate în cele două articole din *Magazin Istoric* și din ziarul *Avântul*, cu argumente desprinse din surse primare.
Astfel, nu considerăm validă prima ipoteză, conform căreia *trimiterea în judecată a lui Ciulei s-ar fi făcut cu intenția de a deruta bănuielile comandantului Armatei a 2-a*, de vreme ce trimiterea în judecată a lui Ciulei a fost cea de-a doua opțiune a lui Sturdza; cea dintâi, după cum am prezentat deja, a fost aceea de a-l împușca pe loc, spre a fi un exemplu trupei demoralizate. O *execuție sumară*, care nu implica trimiterea în fața vreunui complet de judecată.
Mai mult, este evident că acele retrageri discutabile ale Brigăzii 7 Mixtă, și care atrăseseră atenția generalului Averescu, au implicat dispozitivul defensiv al întregii brigăzi și au necesitat un nivel de decizie superior, neputând fi nicicum atribuite în sarcina unui sublocotenent.
Nu considerăm validă nici cea de-a doua ipoteză**,** conform căreia Sturdza, bănuit de trădare, *ar fi aruncat totul în seama locotenentului Ciulei, căruia i-a imputat că s-a retras de pe poziție, fără ordin, împreună cu subunitatea sa*.

În primul rând, la 26 decembrie 1916 Sturdza nu era bănuit de trădare. Deciziile sale anterioare de a se retrage, nejustificat după părerea generalului Averescu, au produs nemulțumirea acestuia, dar de aici, la apariția bănuielilor de trădare mai era cale lungă. Generalul Averescu nu înțelegea retragerile repetate ale lui Sturdza, temându-se probabil și din cauza vecinătății sectorului ocupat de Brigada 7 Mixtă cu trupele ruse. Deciziile din sectorul lui Sturdza ar fi putut influența negativ relația cu aliații ruși, deși paradoxal, aceștia par să fi avut o impresie excelentă despre trupele Armatei a 2-a. În memoriile sale, generalul rus Nikolai A. Monkevitz povestește despre *„regimentele eroicei armate a generalului Averescu",* menționând că a avut ocazia să le întâlnească de mai multe ori și că a fost uimit de *„disciplina lor de fier (…), de organizarea impecabilă*" (Monkevitz și Vinogradski 2019, 33) etc.
În al doilea rând, nu retragerea de pe *Momâia* era cea la care generalul Averescu făcea referire în memoriile sale, ci la cea de la *Soveja*, care avusese loc cu două zile mai devreme, la data de 24 decembrie. Iar în al treilea rând, de fuga precipitată de pe *Momâia* nu fusese acuzat Ciulei, ci Mărculescu.

Nici cea de-a treia ipoteză, conform căreia *Ciulei ar fi fost acuzat* ***deodată*** (s.n.) *de trădare de către colonelul Sturdza,* nu este, în opinia noastră validă. Acest *deodată* induce ideea că Ciulei ar fi fost, în raport cu Sturdza, *țapul ispășitor* sau vinovatul de serviciu, o soluție de moment, o rezolvare subită pentru cele întâmplate pe *Momâia*. Acuzația de trădare adusă sublocotenentului Ciulei nu a fost un act intempestiv, în sensul că nu a survenit *deodată*. Inițial, Sturdza a vrut să dea trupei un exemplu extrem, prin execuția în fața propriilor subordonați, fără judecată, a căpitanului Mărculescu și a sublocotenentului Ciulei, amândoi ofițeri, amândoi comandanți de subunități. Eșecul acestui plan a generat, de fapt, inițierea acuzațiilor de trădare la adresa amândurora. Sesizarea comisarului regal (procurorul militar, s.n.) al

Diviziei 1 Infanterie rămăsese singura opțiune a lui Sturdza, de vreme ce acuzațiile fuseseră publice, iar încercarea de execuție a celor doi ofițeri eșuase.

De ce a sesizat Sturdza Divizia 1 Infanterie? Pe de-o parte, acest eșalon avea competența dată de Codul de justiție militară să instrumenteze cazul, iar pe de altă parte, Curtea Marțială, ca instanță militară, se putea organiza numai de la eșalonul divizie în sus, prin ordin al comandantului structurii respective. Cu excepția ofițerilor care erau, de regulă, judecați de Curtea Marțială, constituită la nivel de armată. Sturdza nu-și putea organiza propria curte marțială la Brigada 7 Mixtă, și, în plus, nici căpitanul Mărculescu și nici sublocotenentul Ciulei nu aparțineau organic de Brigada 7 Mixtă, ci fuseseră detașați la această mare unitate.
Întreaga punere în scenă a acestei *execuții sumare* a fost, în opinia mea, un gest spontan din partea lui Sturdza, menit să impresioneze audiența și să constituie un exemplu în sine pentru soldați, care ar fi trebuit să conștientizeze eventualele consecințe la care s-ar fi expus, dacă ar fi riscat un gest asemănător.

Consider că intenția lui Sturdza, de a-i pedepsi exemplar pe Mărculescu și pe Ciulei nu a fost premeditată, iar argumentele care susțin această afirmație invalidează, în opinia noastră, ipoteza din articolul prof. Nicolau. Afirmația se bazează pe faptul că Sturdza a fost martor al prestației celor doi pe *Momâia,* aspecte confirmate de mărturiile maiorului Constantinescu și ale locotenentului Marinescu. Mai mult, în momentul execuției, nici Mărculescu și nici Ciulei nu au fost legați, după cum cerea procedura, în fața plutonului de execuție și nici măcar dezarmați.

Nu consider validă nici cea de-a patra ipoteză**,** conform căreia *sublocotenentul Ciulei ar fi fost condamnat, deoarece Curtea Marțială ar fi fost intimidată de situația acuzatorului*. Expresia *situația acuzatorului*, utilizată de presa vremii, se referea, probabil, la poziția lui Sturdza în armată și în societate. Afirmația privind influența pe care ar fi avut-o Sturdza în societate este discutabilă. Chiar în memoriile sale, acesta menționează că se simte amenințat de Brătieni, iar orientarea sa politică și a familiei sale era clar una filogermană și profund antirusească. De asemenea, avem rezerve și în ceea ce privește influența pe care ar fi avut-o Sturdza în armată și, mai ales, în rândul ofițerilor din Armata a 2-a, dar în special asupra membrilor completului de judecată din compunerea Curții Marțiale a Armatei a 2-a, pe care am reușit să-i identificăm și pe care îi vom prezenta mai târziu.

Cât despre influența pe care Sturdza ar fi putut-o avea pe lângă generalul Alexandru Averescu, din memoriile acestuia din urmă, reiese că Sturdza nu beneficia de o poziție privilegiată, ci dimpotrivă, Averescu chiar nu și-l dorea în subordine, considerându-l un înfumurat, *„mai mult o încurcătură decât un ajutor”* (Averescu 1992, 104).
Faptul că Sturdza a fost schimbat de la comanda Diviziei 15 Infanterie, aflată în subordinea Armatei a 2-a, unde fusese numit inițial, a fost numit la comanda Diviziei 10 infanterie, aflată în subordinea Armatei a 1-a, care era în refacere în nordul Moldovei, ar putea fi interpretat ca un indiciu în sprijinul acestei afirmații. Iată de ce subscriem opiniei (Otu și Georgescu 2011, 137) că, la momentul judecății

sublocotenentului Ciulei, Sturdza nu avea cum să intimideze completul de judecată, de vreme ce fusese deja raportată dispariția sa, în condiții neelucidate, încă din noaptea de 23/24 ianuarie 1917.
Cea de-a cincea ipoteză, conform căreia *Ciulei a fost executat, iar Sturdza dezertează,* este prezentată greșit din punctul de vedere al cronologiei evenimentelor. După cum am mai spus, Sturdza dezertase încă din noptea de 23/24 ianuarie, fiind considerat, inițial, dispărut. Cadavrul ordonanței sale, urmele de pași pe zăpadă care duceau către liniile inamice și bagajele personale în care i-a fost găsit jurnalul au alimentat bănuielile cu privire la un posibil act de trădare. Însă confirmarea trădării a venit după prinderea lui Crăiniceanu, în ziua de 28 ianuarie, la orele prânzului, și s-a materializat oficial în după-amiaza aceleiași zile, după ce acesta din urmă a mărturisit întâlnirea cu Sturdza și i-au fost găsite manifestele care instigau la trădare.
Ciulei a fost judecat în ziua de 26 ianuarie, a fost condamnat la moarte și executat în dimineața zilei de 28 ianuarie, la ora 10.00, în poligonul de tragere din Bacău, unde se afla punctul de comandă al Armatei a 2-a, a cărei curte marțială îl judecase. Astfel, la ora la care Ciulei murea în fața plutonului de execuție, Crăiniceanu nu fusese încă prins, iar dezertarea lui Sturdza era încă în stadiul de dispariție, în condiții neelucidate.

Cea de-a șasea ipoteză, conform căreia s*e află că Ciulei a fost nevinovat, dar bănuise legăturile lui Sturdza cu inamicul,* este, de asemenea, lipsită de temei. Sturdza nu a intenționat să-l împuște pe Ciulei, fiindcă acesta ar fi bănuit legăturile lui cu inamicul. Această teorie a apărut mai târziu, poate promovată chiar de Mărculescu, după cum vom vedea că apare în memoriul personal al acestuia, și a fost, cu siguranță, alimentată de teoriile țesute în urma dezertării lui Sturdza.
Ciulei nu ar fi putut bănui legăturile lui Sturdza cu inamicul, în primul rând, deoarece intrase în subordinea Brigăzii 7 Mixtă cu numai câteva zile înainte, și ca majoritatea celor nou-veniți, ofițeri și trupă deopotrivă, nici măcar nu-l cunoștea.

În al doilea rând, Ciulei era la un nivel mult inferior al ierarhiei militare, nu făcea parte nici măcar din statul major al brigăzii. Era un ofițer subaltern, după denumirea din epocă, al cărui loc era în mijlocul subunității sale, fapt ce nu i-ar fi permis să stea în preajma lui Sturdza pentru a vedea cum și, mai ales, ce gândește. E chiar foarte probabil ca funcția de comandant al rezervei de batalion să-i fi fost încredințată lui Ciulei de fostul său camarad și coleg de spital, căpitanul Mărculescu, tocmai pentru că astfel îi facilita un cantonament în apropierea sa, știindu-se că, de regulă, rezerva de batalion este localizată în apropierea punctului de comandă, iar comandantul acesteia se află la dispoziția comandantului de batalion.

Nici ultima ipoteză, conform căreia *Sturdza și-ar fi dat seama că ar putea fi demascat și l-a înlăturat pe Ciulei, influențând Curtea Marțială spre o decizie de condamnare la moarte,* nu poate fi validată, în opinia noastră, pe baza argumentelor pe care le vom prezenta în continuare.
Mai întâi, precizăm că această ultimă ipoteză verificată este, de fapt, o combinație a două dintre ipotezele argumentate anterior. Cea dintâi induce ideea premeditării

actului de dezertare de către Sturdza sau cel puțin a existenței sale, chiar și în formă latentă, încă din data de 26 decembrie 1916, când s-a consumat episodul execuției ratate a lui Mărculescu și a lui Ciulei. Cea de-a doua induce ideea că decizia lui Sturdza de a da un exemplu cu cei doi, dar în special cu Ciulei, ar fi fost motivată de teama de a nu fi demascat, astfel că ar fi influențat Curtea Marțială spre o decizie de condamnare la moarte a celui din urmă.
Faptul că, în opinia noastră, Sturdza nu ar fi putut influența Curtea Marțială a Armatei a 2-a este o afirmație pe care am argumentat-o mai sus, împărtășită, de altfel, și în cartea profesorilor Petre Otu și Maria Georgescu.

În ceea ce privește decizia lui Sturdza de a trece la inamic, nu putem aprecia cu exactitate momentul, dar cu siguranță acesta fost după data de 26 decembrie 1916, când a avut loc episodul de pe *Momâia*. Considerăm că, indiferent de crezul său politic și de notorietatea atitudinii sale filogermane, cristalizarea ideii de a trece în tabăra inamicului a avut loc după ce a predat efectiv comanda Brigăzii 7 Mixtă, iar acest eveniment a avut loc la data de 4 ianuarie 1917.
Din memoriile (Scărișoreanu 1934, 174) generalului Romulus Scărișoreanu, reiese că, încă din data de 26 decembrie 1916, Sturdza ar fi fost numit la comanda Diviziei 15 Infanterie, motiv pentru care Scărișoreanu, pe atunci având gradul de colonel, ar fi fost chemat să preia comanda Brigăzii 7 Mixtă. Dar despre această numire, șeful nemijlocit de atunci al acestuia, generalul Eremia Grigorescu, nu știa nimic, iar numirea lui Sturdza nu s-a mai concretizat. Situația validează (Averescu 1992, 104) cele consemnate, cu aceeași dată, în memoriile generalului Alexandru Averescu, care confirma numirea lui Sturdza în subordinea sa, în calitate de comandant de divizie, dar la fel de clar spunea și că nu și-l dorea subordonat și că spera *„să se cureță de el”* (Averescu 1992, 104).

De fapt, unele surse (Kapri 1926, 14) indică o strânsă legătură între momentul în care Sturdza a luat decizia de a trece în tabăra inamicului și modificarea deciziei Marelui Cartier General, care, deși îl numise, inițial, în funcția vacantată prin promovarea generalului Eremia Grigorescu, la comanda Diviziei 15 Infanterie, aflată pe front în subordinea Armatei a 2-a, și-a schimbat decizia, numindu-l la comanda Diviziei 10 Infanterie, aflată în refacere, în adâncimea dispozitivului propriu, în nordul Moldovei. Probabil, simțindu-se respins de șefii ierarhici, ceea ce punea sub semnul întrebării prestația sa de până atunci la comanda brigăzii, refuzul de a i se încredința comanda unei divizii cu renume, aflată la contact cu inamicul, și trimiterea sa în proximitatea *„adevăratului dușman”* (Kapri 1926, 8), după cum obișnuia să afirme, au cântărit decisiv în luarea acelei *„hotărâri nenorocite”* (Kapri 1926, 6) de către Sturdza.
Mai mult, decorația care i-a fost oferită personal de către regele Ferdinand, în urma întrevederii avute cu câteva zile înainte, nu a mai reprezentat decât o palidă consolare. Sau bomboana care ar fi trebuit să îndulcească amărăciunea frustrării.

În această logică, la momentul zilei de 26 decembrie 1916, ipoteza că Sturdza ar fi dat curs *temerii de a nu fi demascat* nu poate fi luată în calcul ca mobil al acțiunilor acestuia, îndreptate împotriva lui Mărculescu și Ciulei.

Curtea

Cu toate acestea, încă persistă întrebarea: *Și, atunci, de unde graba de a-l judeca și condamna pe Ciulei?*
Încercând să răspundem acestei întrebări firești (Otu și Georgescu 2011, 137), referitoare la motivul grabei cu care a fost judecat acest caz, am găsit o posibilă explicație în memoriile (Buttescu 2012, 314) locotenent-colonelului Mihai I. Buttescu. Fostul comandant al Regimentului 2 Vânători „Regina Elisabeta" îl considera vinovat pe generalul Gheorghe Mărdărescu, șeful Statului Major al Armatei a 2-a, care ar fi *pus* în funcția de președinte al Curții Marțiale (completul de judecată era numit prin ordin al comandantului, s.n.) un fost subordonat, un personaj obedient, catalogat de autor ca fiind *un nevropat*, în persoana colonelului Alexandru Alexiu, „*care condamna la moarte pentru motive necercetate suficient (cazul locotenentului Ciulei) și* ***execuțiile erau zilnice*** (s.n.)*"* (Buttescu 2012, 314).

Din verificările efectuate în documentarea prezentei lucrări, a reieșit că afirmația se confirmă în ceea ce privește atât existența relației de subordonare anterioară a colonelului Alexandru Alexiu față de generalul Gheorghe Mărdărescu, cât și îndeplinirea de către colonelul Alexandru Alexiu a funcției de președinte al Curții Marțiale a Armatei a 2-a.
Astfel, în anul 1915 colonelul Alexandru Alexiu a îndeplinit funcția de comandant al *Școlii de Tragere a Infanteriei* de la Mihai Bravu, generalul Gheorghe Mărdărescu fiind șeful său nemijlocit, pe atunci *Inspector Tehnic al Infanteriei*. Mai mult, în *foaia calificativă* pe anul 1918 a celui dintâi, generalul Gheorghe Mărdărescu a afirmat: *„îi cunosc activitatea din campanie* (colonelului Alexandru Alexiu, s.n.) *căci s-a găsit sub ordinele mele aproape tot timpul"* (Arhivele Militare Naționale Române**,** dosar nr. 6, f. 30).
Cât despre confirmarea celei de-a doua afirmații, am identificat *„Adresa nr. 16004"* (Arhivele Militare Naționale Române**,** dosar nr.1691, f. 9-10), din 23 ianuarie 1917, prin care Curtea Marțială a Armatei a 2-a a înaintat Serviciului Justiție Militară din Marele Cartier General un tabel cu componența nominală a curților marțiale care funcționau la diviziile din subordine.

La prima poziție din tabelul anexat acestei adrese, este consemnat colonelul Alexandru Alexiu, președintele Curții Marțiale a Armatei a 2-a. Alături de acesta, completul de judecată, care e posibil să-l fi condamnat și pe Ciulei, mai era format din maiorul Constantin Tănăsescu, maiorul Nicolae Opran, căpitanul Ion Glogoveanu și căpitanul Titus Carapancea. Abordăm componența completului de judecată sub forma unei posibilități, nu a unei certitudini, deoarece completul de judecată ar fi putut fi constituit și din președinte, și din trei dintre membrii permanenți, în funcție de gradul acuzatului și de dispozițiile comandantului care făcea numirea. Armata a 2-a mai avea drept comisar regal pe locotenent-colonelul Gheorghe Pangrati, iar în funcția de substitut de comisar regal, pe maiorul Mihail Protopopescu.
Se confirmă așadar faptul că, la data desfășurării procesului sublocotenentului Constantin Ciulei, colonelul Alexandru Alexiu, comandantul Centrului de Instrucție al Armatei a 2-a (Arhivele Militare Naționale Române**,** dosar nr. 6, f. 27), exercita

funcția de președinte al completului de judecată.
Mai mult, am identificat și un ordin (Arhivele Militare Naționale Române dosar nr. 37, f. 694), semnat de colonelul Alexandru Alexiu, în calitate de președinte al completului de judecată al Curții Marțiale a Armatei a 2-a, prin care căpitanul Mărculescu, care nu fusese prins până în acel moment, era trimis în judecată la respectiva Curte Marțială, sub acuzația de dezertor, împreună cu sublocotenentul Zodilă, despre care am menționat mai sus și despre care se știa că trecuse de bunăvoie la inamic, tot în aceeași zi.

În ceea ce privește afirmația privind ritmicitatea execuțiilor, informația e confirmată parțial de sinteza intitulată *„Monografia Justiției Militare, în timpul războiului nostru"* (Arhivele Militare Naționale Române**,** dosar nr. 924, f. 1), mai precis, de cele consemnate în *„Tablou statistic numeric pe grade și fapte de condamnații la moarte de instanțele penale militare în timpul războiului 1916-1918 executați până la 1 iunie 1918"* (Arhivele Militare Naționale Române**,** dosar nr. 924, f. 14), unde Curtea Marțială a Armatei a 2-a este creditată cu 49 de execuții, de departe cele mai multe dintre toate curțile marțiale și consiliile de război, în perioada analizată.

Cu toate acestea, nu avem certitudinea că toate aceste execuții s-ar fi datorat zelului colonelului Alexandru Alexiu, după cum susține locotenent-colonelul Mihai I.Buttescu, ceea ce ne dă dreptul să avem rezerve față de cele susținute de acesta. Desigur, există și alte opinii față de rapiditatea cu care Curtea Marțială a Armatei a 2-a a judecat dosarul Ciulei, *„o înlănțuire nefericită de evenimente"* (Otu și Georgescu 2011, 137), pusă pe seama contextului general prin care trecea armata română, pe necesitatea de a se restabili ordinea și disciplina, chiar și prin reprimarea urgentă a faptelor grave. Această opinie o vom analiza în continuare.

Îngrijorarea

Pentru o mai bună înțelegere a evenimentelor în speță, am analizat și corespondența purtată între Marele Cartier General și Armata a 2-a, referitoare la acest subiect. Marele Cartier General era îngrijorat de situația din sectorul Brigăzii 7 Mixtă, al cărei raport inițial cu privire la evenimentele din data de 26 decembrie 1916 îl considera *„foarte confuz"* și solicita, prin *„Telegrama nr. 4478"*, din 31 decembrie 1916/13 ianuarie 1917, clarificări Armatei a 2-a, eșalonul superior al acesteia (Arhivele Militare Naționale Române, dosar nr. 160, f. 23).

Situația pe care Marele Cartier General o considera *confuză* era cea raportată telegrafic de Armata a 2-a, care a retransmis Marelui Cartier General, la rândul său, *„Raportul nr. 2709"*, din 28 decembrie 1916, al colonelului Alexandru Sturdza (Arhivele Militare Naționale Române**,** dosar nr. 160, f. 21). Prin acest raport, Sturdza acuza ofițerii batalionului comandat de Mărculescu și pe acesta în mod special de starea necorespunzătoare a trupei din subordine și, în special, de evenimentul din 26 decembrie 1916, de pe *Momâia*. De când intrase în subordinea Brigăzii 7 Mixtă,

acuza Sturdza, Mărculescu arătase, în exercitarea actului de comandă, o *inerție completă*. Nu era la curent cu efectivele pe care le avea în subordine, și raportase câteva zile la rând un efectiv de 500 de militari, în timp ce, în realitate, avea în subordine 700 de militari, pe care nu îi organizase până la acea dată, încă 400 de oameni fiind pe cale de a se prezenta.
În ceea ce privește evenimentul din 26 decembrie 1916, de pe *Momâia*, Mărculescu era acuzat că lăsase oamenii la voia întâmplării, *„nehrăniți, neorientați și nesupravegheați, iar ofițerii raportau fantastic* (neadevărat, s.n.) *de*[spre] *inamic știri necontrolate de căpitan*" (Arhivele Militare Naționale Române, dosar nr. 160, f. 21).

Din acest raport, mai aflăm că Sturdza îl acuza pe Mărculescu de faptul că, zilnic, în sectorul care se afla în responsabilitatea acestuia se producea panică, la care luau parte și ofițerii, care ar fi fost înțeleși să treacă la inamic. Cea mai gravă acuzație însă era aceea că, la 26 decembrie 1916, atunci când s-a produs atacul german și a avut loc defecțiunea Companiei a 3-a, nu numai că Mărculescu se afla la 1 km înapoia pozițiilor batalionului său, *la friptură*, după spusele lui Sturdza, dar a și fugit, lăsând în seama celui din urmă restabilirea poziției. Ulterior, a raportaat că va *ține poziția* de pe șosea, deoarece fusese părăsit de soldați.
„Acest comandant a fost după mine vinovatul principal de trădarea ofițerilor și a trupei", concluziona Sturdza, și încheia raportul prezentând sumar actul execuției lui Mărculescu, pe care l-am descris deja mai sus (Arhivele Militare Naționale Române, dosar nr. 160, f. 21).

Acest raport a fost transmis Marelui Cartier General de către Armata a 2-a, cu *„Telegrama nr. 2881"*, din 29 decembrie 1916/11 ianuarie 1917, și în mod firesc a stârnit îngrijorarea și nedumerirea eșalonului superior. Îngrijorare, pe de-o parte, din cauza acuzațiilor grave de *trădare* și *fugă din fața inamicului* împotriva unui întreg batalion, în frunte cu ofițerii și comandantul acestuia, nedumerire, pe de altă parte, din cauza relatării ambigue a execuției unui ofițer (Arhivele Militare Naționale Române, dosar nr. 160, f. 22).

Prin intermediul *„Telegramei nr. 4478"* din 31 decembrie 1916/13 ianuarie 1917, semnată de generalul Constantin Prezan, transmisă prin aparatul telegrafic „*Hughes*", Marele Cartier General cerea Armatei a 2-a să-i pună în vedere lui Sturdza să raporteze *clar și precis* ce măsuri a luat împotriva ofițerilor pe care îi acuzase că ar fi transmis informații nereale despre inamic, ce măsuri a luat prima dată când s-a produs panică în sectorul unităților sale, când anume constatase că ofițerii se înțelegeau cu soldații *să treacă la inamic*, să nominalizeze ofițerii acuzați de trădare etc. (Arhivele Militare Naționale Române, dosar nr. 160, f. 23).

Din conținutul telegramei, dar mai ales din tonul și atitudinea Marelui Cartier General, reiese că, la acea dată, nu era pusă la îndoială buna-credință a colonelului Alexandru Sturdza. Dimpotrivă, eșalonul superior se interesa chiar și despre măsurile ce fuseseră luate împotriva comandantului plutonului însărcinat cu execuția ratată a celor doi ofițeri, care, în opinia Marelui Cartier General, ar fi trebuit trimis imediat

în judecată în fața consiliului de război al Armatei a 2-a, iar rezultatul sentinței, comunicat ierarhic, cât mai curând posibil.
La *Telegrama nr. 4478*, generalul Gheorghe Mărdărescu, șeful de stat major al Armatei a 2-a, a transmis Marelui Cartier General un răspuns cifrat prin *„Telegrama nr. 2942"* (Arhivele Militare Naționale Române, dosar nr. 160, f. 11-14), în data de 31 decembrie 1916/13 ianuarie 1917, care se află descifrată în același fond (Arhivele Militare Naționale Române, dosar nr. 160, f. 09-10). Aceasta prezintă varianta oficială a evenimentelor de pe *Momâia*, din 26 decembrie 1916, precizând că Sturdza i-ar fi dat ordin lui Mărculescu, în cursul unei vizite în sectorul acestuia, efectuată cu doar o zi înainte, *„să execute imediat pe provocatorii panicelor"* (Arhivele Militare Naționale Române, dosar nr. 160, f. 09v).

Un alt element de interes pentru investigația noastră este faptul că generalul Mărdărescu afirma, în *Telegrama nr. 2942,* că Sturdza s-a deplasat, la data de 26 decembrie, în sectorul batalionului lui Mărculescu de pe *Momâia*, *„dinadins pentru a stabili un exemplu"* (Arhivele Militare Naționale Române, dosar nr. 160, f. 09v). Atacul german, respectiv, predarea Companiei a 3-a, au avut loc în timp ce Sturdza se afla chiar în punctul de comandă al batalionului lui Mărculescu, fiind urmate de fuga de pe poziții a întregului batalion, inclusiv a comandantului acestuia.

Poziția a fost restabilită, se menționează în telegrama Armatei a 2-a, de către Sturdza și locotenentul Marinescu care-l însoțea, *„cu oameni adunați în grabă și focul revolverului său"* (Arhivele Militare Naționale Române, dosar nr. 160, f. 09v) (al lui Sturdza, s.n.). Odată restabilită situația pe *Momâia*, fugarii au fost adunați în careu, *„cu ofițerii în fața frontului"* (Arhivele Militare Naționale Române, dosar nr. 160, f. 09), colonelul Sturdza, se menționa în telegramă, ar fi procedat la o cercetare sumară, după care ar fi anunțat verdictul: *condamnarea la moarte* a căpitanului Stelian Mărculescu și a sublocotenentului Constantin Ciulei, care, conform celor relatate de către șeful de stat major al Armatei a 2-a, au fost *executați* pe loc.

Aici, intervenim cu precizarea că, spre deosebire de cele consemnate în sursa citată din *Magazin Istoric,* în care colonelul Alexandru Sturdza ar fi poruncit *„câtorva soldați să tragă în ei și el însuși ar fi tras câteva focuri de carabină"* (Arhivele Militare Naționale Române, dosar nr. 160, f. 09), în telegrama generalului Gheorghe Mărdărescu este consemnată, în mod oficial, varianta în care însuși Sturdza i-ar fi împușcat pe cei doi ofițeri: *„nu era timpul nici nu era oportun a fi constituit un pluton de execuțiune; a tras însuși comandantul brigadei"* (Arhivele Militare Naționale Române, dosar nr. 160, f. 10).

În mod cert întunericul a contribuit în foarte mare măsură la ratarea execuției, dar mai curând, Sturdza a apucat să tragă numai în Mărculescu, nu și în Ciulei. Probabil că, atunci când a văzut că Sturdza este pe cale să-l omoare, Ciulei a sărit în râul din apropiere și a fugit prin pădure, fiind prins ulterior, în timp ce căpitanul Stelian Mărculescu, *„rănit la gât și la brațul stâng"*, a căzut nemișcat în zăpadă (Nicolau 1974, 87).

Din raportul Armatei a 2-a, reiese că, ulterior, acesta fiind prezumat mort, a sărit în sus la apropierea medicului și a brancardierilor, „*amenințând cu revolverul*” și a fugit în pădure (Arhivele Militare Naţionale Române, dosar nr. 160, f. 10).

Judecata

Revenind la momentul în care fugarii batalionului, comandat de Mărculescu, erau adunați pe șoseaua *Varnița-Răcoasa*, deducem din rapoarte că Sturdza ajunsese pe acel loc după ce restabilise poziția pe *Momâia*, alături de locotenentul Marinescu din Regimentul 10 Călărași și fugarii pe care reușiseră să-i întoarcă din drum, sub amenințarea revolverelor. Oarecum în același timp, a ajuns și Polihroniade, după ce strânsese fugarii, printre care se afla și Ciulei, din *Varnița*.
Hotărât să dea un exemplu drastic, de fapt principalul motiv pentru care venise pe *Momâia*, Sturdza a adunat fugarii batalionului în careu, „*cu ofițerii în fața frontului*” (Arhivele Militare Naţionale Române, dosar nr. 160, f. 10), după cum se arată în raportul Armatei a 2-a, după care au urmat alte două etape, menționate, de asemenea, în raport: *judecata sumară* a acestora, finalizată cu *execuția.*

Nu am găsit în documentarea noastră cum anume a avut loc execuția, având în vedere că, din *Telegrama nr. 2942* a Armatei a 2-a, reiese că ofițerii erau în careu, în fața celorlalți fugari. Am aflat ulterior, din raportele lui Polihroniade, că toți ofițerii din efectivul batalionului erau considerați responsabili, iar zece dintre aceștia, printre care Mărculescu și Ciulei, au fost chiar nominalizați.
E posibil ca, după stabilirea vinovăției lui Mărculescu, în calitatea sa de comandant, și a lui Ciulei, acesta din urmă, după cum am spus, în calitate de comandant al rezervei care ar fi trebuit să execute contraatacul, ceilalți să fi fost trecuți în formație, iar Sturdza să fi tras în cel dintâi. Raportul Armatei a 2-a spune că Mărculescu a căzut nemișcat în zăpadă și a fost considerat mort, după care trupa s-a descoperit și s-a rostit o rugăciune. A urmat o cuvântare „*admonestatoare*” (Arhivele Militare Naţionale Române, dosar nr. 160, f. 10) din partea lui Sturdza, pentru ca spectacolul la care oamenii asistaseră să devină un bun exemplu, după care trupa a plecat spre poziții, sub comanda maiorului Constantinescu.

Se pare că Sturdza ar fi dat dispoziție ca trupului celui „executat” să i se facă cele de cuviință, motiv pentru care medicul batalionului, împreună cu brancardierii s-au apropiat de locul unde acesta zăcea nemișcat în zăpadă, iar Mărculescu „*a sărit în sus amenințând cu revolverul și a fugit în pădure*” (Arhivele Militare Naţionale Române, dosar nr. 160, f. 10v).
Telegrama se încheie cu asigurarea eșalonului superior că ordinea fusese restabilită, dovadă că trupa rezistase cu succes pe poziții a doua zi, respingând un atac german. Totuși, era asigurat eșalonul superior, ca măsură de siguranță, o mitralieră se afla în poziție, în spatele frontului, îndreptată asupra poziției acestei trupe, în cazul în care exemplul ce tocmai îi fusese dat nu ar mai fi fost de ajuns (Arhivele Militare Naţionale Române, dosar nr. 160, f. 10v).

Întrebări

Din *Telegrama nr. 2942*, reiese că, până la momentul execuției sumare, Sturdza nu avusese nicio interacțiune cu Ciulei. Ne este clar că Polihroniade îl cunoștea pe Ciulei, dar nu există indicii că l-ar fi cunoscut și Sturdza.
Și totuși, de ce Sturdza a vrut să-l omoare pe Ciulei?, așa cum sună una dintre ipoteze.

În primul rând, Sturdza venise, în 26 decembrie, pe *Momâia*, fiindcă poziția reprezenta un punct de mare importanță al frontului româno-rus, și înțelesese vulnerabilitatea acestui sector de care răspundea implicit. Cu numai două zile înainte, la 24 decembrie, brigada lui Sturdza se retrăsese *„fără cauze aparente, precipitat și fără a mă preveni la timp*" după cum scria în memoriile sale generalul Averescu, transformându-i Ajunul Crăciunului în cea mai urâtă zi din viață (Averescu 1992, 102). În același timp, Sturdza realiza că acest important sector era ocupat de un batalion *de strânsură*, la a cărui pregătire anterioară nu putuse contribui, comandat de un ofițer pe care știa că nu putea conta.

Despre coeziunea de luptă și disciplina dintr-o astfel de unitate, amintește și generalul Scărișoreanu în memoriile sale, când povestește despre decizia Diviziei 7 Infanterie, căreia i se subordona, de a schimba o companie din Regimentul 3 Vânători, care îi fusese dată, inițial, în sprijin, cu o companie dintr-un regiment de completare, format din resturile altor unități, care fuseseră găsite fără niciun rost în spatele Armatei a 2-a: *„(...) pe lângă că nu avea niciun fel de omogenitate, dar se prezenta și sub un aspect de destrăbălare ce nu inspira nicio încredere, din care cauză nu o trimit niciodată în linia 1-a, și o țin numai în rezervă*" (Scărișoreanu 1934, 193).
În al doilea rând, Sturdza venise *dinadins* să dea un exemplu, fiindcă în sectorul batalionului, în fiecare zi, se producea panică și, ce era și mai grav, la aceste manifestări de panică, participau inclusiv ofițerii.

Panica

După părerea mea, rapiditatea cu care a fost judecat, condamnat și executat Ciulei nu are nicio legătură cu Sturdza, ci cu un fenomen mult mai periculos. Este vorba despre *panică*, un fenomen ce apărea frecvent în rândul trupelor demoralizate și obosite, care fugeau de pe poziție sau, mai grav, dezertau de bunăvoie la inamic. Până la 19 ianuarie 1917, Marele Cartier General nu fusese informat despre acest fenomen prin comunicatele operative ale Armatei a 2-a, ci aflase din comunicatele inamicului. Mai precis, în momentul în care au realizat că germanii nu mint în comunicatele lor cu privire la numărul celor capturați, ba cifrele sunt chiar mai mari, și că totul s-a petrecut într-un termen atât de scurt, și pe un sector de front atât de redus, și-au dat seama că trebuie să ia măsuri drastice.

Panica, frica individuală ori colectivă dusă la extrem, se manifestă pe câmpul de luptă prin *noncombat*, refuzul de a mai lupta, aruncarea armelor și echipamentului,

fuga de pe poziție ori predarea benevolă, ori o combinație a celor de mai sus. În acest gen de situații, frica persistă, nu dispare ușor, dar poate fi controlată. Nivelul acestui control reprezintă o proiecție a moralului trupei și una dintre preocupările esențiale ale ofițerilor acelei trupe. Aceștia ar fi trebuit să fie fermi, un exemplu de stabilitate morală și curaj, și să-și îmbărbăteze permanent subordonații.

Sturdza prevăzuse posibilitatea apariției acestui fenomen în cadrul unităților brigăzii sale, încă de la începutul războiului. La 20 septembrie 1916 a emis *„Circulara privitoare la preîntâmpinarea panicelor"* (Arhivele Militare Naționale Române, dosar nr. 21, f. 176), prin care descria subordonaților panica drept un fenomen simptomatic, care apăruse și în conflictele trecute, dar și în cel prezent atât în armata noastră, cât și în alte armate, și prin care stabilea sarcini concrete comandanților de la toate nivelurile de comandă.

Principala trăsătură a acestui fenomen era considerată *contagiunea*, urmată de *rapiditatea transmiterii* în rândul trupei, având la origini zvonuri, zgomote, mișcări neașteptate, strigăte sau semnale de alarmă etc.
„Panica nu cuprinde în orice mediu, își asigura Sturdza subordonații, *o trupă bine instruită (...) și care-și cunoaște bine pe comandanții săi, o trupă unde domnește (...) solidaritatea frățească între cadre de orice grad și soldați (...) nu se alarmează așa ușor ca alta, unde șefii trăesc la o parte de inferiori, unde încrederea nu există și autoritatea se impune numai prin puterea disciplinară"* (Arhivele Militare Naționale Române, dosar nr. 21, f. 176).

Pentru a evita astfel de manifestări dăunătoare, Sturdza dispunea ca, zilnic, comandanții de companie, de escadroane și baterii să stea de vorbă cu oamenii, să facă *orientarea trupei,* printr-o expunere simplă, sinceră și încrezătoare a situației, și mai ales să interzică, și chiar să pedepsească, colportarea de zvonuri. Concluzia acestui ordin circular era că, prin atitudine, ofițerii puteau influența mult trupa, și o puteau păzi de panică prin puterea autorității morale: *„Problema de rezolvit* (sic!), mai adăuga acesta, *este o cestiune de educațiune, de organizațiune și de conducere și în prima linie* (în primul rând, s.n.) *de personalitate și de caracter"* (Arhivele Militare Naționale Române, dosar nr. 21, f. 177).

Știm din comunicatul Armatei a 2-a că, la 25 decembrie, deci cu numai o zi înainte, Sturdza îi dăduse lui Mărculescu ordinul de a-i executa imediat pe aceia dintre subordonați care propagau zvonuri panicarde. Acest ordin reprezenta un adevărat *cec în alb* și, probabil, Sturdza nu avusese niciun semnal despre vreo măsură de acest fel. La data citirii acestui articol și cunoscându-l pe Mărculescu prin prisma caracterizărilor șefilor lui ierarhici, ne este clar faptul că așteptările lui Sturdza de la un om cu temperamentul lui Mărculescu erau total nerealiste. Lipsit de energie, fire melancolică, bolnăvicioasă, complexat de un tic nervos și o exprimare greoaie, peltică, lui Mărculescu i-ar fi fost imposibil să se impună în fața subordonaților săi, după cum am afirmat anterior, cu atât mai mult să-i împuște.

Cât despre Ciulei, deși în ochii lui Sturdza acesta împărțea vinovăția solidar cu întregul corp ofițeresc al batalionului, nu aceasta era circumstanța agravantă a statutului său, ci în opinia mea, funcția deținută în cadrul batalionului lui Mărculescu, aceea de comandant al rezervei de batalion.

Explicația ar putea fi, în opinia mea, legată chiar de rolul rezervei de batalion care, de regulă, intervine în luptă, executând contraatacul atunci când linia defensivă a batalionului este străpunsă. Ar fi fost deci sarcina lui Ciulei să intre în luptă și să contraatace cu cele două plutoane din subordine, atunci când germanii au ocupat pozițiile batalionului pe *Momâia*. Însă, din mărturia locotenentului Marinescu, reiese că, la primul contact cu inamicul, sublocotenentul care comanda rezerva de batalion ar fi fugit cu tot cu plutoanele din subordine. De asemenea, din raportul lui Polihroniade, reiese că l-ar fi găsit pe Ciulei în *Varnița*, cu mult în spatele frontului, cu tot cu cele două plutoane pe care le comanda.
Această construcție argumentativă invalidează, încă o dată, ipoteza că Sturdza ar fi vrut în mod deliberat să-l omoare pe Ciulei, fiindcă acesta i-ar fi ghicit intențiile de a trece la inamic și că, ulterior, din același motiv, l-ar fi trimis în fața Curții Marțiale.

Pe Mărculescu, Sturdza îl cunoștea anterior evenimentului de pe *Momâia*, așa după cum el însuși precizase, de la *Câmpuri*, când a mers personal la el, fiindcă raporta efective considerabil mai mici decât în realitate. Nu sunt însă elemente care să ne îndreptățească să afirmăm că Sturdza l-ar fi cunoscut anterior și pe Ciulei. Pe Mărculescu, Sturdza îl cunoștea, dar nu îl aprecia defel, considerându-l absolut inert în exercitarea actului de comandă și lipsit de empatie față de situația în care se aflau subordonații lui, despre care nu știa, cum am spus, nici măcar cu aproximație, câți erau.
Deși, la prima vedere, această acuzație nu ar părea foarte gravă, în contextul resubordonării batalionului său Brigăzii 7 Mixtă, Mărculescu ar fi trebuit să știe în orice moment exact câți militari avea în subordine. Cine a făcut armata sau are în vreun fel legătură cu un astfel de sistem, înțelege că, în funcție de efectivele sale, o subunitate este alocată la norma de hrană, i se distribuie echipamentul, armamentul și muniția și i se stabilesc misiunile.

Dacă ar fi fost adevărat că Mărculescu raportase un efectiv de 500 de militari, pe când efectivul real ar fi fost de 700 de oameni, ar fi însemnat, numai din punctul de vedere al hranei, cu 200 de porții de mâncare pe zi mai puțin pentru subordonații săi. Iar rezultatul acestei „scăpări" administrative nu ar fi fost nicicum în măsură să ridice moralul trupei, având în vedere condițiile de trai de pe frontul Armatei a 2-a, pe care le-am prezentat.

Comunicatele

De la data de 31 decembrie 1916/13 ianuarie 1917, când generalul Gheorghe Mărdărescu a informat Marele Cartier General în legătură cu evenimentele din data de 26 decembrie de pe *Momâia*, și până la 20 ianuarie 1917, nu am mai găsit în

arhivele militare nimic notabil referitor la acest subiect. La 28 decembrie, după cum am menționat, Ciulei fusese prins în casa unui gospodar din *Verdea,* și deferit Curții Marțiale, iar dosarul său își urma, ierarhic, cursul.
Între timp, Sturdza predase, la 4 ianuarie 1917, comanda Brigăzii 7 Mixtă, fiind numit la comanda Diviziei 10 Infanterie, o numire care, așa după cum am susținut anterior, pare să-l fi determinat să ia decizia de a trăda. Ceva s-a întâmplat totuși în speța de față, între 31 decembrie 1916 și 20 ianuarie 1917, ceva care să constituie și o explicație a grabei cu care sublocotenentul Ciulei a fost judecat, condamnat și executat. Un alt motiv decât influența lui Sturdza asupra completului de judecată al Curții Marțiale a Armatei a 2-a, ipoteză asupra căreia ne-am pronunțat, prezentând mai sus argumentele noastre.

Astfel, este foarte posibil ca Marele Cartier General, nu Sturdza, să fi vrut să dea un exemplu pentru a opri fenomenul dezertărilor, iar Ciulei să fi fost considerat chiar exemplul potrivit. Se afla deja în custodia autorităților militare după ce încercase să fugă, avea dosarul instrumentat, iar acuzațiile care i se aduceau aveau legătură cu subiectul față de care Marele Cartier General arăta un interes nedisimulat. Altfel nu s-ar explica de ce, din data de 31 decembrie 1916, când Marele Cartier General fusese informat în volum complet de către generalul Mărdărescu în legătură cu cele petrecute pe *Momâia*, reacția eșalonului superior a venit abia în data de 19 ianuarie 1917, când generalul Cristescu a solicitat Armatei a 2-a, cu *„Telegrama nr. 4710"*, să raporteze despre veridicitatea celor susținute de comunicatele inamicului, aspect pe care l-am detaliat mai sus (Arhivele Militare Naționale Române, dosar nr. 160, f. 52).

Probabil, în același curent se înscrie și *„Telegrama nr. 4720*, din 20 ianuarie 1917, prin care Marele Cartier General a cerut Armatei a 2-a să se raporteze de către Brigada 7 Mixtă despre incidentul predării Companiei a 3-a din batalionul comandat de căpitanul Mărculescu" (Arhivele Militare Naționale Române, dosar nr. 160, f. 48v). Telegrama era cifrată și avea caracter *secret,* cerea urgent detalii asupra incidentului, insistând să se precizeze dacă subunitatea a fost capturată prin *„forță majoră sau de bună voe"* (sic!). De asemenea, în raport trebuia să se indice numele ofițerilor responsabili de producerea acestui eveniment.

Răspunsul din partea Brigăzii 7 Mixtă a venit tot prin Armata a 2-a, care a trimis *„Telegrama nr. 3133"*, din 21 ianuarie 1917, cifrată și extraurgentă, în care întreaga conducere a acelui batalion, nu numai căpitanul Stelian Mărculescu, era acuzată (Arhivele Militare Naționale Române, dosar nr. 160, f. 49). Ofițerii acestui batalion erau caracterizați drept *„needucați și neinstruiți"*, iar căpitanul Stelian Mărculescu era acuzat că, la 26 decembrie 1916, în momentul predării intenționate de pe *Momâia,* se afla la 1 km în spatele frontului, ocupându-se de pregătirea propriei mese.

Ineditul situației este că această *Telegramă* nu era semnată de Sturdza, ci de locotenent-colonelul Pascu, cel care preluase comanda Brigăzii 7 Mixtă, după numirea lui Sturdza la comanda Diviziei 8 Infanterie, aflată tot în organica Armatei a 2-a. De subliniat faptul că, deși Brigada 7 Mixtă avea alt comandant, acuzațiile

la adresa lui Mărculescu se menţineau în aceeaşi notă ca şi pe timpul lui Sturdza, situaţie pentru care ar exista cel puţin două explicaţii: cea dintâi, că noul comandant al brigăzii nu vroia să se abată de la „linia" trasată de predecesorul său, iar cea de-a doua, că, pur şi simplu, acesta era adevărul.

Efectul cumulat al acestor două telegrame, credem noi, a grăbit judecata lui Ciulei, care, prin *„Sentinţa nr. 20/1917"* (Arhivele Militare Naţionale Române, dosar nr. 11, f. 410) a Curţii Marţiale a Armatei a 2-a, a fost condamnat la moarte şi executat în dimineaţa zilei de 28 ianuarie 1917. Câteva ore mai târziu, era prins Crăiniceanu, cu pachetul de manifeste instigatoare asupra sa, eveniment care clarifica dispariţia lui Sturdza, dar nu putea schimba soarta lui Ciulei, deja pecetluită.

Justiţia

Administrarea justiţiei militare în Războiul de Întregire s-a desfăşurat în baza prevederilor Codului de justiţie militară, adoptat în anul 1873 după modelul francez, promulgat prin *„Înaltul Decret nr. 828 din 5 aprilie 1873"* şi intrat în vigoare în luna octombrie a aceluiaşi an (Monitorul Oastei 1873). A fost republicat în anul 1881, după care a fost modificat şi completat succesiv, în anii 1881, 1894, 1905, 1906, 1916 şi 1917, în concordanţă cu schimbările sociale, economice şi legislative prin care a trecut societatea românească, dar şi în încercarea de a ţine pasul cu realitatea câmpului de luptă, odată cu intrarea României în Războiul de Întregire.
Cea mai semnificativă modificare a Codului de justiţie militară, în economia speţei de faţă, o reprezintă adoptarea Titlului II adiţional, sub forma *„Legii privitoare la suprimările, modificările şi adăugirile de făcut codului de justiţie militară pentru timpul de mobilizare şi război",* înregistrată cu nr. 3245, din 21 decembrie 1916/3 ianuarie 1917 (Monitorul Oficial 1916, 7529-7530).

Modificarea Codului de justiţie militară prin care s-a adăugat Titlul II adiţional a fost poate una dintre cele mai importante măsuri legislative adoptate în acea perioadă, *„un act fundamentat juridic pe elemente de psihologie militară",* fiind modificată întreaga materie specială referitoare la justiţia militară pentru a se ţine cont de *trebuinţele de neapărată reprimare* a unor fapte (Zidaru 2006, 70). Era un context deosebit de dificil pentru România, care, la momentul adoptării acestui demers, pierduse, după unii autori, în cele câteva luni care trecuseră de la debutul campaniei, două treimi din suprafaţa ţării şi aproximativ 250.000 de militari, morţi, răniţi şi dispăruţi (Torrey 2014, 352), respectiv, două treimi din armele individuale, jumătate din mitraliere şi un sfert din piesele de artilerie, conform altor surse (Bărbulescu şi alţii 2014, 343).

Adoptarea Titlului II adiţional a creat cadrul juridic necesar sancţionării unor noi infracţiuni, precum *trădarea*, *spionajul*, *automutilarea*, *producerea cu rea-credinţă a panicii*, *crearea sau răspândirea de veşti false* etc., şi a dus la înăsprirea pedepselor, în vederea unei grabnice şi exemplare reprimări.

Activitatea *Curții Marțiale* pe timp de mobilizare și război a fost reglementată prin prevederile art. 19-35 din Titlul II adițional. Acestea funcționau la comandamentul fiecărui corp de armată, la comandamentele diviziilor independente sau al acelora care operau izolat, precum și oriunde trebuința serviciului o cerea. Conform *„Instrucțiunilor în ce privește Curțile marțiale"* (Monitorul Oficial 1917, 195-201), numirile în cadrul acestora erau făcute de către comandantul marii unități pe lângă care aceasta funcționa, fiecare curte marțială având atașat și un *comisar regal* (procuror, s.n.), care îndeplinea și funcția de *raportor,* cu atribuții oarecum similare judecătorului de instrucție. Procedura impunea ca sentințele de condamnare a militarilor, precum și cele de condamnare pentru trădare și spionaj, indiferent dacă subiectul era militar ori civil, să fie aduse de îndată la cunoștința comandantului care dăduse ordinul de constituire a Curții Marțiale, împreună cu un referat al comisarului regal. Odată aprobată, sentința Curții Marțiale devenea definitivă și executorie de drept, urmând a fi pusă în executare, indiferent dacă cel condamnat ar fi utilizat sau nu calea de atac a recursului, având în vedere că acesta fusese ridicat prin Înaltul Decret Regal nr. 7, din 10/23 ianuarie 1917.
De subliniat faptul că celeritatea procedurii în fața Curții Marțiale, alături de înăsprirea pedepselor aplicate de Codul de justiție militară au reprezentat mijloace prin care s-a urmărit menținerea unui nivel de disciplină corespunzător printre militari, imperativ cerut de situația de pe front, aflată într-o permanentă dinamică.

Modificarea Codului de justiție militară s-a suprapus pe adoptarea unor măsuri controversate, precum decretarea stării de asediu și suspendarea dreptului la recurs. Aceasta din urmă a fost adoptată de regele Ferdinand I după intrarea României în război, prin *„Înaltul Decret Regal nr. 2930 din 16/29 septembrie 1916"* (Monitorul Oficial 1916, 6266), în baza prevederile art. 67 din Codul de justiție militară. Acesta prevedea că dreptul la recurs pentru persoanele condamnate prin sentințe ale consiliilor de război poate fi suspendat temporar pe timp de război, prin decret regal, în baza avizului Consiliului de Miniștri (guvernului, s.n.).
Înaltul Decret Regal nr. 2930 a fost emis în contextul juridic al existenței pe tot cuprinsul țării a stării de asediu, instituită ca urmare a împrejurărilor create de intrarea României în război. Decizia regelui Ferdinand I a fost justificată prin caracterul vremelnic al demersului și avea la bază raportul ministrului de război, Vintilă I.C. Brătianu, înregistrat cu nr. 8257, din 16/29 septembrie 1916, care consemna: *„Sire, (...) în momentele grele prin care trecem, necesitatea menținerii cu tărie și în cel mai înalt grad a disciplinei militare, reclamă imperios decretarea acestei suspendări a recursurilor la consiliul de revizie, căci numai așa exemplaritatea pedepselor pronunțate de consiliile de război, își vor putea produce efectul ei* (sic!)*, prin executarea lor chiar imediat după pronunțarea sentințelor de condamnare"* (Monitorul Oficial 1916, 6266).

O măsură „ajustată" la perioada dificilă pe care o traversa armata română în campania anului 1916, dacă ar fi să ne ghidăm după data la care au fost publicate, în Monitorul Oficial, documentele justificative în baza cărora a fost emis acest Înalt Decret Regal.

Judecând după data emiterii actului normativ, 16/29 septembrie 1916, *momentele grele* la care făcea referire raportul ministrului de război şi care cu siguranţă au contribuit la adoptarea acestei măsuri, au fost reprezentate de seria de eşecuri militare, suferite de campania armatei române până la acea dată. Cel mai răsunător a fost cel generat de căderea capului de pod fortificat *Turtucaia*, la data de 24 august/6 septembrie 1916, constituit la numai 60 km de Bucureşti, un eveniment considerat a fi fost „*o catastrofă națională*" (Kirițescu 1927).

Alături de acesta, au mai contribuit situația critică din Dobrogea, unde trupele româno-ruso-sârbe pierduseră bătălia pentru *Bazargic* (Kirițescu 1927, 413) (25 august/7 septembrie 1916), iar *Silistra* fusese evacuată fără luptă (Kirițescu 1927, 423) (26 august/8 septembrie 1916), pierderea pasului *Merişor* şi a oraşului minier *Petroşani* (Kirițescu 1927, 230) (7/20 septembrie 1916), precum şi retragerea (Kirițescu 1927, 294) *Corpului de la Olt*, sub presiunea armatei germane, în *bătălia Sibiului* (16/29 septembrie 1916).

Pe lângă scopul declarat, al întăririi ordinii şi disciplinei militare, suspendarea dreptului la recurs mai urmărea şi ridicarea capacităţii combative a armatei şi descurajarea oricărui gen de acţiuni demobilizatoare, având în vedere că luarea *cuvenitelor măsuri,* după expresia menționată în raport, nu fuseseră stabilite în sarcina Ministerului de Justiție, ci în sarcina Ministerului de Război şi a Marelui Cartier General. Marele Cartier General a ordonat înființarea curților marțiale prin „*Ordinul de Zi nr. 322 din 12/25 ianuarie 1917*" (Homoriceanu 1916, 89), la Armata a I-a și la Armata a II-a, la cele cincisprezece divizii de infanterie, la cele două divizii de cavalerie, precum și la Flota de operațiuni. Prin urmare, începând cu data de 12/25 ianuarie 1917, la Marele Cartier General și la armata de operațiuni au funcționat 21 de curți marțiale, cu parchetele militare aferente.
Astfel, în absența recursului la Curtea superioară de justiție militară, decizia Curții Marțiale era supusă aprobării comandantului eșalonului pe lângă care aceasta funcționa, și odată aprobată, se punea *imediat* în executare. După război, această procedură ulterioară hotărârii, de implicare a actului de comandă în actul de justiție, a suscitat cele mai multe comentarii și a generat cea mai mare neîncredere față de obiectivitatea, imparțialitatea și independența actului de justiție militară.

Reparația

Căpitanul Mărculescu a supraviețuit atât acestui straniu incident, cât și războiului, și deși rănit la braț și în regiunea gâtului, a reușit cumva să se strecoare în spatele frontului românesc, până la un spital militar din Botoșani. În momentul apariției sale, scandalul Sturdza era în plină desfășurare, astfel încât statutul i s-a schimbat instantaneu, din *dezertor* devenind victima trădătorului Sturdza și, implicit, *erou*.
A fost sau nu a fost Mărculescu vinovat? Acuzațiile la adresa lui Mărculescu, consemnate în raport de către Polihroniade, au fost însușite ca fiind reale și de către Constantinescu, care a consemnat pe raport propria rezoluție și i-a transmis

mai departe lui Sturdza. Aceste acuzații au fost reconfirmate ulterior de către Constantinescu în declarația pe care acesta a dat-o în fața comisarului regal, la data de 28 februarie, cu mult după ce se aflase despre dezertarea lui Sturdza. Au mai fost confirmate și de către căpitanul Marinescu în declarația sa, dată comisarului regal, dar și de locotenent-colonelul Pascu în raportul înaintat telegrafic Armatei a 2-a, pentru a fi retransmis Marelui Cartier General. Acest raport, care încerca să lămurească eșalonul superior în legătură cu trecerea la inamic a Companiei a 3-a, fusese întocmit la câteva săptămâni după ce Sturdza predase comanda brigăzii, dar transmitea aceeași idee: *„batalionul era rău condus"* (Arhivele Militare Naționale Române, dosar nr. 160, f. 49).

De la începutul carierei sale și până la începutul războiului, Stelian Mărculescu a fost caracterizat drept un ofițer mediocru. Prima modificare a imaginii acestuia în ochii superiorilor apare în *foaia calificativă rezumativă,* care acoperă perioada 15 august 1916 - 8 august 1917. Emisă cu antetul Regimentului 9 Infanterie Râmnicu Sărat, în această foaie calificativă apar primele aprecieri elogioase, în mod evident contrare celor consemnate până atunci. Acestea au drept „autori" pe colonelul Dumitru Todicescu, comandantul Regimentului 9 Infanterie Rm.Sărat, și pe același colonel Alexandru Jecu, asupra căruia am menționat că vom reveni, comandantul Regimentului de Marș al Diviziei 5 Infanterie, fostul comandant al căpitanului Stelian Mărculescu, pe vremea când acesta activa în Regimentul 48 Infanterie.

În viziunea noilor șefi ierarhici, Mărculescu este *„energic și prezentabil în fața frontului, are ochiul câmpului și al comandantului de unitate, cunoaște bine regulamentele militare și le prezintă cu multă preciziune"* (Arhivele Militare Naționale Române, dosar nr. 39, f. 25). Dincolo de aceste aprecieri, inedit este faptul că este prezentat ca fiind cel care a împiedicat planurile de dezertare ale colonelului Sturdza, un episod considerat de evaluatori drept *„un adevărat roman eroic",* fără a fi prezentate alte detalii sau argumente (Arhivele Militare Naționale Române, dosar nr. 39, f. 25).

Singurul care a rămas totuși consecvent evaluării inițiale a fost generalul Aristide Razu, care, deși pare să fi făcut un compromis în ceea ce îl privește pe Mărculescu, a păstrat linia de dinainte de război și a contrazis aprecierile celorlalți comandanți. Generalul Razu a consemnat:*„deși lipsit de energie, totuși bunăvoința în serviciu compensează lipsa de pregătire militară"* (Arhivele Militare Naționale Române, dosar nr. 39, f. 25). Faptul că, în urma acestor aprecieri elogioase, Mărculescu a fost propus la înaintarea în gradul de maior, în mod excepțional, și chiar printr-un raport special, ne îndreptățește să credem că acestă schimbare de atitudine față de persoana sa ar fi putut fi o *reparație morală* față de cele petrecute în seara zilei de 26 decembrie 1916.

Cu siguranță, a contribuit și povestea spusă de el superiorilor, în care s-a prezentat ca fiind cel care ar fi ținut pe loc trupele germane care erau pe cale de a sparge frontul în sectorul generalului Mannerheim, și cel care ar fi surprins primele încercări de trădare ale colonelului Sturdza. Din acest motiv, se consemna în foaia calificativă,

Sturdza ar fi încercat să scape de el și l-a împușcat *„și numai mulțumită prezenței de spirit (...) scapă de glonțul trimis în pieptul său (...) căci a parat lovitura culcându-se"* (Arhivele Militare Naţionale Române, dosar nr. 39, f. 26). Fără alte comentarii!
Mărculescu a fost avansat la gradul de maior la 1 noiembrie 1917, iar în următorii ani, au continuat aprecierile laudative din partea comandantului său de regiment, același colonel Todicescu, care nu a pregetat ca, în foaia calificativă pentru anii 1918-1919, să propună să fie avansat la gradul de locotenent-colonel, în mod excepțional, precum și să i se încredințeze comanda unui regiment.

Aceste propuneri nu au fost agreate de șefii eșaloanelor superioare, comandantul Diviziei 5 Infanterie, generalul Ioan Vernescu, considerând că, în perioada evaluată, nu a survenit nicio împrejurare care să-i dea dreptul lui Mărculescu să fie avansat în mod excepțional. Această opinie a fost împărtășită și de comandantul Corpului III Armată, generalul Dumitru Strătilescu, fost comandant al Diviziei 1 Infanterie, care îl avusese pe Mărculescu subordonat. Mai mult, acesta observa că afirmația deja însușită de comandantul de regiment, precum că Mărculescu l-ar fi împiedicat pe Sturdza de la dezertare, *„nu e sprijinită pe niciun document"* (Arhivele Militare Naţionale Române, dosar nr. 39, f. 30), fiind chiar surprins că această *„afirmațiune"* venea din partea unui ofițer, pe care de altfel îl considera vrednic, de talia colonelului Todicescu.

După anul 1919, activitatea și pregătirea maiorului Stelian Mărculescu au primit din nou aprecieri nefavorabile. Acesta a participat cu Regimentul 9 Infanterie Râmnicu Sărat la campania din Basarabia, în apărarea Nistrului, după care a fost mutat în cadrul Biroului mobilizare la Regimentul 48/49 Infanterie Buzău. A fost avansat la gradul de locotenent-colonel la 1 aprilie 1920, grad cu care a trecut în rezervă în anul 1932.

În vara anului 1917, sublocotenentul Constantin Ciulei a fost decorat (Monitorul Oficial 1917) cu Ordinul *„Coroana României"*, cu spade, în grad de *Cavaler*, pentru bravura și avântul cu care și-a condus plutonul în campania din Dobrogea, la 6 septembrie 1916, în lupta de la *Caciamac*, *„unde a cucerit prima linie de întărire a inamicului"* (Arhivele Militare Naţionale Române, dosar nr. 44, f. 05) și unde a fost, de altfel, rănit.
Și căpitanul Mărculescu a fost decorat (Arhivele Militare Naționale Române, dosar nr.44, f. 03), dar în urma campaniei din Transilvania, din toamna anului 1916, cu una dintre cele mai înalte distincții ale statului român, *Ordinul Steaua României*, cu spade, în grad de *Cavaler.* Distincția i-a fost acordată pentru curajul și avântul cu care și-a condus compania în luptele de la *Bodza-Van* (astăzi, Sita Buzăului, s.n.), unde a alungat inamicul din sat, după un atac la baionetă, și unde a capturat peste 100 de prizonieri. Mărculescu a fost decorat prin același Înalt Decret Regal nr. 681, din 10 iulie 1917, prin care fusese decorat și Ciulei (Monitorul Oficial 1917).

Coincidență sau reparație morală? Nu putem ști. Cert este că propunerile pentru aceste distincții au fost înaintate Biroului Decorații din cadrul Statului Major Regal pe un tabel cu propuneri, inițiate de Regimentul 8 Infanterie Buzău, fiind însușite și susținute de comandantul Diviziei 5 Infanterie, generalul Aristide Razu.

Generalul Razu a exercitat, cel puțin teoretic, comanda Diviziei 5 Infanterie în perioada 23 decembrie 1916 - 29 iulie 1917, dar este posibil ca preluarea efectivă a comenzii Diviziei 5 Infanterie de la generalul Constantin Petala să se fi făcut mai târziu, poate chiar după evenimentele din 26 decembrie 1916, de pe *Momâia*.
Astfel, cu excepția cazului în care generalul Aristide Razu nu și-a marcat debutul la comanda diviziei tocmai cu propunerile de avansare ale lui Mărculescu și Ciulei, pe care ar fi trebuit să le promoveze chiar în primele trei zile de la numirea sa, este foarte posibil ca propunerile de decorare a celor doi ofițeri să fi fost făcute ulterior execuției lui Ciulei și dezertării lui Sturdza, având astfel toate șansele să reprezinte, în fapt, o reparație morală.

Concluzii

Astfel, în baza studiului aprofundat al subiectului, dar și a argumentelor pe care le voi prezenta în continuare, mă consider îndreptățit a crede că nu Sturdza se face vinovat de moartea lui Ciulei. Sturdza va rămâne în istorie drept un trădător, dar nu i se poate atribui și moartea lui Ciulei, chiar dacă el este cel care l-a trimis în fața Curții Marțiale.
În opinia mea, succesiunea de telegrame schimbate între Marele Cartier General și Armata a 2-a arată în mod evident interesul autorităților militare față de o soluționare rapidă și exemplară a cazului „trădătorului" Ciulei. Sturdza nu putea avea o asemenea influență la eșalonul comandat de generalul Alexandru Averescu, în schimb influența eșalonului superior acestuia, Marele Cartier General, nu numai că poate fi luată în discuție, dar *Telegrama* din 21 ianuarie, despre care am vorbit mai sus, este chiar concludentă în acest sens.

Astfel, putem afirma că Sturdza nu ar fi putut influența Curtea Marțială a Armatei a 2-a în ceea ce privește judecata lui Ciulei, în schimb ar fi putut-o face Marele Cartier General, care devenise *dintr-odată* nu numai îngrijorat, dar și interesat de subiect. Aflând despre situația reală a dezertorilor și a celor capturați de inamic, situație care nu apăruse până atunci în raportările zilnice ale Armatei a 2-a, Marele Cartier General s-a temut că un eveniment de genul celui de pe *Momâia*, când o întreagă companie trecuse la inamic de bunăvoie, act care a avut drept consecințe părăsirea pozițiilor și capturarea unor efective de nivelul unui batalion, ar fi putut produce o eventuală contagiune în rândul trupelor deja demoralizate ale Armatei a 2-a, care iernau pe front, fără a avea posibilitatea de a fi înlocuite.

În opinia mea, gravitatea faptelor sesizate de Marele Cartier General nu consta neapărat în predarea benevolă a trupei ori în fuga celorlalți din fața inamicului, ci în faptul că, pe *Momâia*, aceste fapte fuseseră săvârșite de o subunitate, constituită laolaltă cu ofițerii și subofițerii care ar fi trebuit să o comande și să vegheze ca acest gen de fapte să nu aibă loc. Iar această stare de lucruri se petrecea în circumstanțele, deja prezentate, în care fuseseră permise până și execuțiile sumare, iar comandanților le era îngăduit să dețină dreptul de viață și de moarte asupra subordonaților lor.

Toate aceste măsuri, pe care le vom denumi eufemistic „derogatorii" de la prevederile legale, fuseseră adoptate în speranța de a menține ordinea și disciplina în rândul trupelor, ca alternativă la soluția justiției militare, un proces considerat mult mai lent. Iar, atunci când aceiași comandanți au ales totuși această cale, sistemul a pus în aplicare o justiție militară insensibilă la circumstanțe, opacă în fața argumentelor juridice și procedurale, inaccesibilă chiar și unei logici elementare, și în care pregătirea de specialitate a ofițerilor-judecători nu reprezenta o prioritate.

Mai mult, a permis și a încurajat în rândul membrilor completelor de judecată dorința de a satisface „exigențele" marilor comandanți, direct proporționale cu nivelul de comandă pe care aceștia îl exercitau, în detrimentul principiului supremației legii. Un sistem de justiție militară profund subiectiv, care a dat dreptul comandanților eșaloanelor pe lângă care aceste curți marțiale funcționau să numească judecătorii dintre ofițerii subordonați și, în același timp, să valideze sentințele acestora. Fiindcă aceasta este esența acestui caz. Indiferent cum, dar mai ales cât de repede ar fi fost judecat sublocotenentul Ciulei de către Curtea Marțială, sentința sa de condamnare la moarte a fost pusă în executare la 28 ianuarie numai după ce a fost validată de către factorii de decizie ai Armatei a 2-a, *tandemul Mărdărescu – Averescu*. Iar generalul Averescu fusese informat încă din 23/24 ianuarie 1916 în legătură cu ciudata dispariție a colonelului Sturdza și bănuia, chiar după spusele sale, încă din data de 27 ianuarie, că acesta dezertase.

În mod cert actul trădării lui Sturdza rămâne la fel de reprobabil, dar acesta nu poate fi acuzat de circumstanțele în care a fost judecat și executat Ciulei. Acestea rămân în sarcina factorilor de decizie ai Marelui Cartier General și ai Armatei a 2-a, cei care au vrut să dea un exemplu și au dispus Curții Marțiale judecarea cu maximă celeritate, chiar dacă nu erau îndeplinite minime cerințe procedurale, cei care i-au validat sentința de condamnare la moarte, chiar dacă asupra celui care îl acuzase pe Ciulei plana bănuiala de dezertare.
Acestea sunt, de fapt, *împrejurările nefericite*, menționate la începutul acestui articol, cărora i-a căzut victimă sublocotenentul Constantin Ciulei, cel judecat, condamnat și executat după un simulacru de proces, și a cărui vinovăție nici nu mai contează.

Referințe

Anastasiu, Ion. 1927. *Din Crimele Marelui nostru război.* Cluj: Institutul de Arte Grafice „Viața".

Arhivele Militare Naționale Române (AMNR). dosar nr. 6. „fond Direcția Cadre și Învățământ, vol. 7."

—. dosar nr. 11. „fond Registru Ofițeri Rezervă Infanterie."

—. dosar nr. 21. „fond Brigada 7 Mixtă."

—. dosar nr. 37. „fond Brigada 7 Mixtă, Ordine circulare, ordine de zi, rapoarte telefonice."

—. dosar nr. 39. „fond Memorii Bătrâni."

—. dosar nr. 44. „fond Stat Major Regal, Biroul Decorații."

—. dosar nr. 160. „fond Marele Cartier General."

—. dosar nr.1691. „fond Marele Cartier General."

Averescu, Alexandru. 1992. *Notițe zilnice din război.* București: Editura Militară.

Bărbulescu, Mihai, Dennis Deletant, Keith Hitchins, Șerban Papacostea și Teodor Pompiliu. 2014. *Istoria României.* București: Corint Internațional.

Biblioteca Academiei Române (BAR). 1919. „Avântul. Organ politic independent. Ediție de seară a ziarului Izbânda." *P.IV.4.670, 16 noiembrie.*

Brădișteanu, Nicolae. 1972. „«Chemarea» a răsunat în pustiu." *Magazin Istoric.* octombrie nr.10 (67).

Buttescu, Mihai I. 2012. *Vânătorii Reginei Elisabeta. Memoriile unui ofițer din garda regală.* Ediție îngrijită de comandor (r.) Gheorghe Vartic. București: Editura Militară.

Homoriceanu, Nicolae. 1916. *Codul Justiției Militare adnotat.* Ediția a II-a. București: Tipografia Dim.C.Ionescu.

Ioanițiu, Alexandru. 1929. *Războiul României: 1916-1918.* Vol. 1. București: Tipografia Geniului.

Kapri, Valeriu. 1926. *Cazul fostului colonel Alexandru Sturdza, comandantul Diviziei a 8-a română. Un episod din războiul mondial, 1914-1918 pe frontul român.* Oradea: Tipografia Adolf Sonnenfeld.

Kirițescu, Constantin. 1927. *Istoria războiului pentru întregirea României, 1916-1919.* Ediția a II-a. București: Casei Școalelor.

Monitorul Oastei. 1873. nr. 13. 12 mai, 289-334.

Monitorul Oficial. 1920. nr. 8, din 15 aprilie.

—. 1916. nr.135, din 17 septembrie.

—. 1916. nr.224, din 28 decembrie.

—. 1917. nr. 20, din 25 aprilie.

—. 1917. nr. 90, din 16 iulie.

—. 1917. nr. 235, din 10 ianuarie.

Monkevitz, Nikolai A. și Aleksandr N. Vinogradski. 2019. *Aliatul inamic: descompunerea armatei ruse și pericolul bolșevizării României în 1917.* București: Editura Humanitas.

Nicolau, Eugen D. 1974. „Pe urmele unei erori judiciare: cazul sublocotenentului Ciulei." *Magazin Istoric,* nr. 5.

Otu, Petre și Maria Georgescu. 2011. *Radiografia unei trădări. Cazul colonelului Alexandru D. Sturdza.* București: Editura Militară.

Scărișoreanu, General R. 1934. *Fragmente din războiul 1916-1918. Istorisiri documentate.* Ediția a II-a. București: Tiparul Cavaleriei.

Tăslăuanu, Octavian C. 1934. *Sub flamurile naționale. Note și documente din Războiul de Întregire al neamului.* Vol. I. Sighișoara: Editura Miron Neagu.

Torrey, Glenn E. 2014. *România în Primul Război Mondial.* București: Meteor.

Zidaru, Petrache. 2006. *Tribunalele militare, un secol și jumătate de jurisprudență (1852-2000).* București: Univers Juridic.

BULETINUL
UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I”
https://buletinul.unap.ro

Regândirea sistemelor militare de comandă și control

Rethinking military command and control systems

Lt.col.Dr. George-Ion TOROI*
*Universitatea Națională de Apărare „Carol I”
e-mail:george_toroi@yahoo.com

Abstract

Articolul explorează necesitatea regândirii arhitecturii și principiilor fundamentale ale sistemelor C2, analizând elementele esențiale care susțin eficiența operațională: flexibilitatea, modularitatea, supraviețuirea, amprenta redusă și reziliența. În contextul noilor paradigme ale operațiilor, de tip multidomeniu, și al progresului tehnologic accelerat, adaptarea C2 implică integrarea unor tehnologii emergente, precum inteligența artificială, automatizarea și capabilități de răspuns în timp real pentru a optimiza procesul decizional. În mod particular, se accentuează importanța modularității și redundanței pentru a asigura funcționarea sistemelor, în condiții de conflict intens, alături de reducerea vulnerabilității electromagnetice și de creșterea mobilității. Concluziile articolului propun soluții practice pentru adaptarea sistemelor C2, organizate pe cele patru componente: personal, procese, sisteme tehnologice și puncte de comandă, subliniind, în același timp, rolul lor esențial în obținerea avantajului decizional, element crucial al succesului operațional în câmpul de luptă contemporan.

This article explores the need to rethink the architecture and fundamentals of C2 systems, analysing the essential elements that support operational effectiveness: flexibility, modularity, survivability, small footprint and resilience. In the context of new multi-domain operational paradigms and accelerated technological progress, C2 adaptation involves the integration of emerging technologies such as artificial intelligence, automation and real-time response capabilities to optimize decision-making. In particular, it emphasizes the importance of modularity and redundancy to ensure the operation of systems under conditions of intense conflict, as well as reducing electromagnetic vulnerability and increasing mobility. The article's conclusions propose practical solutions for adapting C2 systems organized around the four components of people, processes, technology systems and command posts, highlighting their essential role in achieving decision advantage, a critical element of operational success on the modern battlefield.

Cuvinte-cheie:
C2 (comandă și control); decizie; adaptare; tehnologie; factorul uman.

Keywords:
C2 (command and control); decision; adaptation; technology; human factor.

Info articol
Primit: 4 noiembrie 2024; Evaluat: 15 noiembrie 2024; Acceptat: 2 decembrie 2024; Disponibil online: 17 ianuarie 2025
Citare: Toroi, G.I. 2024. „Regândirea sistemelor militare de comandă și control”.
Buletinul Universității Naționale de Apărare „Carol I”. 13(4): 61-85. https://doi.org/10.53477/2065-8281-24-39

Mediul actual de operare se conturează ca un conglomerat integrat de amenințări, resurse și capabilități, extinzându-se dincolo de domeniile clasice terestru, aerian și maritim, incluzând și spațiul cosmic, cibernetic, spectrul electromagnetic sau dimensiunea informațională. Această complexitate accentuată necesită o regândire a modului în care sunt planificate, desfășurate și conduse operațiile militare, aducând noi provocări pentru conceptele tradiționale de comandă și control. În contextul transformărilor profunde din domeniul apărării, dar și pe fondul unei competiții tot mai acerbe între marile puteri, forțele armate occidentale întreprind măsuri accelerate de adaptare la noile cerințe și oportunități pe care le presupune conflictul armat contemporan (Bailey 2023).

Abordări moderne, precum operațiile multidomeniu, concept dezvoltat de Armata Statelor Unite și implementat și de NATO, pot asigura soluții menite să răspundă acestor noi exigențe, demonstrând necesitatea unei convergențe sporite a capabilităților și sincronizării între diferitele domenii de operare, dar și cu partenerii internaționali. Provocările din partea adversarilor tehnologici de talie mare, cum ar fi China și Rusia, subliniază urgența adaptării forțelor armate la un nou tip de competiție între mari puteri, pe întreg spectrul conflictului. Această tranziție nu se limitează doar la alinierea capabilităților militare, ci presupune un proces amplu de integrare a tehnologiilor avansate, de la inteligența artificială și automatizare, la supravegherea prin sateliți și comunicații digitalizate.

Problema de cercetare

În acest cadru, regândirea sistemelor de comandă și control devine o necesitate strategică pentru orice actor. Totuși, implementarea acestor schimbări nu este lipsită de dificultăți, deoarece mediul de operare în evoluție impune cerințe variate și, adesea, contradictorii asupra acestor sisteme. Articolul de față analizează implicațiile unor astfel de schimbări pentru forțele armate române, principala țintă a acestui studiu, și explorează posibilele direcții de adaptare a sistemelor de comandă și control, în încercarea de a contura un model de comandă viabil în fața provocărilor complexe ale viitorului.

Scopul cercetării

Din acest motiv, lucrarea de față își propune să analizeze factorii care influențează sistemele C2 și să identifice direcții de acțiune pentru ținta principală a acestui studiu, Armata României, în demersul de adaptare a acestora la provocările curente și ale viitorului apropiat. Necesitatea unei astfel de regândiri vine pe fondul transformării modului de înțelegere și de desfășurare a conflictelor armate, dar și al dezvoltărilor accelerate ale sistemelor tehnologice și al impactului acestora asupra modului curent de operare. În plus, având în vedere importanța comenzii și controlului ca element central în procesul operațiilor militare, devine absolut necesar ca demersul de adaptare a forțelor armate să înceapă cu analiza sistemelor de comandă și control.

Metodologia de cercetare

Cercetarea întreprinsă a fost una **de tip calitativ**, având drept scop, inițial, înțelegerea nuanțelor specifice sistemelor de comandă și control, pentru ca, ulterior,

să analizăm provocările acestora, izvorâte din natura și caracterul conflictelor, dar și din tendințele de evoluție a mediului de operare. De asemenea, în consens cu abordarea calitativă întreprinsă, am optat pentru un **raționament de tip inductiv** prin care am construit concluziile și rezultatele obținute din datele empirice avute la dispoziție (Leavy 2023, 9; Creswell și Creswell 2023, 276).

Considerând natura calitativă a studiului, acesta nu a avut ca obiectiv testarea și validarea de ipoteze. Lucrarea a fost direcționată de următoarele **întrebări de cercetare**:

- Ce presupun sistemele de comandă și control?
- Care sunt factorii care influențează sistemele de comandă și control?
- Care sunt aspectele de care trebuie să se țină cont pentru o adaptare eficientă a sistemelor de comandă și control?

Schema logică a cercetării întreprinse se regăsește în figura de mai jos.

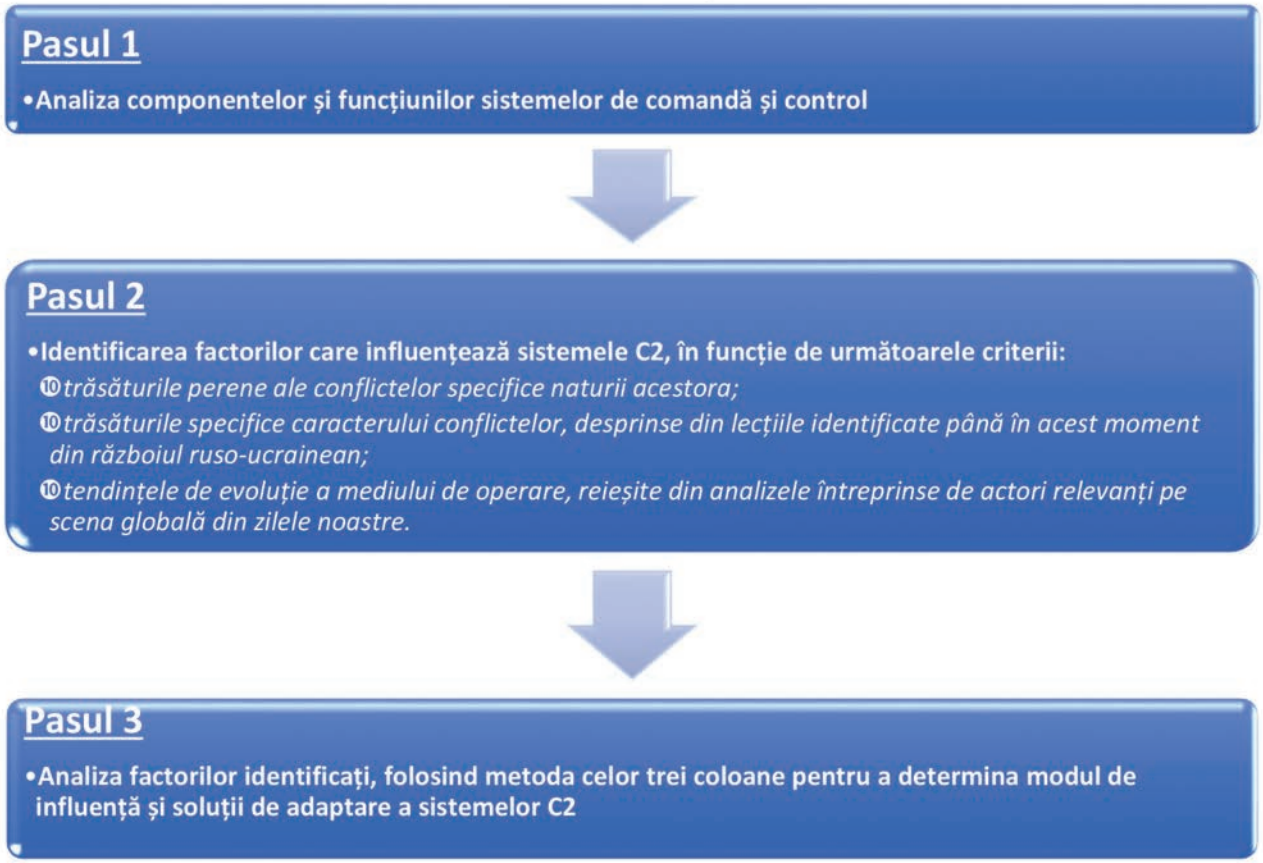


Figura 1 Schema logică a cercetării
Sursa: concepția autorului

Datele utilizate au fost, deopotrivă, **primare și secundare**. Astfel, am utilizat rezultatele unor cercetări anterioare pentru a identifica acele elemente ale naturii perene a conflictului, ale caracterului acestuia, rezultate din războiul ruso-ucrainean, dar și ale tendințelor de evoluție a mediului de operare, care pot influența sistemele de comandă și stat major. Am cules aceste date prin metoda analizei documentare pentru a le selecta pe cele mai relevante, în raport cu scopul studiului și cu întrebările de cercetare. **Eșantionarea** acestor date a fost una **de tip nonprobabilistic**, având la

bază trei criterii de selecție a datelor secundare:

- trăsăturile perene ale conflictelor specifice naturii acestora;
- trăsăturile specifice caracterului conflictelor, desprinse din lecțiile identificate până în acest moment din războiul ruso-ucrainean;
- tendințele de evoluție a mediului de operare, reieșite din analizele întreprinse de actori relevanți pe scena globală din zilele noastre.

Datele primare utilizate au rezultat dintr-un proces propriu de inferență asupra rezultatelor obținute din analiza impactului factorilor identificați, în raport cu cele trei criterii anterioare, asupra sistemelor C2, folosind **metoda brainstormingului individual**. Factorii au rezultat în urma aplicării **metodei de analiză comparativă** a documentelor selectate anterior pentru a ne asigura de relevanța lor operațională.

În ultima fază a cercetării, folosind **metoda analizei tematice**, am determinat acele aspecte necesare adaptării sistemelor de comandă și control, codând datele și organizându-le pe cele patru componente specifice oricărui sistem C2: personal, procese, sisteme tehnologice și puncte de comandă.

Admitem totuși o serie de **limitări ale rezultatelor studiului** nostru, reieșite fie din natura neclasificată a datelor întrebuințate, fie din abordarea metodologică întreprinsă. S-a conștientizat permanent, având în vedere gradul sporit de implicare a cercetătorului în modul de desfășurare a studiului, existența unor potențiale biasuri care ar fi putut influența rezultatele obținute și s-au întreprins constant măsuri reflexive de reducere a interferenței acestora.

Structura lucrării

Lucrarea a fost împărțită în trei părți principale pentru a răspunde celor trei întrebări de cercetare. Astfel, în faza inițială, am analizat caracteristicile, componentele și funcțiunile sistemelor de comandă și control, reliefând, în același timp, relevanța operațională a acestora. În a doua secțiune a lucrării, care reprezintă și centrul de greutate al acesteia, am analizat factorii și modalitatea în care aceștia pot influența modul de funcționare al sistemelor, precum și modalitățile de contracarare a lor, din perspectiva C2. În ultima secțiune, cea dedicată concluziilor și propunerilor, am organizat rezultatele reieșite anterior, în concordanță cu cele patru componente ale oricărui sistem de comandă și control: personal, procese, sisteme tehnologice și puncte de comandă, propunând direcții pertinente și coerente de adaptare a acestora pentru Armata României.

1. Relevanța operațională a sistemelor de comandă și control

De când există umanitatea, conflictele au reprezentat o constantă a acesteia, reflectând cea mai violentă exprimare a societăților. Elaborarea de filosofii de gestionare a acestora pentru a asigura condițiile necesare asigurării victoriei a constituit un demers perpetuu al ființelor umane.

Ne găsim astăzi într-un moment de inflexiune pentru tot ceea ce înseamnă instrumentul militar de putere. Într-un mediu de operare tot mai complex și dinamic (MCDC 2020, 1-2; TC 7-102 2014, 1-2; JCN1/17 2017, 1), abilitatea de a asigura coerența operațională a forțelor armate a devenit crucială pentru succesul misiunilor militare. În acest cadru, sunt necesare dezvoltarea și implementarea unor sisteme de comandă și control (C2) avansate, care să asigure motorul transformării sistemului militar în funcție de provocările mediului de operare. Sistemele C2 reprezintă cortexul operațional al unei forțe militare moderne, permițând o coordonare eficientă a resurselor și o luare rapidă a deciziilor în situații critice, fiind esențiale pentru planificarea și desfășurarea eficientă și eficace a operațiilor de luptă. Aceste sisteme trebuie să fie adaptabile la schimbările rapide din mediul de operare curent și să ofere o imagine completă și înțelegerea corectă a situației operaționale.

Nicio activitate specifică sistemului militar nu este mai importantă decât comanda și controlul (MCDP-6 2018, 1-3). Chiar dacă aceasta nu este în măsură, de una singură, să realizeze atacuri directe asupra adversarului, să influențeze percepțiile acestuia sau să asigure suportul logistic necesar structurilor proprii de luptă, fără comandă și control, niciuna dintre activitățile cruciale pentru succesul operațiilor militare nu ar fi posibilă.

Chiar dacă literatura de specialitate (AJP-3 2019, 1-21 - 1-25) tratează comanda și controlul în rând cu celelalte funcții ale luptei, precum informațiile, manevra, sprijinul prin foc, activitățile informaționale, protecția sau sprijinul logistic, în realitate, niciuna dintre aceste funcții nu ar avea un scop clar fără comandă și control. Aceasta înglobează toate funcțiile și operațiile militare, dându-le sens și armonizându-le într-un întreg semnificativ. Din acest motiv, sistemele de comandă și control au o importanță majoră în context militar, asigurând coordonarea și eficiența acțiunilor desfășurate de forțele armate. Prin urmare, înțelegerea profundă a acestor sisteme este crucială pentru succesul operațiunilor militare.

Comanda și controlul reprezintă autoritatea, responsabilitățile și activitățile comandanților militari în conducerea și coordonarea eficientă a forțelor militare, precum și în punerea în aplicare a ordinelor legate de pregătirea și desfășurarea operațiilor militare (ATP 3.2.2 2016, 1.1).

Comandantul reprezintă un element crucial al sistemului de comandă și control. Rolul său este de a monitoriza și dirija un spectru larg de activități, inclusiv planificarea operațională, organizarea resurselor, evaluarea amenințărilor, luarea deciziilor, precum și supervizarea și instruirea trupelor. Prin intermediul comenzii și controlului, se asigură coeziunea și sincronizarea acțiunilor militare, permițând astfel atingerea obiectivelor stabilite și realizarea eficientă a misiunilor. Un sistem de comandă și control bine dezvoltat asigură optimizarea utilizării resurselor, îmbunătățirea procesului de luare a deciziilor și sporirea capacității de răspuns în situații critice. Astfel, comanda și controlul reprezintă un element indispensabil pentru succesul oricărei operații militare.

Chiar dacă elementul central al C2 este comandantul, acesta nu poate exercita comanda și controlul forțelor și operațiilor de unul singur, având nevoie de sprijin în exercitarea acesteia. Așadar, sistemul de comandă și control presupune mai mult decât comandantul. Personalul implicat, procesele utilizate, sistemele tehnologice sau facilitățile de unde se poate exercita C2 (punctele de comandă), sunt elemente de o însemnătate similară, așa după cum reiese și din Figura 2. Nu se poate vorbi de un C2 eficient fără a lua în calcul, pe lângă comandant, și aceste patru elemente. În continuare, vom face o scurtă analiză a ceea ce presupune fiecare dintre ele pentru a asigura cadrul de analiză în secțiunile următoare privind nevoile de adaptare a sistemelor de comandă și control.

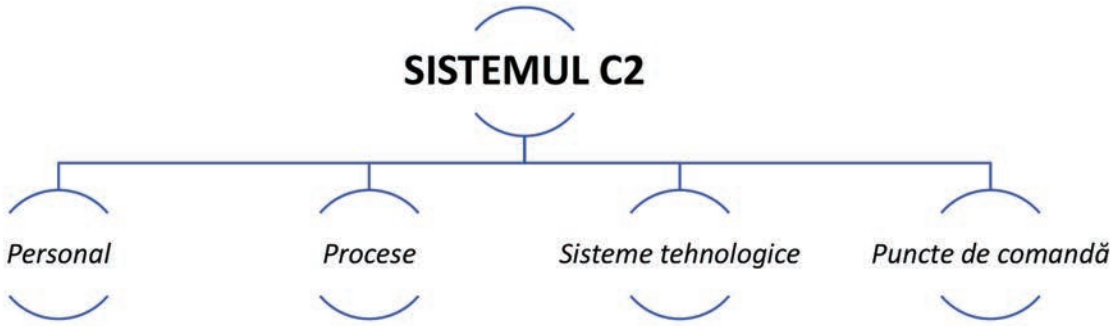


Figura 2 Elementele sistemului de comandă și control
Sursa: Wade 2023, 3-8

Din perspectiva C2, **personalul (Pe)** joacă un rol esențial în eficiența și coerența sistemului de comandă și control. Comandanții reprezintă, așa după cum am menționat anterior, elementul central în acest proces, având responsabilitatea directă de a lua decizii și de a conduce forțele. În plus, autoritatea și stilul de conducere al acestora pot contribui semnificativ la sporirea componentei morale a puterii de luptă (AJP-3.2 2022, 18) a structurilor armate. Simpla prezență a acestora în anumite momente și zone ale luptei poate influența, de multe ori, decisiv deznodământul ei. Sunt nenumărate exemple istorice în sprijinul acestei afirmații. Având în vedere rolul lor decisiv în direcționarea procesului operațiilor și în consecință modul de desfășurare a conflictului, comandanții trebuie să își gestioneze timpul între punctele de comandă (CP) și pozițiile unităților subordonate pentru a înțelege situația, pentru a observa direct operațiile și efectele acestora și pentru a motiva subordonații prin exemplu personal.

Cu toate acestea, este imposibil să aibă o percepție comprehensivă a situației operaționale doar prin aceste măsuri. Timpul reprezintă o limitare majoră a prezenței comandanților în toată aria de operații. Din acest motiv, un rol extrem de important îl are personalul de stat major. Acesta trebuie să sprijine comandanții în luarea și implementarea deciziilor, oferind analize și estimări în ariile funcționale specifice lor, care să crească eficiența deciziilor luate de comandant. Personalul statului major este responsabil de pregătirea planurilor, ordinelor și evaluărilor pentru a asigura controlul eficient al operațiilor. De asemenea, contribuie la integrarea și sincronizarea

puterii de luptă, asigurând informații relevante pentru a facilita înțelegerea situației și progresul misiunilor.
Atunci când se analizează sistemul de comandă și control, trebuie pus accent pe elemente precum stilul de conducere, leadership sau modul de instruire și educare a forțelor, pentru sporirea performanțelor personalului implicat în procesele specifice sistemelor de comandă și control.

A doua componentă a sistemelor C2 este reprezentată de **procesele (Pr)** specifice. Ele reprezintă un element esențial în organizarea activităților în cadrul statelor majore. Integrarea coerentă a acestor procese pentru a facilitat luarea oportună a deciziilor și pentru a sprijini coordonarea eficientă a resurselor și acțiunilor de luptă se realizează prin dezvoltarea unui ritm de luptă bine articulat, integrat cu cel al eșalonului superior și al structurilor subordonate. Procesele de comandă și control joacă un rol vital în asigurarea eficienței operaționale a sistemelor militare. Ele permit coordonarea și sincronizarea acțiunilor din cadrul unei operații militare, contribuind la succesul acesteia. Un aspect crucial al acestor procese este că pot asigura structurii militare cadrul de a anticipa și de a răspunde rapid schimbărilor din mediul de operare.

Un proces major este procesul operației, care include activitățile principale de comandă și control, desfășurate în timpul etapelor de planificare, pregătire, executare și evaluare continuă a operației. Acest cadru permite comandanților să înțeleagă mediul de operare, să vizualizeze și să descrie starea finală a operației, să ia decizii articulate și să direcționeze structurile subordonate pentru a îndeplini propria intenție privind modul de desfășurare a operațiilor (ADP 6-0 2019, 2-14 - 2-16).

Pe lângă procesul operației, comandanții și personalul de stat major folosesc procesele integratoare pentru a sincroniza diferite funcții specifice. Aceste procese constau într-o serie de pași și activități care integrează funcțiile de luptă prin încorporarea mai multor discipline pentru a atinge un anumit obiectiv. Procesele integratoare includ pregătirea informativă a mediului de operare, culegerea informațiilor, managementul țintelor, managementul riscurilor sau managementul cunoștințelor.

Procesele C2 sunt concepute pentru a fi simple și rapide, permițând comandanților să acționeze eficient chiar și în condiții de stres extrem. Acestea trebuie să fie suficient de eficiente pentru a crește ritmul operațiilor, iar secvențele de planificare ale personalului trebuie să fie simplificate pentru a facilita rapiditatea reacțiilor. În plus, procesele C2 trebuie să ofere flexibilitate și adaptabilitate în fața schimbărilor de situație și să permită îmbunătățiri continue pentru a face față provocărilor din ce în ce mai complexe ale mediului de operare. Astfel, prin implementarea și utilizarea optimă a proceselor C2, se poate asigura un flux de lucru eficient și o gestionare eficace a resurselor pentru a atinge obiectivele operaționale stabilite.

Totuși, având în vedere era digitală în care trăim, dar și dinamica sporită a schimbărilor operaționale, comandanții trebuie să aibă la dispoziție instrumente și

tehnologii avansate pentru a-și spori capacitatea de a lua decizii în timp real și de a le putea comunica eficient și la timp. Din acest motiv, a treia componentă a comenzii și controlului, **sistemele tehnologice (ST)**, sunt indispensabile în asigurarea unei comunicări eficiente între diferitele niveluri de comandă și control, precum și în monitorizarea și gestionarea resurselor militare în mod optim. Astfel, pentru a asigura eficacitatea și rapiditatea proceselor de comandă și control în domeniul militar, este crucial să se dezvolte și să se implementeze tehnologii moderne și sisteme informatice performante.

Componentele principale ale sistemelor tehnologice includ aplicațiile destinate utilizatorului final, serviciile de informații și datele, precum și transportul și managementul digital al informației. Aceste elemente lucrează împreună pentru a asigura o comunicare eficientă și o gestionare optimă a informațiilor, sprijinind astfel funcționarea eficientă a sistemului C2.
Timpul reprezintă un factor critic în operațiile militare moderne. Forțele armate trebuie să depună eforturi considerabile pentru a se asigura că desfășoară ciclul decizie acțiune, cunoscut și sub numele inventatorului său, ciclul Boyd (OODA – Observe, Orient, Decide, Act/Observă, Orientează-te, Decide, Acționează), mai repede și mai corect decât adversarul. În acest cadru, abilitatea de a folosi tehnologia în scopul urgentării luării deciziilor oportune poate asigura câștigarea avantajului decizional, în raport cu adversarul.

Ultima componentă a sistemului C2 este reprezentată de **punctele de comandă (PC)**. Ele joacă un rol esențial în asigurarea unei coordonări continue, sincronizării și schimbului de informații dintre diferite structuri. Importanța lor derivă din faptul că oferă o locație fizică, unde personalul, procesele și sistemele tehnologice se integrează pentru a asista comandanții în înțelegerea, vizualizarea, descrierea, direcționarea, conducerea și evaluarea operațiilor militare.

Funcțiile comune tuturor punctelor de comandă includ gestionarea cunoștințelor și a informațiilor, construirea și menținerea unei înțelegeri situaționale corecte, menținerea estimărilor curente pentru susținerea procesului decizional al comandantului, controlul operațiilor în desfășurare, evaluarea acestora și planificarea următoarelor etape ale luptei, precum și coordonarea cu organizațiile interne și externe, în interesul îndeplinirii misiunii încredințate.

Toate aceste patru elemente sunt esențiale pentru eficiența sistemului de comandă și control. Abilitatea de a crea un sistem C2 mai performant decât al adversarului este un demers vital în realizarea precondițiilor pentru succesul operațional (ATP 3.2.2 2016, 1.1). În acest demers, este obligatorie identificarea de soluții pentru eficientizarea **funcțiilor specifice oricărui sistem C2**:

- *dezvoltarea unei înțelegeri situaționale corecte și oportune* care să ofere informații corecte și la timp referitoare la inamic, teren și propriile vulnerabilități;
- *dezvoltarea unor obiective clare și flexibile* care să ajusteze țintele, în funcție de schimbările situaționale;

• *stabilirea de acțiuni adecvate situației* care să direcționeze și să coordoneze eforturile forțelor pentru o acțiune armonizată și viguroasă;
• *monitorizarea continuă* care să permită adaptarea rapidă la schimbările apărute în câmpul de luptă;
• *asigurarea securității operaționale* care să împiedice inamicul să obțină informații privind intențiile reale ale forțelor proprii;
• *generarea unui ritm rapid al acțiunilor* care să exploateze oportunitățile apărute și care să asigure un tempo ridicat al acțiunilor militare și menținerea inițiativei operaționale.

2. Provocări operaționale contemporane la adresa sistemelor de comandă și control și potențiale soluții de adaptare

Rolul acestui capitol este de a identifica factorii care pot influența comanda și controlul în actualul mediu de operare, demers extrem de important pentru stabilirea potențialelor măsuri care trebuie implementate în vederea adaptării sistemelor de comandă și control. În plus, această secțiune își propune ca, în raport cu factorii identificați, să formuleze deducții și concluzii pertinente pentru sistemele de comandă și control, aplicând un instrument critic des utilizat în procesul de planificare a operațiilor militare, analiza pe trei coloane.

Doresc să menționez de la început că factorii analizați în acest capitol au rezultat doar din surse deschise, astfel că una dintre principalele limitări ale rezultatelor studiului întreprins rezultă din natura datelor colectate și analizate. Eșantionarea datelor utilizate a fost una de tip nonprobabilistic, fiind realizată în raport cu trei elemente pe care le considerăm relevante pentru procesul de adaptare a sistemelor de comandă și control:

- trăsăturile perene ale conflictelor specifice naturii acestora;
- trăsăturile specifice caracterului conflictelor, desprinse din lecțiile identificate până în acest moment din războiul ruso-ucrainean;
- tendințele de evoluție a mediului de operare, reieșite din analizele efectuate de actori relevanți pe scena globală din zilele noastre.

2.1. Analiza naturii conflictelor din perspectiva influenței asupra sistemelor C2

Războiul este un fenomen social, fiind cea mai violentă exprimare a societății la un anumit moment. Conform majorității teoreticienilor militari, acesta presupune atât caracteristici care au rămas constante în fața trecerii anilor, cât și caracteristici care s-au transformat odată cu istoria. Natura războiului este componenta atemporală, ea nefiind definită de momentul în care acesta are loc sau de caracteristicile societății din acea perioadă. Astfel, putem afirma că aceasta a rămas constantă de-a lungul timpului. Anumite aspecte fundamentale ale războiului, cum ar fi rolul factorului uman, caracterul violent al confruntărilor, impactul distructiv al lor asupra societăților, incertitudinea constantă sau fricțiunea au rămas constante de-a lungul timpului și se apreciază că au reprezentat trăsături esențiale ale acestora, indiferent

de modul în care s-au transformat. Deși toate aceste caracteristici influențează într-o oarecare măsură sistemele C2, cea mai mare influență o are, fără doar și poate, **nivelul de incertitudine**, specific confruntărilor militare. Modul de influențare a acestuia asupra sistemelor C2, precum și potențialele soluții de limitare a impactului negativ se pot regăsi în analiza din tabelul de mai jos.

TABEL NR. 1

Analiza nivelul de incertitudine specific naturii conflictelor armate, din perspectiva sistemelor de comandă și control

Factor 1 – *Nivelul de incertitudine specific naturii conflictelor armate*	
Deducții	**Concluzii**
1.1. Influențarea procesului de luare a deciziilor (Riscuri sporite)	**1.1.1. Luarea deciziilor în condiții de incertitudine (Pr, Pe)** - antrenarea personalului în acceptarea calculată a riscurilor și gestionarea operațională a acestora; - integrarea eficientă a procesului de management al riscurilor în luarea deciziilor. **1.1.2. Dezvoltarea gândirii critice a personalului (Pr)** - utilizarea instrumentelor analitice de analiză a informațiilor (de exemplu: Red teaming, Alternative Analysis etc.); - educarea personalului în folosirea gândirii critice și creative.
1.2. Dificultăți privind anticiparea modului de evoluție a situației operaționale	**1.1.2. Oportunități privind inducerea în eroare a adversarului (Pr)** - folosirea incertitudinii ca bază pentru construirea unei operații de inducere în eroare a adversarului. **1.2.1. Nevoia de investiție în tehnologia emergentă pentru sporirea posibilităților de colectare și analiză a datelor (ST, Pr)** - integrarea tehnologiei emergente (de exemplu: Inteligența artificială) în sprijinul proceselor specifice realizării înțelegerii operaționale.

2.2. Analiza caracterului conflictelor din perspectiva influenței asupra sistemelor C2

Deși unele aspecte ale conflictelor rămân neschimbate de-a lungul timpului, așa după cum am prezentat anterior, caracterul războiului este cel supus evoluției continue. De-a lungul timpului, acesta s-a schimbat aproape radical, în funcție de circumstanțele momentului în care a avut loc conflictul. Principalii factori generatori de schimbare sunt reprezentați de societate, diplomație, politică și tehnologie (JP-1 2017, I-4). Așadar, această metamorfoză a conflictelor armate este dependentă, în principal, de inovațiile tehnologice și științifice, de schimbările demografice, politice și chiar educaționale ale unei societăți la un moment dat, în mare măsură de caracteristicile proprii mediului de securitate, specific vremurilor respective (UK Ministry of Defence 2020, 1).

Astăzi, într-o lume extrem de complexă și într-o alertă schimbare, sistemele de comandă și control trebuie să țină pasul și să se adapteze la aceste transformări pentru a-și putea menține viabile funcțiile esențiale desfășurării eficiente a operațiilor de luptă. Un prim element definitoriu al societății contemporane este reprezentat de **tehnologizarea** accentuată a acesteia și de sporirea dependenței factorului uman de astfel de tehnologii, iar domeniul militar nu face excepție. Acest aspect aduce cu sine o serie de oportunități, dar și provocări pentru viitoarele sisteme C2.

Capacitatea de a lua decizii mai rapid și mai exact decât adversarul, împreună cu avansul în precizia armelor de lovire la distanță și reducerea timpului necesar angajării

țintelor, reprezintă avantaje cruciale pe câmpul de luptă modern. Tehnologia actuală influențează profund toate ramurile sectorului militar *„și determină adaptarea artei militare și a doctrinelor, manualelor și procedurilor de operare existente."* (Stanciu și Gimiga 2023, 159) Fie că se referă la procesul de detectare și angajare a țintelor, la culegerea și analiza informațiilor sau la comunicare și menținerea imaginii operaționale, tehnologia a schimbat fundamental modul de operare al forțelor armate și, implicit, sistemele de comandă și control.

Dezvoltarea tehnologică a adus cu sine și expansiunea domeniilor de operare specifice forțelor armate, NATO recunoscând relativ recent spațiul și mediul cibernetic în rândul acestora. În consecință, confruntările armate au devenit mult mai complexe, multidimensionalitatea fiind una dintre caracteristicile pregnante ale lor. Vorbim, în ziua de azi, despre necesitatea **abordării multidomeniu a operațiilor militare** în demersul de îndeplinire a misiunilor încredințate (Crilly și Mears 2022; Ellison și Sweijs 2023, 1; NATO 2022; NATO Parliamentary Assembly 2022, 3). O astfel de abordare aduce cu sine provocări suplimentare pentru sistemele C2, impunând adaptări pentru a răspunde complexității și integrării informaționale din multiple domenii (terestru, aerian, maritim, cibernetic, spațial).

Mai mult, evoluția rapidă a **tehnologiei antisatelit** și capacitatea crescută de a desfășura **operații ostile, extinse în spațiul cibernetic** au contribuit semnificativ la adăugarea unor noi dimensiuni într-o imagine deja complexă a modului în care ar putea să se desfășoare un eventual conflict viitor între marile puteri (Nilsson 2023, 49). Toate acestea au un impact direct asupra sistemelor de comandă și control, considerând faptul că forțele armate actuale depind în mare măsură de sateliți pentru navigație, de comunicații, de supraveghere și monitorizare, iar pierderea acestora ar putea compromite grav abilitatea de a coordona, de a sincroniza și de a conduce operațiile în multiple domenii de operare. Mai mult, operațiile ostile în spațiul cibernetic au devenit tot mai sofisticate și prevalente în ultimii ani. Acestea pot include atacuri asupra infrastructurii critice, precum sistemul energetic, rețeaua de transport, rețeaua bancară sau sistemele de apărare, având potențialul de a provoca un impact semnificativ asupra eficienței și securității sistemelor C2.

În plus, ca și consecință directă a dezvoltării tehnologice accentuate, asistăm în domeniul militar la o **sporire a capabilităților tehnice ale senzorilor de culegere de informații**. Acest aspect a condus spre o transparență ridicată a câmpului de luptă. Un element definitoriu în sprijinul acestei afirmații, așa după cum este demonstrat de războiul ruso-ucrainean (Gosselin-Malo 2024), este reprezentat de **folosirea dronelor**. *„Utilizarea sistemelor aeriene fără pilot a creat un câmp de luptă transparent, în care nu mai există niciun refugiu."* (Collins 2023, 8)

Dronele au revoluționat modul de operare al forțelor armate. Versatilitatea lor face din drone o armă extrem de importantă, având potențialul de a sprijini îndeplinirea mai multor funcții ale luptei. Inițial, folosite doar în scopuri de recunoaștere, dronele au devenit arme de atac fatale pentru tehnica blindată, substanțial mai scumpă.

Relevanța lor operațională este demonstrată și de denumirea existentă în literatura de specialitate, aceea de gloanțe magice (Hambling 2020). Impactul acestora este unul extrem de mare și asupra sistemelor de comandă și control. Asigurarea protecției și securității punctelor de comandă reprezintă una dintre cele mai mari provocări în fața acțiunii sistemelor aeriene fără pilot ale adversarului. Totuși, dronele au un rol extrem de important și în sprijinul dezvoltării unei înțelegeri situaționale aprofundate, „*informațiile furnizate de drone și distribuite prin noile rețele digitale de comandă pe câmpul de luptă crescând considerabil viteza de decizie și acțiune.*" (Molloy 2024, 90)

Armatele vestice s-au bucurat de o poziție superioară în toate conflictele de la începutul acestui mileniu, aspect care nu mai este valabil în ziua de astăzi. Lumea se află într-o stare de competiție acerbă, **multipolaritatea** fiind caracteristica fundamentală a societății actuale (IISS 2023, 27). Situația curentă demonstrează că abilitatea de a opera liber, cu acces la majoritatea facilităților tehnologice și operaționale nu mai este valabilă. **Mediul de operare este unul extrem de contestat**, cu potențiali adversari deținând capabilități similare calitativ. Acest aspect pune o presiune suplimentară pe regândirea sistemelor de comandă și control, de la procesele specifice, la tehnologia utilizată sau la modul de organizare a punctelor de comandă. Formatul clasic al acestora din urmă, specific conflictelor începutului de mileniu, extrem de statice, cu o dimensiune impresionantă și cu tehnologie la discreție, face din aceste puncte de comandă o țintă relativ ușoară în fața unui adversar extrem de puternic, ca cei din ziua de azi (Nagl 2024, p. 24). Reducerea și mascarea dimensiunilor, a amprentei termice și electromagnetice sau sporirea mobilității trebuie să reprezinte **demersuri obligatorii pentru a asigura supraviețuirea sistemelor de comandă și control** în mediul de operare actual (Beagle, Slider și Arrol 2023, 10). Mai mult, **creșterea preciziei și letalității armelor, precum și transparența spațiului de confruntare și reducerea timpului de identificare-angajare a țintelor** reprezintă provocări suplimentare pentru aceste sisteme și impun identificarea de soluții viabile pentru sporirea protecției punctelor de comandă în asigurarea funcționalității continue a structurilor militare și a operațiilor desfășurate de acestea.

Creșterea ritmului și complexității operațiilor militare reprezintă, de asemenea, una dintre principalele provocări ale zilelor noastre. Îmbunătățirile în mobilitate, rază de acțiune și letalitate comprimă limitele de timp și spațiu, ceea ce solicită un volum mai mare de informații actualizate și un ritm operațional sporit, punând o presiune suplimentară asupra îndeplinirii eficiente a funcțiilor specifice sistemelor de comandă și control. Mai mult, creșterea letalității armelor impune o dispersie tot mai mare a forțelor pentru a asigura supraviețuirea acestora, ceea ce extinde limitele sistemelor de comandă și control și impune un volum semnificativ de tehnologie și informații pentru coordonarea eficientă a forțelor și operațiilor militare.

Asociați cu transparența sporită a mediului de confruntare, acești factori determină limitări majore privind mascarea forțelor și operațiilor de luptă, ceea ce impune identificarea de soluții alternative privind realizarea surprinderii adversarului, dar și asigurarea protecției forțelor proprii.
În plus, un amestec de sisteme cu echipaj, fără echipaj și autonome va aduce o schimbare suplimentară în letalitate și în modul de utilizare, în timp ce sistemele hipersonice, balistice, rachetele cu rază lungă de acțiune și capacitățile de contracarare a operațiilor în spațiu vor continua să extindă domeniul competitivității. Toate aceste trăsături specifice caracterului actual al conflictelor armate impun nevoia de regândire a sistemelor proprii de comandă și control pentru a răspunde cât mai eficient provocărilor curente.

De asemenea, complexitatea și dinamismul ridicat al transformărilor din mediul actual de operare generează probleme complicate și ascunse, a căror rezolvare devine tot mai greu de identificat. În acest cadru, latura umană a sistemelor C2 trebuie să insiste asupra adoptării și dezvoltării unei **mentalități de tip "red teaming"** care să asigure dezvoltarea gândirii critice și creative personalului propriu (UK Ministry of Defence 2021, 1; **JDP 0-01.1 2023**, 50).

Comandantul continuă să reprezinte un element crucial al sistemului de comandă și control, așa după cum este demonstrat de conflictul în desfășurare ruso-ucrainean. Abilitatea de a inspira și de a motiva personalul din subordine s-a dovedit a fi o calitate deosebită care a sporit capacitatea de reziliență a poporului ucrainean, contribuind la sporirea componentei morale a capacității de luptă. Leadershipul a fost și va rămâne un element definitoriu al conflictelor, care are potențialul de a motiva și de a uni persoane și de a menține capacitatea operațională ridicată a forțelor armate (MCDC 2020, 4). În plus, același conflict a demonstrat că folosirea conceptului de comandă a misiunii a fost fundamental în câștigarea superiorității decizionale a ucrainenilor în fața rușilor. Încrederea în comandanții subordonați și asigurarea libertății privind modalitatea de acțiune a acestora pentru îndeplinirea intenției eșalonului superior reprezintă esența comenzii misiunii.

În plus, având în vedere poziția României de membru în Alianța Nord-Atlantică, eventualele operații militare la care militarii români vor lua parte vor fi, cu siguranță, multinaționale. Din acest motiv, proiectarea viitoarelor sisteme C2 trebuie să țină cont de un aspect crucial al **operațiilor multinaționale**, cel al interoperabilității, în toate cele trei dimensiuni ale sale: tehnică, procedurală și umană (AJP-01, 2022, 71).

Rezultatul analizei impactului caracterului conflictelor actuale asupra sistemelor de comandă și control și a potențialelor soluții de adaptare a acestora se regăsește în tabelul nr. 2.

TABEL NR. 2

Analiza impactului caracterului conflictelor actuale asupra sistemelor de comandă și control

Factor 2 – *Trăsături specifice caracterului conflictelor actuale*	
Deducții	**Concluzii**
2.1. Transparență ridicată a spațiului de confruntare, ca urmare a dezvoltării sistemelor de culegere a informațiilor	**2.1.1. Măsuri sporite de protecție a sistemelor C2 (ST, PC, Pe)** - dezvoltarea și implementarea de tehnologie de protecție a rețelelor în spațiul cibernetic; - protecția fizică a punctelor de comandă – dispersie, măsuri OPSEC, sisteme contra-dronă (EW, sisteme Ra.Art.AA, alte tipuri de arme – de exemplu, laser) etc; - antrenarea personalului privind folosirea măsurilor OPSEC. **2.1.2. Avantaje privind înțelegerea situațională (Pr, Pe)** - ajustarea procesului JISR pentru colectarea datelor relevante; - înțelegerea limitărilor sistemelor de culegere a datelor pentru a nu cădea în capcana de a fi indus în eroare (a vedea nu este sinonim cu a înțelege).
2.2. Volum mare de date, ca urmare a dezvoltării sistemelor de culegere a informațiilor	**2.2.1. Nevoia de investiție în tehnologia emergentă pentru sporirea capacităților de culegere și pentru analiza rapidă a unui mare volum de date (ST, Pr, Pe)** - integrarea inteligenței artificiale în sprijinul proceselor specifice sistemelor de comandă și control; - tehnologizarea sistemelor de colectare pentru a reduce limitările acestora (condiții atmosferice, spectrul electromagnetic, timp – zi/noapte) în demersul de asigurare a înțelegerii situaționale; - trebuie înțeles foarte bine rolul factorului uman și cât de mult trebuie și se poate automatiza decizia. **2.2.2. Situații sporite de erori prin imposibilitatea de analiză a datelor relevante (Pr, Pe)** – luarea deciziilor trebuie să conțină obligatoriu un proces de management al riscurilor; - antrenarea comandanților și personalului comandamentelor în acceptarea riscurilor și gestionarea acestora. **2.2.3. Posibilități sporite de a fi indus în eroare (Pr)** - imposibilitatea de a gestiona volumul mare de date poate contribui la înțelegerea eronată a situației și la crearea oportunităților pentru adversar de a ne induce în eroare; - este nevoie de dezvoltarea unui proces de contracarare a inducerii în eroare, pregătirea constituind un prim element esențial al acestui proces.
2.3. Digitalizarea câmpului de luptă	**2.3.1. Oportunități de accelerare a ciclului propriu decizie-acțiune (Pr, Pe)** - implementarea sistemelor de inteligență artificială și algoritmi de analiză pentru a gestiona volumul mare de date; - dezvoltarea unor mecanisme de prioritizare a informațiilor esențiale pentru luarea deciziilor în timp scurt; - instruirea personalului pentru a optimiza interpretarea și folosirea informațiilor digitale. **2.3.2. Necesitatea unor măsuri avansate de securitate cibernetică și de protecție împotriva interferențelor (Pr, Pe, ST)** - implementarea unui sistem de monitorizare continuă și de apărare împotriva atacurilor cibernetice; - integrarea unor măsuri de redundanță și continuitate operațională, în caz de atacuri cibernetice; - creșterea rezilienței prin instruirea personalului asupra riscurilor cibernetice și măsurilor de securitate.
2.4. Mediul de operare este unul extrem de contestat	**2.4.1. Crearea unor structuri de comandă mai agile, capabile să opereze în medii contestate (PC, Pe, ST)** - optimizarea rețelelor de comunicații pentru mobilitate și securitate sporită; - adoptarea unor practici de dispersie a punctelor de comandă și folosirea de sisteme redundante; - pregătirea personalului pentru a acționa și în mod analogic; - introducerea de măsuri suplimentare de securitate pentru protejarea locațiilor C2 împotriva atacurilor directe și indirecte (de exemplu, drone). **2.4.2. Implementarea unor măsuri de protecție pasivă și activă pentru reducerea amprentei și mascarea punctelor de comandă (ST, PC, Pe)** - dezvoltarea și utilizarea de echipamente și tehnologii pentru reducerea amprentei termice și electromagnetice, inclusiv sisteme de izolare și camuflaj electromagnetic multispectral; - optimizarea arhitecturii C2 pentru a permite o configurație modulară și flexibilă, reducând vizibilitatea și timpul necesar instalării/dislocării în teren; - creșterea capabilităților de detecție preventivă, identificând din timp orice amenințare de supraveghere a adversarului.

Deducții	Concluzii
2.4. Mediul de operare este unul extrem de contestat	**2.4.3. Creșterea mobilității pentru evitarea detectării și atacurilor (Pe, Pr, PC)** - introducerea unor puncte de comandă mobile și a unor echipamente C2 de dimensiuni reduse, care pot fi rapid transportate și instalate în noi locații; - adoptarea unor proceduri de relocare rapidă, menite să crească dificultatea detectării și urmăririi de către adversar; - instruirea personalului pentru operarea în scenarii de mobilitate ridicată, pregătind proceduri și procese rapide de deconectare și reconectare la rețelele de comunicații și date.
2.5. Multidimensionalitatea confruntării	**2.5.1. Dezvoltarea unor structuri C2 integrate și interoperabile (ST, PC, Pr, Pe)** - implementarea de arhitecturi C2 multidomeniu, capabile să gestioneze simultan operații în spațiile terestru, aerian, maritim, cibernetic și spațial; - crearea unor canale de comunicare sigure și rapide între domenii pentru a permite schimbul de informații relevante în timp real; - instruirea personalului C2 pentru a înțelege specificitățile fiecărui domeniu de operare. **2.5.2. Creșterea capacităților de procesare și analiză a datelor provenite din diferite domenii (ST, Pr, Pe)** - utilizarea inteligenței artificiale și a algoritmilor avansați pentru integrarea datelor din mai multe domenii, oferind o imagine operațională coerentă; - crearea unui sistem de prioritizare automată a informațiilor, astfel încât datele critice din orice domeniu să fie semnalate rapid factorilor decizionali; - optimizarea proceselor de coordonare interdomenii pentru a asigura că acțiunile în orice spațiu operațional sunt sincronizate și susțin obiectivele generale ale misiunii. **2.5.3. Flexibilitatea și adaptabilitatea structurilor C2 pentru răspunsul eficient și coerent în mai multe domenii (ST, PC, Pr)** - dezvoltarea unor proceduri și echipamente C2 configurabile pentru a permite adaptarea rapidă la cerințele specifice ale fiecărui domeniu; - introducerea unor module de comandă și control scalabile, care să permită răspunsuri eficiente la niveluri diferite de intensitate și într-o varietate de medii de operare; - formarea continuă a personalului în adaptarea și coordonarea răspunsului pentru operații interdependente în mai multe domenii, crescând astfel reziliența operațională.
2.6. Operații multinaționale	**2.6.1. Necesitatea realizării interoperabilității dintre sisteme C2 (ST, PC, Pr, Pe)** - adoptarea unor standarde comune de comunicații și securitate pentru a permite conectivitatea dintre diverse sisteme C2, facilitând schimbul de informații și coordonarea operațională; - dezvoltarea de protocoale standardizate și de formate comune pentru raportare și transmitere a ordinelor, care să fie ușor de utilizat de toate forțele implicate; - implementarea unor programe de interoperabilitate, prin care forțele partenere să fie familiarizate cu echipamentele și procedurile aliate, crescând astfel coeziunea operațională. **2.6.2. Investiții în pregătirea personalului și antrenamente comune pentru operații multinaționale (PC, Pr, Pe)** - organizarea de exerciții multinaționale periodice pentru a instrui personalul C2 din forțele aliate în lucrul în comun; - crearea unor manuale și proceduri comune de instruire care să includă practici și protocoale pentru coordonarea rapidă, în contexte de operare cu multiple națiuni implicate; - încurajarea schimbului de personal și experiență între națiunile partenere, crescând astfel înțelegerea reciprocă și capacitatea de reacție integrată.
	2.6.3. Dezvoltarea unei infrastructuri de comunicații adaptate operațiilor multinaționale (ST, PC) - implementarea unor rețele de comunicații interoperabile, securizate și eficiente care să susțină schimbul rapid de informații dintre forțele aliate, fără vulnerabilități de securitate; - investiții în tehnologii și echipamente de comunicații portabile, compatibile cu rețelele forțelor partenere, astfel încât informațiile să fie disponibile tuturor părților implicate.

2.3. Analiza tendințelor de evoluție a mediului de operare și influența acestora asupra sistemelor C2

Tendințele de evoluție a mediului de operare reprezintă un factor determinant în analiza modului de adaptare a sistemelor de comandă și control. Într-un context marcat de schimbări rapide și de dezvoltări tehnologice avansate, structurile militare trebuie să-și ajusteze continuu sistemele C2 pentru a face față provocărilor

emergente. Această adaptare presupune nu doar integrarea noilor tehnologii, dar și reevaluarea proceselor decizionale pentru a răspunde eficient la complexitatea și dinamica actualelor și viitoarelor conflicte.

Pentru a identifica influența tendințelor de evoluție a mediului de operare asupra sistemelor C2, este necesar, în primul rând, să înțelegem care sunt aceste tendințe. Astfel, am realizat o analiză comparativă a viziunilor de evoluție a trei actori importanți pe scena relațiilor internaționale, care au publicat recent documente în acest sens: SUA (TRADOC G2 2024), Regatul Unit al Marii Britanii (UK Ministry of Defence 2024) și NATO (NATO 2023).

Toate aceste analize au un element comun, tehnologia. Rolul acesteia este esențial și pentru domeniul militar, ea deținând capacitatea de a modela mediul de operare al viitorului. **Noile tehnologii**, care combină puterea de procesare, conectivitatea, automatizarea, calculul cuantic, învățarea automată și inteligența artificială, vor permite nu doar o nouă generație de sisteme de arme, ci și noi modalități de desfășurare a războiului.

Toate acestea au un impact direct și asupra sistemelor C2 specifice forțelor armate. Tehnologiile novatoare pot sprijini urgentarea procesului de luare a deciziei prin prelucrarea și analiza unui volum mare de date, asigurând premisele generării unei imagini operaționale aproape complete la toate nivelurile de conflict. Printre principalele beneficii ale integrării tehnologiilor emergente în cadrul sistemelor C2, sunt recunoscute a fi (NIAG 2022, 1-29 - 1-30):

- înțelegerea mai rapidă și mai profundă a situației operaționale;
- direcționarea mai rapidă a forțelor, comparativ cu adversarul;
- sincronizarea sporită a efectelor operaționale pe câmpul de luptă;
- îmbunătățirea proceselor, capabilităților și efectelor, realizate prin celelalte funcții ale luptei, precum sprijinul logistic, protecția, sprijinul prin foc sau activitățile informaționale.

În sprijinul comenzii și controlului, în termeni practici, tehnologia are capacitatea de a îmbunătăți:

- culegerea, analiza, fuzionarea, partajarea și, cel mai important, exploatarea datelor din toate sursele pertinente pentru toate domeniile relevante, cu scopul de a oferi cea mai bună înțelegere a situației posibile, asigurând astfel avantajul informațional pe câmpul de luptă;
- utilizarea eficace a acestor informații pentru a lua decizii mai bine informate și mai bine calculate, asigurând astfel avantajul decizional, în raport cu adversarul;
- sincronizarea informațiilor și a efectelor operațiilor în toate mediile și domeniile de operare;
- optimizarea ritmului de luptă pentru un tempo decizional superior adversarului.

Având în vedere dinamica tot mai mare și complexitatea tot mai sporită a confruntărilor militare, este de așteptat ca tehnologia să reprezinte un factor primordial în construirea noilor sisteme C2. Analiza și impactul principalelor tehnologii emergente, cu relevanță în acest sens, sunt prezentate în tabelul de mai jos (NIAG 2022, 3-106 - 1-115; NATO Science & Technology Organization 2020, 41 - 111).

TABEL NR. 3

Analiza impactului principalelor tehnologii emergente în construirea noilor sisteme C2

Tehnologie	Detalii	Cum poate sprijini C2
Inteligența artificială	• Inteligența artificială (IA) reprezintă capacitatea mașinilor de a executa sarcini care, în mod obișnuit, necesită inteligență umană. Aceste sarcini includ recunoașterea de tipare, învățarea din experiență, formularea de concluzii, realizarea de predicții și luarea de decizii sau demararea unor acțiuni. • IA emulează aspecte ale cogniției umane, precum percepția, raționamentul, planificarea și învățarea. Această tehnologie poate executa autonom sarcini, precum planificarea, înțelegerea limbajului, recunoașterea obiectelor și sunetelor, învățarea sau rezolvarea problemelor. • Aceasta este considerată de mulți specialiști a avea cel mai mare impact revoluționar asupra societății, în general, și sistemelor militare, în particular. • Președintele rus, Vladimir Putin, aprecia, în 2017, că „inteligența artificială reprezintă viitorul.(...) Cine devine lider în această sferă va ajunge să conducă lumea." (Russia Today 2017) • Unul dintre avantaje constă în faptul că nu este influențată de factori, precum stresul sau oboseala. (Dragomir și Alexandrescu 2017, 58)	- analiza datelor; - îmbunătățirea capabilităților de colectare a datelor; - dezvoltarea sistemelor de lovire și a efectului acestora; - executarea anumitor sarcini în punctele de comandă; - sporirea posibilității de dezinformare (de exemplu, deep fake); - sprijinirea procesului de planificare a operațiilor prin asigurarea unor metode rapide și mai eficiente de comparare și analiză (jocuri de război) a cursurilor de acțiune.
Tehnologia "Blockchain" sau tehnologia blocurilor	• *Blockchain* este o tehnologie de registru distribuit care combină elemente din criptografie, mecanisme de consens și sisteme distribuite. Aceasta permite stocarea descentralizată și securizată a datelor printr-o structură de blocuri de informații înlănțuite, partajate, replicate și sincronizate între membrii rețelei. • Blockchain asigură o securitate ridicată a datelor prin imposibilitatea de a modifica un bloc existent, fără a altera toate blocurile ulterioare. Astfel, tehnologia previne alterarea retroactivă a datelor și asigură integritatea informației. • În context militar, blockchain oferă potențialul pentru un schimb de date coerent între diferite structuri ierarhice, cum ar fi rețelele de senzori sau posturile de comandă. Aceasta facilitează un flux sigur și sincronizat de informații în medii distribuite și complexe.	- sporirea schimbului de date; - asigurarea înțelegerii situaționale; - asigurarea securității datelor și comunicațiilor.
Augmentarea umană (Human Augmantation)	• Augmentarea umană se referă la tehnologiile utilizate pentru a îmbunătăți performanța umană. În context militar, aceasta include domeniile umane fiziologice, sociale, cognitive, precum și interfețe avansate om-mașină. • Principalele categorii de îmbunătățire a performanței umane includ: o *Simțuri îmbunătățite/extinse* (de exemplu, vedere augmentată, auz, gust, miros), care adaugă noi dimensiuni informaționale pentru sistemele C2; o *Cogniție sporită*, obținută prin identificarea stării cognitive umane și adaptarea feedbackului computerizat la nevoile utilizatorului, accelerând procesul decizional; o *Acțiune augmentată*, realizată prin monitorizarea acțiunilor umane și maparea lor în medii locale, la distanță sau virtuale.	- sporirea capacității de înțelegere situațională; - sporirea eficienței de analiză și procesare umană a datelor; - îmbunătățirea ritmului de lucru al personalului; - revoluționarea schimbului de informații dintre persoane; - îmbunătățirea procesului de luare a deciziilor prin limitarea influențelor biasurilor cognitive.

Tehnologie	Detalii	Cum poate sprijini C2
Internet of Battle Things (IoBT)	• Ideea de bază a IoBT este de a conecta toate elementele disponibile pe câmpul de luptă (vehicule, drone, soldați, dispozitive portabile, arme, senzori etc.) într-o rețea autoconfigurabilă pentru a facilita schimbul de informații. Astfel, se pot partaja, de exemplu, starea de sănătate a soldaților printr-un sistem de monitorizare, imaginile captate de camera unei arme cu structurile de informații din punctul de comandă ori se pot transmite video de la un UAV, avion sau satelit la o patrulă de cercetare din zonă.	- schimb facil de informații; - sprijinirea monitorizării situației; - asigurarea înțelegerii situaționale; - sprijinul evaluării pagubelor BDA (Battle Damage Assessment).
Tehnologia 5G/6G/7G	• Tehnologia de telefonie mobilă este utilizată nu doar pentru a conecta persoane cu dispozitive portabile (de exemplu, smartphone-uri), ci și pentru a conecta aproape toate tipurile de dispozitive (computere, senzori etc.). Tehnologia 5G va fi disponibilă pentru următorii 10 ani, în timp ce 6G, aflată momentan în faza de definire, ar putea fi complet disponibilă până în 2035, conform estimărilor, oferind acoperire mai mare, viteze de transmisie ridicate, precizie de localizare la nivel de centimetru și calcul la marginea rețelei. În jurul anului 2040, 7G ar putea fi în fazele de planificare. Ambele tehnologii permit utilizarea "network slicing", care facilitează implementarea de rețele „private" cu echipamente comerciale standard, folosind rețele comerciale.	- securizarea datelor transmise; - sporirea înțelegerii situaționale.
Tehnologia cuantică	• Tehnologiile cuantice vor juca un rol important în îmbunătățirea capacităților de înțelegere situațională, comunicații și securitate cibernetică. Categoriile în care pot fi împărțite tehnologiile cuantice în contextul C2 sunt: senzoriale, de comunicații și calcul. Principalele realizări până în 2040 pentru fiecare categorie ar putea fi: o *senzoriale*: senzori cuantici pentru aplicații C2, dispozitive portabile de navigare cuantică; o *comunicații:* legături cuantice securizate punct-la-punct, internet securizat pentru apărare, care combină comunicațiile cuantice și clasice; o *calcul:* calculatoarele cuantice vor depăși puterea de calcul a computerelor clasice.	- sporirea înțelegerii situaționale; - asigurarea securității cibernetice.
Hiperautomatizare (robotizare)	• Pentru a excela în automatizare, combinarea mai multor tehnologii poate contribui la crearea unor spații inteligente – medii fizice în diverse domenii, în care oamenii și tehnologia permit sistemelor să interacționeze, să se conecteze și să se coordoneze, încercând să reducă la minimum intervenția umană și să optimizeze eforturile. • Este de așteptat ca, până în 2040, hiperautomatizarea să atingă un nivel amplu de expansiune, procesele digitale să devină o parte esențială a oricărei operații militare, incluzând automatizarea proceselor robotice pentru a reduce intervenția umană (mai ales în sarcinile repetitive) și luarea deciziilor bazate pe IA în toate etapele OODA. Intervenția umană se va concentra doar pe activități de mare valoare în planificarea și atribuirea sarcinilor, precum și în decizii importante (Human-in-the-Loop).	- reorganizarea structurilor de forțe; - reconfigurarea modalității de transmitere a ordinelor; - sporirea eficienței proceselor operaționale; - sporirea letalității; - interoperabilitatea om-robot; - luarea deciziei într-un timp cât mai redus.

Chiar dacă asistăm la o tehnologizare fără precedent a societății, apreciem că **decizia va continua să reprezinte un atribut al factorului uman**, cel puțin în viitorul apropiat. Asociind această afirmație cu incertitudinea sporită a mediului de operare, dar și cu faptul că modul de funcționare a creierelor este predispus la greșeli și prejudecăți sistemice (AJP3.10.2 2020, 42), viitoarele sisteme C2 trebuie să se adapteze, având în continuare comandantul ca element central al procesului operației. Aceasta impune necesitatea de pregătire și educare adecvată a acestuia pentru a fi în măsură să îndeplinească eficient funcțiile specifice de direcționare a întregii operații militare. Comandanții vor trebui să aibă dezvoltate abilități de înțelegere corectă a mediului de operare, de vizualizare a modului de rezolvare

a problemei operaționale, de descriere eficientă a acestei căi subordonaților, de direcționare a execuției, în raport cu evoluția volatilă a situației din câmpul tactic, de conducere prin leadership a forțelor și de evaluare continuă a progresului pentru a asigura adaptarea oportună a operației la provocările din mediul de operare. În plus, pregătirea comandanților trebuie să includă și o componentă de reflecție internă asupra propriilor limitări cognitive care pot influența calitatea procesului decizional. Rațiunea includerii unei asemenea componente de educare este demonstrată de presupunerile de planificare eronate, făcute de ruși la începutul conflictului, și de consecințele incomensurabile ale unor astfel de decizii, bazate pe prejudecăți greșite. Ceea ce trebuia să fie o operație specială de 3 zile (Watling și Reynolds 2022, 1) s-a transformat, pentru ruși, într-un conflict care durează de aproape 3 ani, în care s-au investit considerabile resurse și efort.

Rezultate, concluzii și propuneri

În era informației, deși unele aspecte ale comenzii și controlului (C2) rămân neschimbate, precum natura războiului, incertitudinea și presiunea timpului, evoluțiile tehnologice au adus schimbări fundamentale. Lumea contemporană este marcată de instabilitate și de un ritm rapid al schimbărilor, iar aceste caracteristici se reflectă și în contextul militar. Într-o astfel de eră, sistemele de C2 trebuie să fie extrem de adaptabile și să funcționeze eficient, indiferent de tipul de conflict sau de mediul în care operează. Tehnologia are un rol crucial în îmbunătățirea capacităților C2, dar vine și cu riscuri considerabile. Pe de-o parte, tehnologia poate contribui la optimizarea deciziilor și la o coordonare mai eficientă, dar, pe de altă parte, există pericolul de a deveni supradependenți de echipamente și de a crea supraîncărcare informațională. Aceasta poate induce o iluzie periculoasă, aceea că războiul poate fi gestionat cu precizie absolută, ceea ce nu este realist. În plus, cu cât sistemele C2 devin mai elaborate și mai conectate, cu atât cresc riscurile de perturbare, de atacuri cibernetice sau supraîncărcare informațională. Din acest motiv, trebuie găsite soluții de protecție și de optimizare a fluxurilor de date specifice sistemelor de comandă și control. Creșterea resurselor destinate cercetării și inovării în domeniul tehnologiilor emergente, pentru a asigura păstrarea unui avantaj competitiv, în raport cu adversarii, poate asigura descoperiri care să sprijine eficientizarea sistemelor C2.

Totuși, articolul de față nu s-a dorit a fi o foaie de parcurs pentru adaptarea sistemelor de comandă și control, ci, mai degrabă, a încercat să scoată în evidență anumite elemente extrem de importante care trebuie avute în vedere la realizarea planului de transformare. Analiza caracteristicilor imuabile ale naturii conflictelor, precum și cele ale caracterului celor actuale, dar și a tendințelor de evoluție a mediului de operare a reprezentat pilonii pe care am construit rezultatele prezentate.

Deși înțelegem că procesul de transformare a sistemului de comandă și control românesc nu trebuie să constituie un efort individual, ci unul colectiv și bine direcționat de către factorii de decizie de la cel mai înalt nivel din Armata României,

apreciem că articolul de față poate sprijini acest demers cel puțin prin două **elemente extrem de valoroase**:

- rezultatele obținute, care pot constitui piloni de adaptare a sistemelor C2;
- modalitatea științifică prin care am dezvoltat aceste rezultate. Identificarea, într-o primă fază, a factorilor care pot influența sistemele C2 și a modului în care o pot face, ulterior, printr-un proces de inferență, determinarea modului de adaptare a acestora, considerăm a fi abordarea corectă spre transformarea sistemelor de comandă și control din Armata României.

În continuare, vom prezenta **cele mai importante rezultate, obținute** în urma demersului științific întreprins, sub formă de recomandări pentru ținta principală a acestui studiu, factorii decizionali ai Armatei României, organizate pe cele patru componente ale sistemelor de comandă și control, evidențiate în prima secțiune a acestei lucrări. Aceste rezultate au survenit în urma unei analize tematice a datelor reieșite din aplicarea în secțiunea anterioară a metodei *„analiza factorilor pe trei coloane"*. Toate aceste date rezultate au fost supuse, în această etapă, unui proces riguros de analiză, cu scopul de a asigura organizarea lor pe teme mai ample, care, ulterior, au fost încadrate în cele patru mari categorii ale sistemelor de comandă și control, în raport cu specificul fiecăreia dintre ele.

Personal

- Comandantul va continua să rămână elementul central al procesului de luare a deciziei. Acest aspect impune nevoia de pregătire constantă a acestuia. În plus, crearea unui sistem de transfer al memoriei instituționale din generație în generație, de la un comandant către viitorii comandanți poate eficientiza demersul de pregătire.
- Leadershipul trebuie să rămână elementul fundamental al comandanților militari.
- Nevoia de adoptare a unei mentalități de tip *"red teaming"* care să asigure dezvoltarea gândirii critice și creative personalului propriu.
- Dezvoltarea unei gândiri critice și creative, focusată pe declanșarea de efecte care să încetinească ciclul decizie-acțiune al inamicului.
- Nevoia de instruire a personalului în operarea sistemelor digitale, pe fondul tehnologizării sistemelor de comandă și control.
- Pregătirea personalului pentru a acționa și, în mod analogic, considerând posibilitatea crescută de a acționa într-un mediu contestat împotriva unui adversar cu capabilități sporite de război electronic.
- Educația personalului trebuie să se focuseze pe cum ar trebui să gândească și mai puțin pe ce ar trebui să gândească. O astfel de abordare poate asigura flexibilitatea mentală necesară personalului de a se adapta și de a răspunde eficient provocărilor care pot apărea în mediul de operare tot mai volatil și incert.
- Înțelegerea modului în care funcționează creierul uman în timpul luării deciziilor și al erorilor de judecată care pot apărea ca urmare a propriilor biasuri cognitive.
- Implementarea și antrenarea conceptului de „comandă prin misiune" (Mission Command) trebuie să înceapă din timp de pace. Dacă acesta nu se implementează în modul de lucru zilnic, este puțin probabil că se va realiza eficient în caz de război.
- Necesitatea realizării interoperabilității umane dintre sistemele C2 proprii și cele

ale aliaților, pe fondul probabilității crescute de desfășurare a operațiilor militare în mediu multinațional.

Procese

- Adaptarea ritmului de luptă al unităților pentru a scurta timpul de luare a deciziilor prin includerea tehnologiilor emergente.
- Scurtarea procesului decizie-acțiune propriu.
- Optimizarea proceselor operaționale prin utilizarea tehnologiilor emergente.
- Abilitatea de a transmite în timp real imaginea operațională de ansamblu la cele mai de jos eșaloane și de actualizare automată a acesteia la toate nivelele de comandă.
- Reducerea dimensiunii ordinelor transmise sau utilizarea tehnologiei emergente pentru a asigura înțelegerea rapidă a acestora. De exemplu, ordinele de operații la nivel de corp de armată NATO ajung în mod regulat la 750 de pagini, iar cele de nivel întrunit, la 1.000 de pagini. Sunt puține persoane într-un comandament care le citesc în totalitate (Storr 2023, 87).
- Necesitatea realizării interoperabilității procedurale dintre sistemele C2 proprii și cele ale aliaților, pe fondul probabilității crescute de desfășurare a operațiilor militare în mediu multinațional.

Sisteme tehnologice

- Transformarea digitală a punctelor de comandă prin integrarea tehnologiilor emergente în sprijinul eficientizării proceselor specifice funcțiilor sistemelor de comandă și stat major (înțelegere situațională, decizie etc.).
- Utilizarea sistemelor tehnologice performante pentru ușurarea întocmirii, transmiterii, lecturării și înțelegerii rapide a ordinelor scrise. Acest lucru poate reduce timpul de planificare a noilor operații, cu efect direct asupra diminuării ciclului propriu decizie-acțiune (OODA).
- Nevoia de identificare de soluții tehnice de protecție a sistemelor C2: cibernetică, reducerea amprentei electromagnetice și termice etc.
- Dependența de tehnologie poate crea și vulnerabilități într-un mediu contestat și în fața unui adversar cu capabilități sporite de război electronic.
- Necesitatea realizării interoperabilității tehnice dintre sistemele C2 proprii și cele ale aliaților, pe fondul probabilității crescute de desfășurare a operațiilor militare în mediu multinațional.

Puncte de comandă

- Asigurarea de măsuri de protecție sporită: fizice și electromagnetice.
- Regândirea modului de organizare a punctelor de comandă (dimensiunea curentă a lor este mult prea mare și sunt mult prea statice, ceea ce le face extrem de vulnerabile într-o perioadă în care a crescut precizia armelor de la distanță și s-a redus timpul dintre detecție și angajare la doar câteva minute) pentru a răspunde provocărilor crescânde ale mediului de operare și pentru a asigura supraviețuirea acestora și funcționalitatea continuă a C2 (de exemplu, adoptarea unor practici de dispersie a punctelor de comandă și folosirea de sisteme redundante. S-ar putea să fie nevoie ca modulele integrate și cele funcționale să nu mai acționeze din același loc, iar când

ne referim la Punctul de comandă de bază, să nu mai înțelegem o singură locație, ci o multitudine de locuri/module care împreună, prin suportul tehnologic, să întrunească funcțiunile acestui punct de comandă).
- Introducerea de măsuri suplimentare de securitate pentru protejarea fizică și electromagnetică a locațiilor C2 împotriva atacurilor directe și indirecte (de exemplu, împotriva dronelor sau sistemelor de EW ale adversarilor).
- Reducerea și mascarea dimensiunilor, a amprentei termice și electromagnetice a punctelor de comandă (de exemplu, investiția în baterii silențioase care să permită funcționarea pentru o perioadă cât mai mare a sistemelor tehnice din PC, care să înlocuiască zgomotoasele grupuri electrogene; identificarea de soluții care să înlocuiască sistemele de aer condiționat care produc un zgomot mare și care pot deconspira locația punctelor de comandă). *„Războiul dintre Rusia și Ucraina arată clar că semnătura electromagnetică emisă de punctele de comandă din ultimii 20 de ani nu poate supraviețui în fața ritmului și preciziei unui adversar care deține tehnologii bazate pe senzori, război electronic, sisteme aeriene fără pilot sau cu acces la imagini satelitare.*" (Nagl 2024, 24)
- Utilizarea măsurilor de inducere în eroare a adversarului prin crearea de puncte de comandă false poate constitui o soluție în demersul de sporire a protecției sistemelor C2 (Nagl 2024, 242).
- Sporirea mobilității punctelor de comandă pentru evitarea detectării și a atacurilor. Mutarea constantă a PC pentru a evita detectarea cu realizarea continuă a funcționalității C2.
- Necesitatea realizării interoperabilității dintre sistemele C2 proprii și cele ale aliaților, pe fondul probabilității crescute de desfășurare a operațiilor militare în mediu multinațional.

În plus, principiile care trebuie să stea la baza noilor sisteme de comandă și control, pentru a asigura un grad sporit de adaptabilitate la provocările curente și viitoare din mediul de operare, sunt flexibilitatea, modularitatea, supraviețuirea, amprenta redusă la sol și reziliența.

Flexibilitatea presupune capacitatea sistemului de comandă și control (C2) de a se adapta rapid la schimbările din mediul de operare. Acest principiu implică atât structuri și proceduri adaptabile, cât și folosirea tehnologiei care permite răspunsuri rapide la provocările neprevăzute. Flexibilitatea sistemului C2 este crucială pentru a răspunde rapid la noi amenințări sau oportunități, precum și pentru a ajusta prioritățile și resursele, în funcție de evoluția situației din câmpul de luptă.

Modularitatea presupune construirea sistemului din componente independente, dar interoperabile, care pot fi combinate și reconfigurate, în funcție de nevoi. În contextul C2, acest principiu permite crearea de structuri personalizate care se potrivesc fiecărei misiuni și facilitarea modernizării prin integrarea de noi tehnologii, fără a afecta întregul sistem. Modularitatea oferă forțelor armate capacitatea de a optimiza resursele și de a îmbunătăți eficiența operațională.
Supraviețuirea se referă la capacitatea sistemului C2 de a funcționa în condiții potrivnice,

inclusiv în medii contestate. Acest principiu se poate realiza prin dispersie adecvată, mărime redusă, redundanță, mobilitate, camuflaj, măsuri de inducere în eroare, măsuri OPSEC, precum și prin integrarea sistemelor antidronă și a altor tehnologii defensive pentru realizarea protecției fizice și cibernetice adecvate. Scopul este de a reduce vulnerabilitatea în fața atacurilor inamice și de a asigura continuitatea operațiilor.

Amprenta redusă la sol presupune minimizarea dimensiunii fizice și a semnăturii electromagnetice a punctelor de comandă, reducând astfel șansele de a fi detectate și lovite de inamic, (o soluție poate fi dispersia și conducerea operațiilor din mai multe locații distanțate care să opereze ca un întreg). Un sistem C2 cu o amprentă redusă este mai greu de identificat și localizat, contribuind la siguranța personalului și a echipamentelor. Acest principiu este esențial în fața adversarilor care dispun de capabilități avansate de supraveghere și de atac.

Reziliența se referă la capacitatea sistemului de a-și reveni rapid după o întrerupere sau un atac și de a menține funcționalitatea pe termen lung. Reziliența include redundanța sistemelor, procese de backup și planuri de continuitate care să permită operarea chiar și în caz de pierderi sau disfuncții. Acest principiu asigură că, în fața unui atac sau a unei defecțiuni, sistemele C2 pot continua să își îndeplinească misiunea esențială, fără a compromite eficiența generală a operațiilor.

În concluzie, adaptarea sistemelor de comandă și control la provocările mediului contemporan de operare necesită o abordare holistică și integrată, care să țină cont atât de evoluția tehnologică, cât și de schimbările în dinamica conflictelor globale și de tendințele de evoluție a mediului de operare. În acest sens, sistemele C2 trebuie să găsească un echilibru între utilizarea tehnologiei și adaptabilitatea umană. Sunt, de asemenea, cruciale dezvoltarea și implementarea unor strategii flexibile, care să permită adaptarea rapidă la schimbările neprevăzute, dar și testarea obligatorie în diferite contexte a potențialelor soluții de adaptare a sistemelor de comandă și control. Aceasta va asigura o funcționare coerentă și flexibilă, esențială în fața provocărilor complexe și dinamice ale războiului modern.

Referințe

ADP 6-0. 2019. *Mission Command: Command and Control of Army Forces.* Washington DC: US Headqurters Department of the Army.

AJP-01. 2022. *Allied Joint Doctrine, Edition F, Version 1.* NATO Standardization Office.

AJP-3. 2019. *Allied Joint Doctrine for the conduct of operations.* C, Version 1. NATO Standardization Office.

AJP3.10.2. 2020. *Allied Joint Doctrine for operations security and deception,* edition A, version 2. NATO Standardization Office.

AJP-3.2. 2022. *Allied Joint Doctrine for Land Operations, edition B, version 1.* NATO Standardization office.

ATP 3.2.2. 2016. *Command and Control of Allied Land Forces.* B, Version 1. NATO Standardization Office.

Bailey, Kathryn. 2023. "Army looks to transform future command and control". https://www.army.mil/article/267509/army_looks_to_transform_future_command_and_control.

Beagle, Lt. Gen. Milford "Beags", Brig. Gen. Jason C. Slider și Lt. Col. Matthew R. Arrol. 2023. "The Graveyard of Command Posts." *The Military Review* 10-24. https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2023/Graveyard-of-Command-Posts/.

Collins, Major General Charles. 2023. "Mobilizing the British Army." *The British Army Review* (182): 6-9.

Creswell, John W. și J. David Creswell. 2023. *Research design. Qualitative, Quantitative, and Mixed Methods Approaches,* Ediția a șasea. Los Angeles: Sage Publications.

Crilly, Martin și Alan Mears. 2022. "Multi Dimensional and Domain Operations (MDDO)". https://wavellroom.com/2022/01/26/mddo/.

Dragomir, Florentina-Loredana și Gelu Alexandrescu. 2017. „Aplicaţii ale inteligenţei artificiale în fundamentarea deciziei." *Buletinul Universităţii Naţionale de Apărare „Carol I"* 56-61.

Ellison, Davis și Tim Sweijs. 2023. *Breaking Patterns Multi-Domain Operations and Contemporary Warfare.* Hague: The Hague Centre for Strategic Studies.

Gosselin-Malo, Elisabeth. 2024. "Drone warfare in Ukraine prompts fresh thinking in helicopter tactics". https://www.defensenews.com/global/europe/2024/07/19/drone-warfare-in-ukraine-prompts-fresh-thinking-in-helicopter-tactics/.

Hambling, David. 2020. "The «Magic Bullet» Drones Behind Azerbaijan's Victory Over Armenia". https://www.forbes.com/sites/davidhambling/2020/11/10/the-magic-bullet-drones-behind--azerbaijans-victory-over-armenia/.

JCN1/17. 2017. *Joint Concept Note (JCN) 1/17 Future Force Concept.* UK Ministry of Defence.

JDP 0-01.1. 2023. *Joint Doctrine Publication 0-01.1 UK Terminology Supplement to NATOTerm.* Edition B. UK Ministry of Defence.

JP-1. 2017. *Joint Publication 1 Doctrine for the Armed Forces of the United States.* US Joint Chiefs of Staff.

Leavy, Patricia. 2023. *Research Design – Quantitative, Qualitative, Mixed Methods, Arts-Based, and Community-Based Participatory Research Approaches,* Ediția a doua. New York: The Guilford Press.

Multinational Capability Development Campaign [MCDC]. 2020. "Future Leadership". https://assets.publishing.service.gov.uk/media/5fdccd0de90e07452ec36ee8/20201210-MCDC_Future_Leadership-web.pdf.

MCDP-6. 2018. *Command and Control.* US Marines Corps.

Molloy, Dr Oleksandra. 2024. *Drones in Modern Warfare: Lessons Learnt from the War in Ukraine.* Australian Army Research Centre.

Nagl, John A. 2024. *A call to arms: Lessons from Ukraine for the Future Force.* Strategic Studies Institute, UIS Army War College.

NATO. 2022. *Initial Alliance Concept for Multi-Domain Operations.* Norfolk: NATO Allied Command Transformation.

NATO. 2023. *Strategic Foresight Analysis 2023.* Norfolk: NATO Allied Command Transformation.

NATO Parliamentary Assembly. 2022. *The future of Warfare.* NATO Science and Technology Committee.

NATO Science & Technology Organization. 2020. *Science & Technology Trends 2020-2040 - Exploring the S&T Edge.* Bruxelles. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf.

NATO Industrial Advisory Group [NIAG]. 2022. *Command and Control Capabilities in support of Multi Domain Operations (Multi Domain C2).*

Nilsson, Niklas. 2023. "Commanding Contemporary and Future Land Operations." În *Advanced Land Warfare. Tactics and Operations*, de Mikael Weissmann și Niklas Nilsson, 43-62. Oxford University Press.

Russia Today. 2017. https://www.rt.com/news/401731-ai-rule-world-putin/.

Stanciu, Cristian-Octavian și Silviu-Iulian Gimiga. 2023. „Noile tehnologii și impactul lor asupra domeniului militar." *Buletinul Universității Naționale de Apărare „Carol I"* 12 (2): 157-169.

Storr, Jim. 2023. "The Command of Land Forces." În *Advanced Land Warfare. Tactics and Operations*, de Niklas Nilsson Mikael Weissmann, 87-103. Oxford University Press.

TC 7-102. 2014. *Training Circular No. 7-102 Operational Environment and Army learning.* Washington DC: Headquarters Department of the Army.

The International Institute for Strategic Studies [IISS]. 2023. *Strategic Survey 2022. The Annual Assessment of Geopolitics.* Londra: Routledge.

TRADOC G2. 2024. *The Operational Environment 2024-2034: Large-Scale Combat Operations.* US Army Training and Doctrine.

UK Ministry of Defence. 2020. *Introducing the Integrated Operating Concept 2025.*

—. 2021. "*Red Teaming Handbook*". https://assets.publishing.service.gov.uk/media/61702155e90e0719 7867eb93/20210625-Red_Teaming_Handbook.pdf.

—. 2024. *Global Strategic Trends: Out to 2055.*

Wade, Norman M. 2023. *AODS 7 The Army Operations & Doctrine Smartbook - Multidomain operations* . The Lightning Press.

Watling, Jack, și Nick Reynolds. 2022. *Operation Z. The Death Throes of an Imperial Delusion.* Royal United Services Institute for Defence and Security Studies.

BULETINUL
UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I”
https://buletinul.unap.ro

Impactul noilor capabilități de sprijin prin foc din perspectiva funcțiilor întrunite

Impact of new fire support capabilities from a joint functions perspective

Lt.col.drd. Adrian MIREA*
*Universitatea Națională de Apărare „Carol I”
e-mail: mirea.adrian82@gmail.com

Abstract

Articolul evidențiază utilitatea cadrului operațional descris de funcțiile întrunite pentru a înțelege impactul pe care o capabilitate disponibilă îl are, din punct de vedere acțional, asupra operației. Totodată, acest cadru poate fi exploatat și în scopul identificării unei nevoi de capabilități la nivelul grupărilor de forțe actuale, necesar în îndeplinirea misiunilor încredințate. Pentru a putea argumenta cele menționate, am avut în atenție o capabilitate de asigurare a sprijinului prin foc, recent intrată în înzestrarea structurilor de forțe armate naționale – sistemele M142 HIMARS (High Mobility Artillery Rocket System). Dacă, în prima parte a articolului, am detaliat succint aspecte privind cadrul operațional descris de funcțiile întrunite, în cea de-a doua parte, am prezentat o perspectivă argumentată referitoare la impactul pe care capabilitățile sistemelor HIMARS îl au asupra modului de conceptualizare a operațiilor. Scopul articolului este de a argumenta, printr-un exemplu concret, posibilitatea întrebuințării cadrului operațional descris de funcțiile întrunite pentru a înțelege întregul potențial al unei capabilități existente sau de perspectivă pentru structurile de forțe armate naționale.

The article highlights the usefulness of the operational framework described by the joint functions to understand the impact that an available capability has on the operation from an actional point of view. At the same time, this framework can also be exploited for the purpose of identifying a need for capabilities at the level of the current joint force in order to be able to accomplish the assigned missions. In order to argue the above, I have focused on a fire support capability that has recently become part of the national armed forces structures - the M142 HIMARS (High Mobility Artillery Rocket System). If in the first part of the article I briefly detailed aspects of the operational framework described by the joint functions, in the second part I presented a reasoned perspective on the impact that the capabilities of HIMARS systems have on the way of conceptualizing operations. The article aims to argue, through a concrete example, the possibility of using the operational framework described by the joint functions to understand the full potential of an existing or prospective capability for national armed forces structures.

Cuvinte-cheie:
funcții întrunite; sisteme HIMARS; sprijin prin foc; cadru operațional; capabilitate.

Keywords:
joint functions; HIMARS systems; fire support; operational framework; capability.

Info articol
Primit: 25 octombrie 2024; Evaluat: 18 noiembrie 2024; Acceptat: 29 noiembrie 2024; Disponibil online: 17 ianuarie 2025
Citare: Nistorescu, C.V. 2024. „Impactul noilor capabilități de sprijin prin foc din perspectiva funcțiilor întrunite”. *Buletinul Universității Naționale de Apărare „Carol I”*, 13(4): 86-97. https://doi.org/10.53477/2065-8281-24-40

Integrarea capabilităților noi de sprijin prin foc, conform programelor de înzestrare curente sau de perspectivă, impune, din punctul meu de vedere, și o înțelegere a modului în care comandantul militar poate valorifica întregul lor potențial în operație. Funcțiile luptei constituie un context util de conceptualizare a modului în care noile capabilități pot fi exploatate oportun, conform nevoilor operaționale ale structurilor de forțe care le dețin sau le vor deține la un moment dat. Prin intermediul acestui articol, mi-am propus evidențierea unei modalități utile de înțelegere a impactului pe care îl au noile capabilități de sprijin prin foc ale structurilor de forțe armate naționale, precum și a modului în care comandantul și statul său major pot conceptualiza valorificarea noilor posibilități, oferite de acestea, în planificarea și conducerea operațiilor structurilor de forțe proprii.

Pentru realizarea acestei lucrări, am avut în vedere metoda analizei documentare, cu scopul de a selecta, a revizui și a evalua într-un mod sistematic surse publice (neclasificate) de informare. În acest fel, am urmărit ilustrarea sintetizată a unei perspective privind potențialele implicații ale integrării de noi capabilități militare la nivel național. Am considerat ca fiind suficient de relevantă abordarea influenței unui număr limitat de posibilități ale echipamentelor militare, nou intrate în înzestrare sau de perspectivă, folosind cadrul de manifestare a funcțiilor luptei, întrucât, din punctul meu de vedere, modalitatea construirii perspectivei poate fi extrapolată și la nivelul altor tipuri de echipamente, capabilități sau servicii disponibile structurilor de forțe armate naționale.

Funcțiile întrunite reprezintă un instrument, existent la dispoziția comandantului și statului său major, folosit în special pentru a asigura o abordare integrală a tuturor aspectelor specifice unei operații, precum și pentru a vizualiza activitățile specifice structurilor de forțe disponibile în cadrul operațional creat. Funcțiile întrunite sunt, practic, o descriere a capabilităților disponibile structurilor de forțe. Nevoile concrete ale grupării de forțe pentru desfășurarea unei operații sunt determinate de comandant prin prisma funcțiilor întrunite (NATO 2022a, 105). Din această perspectivă, funcțiile întrunite vin să argumenteze cerințele actuale ale unei grupări de forțe, dar și nevoia structurilor de forțe armate, de a dispune de capabilități moderne, adaptate mediului de confruntare actual.

Cadrul operațional descris de funcțiile întrunite

Atât din perspectivă NATO (NATO 2022a, 105), cât și din perspectivă națională (SMG 2011, 70; SMG 2014, 26), funcțiile întrunite vizează:

- manevra și focul întrunit;
- comanda și controlul (C2);
- informațiile;
- protecția forței;
- operațiile informaționale (INFO OPS);
- sustenabilitatea;
- cooperarea civili-militari (CIMIC).

Trebuie menționat faptul că, diferit de reglementările NATO, la nivel național sunt șapte funcții întrunite, întrucât manevra este asociată cu focul întrunit într-o singură funcție. În cele ce urmează, voi prezenta pe scurt ideile principale ale fiecărei funcții întrunite pentru a le putea aborda, în cea de-a doua parte a acestei lucrări, în interpretarea impactului potențial al unor noi capabilități.

Manevra și focul întrunit (*manevra și aplicarea puterii de foc*, conform doctrinei Armatei României) integrează, din perspectivă națională, așa după cum am menționat, două funcții întrunite, potrivit doctrinelor NATO. *Manevra* are ca scop principal obținerea unei poziții avantajoase, în raport cu inamicul, care ar permite amenințarea sau aplicarea forței asupra acestuia. La nivel operativ, manevra reprezintă procesul prin care puterea de luptă este concentrată acolo unde ar avea efect decisiv în prevenirea, dezorganizarea sau neutralizarea operațiilor inamicului (NATO 2019, 1-21). Cu toate că se manifestă, de regulă, în plan fizic, manevra poate avea efecte asupra moralului forțelor inamicului prin generarea de incertitudine, confuzie și paralizie. *Focul întrunit*, aplicat de structuri din două sau mai multe categorii de forțe armate, are ca scop principal influențarea capacității de luptă a inamicului. Efectele focului întrunit se manifestă, în principal, în plan fizic, însă ele pot afecta componentele psihologică și morală ale puterii de luptă, având astfel impact asupra voinței de a lupta a inamicului.

Comanda și controlul (C2), ca funcție întrunită, vizează exercitarea autorității de către comandant asupra forțelor aflate la dispoziție pentru îndeplinirea misiunii. Operațiile sunt caracterizate de o planificare și direcționare centralizată, pentru a asigura unitatea de efort, și de o autoritate de execuție descentralizată până la cel mai mic eșalon capabil să utilizeze eficient structurile de forțe. Un element reprezentativ este arhitectura de comandă și control, care, în mediul de operare actual, este dependentă de capabilitățile ce exploatează spectrul electromagnetic tot mai congestionat și mai contestat (NATO 2022b, 49).

Informațiile au rolul de a asigura o înțelegere continuă și coordonată a mediului de confruntare, venind în sprijinul comandantului prin identificarea condițiilor necesare îndeplinirii obiectivelor, prin evitarea producerii de efecte nedorite și prin evaluarea impactului acțiunii inamicului, forțelor proprii sau al altor actori asupra concepției operației. Funcția întrunită *informații* este un instrument esențial pentru desfășurarea procesului de luare a deciziei, deoarece integrează activitățile comandantului, statului major și elementelor de culegere pentru a genera produsele de informații necesare, rezultate ale ciclului informațional (direcționare-culegere-procesare-diseminare).

Protecția forței este o funcție orientată pe eliminarea sau diminuarea vulnerabilității personalului, echipamentelor, facilităților, operațiilor și activităților în fața potențialelor amenințări sau pericole pentru a asigura libertatea de acțiune și eficiența operațională în îndeplinirea misiunii. Protecția forței este o responsabilitate a comandanților de la toate nivelurile ierarhice, dar și o responsabilitate fundamentală

permanentă a întregului personal. Dintre aspectele reprezentative ale acestei funcții, menționez apărarea antiaeriană, apărarea CBRN (Chimică, Biologică, Radiologică și Nucleară), asigurarea genistică și securitatea operației.

Operațiile informaționale (INFO OPS), ca funcție întrunită, integrează acele acțiuni și activități care produc efecte asupra capacității de înțelegere și de percepție, asupra voinței de a lupta și asupra capabilităților entităților țintă, cu scopul de a asista îndeplinirea obiectivelor stabilite. Facilitatorii cheie ai acestei funcții includ operațiile psihologice, inducerea în eroare, războiul electronic și distrugerea fizică (SMG 2014, 33).

Sustenabilitatea privește asigurarea coerentă a suportului necesar desfășurării operației până la îndeplinirea misiunii. Acest suport vizează, în principal, asigurarea de resurse (umane și materiale), sprijinul medical și sprijinul de geniu. Reabilitarea, reaprovizionarea și regenerarea elementelor forței sunt rezultate ale sustenabilității și au un rol important în menținerea nivelului necesar capacității de luptă. Gradul de sustenabilitate are impact asupra ritmului, duratei și intensității tuturor tipurilor de operații.

Cooperarea civili-militari (CIMIC) constă în coordonarea și cooperarea comandanților militari cu actori civili din zona de operații pentru îndeplinirea obiectivelor forței. Prin intermediul acestei funcții, comandantul poate crea și menține condițiile favorabile îndeplinirii misiunii proprii, exploatând avantaje de natură morală, materială sau tactică, în detrimentul inamicului. Interacțiunile civil-militari reprezintă un instrument important în atingerea obiectivelor de nivel strategic și operativ, întrucât actorii civili din zona de operații pot avea un impact asupra finalității situației conflictuale sau a crizei în desfășurare.

Prin intermediul cadrului operațional descris de funcțiile întrunite, comandantul asociază acțiunile și activitățile structurilor de forțe pentru a genera efecte, urmărind a influența capacitatea inamicului de a înțelege, nivelul de capabilități disponibile acestuia, precum și voința lui de a lupta. Într-o manieră similară, activitățile și acțiunile structurilor de forțe disponibile produc efecte cu potențial de a influența capacitatea de înțelegere, nivelul de capabilități și voința de a lupta, din perspectiva forțelor proprii sau a altor actori aflați în zona de responsabilitate.

Capabilitățile disponibile la nivelul structurilor de forțe definesc fiecare funcție întrunită, însă, luate separat, aceste capabilități pot fi valorificate în cadrul mai multor funcții. Comandantul, pentru a-și îndeplini misiunea, poate alege dintr-o multitudine de capabilități disponibile și le poate asocia sau integra în mai multe moduri pentru a îndeplini funcțiile întrunite, enumerate mai sus. El va detalia, prin ordinul de operație, modalitatea concretă de utilizare a forțelor și mijloacelor disponibile, însă acestea nu sunt exclusiv asociate unei singure funcții. O acțiune a unei forțe sau capabilități disponibile poate și va fi exploatată în cadrul mai multor funcții întrunite.

https://doi.org/10.53477/2065-8281-24-40

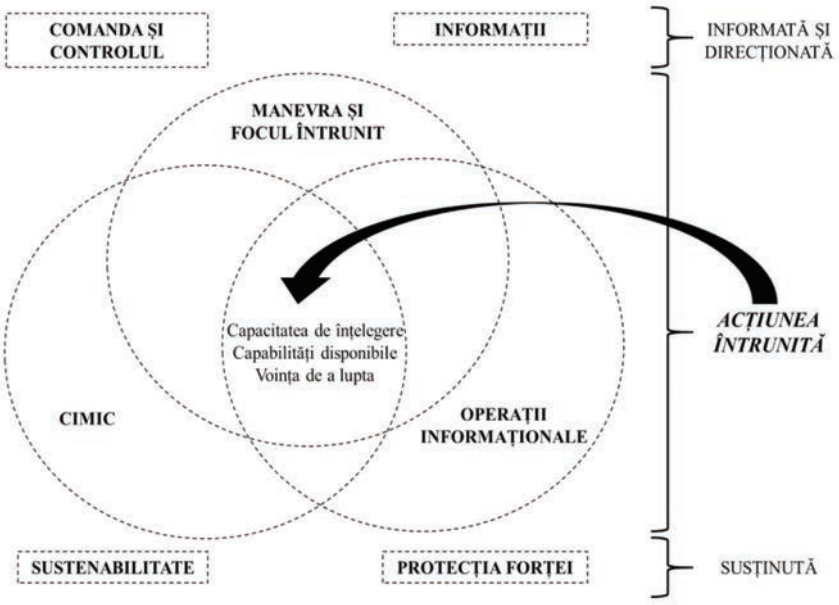


Figura 1 Cadrul acțional descris de funcțiile întrunite
Sursa: Adaptare conform AJP-01 Allied Joint Publication, 2022, p. 106.

Impactul noilor sisteme de sprijin prin foc asupra funcțiilor întrunite

Condițiile concrete în care puterea de luptă a unei forțe poate fi aplicată eficient vizează înțelegerea naturii conflictului și a contextului de manifestare a acestuia, mediul concret de operare, entitățile țintă cu amenințările existente, precum și capabilitățile disponibile structurilor proprii, ale inamicului sau ale altor actori prezenți în zona de responsabilitate.

De cele mai multe ori, posibilitățile mărite ale sistemelor moderne de sprijin prin foc sunt vizualizate că au implicații asupra cadrului geografic de manifestare a acțiunii, prin bătaia maximă superioară la care acestea pot lovi țintele – în zona de operații din adâncimea dispozitivului de luptă inamic, în zona de operații de la contact sau în zona de spate. Un exemplu în acest sens poate fi înzestrarea structurilor de forțe terestre ale Armatei României cu sisteme de tip M142 HIMARS (High Mobility Artillery Rocket System) care, în primă instanță, ne duce cu gândul la distanța maximă la care acestea pot angaja ținte – 70 km (pentru GMLRS – Guided Multiple Launch Rocket System) și 300 km (pentru ATACMS – Army Tactical Missile System). O reprezentare ilustrativă a impactului pe care bătaia maximă a sistemelor de sprijin prin foc îl poate avea asupra mediului de acțiune o regăsim în *Field Manual FM 3-0 Operations* din 2022.

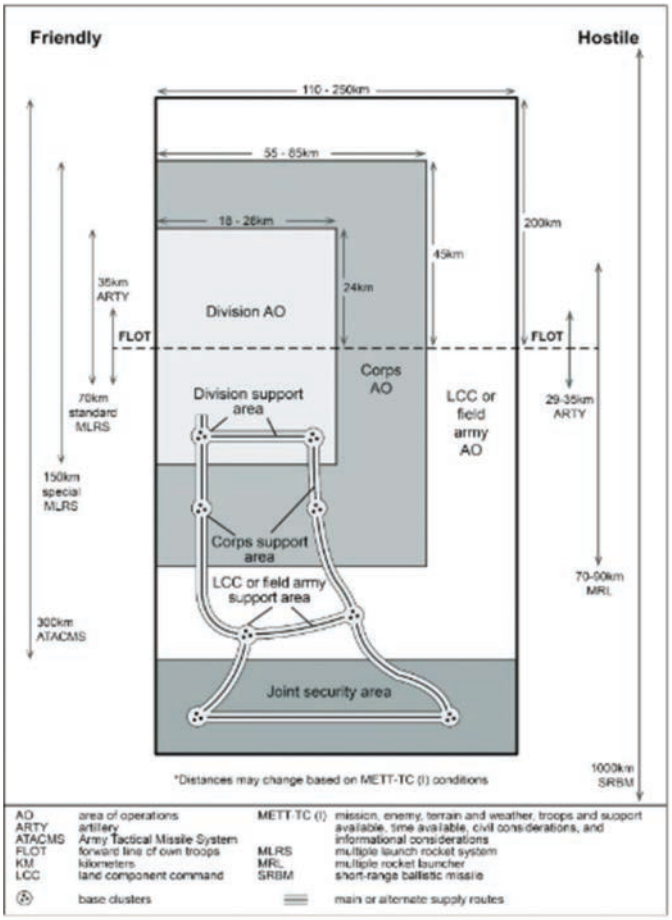


Figura 2 Model doctrinar de reprezentare a dimensiunilor front și adâncime
Sursa: Field Manual FM 3-0 Operations, 2022, p. 6-8.

În această reprezentare, se poate observa influența bătăii maxime a sistemelor de sprijin prin foc (disponibile ambilor adversari) asupra conceptualizării zonei de operații la nivel operativ și tactic.
Având în vedere întreaga gamă de posibilități, oferite de sistemele HIMARS (bătaie mărită față de sistemele de artilerie pe care le-au înlocuit, precizie îmbunătățită, o varietate mai mare a munițiilor potențiale, avantajul reducerii la minimum a eventualelor efecte colaterale etc.), putem explora multiple modalități de valorificare a acestor sisteme în cadrul operațional descris de funcțiile întrunite.
Am prezentat în Tabelul nr. 1 o perspectivă personală privind înzestrarea forțelor terestre naționale cu sisteme HIMARS, unde am integrat principalele aspecte, sub forma unei analize SWOT.

Cu toate că, la nivel național, au fost achiziționate doar anumite tipuri de muniții (Defence DataBase 2024), pentru elaborarea acestei lucrări, am avut în vedere sistemele HIMARS ca platforme cu potențialul de a întrebuința toată gama de muniții disponibile unor astfel de sisteme. Un alt aspect care trebuie menționat este faptul că, în detalierea perspectivei contribuției și integrării în funcțiile întrunite a sistemelor HIMARS, am abordat și unele aspecte privind potențialul de perturbare a funcțiilor întrunite pentru un potențial inamic.

https://doi.org/10.53477/2065-8281-24-40

TABEL NR. 1

Analiza SWOT privind înzestrarea structurilor de forțe terestre naționale cu sisteme HIMARS

STRENGHTS (Puncte tari)	**WEAKNESSES (Puncte slabe)**
- Sunt sisteme validate ca fiind performante în conflicte recente (Irak, Afganistan, Ucraina) - Înzestrarea cu astfel de sisteme contribuie la descurajarea unei agresiuni armate la adresa României - Au capacitatea de a sprijini prin foc atât operații întrunite, cât și operații multidomeniu - Au un grad ridicat de mobilitate, fiind transportabile, inclusiv pe cale aeriană, oferind flexibilitate crescută - Asigură un grad ridicat de interoperabilitate tehnică cu aliații, din perspectiva sistemelor de comandă și control - Sunt capabile de a executa foc pe tiparul *shoot and scoot* (trage și fugi), asigurând un grad ridicat de supraviețuire în mediul de confruntare actual - Pot angaja cu precizie ținte la distanțe considerabil mai mari decât sistemele de artilerie clasice din dotare - Folosesc sistemul avansat de comandă și control al sprijinului prin foc – IFATDS (International Field Artillery Tactical Data System) care permite planificarea, coordonarea și execuția automatizată a focului - Dispun de un sistem logistic integrat, având muniția containerizată și posibilitatea încărcării mecanizate (Forțele Terestre Române 2024) - Pot utiliza o varietate mare de muniții cu diverse tipuri de încărcături - Munițiile sunt proiectate să reducă la minimum riscul producerii de victime sau pagube colaterale - Munițiile lansate au viteză mare și o semnătură radar redusă, ceea ce le face dificil de detectat și interceptat, fiind greu de deosebit de alte muniții convenționale	- Necesitatea alocării de resurse dedicate protecției fizice, precum și protecției antiaeriene/antirachetă a sistemelor HIMARS, întrucât acestea sunt ***ținte prioritare*** pentru un potențial inamic în toate tipurile de operații - Necesitatea asocierii cu sistemele HIMARS a unor platforme de război electronic și a unor radare performante, pentru a descoperi și a combate dronele, în special cele de cercetare, asigurându-le o protecție multispectrală, adaptată conflictului actual - Protecția multispectrală presupune, din punctul meu de vedere, și implementarea unor măsuri moderne, adecvate protejării acestor sisteme, precum mascarea multispectrală sau întrebuințarea de machete ori replici „convingătoare" ale sistemelor HIMARS - Bruiajul, executat de inamic în zona țintelor, poate avea efecte asupra preciziei muniților (Marquardt, Bertrand și Cohen 2023) - Exploatarea sistemelor HIMARS este dependentă de asigurarea cu materiale de resort din surse externe, în special cu muniții. Acest aspect poate fi problematic în situații de criză/conflict, când cererea poate fi mare, iar repartizarea resurselor va fi prioritizată.
OPPORTUNITIES (Oportunități)	**THREATS (Amenințări)**
- Potențialul susținerii pe plan local a operativității sistemelor HIMARS, prin intermediul Aerostar S.A. Bacău (Lockheed Martin 2024) - Participarea la exerciții multinaționale, valorificând statutul României de membru în comunitatea ASCA (Artillery System Cooperation Activities) (Orjanu 2023) - Permite accesul la muniții emergente pentru astfel de sisteme (de ex.: Extended Range GMLRS, cu o bătaie maximă de 150 km și Precision Strike Missiles, cu o bătaie maximă de 499 km), inclusiv pentru muniții cu sisteme de corecție a traiectoriei imediat după lansare pentru a fi mai greu de identificat cu radarele de contrabaterie	- Riscul valorificării parțiale a potențialului sistemelor HIMARS, din cauza limitărilor actualelor capabilități naționale ISR (Intelligence, Surveillance and Reconnaissance/Informații, Supraveghere și Cercetare) - Reducerea în timp a eficienței operaționale a sistemelor HIMARS, ca urmare a lecțiilor identificate în conflictul ruso-ucrainean - Dezvoltarea de noi capabilități sau implementarea de noi tactici, destinate contracarării efectelor sistemelor HIMARS, ca urmare a lecțiilor identificate (Newsweek 2024), (Goldstein și Waechter 2023) - Dependența de informații satelitare pentru achiziția țintelor, dar și pentru ghidarea GPS a muniților, în condițiile în care există, la nivel mondial, capabilități de luptă antisatelit (VPK News 2023)

Manevra și focul întrunit

Principala contribuție a sistemelor HIMARS în cadrul funcției întrunite *manevra și focul întrunit* constă în potențialul de a diminua capacitatea de luptă a structurilor de forțe ale inamicului fie în mod direct prin distrugerea diverselor echipamente militare, fie în mod indirect prin influențarea psihologică și a stării moralului trupelor inamice. Precizia muniților trase de sistemele HIMARS poate fi valorificată cu precădere asupra țintelor fixe, așa cum sunt elementele de infrastructură folosite de inamic sau concentrările de forțe – pe anumite direcții de efort –, la obiective sau aflate în diverse raioane. Dacă avem în vedere varietatea de muniții (inclusiv de submuniții) (Defence DataBase 2024) care pot fi lansate de sistemele HIMARS, putem avea în vedere o gamă largă de efecte asupra inamicului venind în sprijinul direct al efortului structurilor de manevră ale forțelor proprii.

Din perspectiva inamicului, funcția *manevra și focul întrunit* este perturbată prin capacitatea sistemelor HIMARS de a executa rapid foc precis asupra țintelor de mare valoare din dispozitivul său de luptă. Astfel, prin folosirea loviturilor cu submuniții (inclusiv cu mine antiblindate) în anumite zone sau momente ale operației, se pot obține diverse efecte asupra forțelor de manevră ale inamicului, precum dezorganizarea acțiunilor ofensive, blocarea sau întârzierea introducerii în luptă a rezervelor. Menționez, aici, contribuția directă a sistemelor HIMARS în Donbas pentru blocarea ofensivei forțelor ruse pe direcția Bakhmut-Kramatorsk, din iulie 2022 (Nistorescu 2024, 79). Un alt aspect al dispunerii de sisteme HIMARS care poate perturba această funcție întrunită a inamicului este, din punctul meu de vedere, și efectul de polarizare a unor resurse de sprijin prin foc, destinate special detecției și combaterii HIMARS pe întreaga durată a operației.

O altă contribuție importantă a sistemelor HIMARS la perturbarea funcției întrunite *manevra și focul întrunit* a inamicului este eficiența ridicată a acestora în executarea focului de contrabaterie (Global Defense News 2023). Eficiența sistemelor HIMARS în astfel de situații este fundamentată pe mobilitatea ridicată, dispunerea de sistem automatizat de conducere a focului, capacitatea de a executa misiuni de foc de tip *shoot and scoot*, toate asociate cu precizia și letalitatea ridicate la țintă. Un alt avantaj în acest domeniu poate fi și dezvoltarea și întrebuințarea munițiilor cu sisteme de corectare a traiectoriei imediat după lansare, pentru a face imposibilă detecția exactă a pozițiilor de tragere cu radare de contrabaterie (Kadam 2022).

Comanda și controlul

Funcția întrunită *comanda și controlul* este îmbunătățită prin înzestrarea structurilor de forțe cu sisteme HIMARS, din mai multe puncte de vedere. Unul dintre acestea este perspectiva comenzii și controlului eficient al sprijinului prin foc, datorită exploatării sistemului IFATDS. Rapiditatea cu care se desfășoară planificarea și execuția automatizată a misiunilor de foc are implicații asupra capacității de reacție, sub forma focului de contrabaterie, împotriva sistemelor de sprijin prin foc ale inamicului, care vizează perturbarea exercitării comenzii și controlului la nivel grupare de forțe. Capacitatea de reacție poate fi valorificată și în situația combaterii țintelor de oportunitate, apărute în dinamica acțiunilor, în mod special a celor clasificate ca fiind ținte senzitive – TST (Time Sensitive Target), unde HIMARS poate reprezenta singura capabilitate eficientă existentă la dispoziția comandantului. Având în vedere funcția *comanda și controlul* din perspectiva inamicului, sistemele HIMARS s-au dovedit eficiente în special în lovirea țintelor de tip punct de comandă, perturbând astfel funcționalitatea sistemului de comandă și control de la diferite eșaloane tactice ale inamicului (BBC 2022).

Informații

Capabilitățile sistemelor HIMARS sunt integrate și asistă funcția întrunită *informații* prin contribuția la imaginea operațională, valorificând caracteristicile sistemului modern de comandă și control al focului – IFATDS și exploatând datele și informațiile privind achiziția țintelor.

Perturbarea funcției *informații* a inamicului cu sisteme HIMARS se poate realiza prin distrugerea fizică a echipamentelor destinate transmiterii sau culegerii de date așa cum sunt, de exemplu, centrele de comunicații (Kadam 2022) sau radarele de contrabaterie (New Voice of Ukraine 2023). Exploatarea sistemelor HIMARS în cadrul unor planuri de inducere în eroare poate contribui la degradarea capacității inamicului de a înțelege situația operațională reală, prin stimularea senzorilor și furnizarea deliberată a anumitor informații, cum ar fi, de exemplu, mutarea efortului principal al grupării de forțe pe o anumită direcție prin dislocarea și folosirea unor poziții de lansare în acest scop. Pentru exemplificare, aduc în atenție rolul sistemelor HIMARS în inducerea în eroare a inamicului și atragerea atenției asupra provinciei Herson, urmată de contraofensiva din Harkov (Toroi 2024, 34).

Protecția forței

Impactul înzestrării cu sisteme HIMARS asupra funcției întrunite *protecția forței* poate fi înțeles, din punctul meu de vedere, prin prisma a două aspecte: unul pozitiv și unul negativ. Aspectul pozitiv este reprezentat, în principal, de capacitatea ridicată a sistemelor HIMARS de a combate eficient de la distanță sistemele de lovire ale inamicului, îndeosebi ale celor care reprezintă un risc ridicat la adresa structurilor de forțe proprii – așa cum sunt mijloacele tactice cu capabilități de utilizare a armelor de distrugere în masă.

Aspectul negativ ar fi, din punctul meu de vedere, necesitatea alocării de resurse suplimentare sau a unora special destinate, pentru siguranța nemijlocită și apărarea apropiată a sistemelor HIMARS, precum și pentru apărarea antiaeriană și antirachetă a acestora pe toată durata operației. Acest lucru este și o consecință a faptului că, așa după cum am precizat anterior, sistemele HIMARS disponibile unei grupări de forțe reprezintă ținte prioritare pentru orice potențial inamic.

Din perspectiva inamicului, funcția *protecția forței* este perturbată, în primul rând, de nevoia constantă de diminuare a efectelor unui potențial atac cu sisteme HIMARS, care poate avea loc la distanțe considerabile de aliniamentul de contact. Astfel, pentru protecția elementelor de infrastructură importante pentru inamic, a concentrărilor de forțe sau de resurse de orice tip ori pentru protecția altor diverse obiective din dispozitivul de luptă, inamicul va trebui să adopte unele măsuri specifice și să aloce resurse suplimentare (de război electronic sau de apărare antiaeriană și antirachetă) în vederea limitării riscului angajării cu sisteme HIMARS.

Operații informaționale (INFO OPS)

Dispunerea de sisteme HIMARS la nivelul grupării de forțe și folosirea lor cu succes pe parcursul operațiilor se poate realiza în cadrul *operațiilor informaționale* pentru a impulsiona voința de a lupta și moralul trupelor proprii. Un exemplu elementar în acest domeniu este promovarea succesului acțiunilor sistemelor HIMARS în rândul forțelor proprii. Totodată, înzestrarea forțelor proprii cu sisteme HIMARS și implicațiile acestui aspect, precum împingerea concentrărilor de resurse ale inamicului la distanțe mai mari față de linia frontului, pot avea efecte

demoralizatoare asupra structurilor de forțe ale acestuia aflate în zona de operații de la contact (Kosoy 2024).
Un alt aspect, menționat și în cadrul funcției întrunite *informații* este valorificarea statutului sistemelor HIMARS, de țintă prioritară pentru inamic, în cadrul planurilor de inducere în eroare a acestuia. Contribuția sistemelor HIMARS la degradarea capacității inamicului de a înțelege situația operațională poate fi semnificativă.

Ca element caracteristic funcției întrunite *operații informaționale* din perspectiva inamicului, menționez concentrarea acestuia pe aspecte de propagandă, promovând distrugerea sistemelor HIMARS (Tass 2024) sau maniera neconvențională de întrebuințare a lor – împotriva unor persoane sau obiective civile (Avia.Pro 2022). Perturbarea acestei funcții întrunite se poate realiza, în primul rând, prin conștientizarea aspectelor menționate, urmând a implementa măsuri de contracarare sau de valorificare a lor în cadrul operațiilor informaționale proprii.

Sustenabilitate
Din punctul de vedere al *sustenabilității*, înzestrarea cu sisteme HIMARS are un impact major asupra geometriei mediului de operații. Dacă din perspectiva operațiilor proprii, principala contribuție la sustenabilitate este, din punctul meu de vedere, combaterea sistemelor de sprijin prin foc care ar putea perturba fluxul de resurse, în ceea ce privește operațiile inamicului, sistemele HIMARS au demonstrat un potențial ridicat de a afecta sustenabilitatea acestora. Bătaia maximă la care sistemele HIMARS pot angaja precis și eficient ținte a fost intens valorificată (și mediatizată) în conflictul ruso-ucrainean pentru a lovi elemente de infrastructură, raioane de concentrare a forțelor, depozite de muniții sau bazele de antrenament ale soldaților ruși (Kosoy 2024). Am putut observa astfel că înzestrarea structurilor de forțe proprii cu sisteme HIMARS poate determina o revizuire a modului de dispunere a resurselor inamicului la distanțe considerabile față de linia frontului, pentru a le scoate de sub bătaia acestor sisteme.

Cooperarea civili-militari (CIMIC)
Avantajul folosirii de muniții care urmăresc, din punct de vedere constructiv, reducerea riscului producerii de victime sau pagube colaterale poate fi exploatat în cadrul acestei funcții întrunite, pentru consolidarea suportului cauzei proprii din partea populației civile aflate în zona de operații. De altfel, populația din teritoriul ocupat de inamic poate reprezenta o sursă importantă de informații privind utilizarea de echipamente militare sau desfășurarea unor activități de către forțele acestuia, informații care pot fi exploatate, inclusiv în planificarea și executarea misiunilor de foc cu sistemele HIMARS.

În ceea ce privește perturbarea funcției întrunite *cooperarea civili-militari* a inamicului, aduc în atenție relația de proporționalitate între aceste funcții ale părților aflate în conflict. Astfel, progresele obținute prin acțiunile forțelor proprii, desfășurate în domeniul funcțional al cooperării civili-militari, consolidează această funcție întrunită în favoarea propriei cauze și, în mod evident, în detrimentul cauzei inamicului.

Concluzii

Exploatarea cadrului operațional descris de funcțiile întrunite poate fi făcută dincolo de rolul lor de bază – instrumentul comandantului militar și al statului său major, – pentru a asigura o abordare cuprinzătoare a aspectelor unei operații. Având în vedere că modul de îndeplinire a funcțiilor întrunite într-o operație reprezintă și o descriere a capabilităților disponibile forței, se pot argumenta, pe baza lor, și unele nevoi noi, prin a căror soluționare se facilitează îndeplinirea misiunii, în condițiile mediului de confruntare actual.

Funcțiile întrunite pot constitui un cadru propice înțelegerii și valorificării potențialului capabilităților disponibile comandantului militar, însă, totodată, aceste funcții pot fundamenta cerințele structurilor de forțe naționale, având în vedere misiunile pe care acestea le au sau le pot avea într-un anumit context. Mai mult decât atât, conceptualizând îndeplinirea funcțiilor întrunite la nivelul unui potențial adversar sau al unui alt actor prezent în zona de operații, putem avea o percepție completă asupra potențialului capabilităților disponibile acestora, aspecte care pot fi valorificate atât în înțelegerea mediului de confruntare, în ansamblu, cât și în determinarea centrelor de greutate pentru entitățile vizate.

Prin exemplul folosit în cadrul lucrării – înzestrarea structurilor de forțe terestre naționale cu sisteme HIMARS –, am argumentat o modalitate utilă, din punctul meu de vedere, pentru fundamentarea modului de valorificare a unor capabilități existente sau a unora de perspectivă. Totodată, în elaborarea lucrării de față, am prezentat și am argumentat o viziune referitoare la impactul înzestrării structurilor de forțe armate naționale cu sistemele HIMARS, abordând contribuția sau influența acestora în îndeplinirea fiecărei funcții întrunite în parte, cu exemple din conflictul ruso-ucrainean în desfășurare.

Referințe

Avia.Pro. 2022. ”ВСУ показали особенность применения РСЗО Himars в условиях контрбатарейной борьбы” *(The AFU showed the peculiarity of using Himars MLRS in the conditions of counter-battery combat).* https://avia.pro/news/vsu-pokazali-osobennost-primeneniya-rszo-himars-v-usloviyah-kontrbatareynoy-borby.

BBC. 2022. ”Ukraine: What are Himars missiles and are they changing the war?” https://www.bbc.com/news/world-62512681.

Defence DataBase. 2024. ”M142 HIMARS multiple rocket launcher”. https://defencedb.com/profile_page.php?item_id=16.

Forțele Terestre Române. 2024. „Sistemul de rachete cu lansare multiplă M-142 HIMARS”. https://forter.ro/inzestrare/sistemul-de-rachete-cu-lansare-multipl%C4%83-m-142-himars.

Global Defense News. 2023. ”Using HIMARS Ukrainian forces destroy five Russian MSTA-S howitzers in key counter-offensive”. https://armyrecognition.com/focus-analysis-conflicts/army/conflicts-in-the-world/russia-ukraine-war-2022/using-himars-ukrainian-forces-destroy-five-russian-msta-s-howitzers-in-key-counter-offensive.

Goldstein, Lyle și Nathan Waechter. 2023. "The Diplomat". https://thediplomat.com/2023/06/china-considers-countermeasures-to-us-himars-missile-system/.

Kadam, Tanmay. 2022. "Kudos HIMARS! Russian Military Experts Say US Systems Are Confusing Counter-Battery Ops By Changing Trajectory". https://www.eurasiantimes.com/kudos-himars-russian-military-experts-say-us-systems-are-confusing-counter-battery-ops-by-changing-trajectory/.

Kosoy, Daniel. 2024. "HIMARS, Ukraine's Original Game Changer." *United24 Media*. https://united24media.com/war-in-ukraine/himars-ukraines-original-game-changer-1613.

Lockheed Martin. 2024. "Aerostar and Lockheed Martin open the first European HIMARS Sustainment Centre in Romania". https://news.lockheedmartin.com/2024-05-30-aerostar-and-lockheed-martin-open-the-first-european-himars-sustainment-centre-in-romania?_gl=1*1scrj9n*_gcl_au*NDM3NzExMjQwLjE3MzEwMDcxNzc.

Marquardt, Alex, Natasha Bertrand și Zachary Cohen. 2023. "Russia's jamming of US-provided rocket systems complicates Ukraine's war effort." *CNN*. https://edition.cnn.com/2023/05/05/politics/russia-jamming-himars-rockets-ukraine/index.html.

NATO. 2019. *Allied Joint Doctrine for the Conduct of Operations AJP-3*. NATO Standardization Office.

—. 2022a. *Allied Joint Doctrine AJP-01*. NATO Standardization Office.

—. 2022b. *Allied Joint Doctrine for Land Operations AJP-3.2*. NATO Standardization Office.

New Voice of Ukraine. 2023. "HIMARS strike destroys rare Yastreb-A counter-battery radar in Russian Rear – video". https://english.nv.ua/nation/video-of-himars-destroying-russian-yastreb-a-counter-battery-radar-in-donetsk-oblast-50436872.html.

Newsweek. 2024. "Strikes on Ukraine's Most Prized Assets Raise Alarm". https://www.newsweek.com/ukraine-russia-strikes-helicopters-abrams-bradleys-1879148.

Nistorescu, Claudiu-Valer. 2024. „Asimetrii generate de noile sisteme de armament și rolul lor în obținerea succesului pe câmpul de luptă. Efectele generate de sistemul HIMARS în conflictul din Ucraina." *Buletinul Universității Naționale de Apărare „Carol I"* 13 (3): 72-83.

Orjanu, Gheorghiță. 2023. „HIMARS deschide ușa. Artileria Armatei României a intrat în «clubul select» ASCA. SUA – rol cheie în primirea României în ASCA." *Defense Romania*. https://www.defenseromania.ro/himars-deschide-usi-artileria-armatei-romaniei-a-intrat-in-clubul-select-asca-sua-rol-cheie-in-primirea-romaniei-in-asca_622036.html.

SMG. 2011. *Doctrina Armatei României SMG-103*. București: MApN.

—. 2014. *Doctrina pentru operații întrunite a Armatei României SMG/ PF-3*. București: MApN.

Tass. 2024. "Russia's strike destroys four HIMARS launchers, 35 foreign personnel in Ukraine ooperation". https://tass.com/politics/1814677.

Toroi, George-Ion. 2024. "A theoretical analysis of the art of deception." *Strategic Impact*, No. 2: 25-47.

VPK News. 2023. "The Russian Armed Forces revealed the weak points of HIMARS". https://vpk.name/en/714706_the-russian-armed-forces-revealed-the-weak-points-of-himars.html.

BULETINUL
UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I"
https://buletinul.unap.ro

Complexitatea tranziției la nivelul operațiilor specifice luptei armate. Soluții pentru eficientizarea procesului

The Complexity of the Transition in Combat Operations and Potential Solutions to Streamline the Process

Lt.col.Dr. Claudiu-Valer NISTORESCU*
*Facultatea de comandă și stat major, Universitatea Națională de Apărare „Carol I"
e-mail: nistorescu_claudiu@yahoo.com

Abstract

Conflictele armate contemporane, precum cel din Ucraina, Fâșia Gaza sau Nagorno-Karabah, scot în evidență dificultatea operațiilor specifice luptei armate. În ciuda transparenței accentuate a câmpului de luptă, natura conflictului, marcat de fricțiune, incertitudine, violență și o letalitate crescută, subliniază rolul esențial al factorului uman. Omul rămâne, în continuare, principalul motor al procesului operațional, planificarea, pregătirea, execuția și evaluarea constantă a operațiilor militare purtând amprenta procesului uman de luare a deciziei.
În acest context, tranziția realizată la nivelul operațiilor specifice luptei armate se identifică drept unul dintre cele mai dificile procese, mai ales atunci când este neanticipat. Având în vedere sensibilitatea tranziției în cadrul operațiilor specifice luptei armate, analiza realizată își propune să identifice principalele vulnerabilități și riscuri ale procesului, factorii declanșatori și indicatorii care pun în evidență necesitatea realizării lui, dar și o serie de soluții pentru eficientizarea acestuia. Demersul științific este unul de tip calitativ și ia în considerare, empiric, impactul noilor tehnologii și sisteme de armament asupra desfășurării operațiilor specifice luptei armate.

The contemporary armed conflicts that have recently taken place in Ukraine, the Gaza Strip, and Nagorno-Karabakh serve to illustrate the inherent difficulties associated with combat operations. Despite the high degree of transparency on the battlefield, the nature of the conflict, characterized by friction, uncertainty, violence, and high lethality, underscores the pivotal role of the human factor. The operational process remains primarily driven by human decision-making, with the constant planning, preparation, execution, and evaluation of military operations shaped by the human decision-making process.
In this context, the transition during combat operations is identified as one of the most challenging processes, particularly when unanticipated. In light of the sensitivity of the transition in combat operations, the analysis seeks to identify the principal vulnerabilities and risks inherent to the process, the triggers and indicators that signal its necessity, as well as a series of solutions to enhance its efficiency. The scientific approach is qualitative and empirically oriented, with a focus on examining the impact of new technologies and weapon systems on the conduct of combat operations.

Cuvinte-cheie:
operații specifice luptei armate; tranziție; punct culminant; oportunitate tactică; poziție de avantaj.

Keywords:
combat operations; transition; culmination point; tactical opportunity; position of advantage.

Info articol
Primit: 11 octombrie 2024; Evaluat: 1 noiembrie 2024; Acceptat: 2 decembrie 2024; Disponibil online: 17 ianuarie 2025
Citare: Nistorescu, C.V. 2024. „Complexitatea tranziției la nivelul operațiilor specifice luptei armate. Soluții pentru eficientizarea procesului". *Buletinul Universității Naționale de Apărare „Carol I"*, 13(4): 98-113. https://doi.org/10.53477/2065-8281-24-41

Studiile și literatura de specialitate scot în evidență că unul dintre cele mai dificile aspecte ale operațiilor specifice luptei armate îl reprezintă *tranziția* de la o formă de luptă la alta, acest lucru având un impact direct asupra echilibrului dintre capabilitățile ofensive și cele defensive la nivelul forței (Jones, Palmer și Bermudez Jr. 2023). Acum, aproape 500 de ani, Machiavelli, în lucrarea sa *Principele*, sublinia această dificultate, afirmând că *„nu există subiect mai delicat, mai periculos sau mai incert în ceea ce privește succesul, decât orientarea unui lider către schimbare"* (Machiavelli 2012, 55). Afirmația lui rămâne pertinentă și astăzi, în ceea ce privește capacitatea liderilor de a accepta nevoia de schimbare și abilitatea acestora de a ghida entitatea subordonată către o tranziție eficientă de la o situație de luptă la alta.

Ambiguitatea luptei armate, oportunitatea, șansa sau lipsa ei impun adesea schimbarea formei de manifestare a acesteia. Tranziția, la nivelul operațiilor specifice luptei armate, poate fi o consecință a punerii în aplicare a planului de operații și are la bază o decizie de execuție, dar, totodată, ea poate fi impusă de schimbări ale situației operaționale neprevăzute, având la bază, în acest caz, o decizie de ajustare a operației. Astfel, această activitate poate fi întreprinsă fie în vederea exploatării unor oportunități tactice, fie din cauza insuficienței capacității de luptă a forțelor proprii. Primele abordări teoretice ale conceptului își au originea în perioada interbelică, ele fiind dezvoltate de armata germană. Respectând cerințele relației dialectice dintre apărare și ofensivă – relație descrisă de Clausewitz –, armata germană, într-unul dintre manualele sale de luptă, scotea în evidență faptul că *„situațiile impredictibile din timpul bătăliilor necesită adesea schimbarea formei de luptă. Trecerea de la atac la apărare poate avea loc atunci când se impune menținerea unei poziții cucerite sau în situația în care inamicul exercită o presiune mare asupra forțelor proprii"* (Finkel 2011, 77). În consecință, tranziția, la nivelul operațiilor militare specifice luptei armate, înseamnă schimbare și de cele mai multe ori, această schimbare este impusă și se realizează violent. Ea generează frustrare și fricțiuni la nivelul operației militare, impunând luarea unor decizii în timp scurt și recalibrarea formei și procedeelor de luptă. Mai mult decât atât, în situația în care comandantul nu este conștient de necesitatea tranziției și aceasta nu este realizată oportun, efectele pot fi devastatoare pentru forțele subordonate.

Descrierea tranziției ca și concept nu este tratată complex la nivelul doctrinei aliate. Totuși, *Doctrina pentru operațiile forțelor terestre – AJP 3-2* subliniază faptul că *„forțele trebuie să fie capabile să execute tranziția rapidă în cadrul întregului spectru al operațiilor și activităților tactice și de asemenea să exploateze mediul informațional pentru câștigarea unei poziții de avantaj"* (Allied Joint Publication, AJP-3.2 2022, A-V). În concluzie, putem desprinde ideea că tranziția presupune schimbare nu numai în cadrul operațiilor specifice luptei armate, ci și la nivelul temelor de campanie. *Manualul de tactică pentru operațiile forțelor terestre – ATP 3.2.1* identifică necesitatea ca forțele tactice să *„realizeze o tranziție rapidă de la o activitate tactică la alta cu scopul de a-și îndeplini obiectivele stabilite"* (Allied Tactical Publication, ATP-3.2.1 2022, 1-7). Aceeași publicație scoate în evidență faptul că *„atât comandantul structurii militare, cât și subordonații săi trebuie să fie pregătiți, deopotrivă mental și*

fizic, pentru a realiza tranziția rapidă între ofensivă, apărare și operații intermediare" (Allied Tactical Publication, ATP-3.2.1 2022, 1-14). Doctrina Armatei Statelor Unite subliniază că *„tranziția are loc atunci când comandantul, în urma unei evaluări a operației, decide că trebuie să schimbe elementul decisiv al operației și să treacă la o altă formă de luptă."* (Department of the Army, ADP 3-90 2019, 1-42).

Conform reglementărilor doctrinare și manualelor de luptă, necesitatea tranziției apare din diverse motive și nu doar ca un efect direct al culminării operației sau din cauza unui eșec temporar. Astfel, tranziția este inerentă în desfășurarea activităților pentru îndeplinirea misiunii și presupune fie schimbarea formei de luptă, fie trecerea de la operații de luptă la operații de stabilitate. Tranzițiile pot fi dificile, mai ales dacă sunt neanticipate și de aceea pe timpul planificării, comandanții, sprijiniți de statul major, identifică situațiile în care tranziția se poate produce, precum și indicatorii care informează asupra necesității ei, reducând astfel nivelul fricțiunii și dificultățile procesului de adaptare. Studiile de specialitate identifică următoarele situații în care tranziția are loc în cadrul unor operații militare (www.globalsecurity.org 2003):

1. tranziția de la operații specifice luptei armate (ofensivă și apărare) către operații de stabilitate; această situație presupune îndeplinirea obiectivelor stabilite și atingerea stării finale dorite, încetarea operațiilor de luptă și transferul treptat al responsabilității către autoritățile guvernamentale;
2. tranziția în cadrul operațiilor specifice luptei armate de la operații și acțiuni tactice ofensive la cele defensive și invers, incluzând o serie de operații intermediare.

Analiza efectuată vizează îndeosebi a doua situație, obținerea unor rezultate privind realizarea tranziției la nivelul operațiilor specifice luptei armate fiind un real beneficiu, în contextul desfășurării unui conflict convențional de mare amploare și intensitate în proximitatea granițelor României. Determinarea unor potențiale soluții pentru eficientizarea procesului se constituie în principalul obiectiv de cercetare a prezentului demers. Subsecvent acestui obiectiv, eforturile de cercetare au fost concentrate în vederea identificării factorilor declanșatori ai tranziției, descrierii rolului componentelor principale ale acesteia și impactului lor asupra mecanismelor de desfășurare a procesului, precum și a indicatorilor care avertizează asupra unei potențiale situații care impune realizarea tranziției. În acest sens, evaluarea a luat în considerare tranziția de la apărare la ofensivă și tranziția de la ofensivă la apărare.

Pentru orientarea și direcționarea activității de cercetare, ne-am propus să răspundem la următoarele întrebări cheie:

- Care sunt situațiile în care o structură tactică de forțe terestre este nevoită să recurgă la tranziție pe timpul desfășurării luptei armate?
- Care sunt componentele tranziției și ce impact au acestea asupra declanșării ei?
- Care sunt indicatorii care avertizează asupra culminării unei forțe militare (proximitatea atingerii punctului culminant de către aceasta) în operația ofensivă?

• Care sunt indicatorii care avertizează asupra culminării unei forțe militare (proximitatea atingerii punctului culminant de către aceasta) în operația defensivă?
• Care sunt potențialele măsuri ce trebuie întreprinse pentru e eficientiza procesul tranziției?

Obținerea unui răspuns la aceste întrebări de cercetare contribuie la realizarea unui tablou cuprinzător al fundamentelor și mecanismelor tranziției în cadrul operațiilor specifice luptei armate. Complexitatea problemei de cercetare, un rezultat intrinsec al complexității luptei armate, nu oferă posibilitatea efectuării unei analize exhaustive a subiectului. Cu toate acestea, rezultatele obținute pot fi utile comandanților și liderilor militari, precum și specialiștilor și teoreticienilor din domeniu.

Situațiile care impun realizarea tranziției la nivelul operațiilor specifice luptei armate

Executarea tranziției în cadrul operațiilor specifice luptei armate reprezintă o activitate care presupune riscuri ridicate și impune o sincronizare atentă a tuturor capabilităților disponibile și acțiunilor desfășurate. Tranziția de la o formă de luptă la alta are loc fie când forța angajată într-un anumit tip de operație nu o mai poate susține, fie când, datorită unei poziții de avantaj relativ, forțele proprii se află într-o situație în care pot prelua inițiativa. Edificatoare, în acest sens, este observația generalului englez Rupert Smith, care, în lucrarea sa *The Utility of Force*, sublinia că esența tuturor tacticilor și manevrelor și, în general, cea mai mare dilemă tactică constă în obținerea unui echilibru între necesarul de efort alocat pentru lovirea inamicului, în scopul obținerii obiectivelor ofensive și necesarul de efort depus pentru contracararea ripostelor acestuia (Smith 2019, 14). Prin aceasta, el subliniază importanța și necesitatea menținerii unui echilibru între capabilitățile ofensive și cele defensive pentru asigurarea succesului și evitarea înfrângerii. În consecință, la nivelul operațiilor tactice de luptă, identificăm următoarele situații în care comandanții militari trebuie să recurgă la tranziție:

➢ în ofensivă, când forțele proprii nu mai pot susține operația în curs de desfășurare și continuă acțiunile pe principalele direcții de înaintare;
➢ în ofensivă, când forțele proprii sunt nevoite să își consolideze obiectivele cucerite sau să facă o pauză operațională în vederea reluării ulterioare a operațiilor ofensive;
➢ în apărare, când forțele proprii se află într-o poziție de avantaj și pot prelua inițiativa, trecând la acțiuni ofensive contra unui inamic care nu mai poate desfășura operații defensive într-un mod coeziv, retrăgându-se;
➢ în apărare, când forțele proprii nu mai pot desfășura o apărare eficientă și sunt nevoite să se retragă.

În fiecare dintre situațiile enumerate anterior, realizarea tranziției are la bază materializarea unui cumul de factori care se raportează la situația operațională

a părților combatante. Astfel, de regulă, concretizarea unei poziții de avantaj pentru unul dintre combatanți este conectată direct sau indirect de existența unei vulnerabilități sau chiar a unui eșec al oponentului. În concluzie, inițierea tranziției este condiționată de factorii specifici fiecărei situații și depinde de capacitatea uneia dintre părți de a evalua corect indicatorii care informează asupra unei potențiale situații de schimbare.

Componentele tranziției și impactul lor asupra realizării procesului

Tranziția la nivelul operațiilor specifice luptei armate nu se concretizează numai în plan fizic, ci și în plan mental. Mai mult decât atât, conștientizarea de către comandanți a necesității realizării tranziției de la o formă de luptă la alta, acceptarea noii situații și asumarea unor riscuri se realizează, inițial, în plan mental. Astfel, în urma înțelegerii noii situații și a acceptării în plan mental a nevoii de schimbare, comandantul declanșează, prin decizia sa, realizarea tranziției în plan fizic. În acest sens, literatura de specialitate identifică două componente cheie ale tranziției: *componenta mentală* și *componenta fizică* (Baillergeon 2019, 176). Aceste componente generează divizarea procesului tranziției în două faze distincte, ele fiind unice, dar, totodată, interconectate.

a. Componenta mentală a tranziției

În faza sa inițială, schimbarea se realizează în plan mental, iar comandantul este principalul element declanșator al acesteia. În urma evaluării permanente a situației și a raportării capabilităților proprii la obiectivele propuse și capabilitățile inamicului, comandantul este cel care decide și inițiază tranziția. Tot în această fază, statul major, pe baza îndrumărilor comandantului, inițiază planificarea unei noi operații. Prin declanșarea unui nou proces de planificare, sunt transmise subordonaților semnalele necesare realizării în plan mental a schimbării. Factorii care stau la baza conștientizării nevoii de schimbare a formei de luptă sunt *oportunitatea tactică* pe câmpul de luptă și *punctul culminant* al operației.

Oportunitatea, fără a avea o definire clară, este eminamente de ordin tactic. Doctrina Armatei Statelor Unite subliniază conexiunea dintre oportunitatea tactică și existența unei poziții de avantaj relativ, oportunitatea tactică reprezentând „*o locație sau un set de condiții favorabile în cadrul zonei de operații ce îi pot conferi comandantului din teren fie libertatea de acțiune temporară pentru a-și crește puterea de luptă în comparație cu cea a inamicului, fie posibilitatea de a-l determina pe inamic să accepte riscuri care să-l pună într-o situație dezavantajoasă*" (Department of the Army, ADP 3-0 2019, 4-5). În consecință, oportunitatea tactică este efemeră și presupune existența în timp și spațiu a unei situații avantajoase care poate fi exploatată în scopul lovirii vulnerabilităților inamicului și obținerii ulterioare a succesului. În operațiile tactice, poziția de avantaj se materializează sub diferite aspecte (Department of the Army, FM 3-0 2017, 1-18):

• **fizic/geografic** – poziționarea elementelor de manevră proprii, în raport cu cele ale inamicului, menținerea unor puncte cheie ale terenului, controlul unor zone destinate refacerii capacității de luptă etc.;
• **temporal** – devansarea inamicului la nivelul ciclului decizional, ritmul operației și viteza de acțiune, viteza fluxului informațional, eficiența relației *sensor to shooter* etc.;
• **al libertății de acțiune** – menținerea securității liniilor de comunicații, oportunitatea exploatării unor capabilități de lovire, dispuse în afara razei de acțiune a armamentului inamicului, protecția zonelor de spate, crearea unui sistem propriu de tip A2AD etc.;
• **al moralului și voinței de luptă** – legitimitatea cauzei, leadershipul eficient, alocarea rațională a resurselor, înzestrarea cu sisteme de armament performante, nivelul ridicat al instruirii și al interoperabilității etc.;
• **obținerea unei puteri de luptă superioare** – rezultată din superioritatea razei de acțiune, acurateții și letalității sistemelor de armament, concentrării forțelor sau inducerii în eroare a inamicului.

Oportunitatea tactică poate apărea în cadrul atât al operației ofensive, cât și al operației de apărare. Ea apare în timpul luptei, în condiții de incertitudine, ambiguitate și haos și poate fi un rezultat al acțiunilor forțelor proprii sau erorilor inamicului. Abilitatea de a exploata oportunitățile apărute depinde de flexibilitatea și de libertatea de gândire a comandantului, de inițiativa, de viteza și îndrăzneala acestuia, dar și a comandanților subordonați. Declanșarea și executarea unei acțiuni pentru exploatarea unei potențiale oportunități presupun existența unor riscuri. Aceste riscuri trebuie asumate în mod calculat de către comandantul structurii care urmează a fi angajat în luptă, dar și de către superiorul acestuia. Alocarea suficientă de resurse și o superioritate calitativă a înzestrării sprijină asumarea riscului de către comandant.

Exploatarea unei oportunități tactice generează, de regulă, alte oportunități tactice care pot *„crea noi cursuri de acțiune sau pot arăta noi direcții de exploatat în atingerea obiectivului eșalonului superior mai devreme sau cu un efort mai mic"* (Statul Major al Forțelor Terestre, FT 2 2019, 95). De regulă, oportunitatea este asociată operațiilor tactice ofensive și depinde intrinsec de abilitatea forțelor proprii de a menține inițiativa. Dar șansa de a exploata o oportunitate poate apărea și în apărare. Executarea unui contraatatac la momentul și locul potrivit, scoaterea forțelor proprii dintr-o situație dezavantajoasă, prevenirea înfrângerii sau distrugerii forțelor proprii depind direct de exploatarea unei oportunități tactice.

Punctul culminant al operației, al doilea factor determinant al tranziției, reprezintă acel punct în care o forță nu mai poate continua cu succes operația în care este angajată (Allied Joint Publication, AJP-5 2019, 3-12) și trebuie să schimbe forma de luptă (Department of the Army, ADP 3-0 2019, 2-9). De regulă, punctul culminant este asociat cu operația ofensivă, dar acesta își găsește aplicabilitatea și în cadrul operației de apărare (Friedman 2017, 105). De aceea conceptul trebuie abordat

din perspectiva atât a atacatorului, cât și a apărătorului (Weiss 2021, 263) Astfel, în cadrul operațiilor tactice ofensive, o forță atinge punctul culminant atunci când nu mai poate susține operația ofensivă și trebuie să treacă la apărare pentru a evita înfrângerea. În același timp, în desfășurarea operațiilor tactice defensive, o forță atinge punctul culminant atunci când nu mai este capabilă să se apere cu succes și să creeze condițiile trecerii la contraofensivă. În această din urmă situație, pentru evitarea înfrângerii, forța aflată în apărare trebuie întărită, scoasă din luptă sau trebuie să execute operații de retragere.

Analizând aceste două contexte în care o forță tactică poate experimenta atingerea punctului culminant, identificăm punctual principalele cauze care determină respectiva situație.

TABEL NR. 1

Factori generatori ai punctului culminant în operațiile specifice luptei armate

ÎN CADRUL OPERAȚIEI OFENSIVE STRUCTURA TACTICĂ	ÎN CADRUL OPERAȚIEI DEFENSIVE STRUCTURA TACTICĂ
Nu mai realizează o putere de luptă superioară forței aflate în apărare.	Nu mai dispune de puterea de luptă necesară pentru a stopa ofensiva inamicului.
Nu mai dispune de forțe pentru a fi introduse în luptă, în scopul dezvoltării operației ofensive, pierzând astfel inițiativa.	Nu poate organiza o apărare coezivă.
Nu mai poate susține din punct de vedere logistic continuarea atacului.	Este în situația de a fi copleșită cantitativ de forțele inamicului aflat în ofensivă.

În cadrul operațiilor specifice luptei armate, forțele tactice se pot confrunta cu unul sau mai mulți factori cauzatori ai culminării operației, concomitent sau secvențial. Indiferent de situație, rolul comandantului este esențial în evaluarea riscului și a posibilității de a atinge punctul culminant de către forțele subordonate. Acest fapt va sprijini semnificativ procesul tranziției. În caz contrar, dacă acest risc nu este identificat la timp, tranziția se va realiza necorespunzător și cu efecte devastatoare asupra forței tactice angajate în operație. De exemplu, dacă comandantul unei structuri tactice care execută acțiuni ofensive nu sesizează la timp limitările severe în a dezvolta acțiunile prin introducerea unor forțe proaspete în luptă, acest lucru poate genera o vulnerabilitate. Vulnerabilitatea respectivă poate fi exploatată de către inamic, odată ce acesta identifică atingerea punctului culminant de forțele proprii. Executarea unui contraatac de către acesta poate surprinde forțele brigăzii într-o postură și într-o locație nefavorabilă respingerii lui. Tot comandantul, pe baza informațiilor avute, a analizelor și estimărilor statului major, identifică, în timp și spațiu, posibilitatea ca inamicul să ajungă în punctul culminant al operației sale. Determinarea acestui fapt se poate constitui într-o oportunitate valoroasă și asigură premisele preluării inițiativei de către forțele proprii și obținerii ulterioare a succesului. Neconștientizarea situației sau indecizia poate duce la pierderea oportunității de a lovi inamicul, în timp ce acesta se află într-o poziție dezavantajoasă.

Analiza structurii operațiilor specifice luptei armate, precum și a etapelor principale ale acestora permite determinarea mai multor indicatori, care pun în evidență situațiile în care o forță tactică atinge sau este pe cale să atingă punctul culminant

al operației. În continuare, este prezentată o listă a respectivilor indicatori și a posibilelor măsuri care se impun a fi luate, în situația apariției lor atât pentru evitarea culminării, cât și pentru exploatarea unor oportunități. Lista este departe de a fi completă și trebuie subliniat faptul că un inamic adaptiv și inteligent va căuta să ascundă acești indicatori.

TABEL NR. 2

Indicatori ai punctului culminant al unei forțe aflate în ofensivă

INDICATOR	MĂSURI
Obținerea de informații referitoare la inițierea unor acțiuni defensive: consolidarea unor aliniamente cucerite, retragerea pe aliniamente favorabile, extinderea dezvoltării frontale a unităților din eșalonul întâi	Interzicerea prin foc și manevră a acțiunilor de consolidare
Reducerea drastică a *tempoului* acțiunilor ofensive	Distrugerea coerenței operației ofensive prin lovirea selectivă a elementelor de comandă și control
Insuficiența realizării concentrării de forțe în cadrul atacurilor pe direcțiile principale de ofensivă	Interzicerea inamicului să disloce forțe din alte zone de operații
Capturarea unui număr mare de prizonieri din cadrul forței aflate în ofensivă sau evaluările proprii a ratei mari a pierderilor inamicului pe câmpul de luptă	Intensificarea efortului apărării pentru creșterea intensității loviturile în zonele de operații afectate
Indicatori ai lipsei de sincronizare a funcțiilor luptei în cadrul atacurilor executate de inamic	Executarea de lovituri precise care să fragmenteze coerența acțiunilor de luptă
Identificarea în zona de dispunere a eșalonului întâi a unor forțe a căror destinație era cunoscută ca făcând parte din rezervă	Identificarea opțiunilor pentru posibilitatea unei eventuale schimbări a formei de luptă de către forțele proprii
Interceptarea liniilor de comunicații de către forțele proprii și blocarea fluxului logistic pentru unitățile din eșalonul întâi ale inamicului	Dislocarea forțelor și sistemelor de armament atât pentru protejarea flancurilor proprii, cât și pentru realizarea unei eventuale încercuiri a inamicului
Descoperirea de către forțele aflate în apărare a unei cantități mari de echipamente și tehnică de luptă abandonate	Intensificarea loviturilor asupra inamicului, pregătiri pentru schimbarea formei de luptă

TABEL NR. 3

Indicatori ai punctului culminant al unei forțe aflate în apărare

INDICATOR	MĂSURI
Informații și rapoarte privind pătrunderi ale forțelor inamicului în ZO ale unităților vecine	Cereri de informații/clarificări de la eșalonul superior și privind necesitatea de a redisloca forțele proprii, inclusiv sistemele principale de armament
Informații și rapoarte privind capturarea și ocuparea de către inamic a unor puncte cheie din zona de spate a forțelor proprii	Deplasarea rapidă a rezervelor pentru contracararea acestor acțiuni
Rapoarte privind moralul scăzut al militarilor și evidenta epuizare fizică și psihică a acestora	Înlocuiri eșalonate ale forțelor, contracararea acțiunilor de subminare a voinței de luptă, întreprinse de inamic
Neutralizarea sistemelor de artilerie și rachete antiaeriene ale forțelor proprii	Redistribuirea sistemelor de armament disponibile, solicitarea de sprijin din partea eșalonului superior
Diminuarea drastică a PL a unităților din eșalonul doi destinate executării contraatacurilor	Solicitarea de sprijin din partea eșalonului superior pentru reconstituirea rezervelor
Angajarea eșalonului doi sau a rezervelor, urmată de imposibilitatea regenerării sau înlocuirii acestora	Conștientizarea culminării și solicitarea scoaterii din luptă
Lovirea și distrugerea sistemului logistic	Conștientizarea culminării și solicitarea scoaterii din luptă
Creșterea semnificativă a pierderilor, în urma atacurilor inamicului	Solicitări de înlocuiri ale forțelor și sistemelor de armament, dislocarea principalelor sisteme de armament pe direcțiile principale de pătrundere
Indicii și informații privind concentrările de forțe superioare ale atacatorului pe direcțiile principale de ofensivă	Repoziționarea forțelor și a principalelor sisteme de armament, informarea eșalonului superior

Acești indicatori sunt determinați de statul major în cadrul procesului de planificare a operației, încadrându-se în *Cerințele critice de informații ale comandantului (Commander's Critical Information Requirements/CCIR)*, care reprezintă acea „cerință de informații identificată de comandant și statul major ca fiind esențială pentru facilitarea luării deciziei în timp util" (Statul Major al Forțelor Terestre, FT 2 2019, 22). Mai exact, indicatorii respectivi stau la baza *Cerințelor de informații*

ale forțelor proprii (Friendly Forces Information Requests/FFIR) și *Elementelor de informații critice despre forțele proprii (Essential Enemy Friendly Information/EEFI*). FFIR desemnează acele informații pe care comandantul trebuie să le cunoască referitor la situația forțelor proprii, iar EEFI reprezintă acele informații care trebuie ascunse de inamic. Odată stabiliți în procesul de planificare, indicatorii trebuie monitorizați constant pentru a furniza comandantului avertizări asupra situației, inclusiv proximitatea culminării forțelor proprii. Nu în ultimul rând, comandantul și statul său major trebuie să țină cont de posibilitatea ca inamicul să desfășoare operații de inducere în eroare și ca anumiți indicatori ai punctului culminant să nu furnizeze informații reale referitor la starea operațională a capabilităților inamice. De aceea un imperativ al procesului operațional desfășurat de forțele proprii îl reprezintă elaborarea de *„proceduri eficiente de contracarare a acțiunilor de inducere în eroare, desfășurate de adversarii lor, pentru ca îndeplinirea propriei misiuni să nu fie periclitată."* (Toroi și Stanciu 2023).

Cu certitudine identificarea și exploatarea oportunităților tactice pe câmpul de luptă pot genera succesul pe câmpul de luptă. Determinarea punctului culminant al inamicului și identificarea riscului crescut de atingere a propriului punct culminant pot face, de asemenea, diferența dintre victorie și înfrângere. Exemplele din trecut nu sunt puține și subliniază faptul că *„unul dintre cele mai dificile lucruri pentru un comandant este să admită propria înfrângere sau cu alte cuvinte imposibiltatea de a obține succesul"* (Baillergeon 2019, 181). Acest lucru este adevărat mai ales pentru un comandant aflat în ofensivă și care va accepta cu greu, în plan mental, imposibilitatea atingerii obiectivelor inițiale. În iarna anului 1994, comandanții forțele ruse, angajate în asaltul asupra orașului Groznîi, nu au conștientizat riscul la care se expuneau și nu au acceptat neputința cuceririi orașului. Frustrarea și ignorarea indicatorilor punctului culminant au condus la dezastrul forțelor mecanizate rusești: *„în câteva ore unitățile rusești au fost blocate pe străzile orașului, blindatele lor distruse de inamicul care trăgea nestingherit de pe acoperișurile clădirilor și de la demisoluri, poziții care nu puteau fi neutralizate de loviturile tancurilor"* (Oliker 2001, 13). După mai mult de 20 de ani, *Institute for the Study of War* (ISW), într-una dintre analizele sale privind desfășurarea conflictului din Ucraina, sublinia că *„forțele ucrainene au înfrânt campania rusească în faza ei inițială. Această campanie ce a avut ca scop cucerirea, printr-o serie de operații mecanizate și de desant aerian, orașele Kiev, Harkov, Odessa și alte localități importante ale Ucrainei, pentru a forța o schimbare guvernamentală, a eșuat. Operațiile ofensive au culminat* (la data realizării raportului – nota autorului). *Forțele rusești continuă să realizeze succese minore, dar cel mai probabil sunt incapabile să își atingă obiectivele inițiale în acest mod."* (Kagan, Barros și Stepanenko 2022). Câteva zile mai târziu, același institut de cercetare publica un studiu referitor la cauzele culminării ofensivei rusești din zona Kievului, unul dintre indicatorii elocvenți fiind întreprinderea unor acțiuni specifice apărării, inclusiv plantarea de câmpuri de mine (Kagan 2022). Câteva luni mai târziu, forțele rusești surprinse de contraofensiva ucraineană din Harkov reușeau să evite încercuirea la Izyum și, implicit, o înfrângere catastrofală (Kofman și Evans 2022). Același lucru avea să se întâmple și în zona de operații Herson, comandanții ruși retrăgându-și

forțele pe malul stâng al Niprului, poziția de avantaj a forțelor ucrainene fiind dificil de contestat la acel moment (Hird și alții 2022)

Punctul culminant al operației și oportunitatea tactică sunt interconectate în timp și spațiu. Ele joacă un rol important în declanșarea tranziției, inițial, în plan mental și, ulterior, în plan acțional. Modul în care aceste caracteristici ale acțiunii militare sunt gestionate influențează în mod direct rezultatul operației tactice. În acest sens, atingerea punctului culminant de către forțele proprii reprezintă nu numai pierderea inițiativei și schimbarea formei de luptă, ci și o oportunitate pentru inamic. Dacă acesta devine conștient de inevitabilitatea atingerii punctului culminant de către forțele proprii, își va intensifica eforturile pentru exploatarea situației create. De aceea protejarea informațiilor referitoare la acest eveniment și mascarea indicatorilor aferenți lui constituie o prioritate pentru comandantul forțelor proprii. În aceeași măsură, atingerea punctului culminant de către inamic reprezintă o oportunitate pentru forțele proprii. În concluzie, determinarea situațiilor în care forțele proprii sau forțele inamicului pot atinge punctul culminant reprezintă o prioritate a procesului de planificare a operației.

b. Componenta fizică a tranziției

A doua componentă cheie a tranziției este de natură fizică și reprezintă totalitatea acțiunilor întreprinse pentru pregătirea și executarea tranziției în plan tactic-operativ de la o formă de luptă la alta (Baillergeon 2019, 175). Raportându-ne la această componentă, analiza va lua în considerare tranziția de la ofensivă la apărare și tranziția de la apărare la ofensivă, evidențiind factorii principali pe care comandantul și statul său major trebuie să-i ia în considerare, în scopul eficientizării procesului.

➢ *Realizarea tranziției de la ofensivă la apărare*

Tranziția de la ofensivă la apărare este solicitantă, deopotrivă în plan mental și fizic, comandanții și forțele subordonate fiind nevoiți să își reconfigureze operațiile și să schimbe forma de luptă, în condițiile desfășurării acțiunilor inițiale. Dificultatea tranziției de la ofensivă la apărare este rezultatul interacțiunii următorilor factori:

- nevoia adoptării unei posturi defensive este generată de culminarea operației ofensive sau în scopul evitării culminării acesteia;
- reorganizarea dispozitivului de luptă pentru apărare constituie o provocare, având în vedere dispersarea forțelor;
- necesitatea identificării și ocupării terenului care să permită executarea operației de apărare;
- moralul scăzut al forțelor, cauzat de apariția sentimentului de „înfrângere", odată cu oprirea acțiunilor defensive.

Specialiștii și teoreticienii militari au identificat două principale metode care permit unei forțe aflate în ofensivă să treacă la apărare într-un mod algoritmizat (Department of the Army, FM 3-90 2023, 3-12). Primul procedeu presupune ca, în momentul în care comandantul conștientizează că operația ofensivă nu mai poate fi susținută, forțele de la contact să execute acțiuni ofensive cu obiectiv limitat, în

scopul cuceririi unor puncte cheie din teren care să permită organizarea ulterioară a dispozitivului de apărare. Această metodă prezintă atât avantaje, cât și dezavantaje. În ceea ce privește avantajele, procedeul facilitează realizarea unei adâncimi mai mari a dispozitivului de apărare, câștigarea de timp pentru forțele principale, concomitent cu menținerea permanentă a contactului cu inamicul. Dezavantajul major este reprezentat de dificultatea executării acțiunilor ofensive cu caracter limitat de către forțele de la contact, cu scopul de a crea o zonă de acoperire. Al doilea procedeu prin care tranziția de la ofensivă la apărare se poate realiza presupune organizarea zonei de acoperire pe aliniamentul pe care forțele aflate în ofensivă au fost oprite, facilitându-se deplasarea către înapoi a forțelor principale, pentru organizarea apărării pe un aliniament puternic în teren. Principalele avantaje ale procedeului implică existența posibilității de a organiza apărarea pe o formă tare din teren, exceptând nevoia de a angaja parte din forțe într-un teren necunoscut. În același timp, dezavantajele acestui procedeu implică lipsa de adâncime și nevoia de coordonare a acțiunilor de trecere prin dispozitivul forțelor proprii.

În situația în care forțele proprii sunt în ofensivă și comandantul realizează faptul că este aproape de culminare și tranziția este necesară, acesta poate concentra efectele sistemelor de armament, în scopul:

- ocupării unor puncte cheie din teren care să-i permită organizarea apărării pe un aliniament favorabil, oferindu-i, totodată, adâncime dispozitivului de luptă;
- sprijinirii dezangajării unor forțe aflate în contact și care nu mai dispun de suficientă putere de luptă pentru a rupe contactul;
- lovirii forțelor inamicului care se pregătesc pentru executarea contraatacului;
- protecției antiaeriane a forțelor proprii în timpul realizării înlocuirilor și regrupărilor;
- realizării unei concentrări de sisteme antitanc pentru stoparea unor atacuri cu blindate ale inamicului pentru a realiza breșe pe perioada organizării dispozitivului de apărare de către forțele proprii.

În funcție de situație, comandantul forțelor proprii va opta pentru unul dintre cele două procedee, luând în considerare riscurile aferente, capabilitatea forțelor proprii de a realiza eficient tranziția, sprijinul acordat de eșalonul superior, tipul de operație care urmează a fi desfășurat, acțiunile inamicului.

➢ *Realizarea tranziției de la apărare la ofensivă*

Tranziția de la apărare la ofensivă se realizează *„anticipând când și unde forțele inamicului vor atinge punctul culminant sau vor avea nevoie de o pauză operațională înainte de a putea continua operația.*" (Department of the Army, FM 3-90 2023, 8-24). Pentru ca o forță aflată în apărare să poată trece eficient la ofensivă, schimbând forma de luptă, o serie de condiții trebuie îndeplinite: inamicul a pierdut inițiativa și nu mai dispune de forțe suficiente pentru dezvoltarea operațiilor; inamicul nu mai reușește să realizeze o superioritate aeriană pe direcțiile principale de ofensivă; puterea de luptă a inamicului nu se mai realizează la un nivel superior față de cea a forței aflate în apărare.

Comandantul forței aflate în apărare dispune de o scurtă fereastră de oportunitate pentru a trece la ofensivă și pentru a exploata dezavantajul temporar în care se află atacatorul. Oportunitatea de a trece la ofensivă depinde direct de disponibilitatea capabilităților de neutralizare a apărării antiaeriene a inamicului și a apărării antiblindate pe principalele direcții de ofensivă. Constituirea eșalonului doi și a rezervelor constituie, de asemenea, o premisă pentru schimbarea formei de luptă. Odată ce decizia este luată, comandantul structurii tactice are două opțiuni pentru a schimba forma de luptă: restructurarea dispozitivului de luptă și trecerea la ofensivă cu forțele aflate la contact; înlocuirea forțelor aflate în contact și trecerea la ofensivă cu forțele din eșalonul al doilea (Department of the Army, FM 3-90 2023, 8-25).
Ambele situații prezintă atât avantaje, cât și dezavantaje și presupun concentrarea forțelor pe anumite direcții, în scopul realizării unui raport de forțe favorabil. De multe ori, acest lucru implică predarea unor zone de operații către alte forțe sau menținerea acestora sub control propriu, cu un minim de forțe care să poată preveni eventuale pătrunderi ale inamicului. Primul procedeu presupune folosirea forțelor aflate deja în contact cu inamicul, el având o serie de avantaje:

- timpul necesar trecerii la ofensivă este mai mic decât în situația înlocuirii forțelor de la contact, acest lucru permițând exploatarea oportunității create, fără a acorda inamicului suficient timp pentru consolidarea apărării;
- procedeul este mai puțin complicat, deoarece nu implică coordonarea înlocurii forțelor (fie că vorbim despre o înlocuire pe poziție sau despre o înlocuire prin depășirea forțelor aflate la contact);
- forțele de la contact înțeleg și se raportează la situația tactică existentă mai bine decât o pot face forțele nou introduse în luptă;
- din perspectivă umană, forțele aflate deja în contact au dobândit deja un „feeling" despre maniera în care inamicul acționează și sunt conștiente de punctele tari și de vulnerabilitățile acestuia.

Totodată, alegerea acestui procedeu presupune și o serie de dezavantaje:

- planificarea și pregătirea operației ofensive, concomitent cu executarea acțiunilor defensive curente sunt extrem de solicitante atât pentru statul major, cât și pentru subordonați;
- din cauza acțiunilor executate până la momentul trecerii la ofensivă, există un risc ridicat ca forțele de la contact să nu fie în cea mai bună stare fizică și psihică;
- o parte dintre echipamentele și sistemele de armament ale forțelor de la contact pot fi neoperaționale, iar forțele aflate deja în contact pot avea dificultăți de natură logistică; în consecință, se impune înlocuirea echipamentelor și armamentului esențial, chiar suplimentarea acestora și, deopotrivă, realizarea stocurilor logistice.

Al doilea procedeu presupune trecerea la ofensivă cu forțe care nu se află în contact cu inamicul. De regulă, ele sunt generate de eșaloanele 2 ale marilor unități de nivel brigadă sau divizie, ori de unități aflate în rezervă. Există o serie de avantaje ale acestui procedeu:

- forțele care nu se află în contact direct cu inamicul vor fi într-o condiție fizică și mentală mult mai bună decât cele deja angajate în operație;

- forțele neangajate în operație nu ar trebui să aibă probleme de natură logistică;
- planificarea operației se face în afara contactului și nu presupune executarea și conducerea unor alte acțiuni.

Ca dezavantaje, identificăm:

- înlocuirea forțelor de la contact presupune un timp mai mare necesar trecerii la ofensivă;
- realizarea unei aglomerări mari de forțe pe itinerariile de afluire și defluire din zona de contact, precum și în zona de contact; acest lucru impune măsuri stricte de coordonare a forțelor, dar și riscuri mai mari, inamicul identificând mult mai ușor înlocuirile și concentrările de forțe;
- în situația înlocuirii forțelor prin procedeul introducerii în luptă, forțele care trec la ofensivă au un timp redus pentru a se conecta direct la situația tactică existentă.

Aflate în apărare, de regulă, forțele proprii nu dețin inițiativa și trebuie să-și utilizeze eficient sistemele de armament din dotare, în scopul forțării inamicului să eșueze în atacul lor. Astfel, comandanții trebuie să aibă în vedere:

- lovirea blindatelor inamicului pe direcțiile principale de ofensivă;
- lovirea eșalonului doi în raioanele de dispunere, în timpul apropierii de aliniamentul de contact și în timpul introducerii în luptă;
- lovirea sistemului logistic;
- protecția antiaeriană a forțelor proprii, dispuse în raioanele de dispunere (eșalonul doi), pentru a menține opțiunea executării unui contraatac și trecere la contraofensivă;
- executarea unor acțiuni ofensive cu caracter limitat care să permită cucerirea unor puncte cheie din teren care să faciliteze, ulterior, trecerea la ofensivă.

Ca și concluzie, indiferent de procedeul ales de comandant pentru a realiza tranziția de la apărare la ofensivă, scopul operației, sarcinile cheie și starea finală trebuie transmise clar forțelor subordonate. De asemenea, comandantul, sprijinit de statul său major, trebuie să aibă în vedere următoarele aspecte pentru executarea operației ofensive: elaborarea schemei de manevră, operațiile în adâncime pentru obținerea controlului asupra punctelor cheie din teren și pentru slăbirea puterii de luptă a inamicului, securitatea flancurilor și a zonei de spate, operația decisivă care să lovească centrul de greutate al inamicului, precum și menținerea capabilității de a dezvolta ofensiva, operații de mobilitate și contramobilitate, generarea permanentă a rezervelor, alocarea judicioasă a sistemelor de armament pentru realizarea efectelor dorite pe câmpul de luptă.

Concluzii

Lupta armată, prin natura ei, rămâne un fenomen uman unic, marcat, totodată, de caracterul mereu în schimbare al războiului. Tranziția și nevoia de schimbare, la fel ca principiile operațiilor, rămân o constantă a luptei armate și depind,

deopotrivă, de imuabilitatea naturii acesteia din urmă, dar și de caracterul variabil al fenomenului amintit.
Tranziția, prin componentele sale, mentală și fizică, se distinge ca un proces extrem de sensibil la nivelul luptei armate, generator de frustrare, fricțiune și de o inerentă creștere a riscului. Comandantul, în rolul său de promotor al procesului operațional, înțelegând contextul operațional și vizualizând efectele care trebuie obținute, direcționează și coordonează eforturile forțelor din subordine, în scopul efectuării eficiente a procesului tranziției. El, ca principal factor de decizie, este cel care inițiază tranziția, indiferent dacă aceasta vine din nevoia exploatării unei oportunități sau din cea a evitării punctului culminant. De aceea exprimarea clară a intenției comandantului este esențială pentru succesul tranziției, deopotrivă când se realizează de la apărărare la ofensivă, sau de la ofensivă la apărare. Totodată, având în vedere incertitudinea și riscurile inerente unei situații care presupune o schimbare în postura operațională, comandantul trebuie să asigure un climat favorabil realizării acesteia, *comanda misiunii* fiind un instrument eficient pentru a conferi autoritatea și libertatea de acțiune, necesară comandanților subordonați. Numai o filozofie de comandă centrată pe încredere reciprocă, profesionalism și datoria comandanților subordonați de a acționa, încadrându-se în intenția eșalonului superior, creează premisele pentru obținerea succesului sau pentru evitarea înfrângerii.

Analiza realizată, pornind de la o interogare temeinică a literaturii de specialitate și explorând dimensiunile luptei armate, în contextul noilor tendințe și tehnologii care se manifestă în cadrul conflictelor contemporane, oferă un răspuns întrebărilor de cercetare. Aceste răspunsuri se materializează într-o serie de rezultate care pot fi benefice comandanților nivelului tactic în realizarea procesului operațional, în toate fazele acestuia – planificare, pregătire, execuție și evaluare.

În primul rând, explorând direcțiile de cercetare aferente obiectivelor propuse, am identificat potențialele situații în care tranziția se poate manifesta la nivelul luptei armate. Analiza principalelor componente ale tranziției a contribuit la determinarea mecanismelor de realizare a procesului, creând, totodată, oportunitatea de a identifica opțiuni pentru îmbunătățirea procesului. Rezultatele cercetării indică faptul că succesul în cadrul componentei fizice (acționale) a tranziției depinde direct de modul în care este gestionată dimensiunea mentală a procesului. De asemenea, rezultatele cercetării scot în evidență că, atât în situația exploatării unei oportunități, cât și în cazul abordării punctului culminant, decizia comandantului este crucială. De aceasta depinde abilitatea forțelor din subordine de a executa acțiunile necesare tranziției. În consecință, succesul sau înfrângerea dezastruoasă a forțelor proprii este influențată de abilitatea comandantului de a exploata o poziție de avantaj sau de a crea una, atunci când ea nu există. Oportunitatea vine ca un rezultat al existenței în spațiu și timp a unei poziții de avantaj, dar în același timp, evitarea punctului culminant este influențată de obținerea temporară a acesteia. Din această perspectivă, trebuie conștientizat faptul că, în luptă, acele „ferestre de oportunitate", care oferă un avantaj relativ, sunt limitate în timp și trebuie exploatate rapid astfel încât obiectivele stabilite să fie atinse.

Identificarea unor inicatori ai punctului culminant informează comandantul și sprijină decizia acestuia pe timpul execuției, în scopul limitării efectelor situațiilor critice sau exploatării oportunităților. Mai mult decât atât, respectivii indicatori pot sprijini comandantul și statul său major în timpul procesului de planificare, determinarea anticipată a situațiilor critice sau a potențialelor oportunități facilitând o tranziție eficientă. Utilizarea eficientă a sistemelor de armament din dotarea structurii tactice de forțe terestre poate facilita procesul de tranziție. Superioritatea tehnologică asigură premisele câștigării unei poziții relative de avantaj. De aceea, în situația în care eșalonul superior dispune de capabilități superioare din punct de vedere calitativ, inclusiv de noi sisteme de armament, structurile înzestrate cu acestea trebuie alocate în sprijinul forțelor care inițiază tranziția, indiferent de situația manifestării acesteia.

În final, dorim să accentuăm, încă o dată, că realizarea tranziției în cadrul operațiilor specifice luptei armate reprezintă într-adevăr o provocare și, deopotrivă, un test pentru comandantul structurii tactice de forțe terestre. Implicațiilor de natură tactic-operative inerente acestui proces li se adaugă probleme generate de factorul civil. Fluxurile de refugiați, victimele colaterale, asigurarea sprijinului umanitar îngreunează operațiile militare și, implicit, procesul tranziției. De aceea comandantul trebuie să acorde o atenție deosebită atât aspectelor militare, cât și celor civile. În acest sens, trebuie evaluat permanent impactul acțiunilor militare, îndeosebi al sistemelor de armament, în ceea ce privește riscul producerii victimelor și pagubelor colaterale.

Referințe

Allied Joint Publication, AJP-5. 2019. *Allied Joint Doctrine for the Planning of Operations.* Bruxel: NATO Standardization Office (NSO).

Allied Join Publication, AJP-01. 2022. *Allied Joint Doctrine.* Edition F, Version 1. Bruxel: NATO Standardization Office (NSO).

Allied Joint Publication, AJP-3.2. 2022. *Allied Joint Doctrine for Land Operations.* Edition B. Bruxelles: NATO Standardization Office (NSO).

Allied Tactical Publication, ATP-3.2.1. 2022. *Allied Land Tactics.* Edition C, Version 1. Brussels: NATO Standardization Office (NSO).

Baillergeon, Frederick A. 2019. *Transitions: Adapting to Change in Division Large-Scale Combat Operations.* Vols. Large-Scale Combat Operations – The Division Fight. US Army Command and General Staff College Press Book, Army University Press.

Department of the Army, FM 3-0. 2017. *Operations.* US Army.

Department of the Army, ADP 3-0. 2019. *Operations.* US Army.

Department of the Army, ADP 3-90. 2019. *Offense and Defense.* SUA: US Army.

Department of the Army, FM 3-90. 2023. *FM 3-90, Tactics.* US Army.

Finkel, Meir. 2011. *On Flexibility, Recovery from Technological and Doctrinal Surprise on the Battlefield.* Stanford: Stanford University Press.

Friedman, B.A. 2017. *On Tactics: A Theory of Victory in Combat.* Annapolis, Maryland: Naval Institute Press.

Hird, Karolina, Grace Mappes, Kateryna Stepanenko, Madison Williams, Yekaterina Klepanchuk, Nicholas Carl și Mason Clark. 2022. ”Russian Offensive Campaign Assessment, November 9”. https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-november-9.

Jones, Seth G., Alexander Palmer și Joseph S. Bermudez Jr. 2023. ”Ukraine’s Offensive Operations: Shifting the Offense-Defense Balance.” *CSIS Brief.*

Kagan, Frederick W. 2022. ”What Stalemate Means in Ukraine and Why it Matters”. https://www.understandingwar.org/backgrounder/what-stalemate-means-ukraine-and-why-it-matters.

Kagan, Frederick W., George Barros și Kateryna Stepanenko. 2022. ”Russian Offensive Campaign Assessment, March 19”. https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-march-19.

Kofman, Michael și Ryan Evans. 2022. ”Ukraine’s Kharkhiv Operation and the Russian Military’s Black Week”. https://warontherocks.com/2022/09/ukraines-kharkhiv-operation-and-the-russian-militarys-black-week/.

Machiavelli, Niccolo. 2012. *The Prince, Marea Britanie.* Londra: Amber Books Ltd.

Oliker, Olga. 2001. *Russia’s Chechen Wars 1994–2000: Lessons from Urban Combat.* Santa Monica, SUA, California: Arroyo Center, RAND Corporation.

Smith, Rupert. 2019. *The Utility of Force*. Londra: Penguin Books, Penguin Random House.

Statul Major al Forțelor Terestre, FT 2. 2019. *Manualul activității de stat major a comandamentelor din forțele terestre în operații.* București: Statul Major al Forțelor Terestre.

Toroi, George-Ion și Cristian Octavian Stanciu. 2023. „Sprijinul structurilor de informații în contracararea acțiunilor de inducere în eroare ale adversarului la nivel operativ.” *Buletinul Universității Naționale de Apărare „Carol I”* 12 (2): 142-156.

Weiss, Geoffrey F. 2021. *The New Art of War - The Origins, Theory, and Future of Conflict.* Cambridge : Cambridge University Press.

www.globalsecurity.org. 2003. ”Chapter 8: CA Methodology: Transition”. https://www.globalsecurity.org/military/library/policy/army/fm/3-05-401/chpt8.htm.

BULETINUL
UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I"
https://buletinul.unap.ro

Jocul pentru dezvoltarea și evaluarea conceptelor – cadrul de colectare a datelor în cercetarea științifică în domeniul științe militare

Concept development assessment game – suitable collecting framework in scientific military research

Lt. col. Dr. George-Ion TOROI*
*Universitatea Națională de Apărare „Carol I"
e-mail: george_toroi@yahoo.com

Abstract

Cercetarea științifică este crucială pentru progres în toate domeniile societății, inclusiv în sfera militară. Totuși, pe măsură ce mediul de securitate devine tot mai dinamic, imprevizibil și complex, metodele de cercetare în științele militare trebuie să răspundă provocărilor contemporane, oferind cadre flexibile pentru evaluarea și testarea unor noi concepte, necesare adaptării structurilor de forțe. Acest articol analizează Jocul pentru Dezvoltarea și Evaluarea Conceptelor (CDAG) care oferă un cadru structural de colectare a datelor calitative în cercetarea specifică domeniului militar. Jocul reprezintă un instrument calitativ, utilizat pentru testarea și rafinarea unor concepte în faza incipientă de dezvoltare, oferind un cadru controlat și flexibil pentru colectarea datelor necesare. În plus, acesta asigură mecanismul de utilizare a unei game variate de metode de colectare, precum observația, focus grupul sau chestionarul, creând astfel posibilitatea realizării triangulației datelor colectate și, implicit, a premiselor unor rezultate valoroase pentru demersul de transformare a structurilor militare.

Scientific research is crucial for progress across all areas of society, including the military sphere. However, as the security environment becomes increasingly dynamic, unpredictable, and complex, research methods in military sciences must address contemporary challenges by providing flexible frameworks for evaluating and testing new concepts necessary for the adaptation of force structures. This article analyzes the Concept Development Assessment Game (CDAG), which offers a structured framework for collecting qualitative data in military-specific research. The game serves as a qualitative tool used for testing and refining concepts at an early stage of development, providing a controlled and flexible environment for collecting necessary data. Moreover, it ensures a mechanism for employing a wide range of data collection methods, such as observation, focus groups, or questionnaires, thereby enabling the triangulation of collected data and, consequently, the foundation for valuable outcomes in the effort to transform military structures.

Cuvinte-cheie:
CDAG; știință militară; metodă de colectare a datelor; cercetare științifică.

Keywords:
CDAG; military science; collection method; scientific research.

Info articol
Primit: 12 noiembrie 2024; Evaluat: 29 noiembrie 2024; Acceptat: 4 decembrie 2024; Disponibil online: 17 ianuarie 2025
Citare: Toroi, G.I. 2024. „Jocul pentru dezvoltarea și evaluarea conceptelor – cadrul de colectare a datelor în cercetarea științifică în domeniul științe militare. *Buletinul Universității Naționale de Apărare „Carol I"*, 14(3): 114-128. https://doi.org/10.53477/2065-8281-24-42

Într-un mediu de securitate în continuă schimbare, caracterizat de competiție acerbă între actori (Joint Doctrine Note 1-19 2019, 1; Mazarr, Blake și alții 2018, 1; Mazarr, Blank și alții 2022, 111-113); (MCDP 1-4 2020, 1-3), în care conflictele și tehnologiile evoluează rapid, adaptarea forțelor la provocările curente reprezintă o necesitate operațională care să asigure premisele succesului operațional în potențialele conflicte ale viitorului (Nistorescu 2024, 195).

În acest context, cercetarea și dezvoltarea conceptuală în domeniul științelor militare necesită metode flexibile și inovatoare de testare și de evaluare în demersul de adaptare la aceste provocări. Jocul pentru Dezvoltarea și Evaluarea Conceptelor (Concept Development and Assessment Game – CDAG) se impune ca o metodă calitativă esențială, permițând analiza în profunzime a unor concepte teoretice într-un cadru controlat, în care riscurile operaționale sunt reduse. CDAG oferă cercetătorilor o platformă pentru a testa scenarii complexe, de la noi doctrine și strategii până la tehnologii emergente și proceduri operaționale, sprijinind astfel adaptarea continuă a structurilor de apărare.

Întrucât științele militare se bazează atât pe colectarea riguroasă de date, cât și pe interpretarea calitativă a fenomenelor, CDAG reprezintă un cadru ideal pentru culegerea și analiza datelor calitative relevante. Prin natura sa exploratorie, această metodă permite cercetătorilor să surprindă nuanțele și complexitatea comportamentelor și percepțiilor participanților, creând astfel o bază solidă pentru înțelegerea și îmbunătățirea conceptelor studiate.

Problema de cercetare

Deși există lucrări care tratează aspecte ale Jocului pentru Dezvoltarea și Evaluarea Conceptelor (CDAG) în context militar, în literatura românească cercetările aprofundate asupra acestuia rămân extrem de limitate. Lipsa de abordări sistematice reprezintă un gol semnificativ în literatura românească de specialitate, necesitând o investigație atentă pentru a clarifica și a structura modalitățile prin care CDAG poate susține cercetarea științifică militară și poate furniza rezultate fiabile în domeniu.

Scopul cercetării

Din acest motiv, studiul de față intenționează să asigure o înțelegere aprofundată a modului corect de utilizare a CDAG în colectarea datelor, dar și să exploreze avantajele și limitele jocului ca instrument de culegere a datelor în cercetarea științifică militară, evidențiind rolul său în adaptarea continuă a doctrinei și a structurilor de apărare.

Ținta cercetării

Lucrarea de față se adresează tuturor cercetătorilor din domeniul științe militare, dar în special celor aflați la început de drum, pentru a le oferi un cadru structural adecvat, coerent și valid de colectare a datelor, specific domeniului militar, dar și pentru a oferi îndrumări viabile privind opțiunile metodologice necesare realizării coerenței logice a cercetărilor lor atunci când optează pentru un astfel de instrument.

Metodologia cercetării

Metodologia folosită a fost una de tip calitativ, cu scopul de a înțelege și de a prezenta nuanțele CDAG, metoda principală utilizată fiind cea a analizei documentare. Această metodă mi-a permis să explorez în profunzime tematica și să identific elementele esențiale ale CDAG-ului, oferindu-mi astfel o înțelegere amplă și detaliată a subiectului.

Având în vedere natura calitativă a studiului, următoarele întrebări de cercetare au ghidat demersul științific:

- Ce este CDAG și cum se desfășoară?
- Care sunt beneficiile și avantajele utilizării CDAG în cercetarea științifică din domeniul științe militare?
- Care sunt posibilele limitări ale folosirii CDAG și cum pot fi diminuate?

Structura lucrării

Am organizat lucrarea pe două mari secțiuni pentru a găsi răspunsuri la întrebările de cercetare. Astfel, prima secțiune am dedicat-o prezentării teoretice a ceea ce este CDAG și am oferit un ghid practic de organizare și de întrebuințare a acestuia pentru a asigura cadrul eficient de operare. Secțiunea a doua, în schimb, am dedicat-o prezentării principalelor avantaje ale utilizării acestui instrument ca și cadru de colectare a datelor în cercetările specifice domeniului militar, precum și a principalelor limite și considerente care trebuie avute în vedere la optarea pentru un astfel de joc.

CDAG – ce este și cum se desfășoară?

Jocul pentru dezvoltarea și evaluarea conceptelor (Concept Development Assessment Game – CDAG) reprezintă un instrument practic, validat de NATO, care asigură în interiorul Alianței cadrul necesar de îmbunătățire a diferitelor documente conceptuale. Având în vedere că denumirea jocului nu este implementată în limba română, vom utiliza interschimbabil, pe parcursul acestui articol, termenii CDAG și *„Joc pentru dezvoltarea și evaluarea conceptelor”*, ambii făcând referire la același concept.

NATO prevede că această metodă poate fi utilizată pentru a testa și a perfecționa o varietate mare de documente, cum ar fi doctrine, concepte, politici, manuale sau procese specifice, fiind deja testată în cadrul unor proiecte importante ale Alianței (NATO ACT 2014, 2).

CDAG este un joc de război analitic, dezvoltat în colaborare de Comandamentul Aliat pentru Transformare al NATO și Organizația pentru Cercetare a Ministerului Apărării din Olanda (NATO ACT 2011, 12). În general, jocurile de război sunt recunoscute a fi metode eficiente în cadrul experimentărilor în domeniul apărării (UK Ministry of Defence 2021a, 58). CDAG reprezintă o metodă calitativă, folosită pentru a testa și a dezvolta documente conceptuale (NATO ACT 2021, 30).

Deși unii cercetători admit că nu există o definiție universal acceptată a cercetării calitative (Salmons 2022, 2), aceasta fiind greu de realizat (Hennink, Hutter și Bailey

2020, 41), este recunoscut faptul că atunci când se încearcă explicarea, înțelegerea sau descrierea fenomenelor, proceselor sau comportamentelor, acest tip de abordare este cea mai adecvată (Hennink, Hutter și Bailey 2020, 43; Ravitch și Carl 2021, 49). Așadar, prin natura sa exploratorie, cercetarea calitativă oferă oportunitatea de a obține date concludente despre fenomenele cercetate, concentrându-se pe context, pe perspectivele individuale și pe înțelegerea subtilităților asociate cu subiectul de studiu. (Salmons 2022, 2; Merriam și Grenier 2019, 5).

Din acest motiv, natura calitativă a CDAG limitează și canalizează eforturile cercetătorilor către studii care urmăresc înțelegerea fenomenelor și a nuanțelor acestora sau a trăirilor și a perspectivelor participanților asupra conceptelor testate. Natura obiectivelor și întrebărilor de cercetare constituie factorii esențiali care canalizează direcția de cercetare, în funcție de care se poate opta pentru o abordare calitativă (Leavy 2023, 9; Leavy 2020, 2). În cazul cercetărilor specifice domeniului militar, cercetarea calitativă prin metoda CDAG poate fi folosită pentru a testa maniera în care reacționează structurile militare la introducerea unui nou sistem de armament sau tehnologie ori pentru a evalua adaptabilitatea unei anumite strategii de apărare. În astfel de cazuri, metoda calitativă permite cercetătorilor să obțină o înțelegere detaliată a percepțiilor, a dinamicii echipei și a posibilelor provocări întâmpinate de participanți, oferind informații detaliate asupra comportamentelor și interacțiunilor reale. De asemenea, jocul poate fi folosit drept cadru de colectare a datelor în vederea explorării reacțiilor și impresiilor participanților față de o nouă doctrină sau procedură, testând modul în care aceasta se integrează în procesele decizionale și identificând posibile puncte de îmbunătățire. În astfel de cazuri, cercetarea calitativă oferă nu doar feedback în ceea ce privește viabilitatea procedurilor și doctrinelor testate, dar și în ceea ce privește adaptabilitatea membrilor la acestea. Astfel, CDAG poate fi o metodă eficientă pentru cercetarea calitativă în domeniul militar, concentrându-se pe o înțelegere aprofundată a reacțiilor și perspectivelor participanților, facilitând astfel adaptarea și rafinarea conceptelor militare, în funcție de nevoile reale.

Jocul pentru dezvoltarea și evaluarea conceptelor este unul de tip "table-top", concentrat pe rezolvarea unor situații, create prin întrebuințarea cardului concept pus la dispoziție. Ideea jocului este de a testa conceptul dezvoltat anterior și de a identifica lacunele existente și căile de optimizare a acestuia. Din acest motiv, jocul nu este indicat a fi folosit pentru a iniția demersul de cercetare. Rolul său este de a consolida o idee, un concept, utilizând alte metode și de a identifica soluții de maturizare a conceptului.

Din acest motiv, înainte de a opta pentru un astfel de joc, se recomandă testarea viabilității aplicării sale, NATO oferind un îndrumar în acest sens, prin care, în funcție de nivelul de maturitate al conceptului supus analizei și de cel al operațiilor militare, se poate testa oportunitatea folosirii CDAG, așa după cum se poate remarca în Figura 1.

Figura 1 Aplicabilitatea întrebuințării CDAG
Sursa: NATO ACT 2014, 6.

Jocul presupune **roluri și responsabilități** clar definite. La minimum, trebuie să existe:

- echipe de joc;
- analiști;
- lider de concept/consilier;
- moderator.

Echipele de joc sunt cele care testează conceptul în cadrul jocului. Jocul nu este unul cu adversari precum jocul de război, toate echipele participante îndeplinind aceleași responsabilități și având aceeași problemă de rezolvat. Nu este un număr limitat de echipe. Trebuie să existe minimum două, fiecare dintre ele fiind formate din 6-8 jucători care au experiență în domeniul specific conceptului testat și care sunt din categoria de personal care, în cazul implementării, va opera în mod curent cu acesta. Rolul echipelor este de a analiza și de a critica produsul testat, respectând regulile jocului, pentru a identifica vulnerabilitățile acestuia într-o situație reală.

Analiștii au rolul de a colecta date, fiind cel puțin unu la fiecare echipă de joc. Prin urmare, rolul lor este crucial pentru etapa de culegere a datelor, specifică demersului științific. De aceea trebuie să existe obligatoriu o etapă preliminară jocului, în care să se realizeze pregătirea acestora. Se recomandă ca fiecare echipă de lucru să aibă repartizat cel puțin un analist pe întreaga perioadă de desfășurare a jocului, care să monitorizeze, pe lângă răspunsurile oferite, și reacțiile participanților pe parcursul jocului, precum și soluțiile alternative la care s-a renunțat în timpul rundelor. Mai mult, procesul de analiză a datelor trebuie să ia în calcul și potențiale influențe ale biasurilor fiecărui analist. Adoptarea de măsuri reflexive în timpul procesului de colectare poate asigura reducerea influențelor propriilor prejudecăți asupra datelor colectate.

Liderul de concept este cel care a dezvoltat conceptul/documentul/produsul care urmează să fie testat și rafinat în cadrul CDAG. Implicarea sa în joc trebuie să fie redusă la maximum pentru a nu influența participanții cu privire la eventualele soluții. Acesta ar trebui să se rezume la lămurirea, în caz de nevoie, a unor aspecte specifice conceptului dezvoltat de el.

Moderatorul reprezintă un element cheie în timpul uneia dintre etapele rundelor de joc, cea plenară. El este cel care ghidează discuțiile dintre echipe spre îndeplinirea obiectivelor stabilite pentru fiecare rundă. Este recomandat ca moderatorul să fie o persoană care înțelege conceptul, dar diferită de cea care l-a dezvoltat anterior, tocmai pentru a nu influența discuțiile dintre echipe.

Toate aceste funcții sunt extrem de importante pentru rezultatele CDAG. Din acest motiv, o atenție deosebită trebuie să se acorde **strategiei de eșantionare**. Având în vedere natura calitativă a datelor și metodelor specifice de colectare a acestora pe timpul jocului, eșantionarea trebuie să fie una de tip nonprobabilistic, cel mai posibil de tip subiectiv, având la bază anumite criterii predefinite (Rassel și alții 2020, 243), presupunând alegerea eșantionului în mod deliberat, nu la întâmplare (Moser și Korstjens 2018, 11). Această modalitate de abordare reprezintă o practică extinsă în cadrul cercetărilor de tip calitativ (Dawson 2019, 49; Hennink, Hutter și Bailey 2020, 164; Braun și Clarke 2013, 55). Experiența participanților, omogenitatea grupurilor sau nivelul de interes trebuie să se regăsească printre criteriile predefinite de selectare a eșantionului.

TABEL NR. 1

Programul CDAG – model orientativ

Orar	Sâmbătă	Luni	Marți	Miercuri
08.00 – 11.00	❖ Activități administrative ❖ Prezentări	Runda 1	Runda 3	Runda 5
12.00 – 15.00		Runda 2	Runda 4	Runda 6

Jocul presupune parcurgerea a **șase runde**, pe parcursul a maximum patru zile, conform programului din tabelul de mai jos. Perioade mai lungi de atât s-au dovedit ineficiente sub aspectul rezultatelor, având în vedere gradul de interes și de atenție al participanților.

Prima zi trebuie dedicată obligatoriu desfășurării de activități administrative de pregătire a participanților și a spațiilor de lucru. Astfel, susținerea unor serii de prezentări cu privire la metodologia și obiectivele jocului, scenariul aplicat, componența echipelor și rolul participanților, cât și conceptul care va fi testat trebuie să se regăsească în cadrul acestor activități de pregătire. Rolul acestor prezentări este de a garanta nivelul optim de înțelegere al participanților în ceea ce privește modalitatea de desfășurare a jocului și așteptările legate de rezultate.
De asemenea, având în vedere că una dintre metodele de colectare a datelor de la participanți este chestionarul, așa după cum voi prezenta ulterior, este recomandat ca, pentru a optimiza jocul, în prima zi să se explice și metodologia de completare a acestuia.

În plus, pentru a asigura rigurozitatea jocului, se recomandă stabilirea unui set de reguli, care să fie prezentate participanților tot în cadrul activităților administrative, acestea rămânând în permanență afișate în format fizic în zonele de lucru, pe întreaga

durată a jocului. Mai mult, în prima zi este necesară repartizarea spațiilor de lucru pentru fiecare echipă, asigurându-se și suportul logistic necesar: laptopuri, flipchart, markere, pixuri, evidențiatoare, post-it etc., creându-se, astfel, cadrul optim de desfășurare a jocului în zilele următoare.

Așa după cum am menționat anterior, CDAG presupune un număr de șase runde, fiecare dintre acestea desfășurându-se timp de aproximativ trei ore, ele fiind independente, rezultatele dintr-o rundă neinfluențând activitățile din cele subsecvente. În cadrul fiecărei runde, echipele de joc, în acest caz, două la număr, desfășoară aceleași 4 faze principale, conform Figurii 2, astfel:

- faza introductivă;
- faze de lucru;
- faza plenară;
- chestionar rundă.

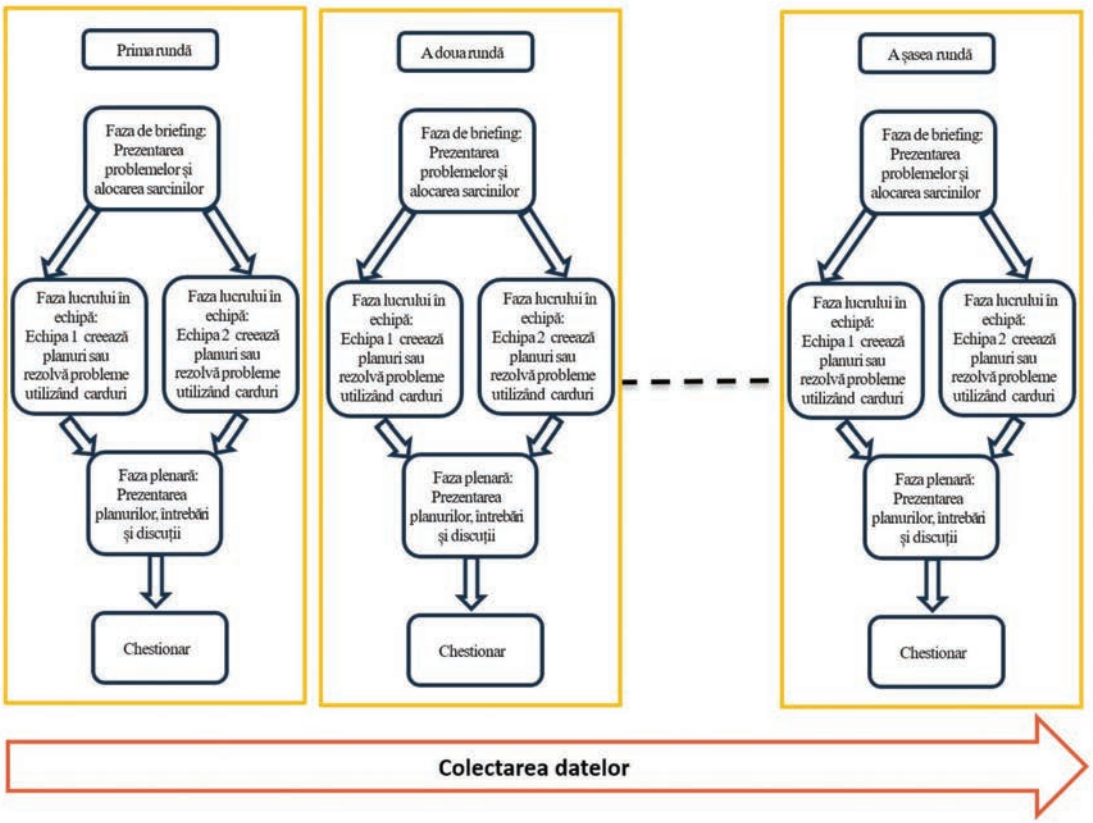


Figura 2 Fazele rundelor CDAG
Sursa: NATO ACT 2014, 16.

Fiecare rundă începe cu o **fază introductivă**, desfășurată în plen de către toate echipele de joc, împreună cu moderatorul și liderul de concept. În cadrul acesteia, sunt prezentate aspecte relevante pentru joc, precum: scenariul, vigneta specifică rundei, problema care trebuia rezolvată și cardul concept care putea fi întrebuințat pentru soluționarea acesteia. Această fază durează aproximativ 10-15 minute.
Scenariul întrebuințat poate fi același pentru toate rundele jucate sau poate diferi, în funcție de obiectivele jocului și de conceptul care se dorește a fi testat. Totuși,

pentru a nu crea confuzie în rândul participanților, se recomandă utilizarea aceluiași scenariu pe întreg parcursul CDAG. De asemenea, folosirea unui design concis al scenariului reprezintă o practică recunoscută a CDAG pentru a nu încurca participanții cu detalii și pentru a reuși menținerea atenției acestora asupra cardului concept testat (Collins și Hasberg 2018, 245).

Fiecare rundă presupune o vignetă specifică, independentă de celelalte, care este plasată în contextul scenariului și care asigură echipelor informațiile necesare rezolvării problemei primite, oferind cadrul de discuții și analiză. Pe lângă acestea, vigneta conține și informații cu privire la rolul pe care echipa îl asigură pentru soluționarea situației primite. Menționăm că toate echipele primesc aceleași documente, roluri și sarcini de rezolvat pe întreg parcursul jocului.

În plus, în faza de început a fiecărei runde, echipele primesc câte un card concept specific rundei respective. Acesta reprezintă fie un extras, fie tot conceptul care se dorește a fi testat. Rolul cardului concept este de a oferi un potențial instrument de rezolvare a problemei primite prin vignetă. Echipele au opțiunea de a-l întrebuința sau nu, putând propune soluții alternative, în funcție de opțiunea fiecăreia.

A doua fază a rundei este cea de lucru, constă în identificarea soluțiilor pentru problema cu care echipele s-au confruntat. Ea durează aproximativ 90 de minute, fiecare echipă desfășurându-și activitatea separat, în câte o încăpere, alocată special. Pentru generarea de soluții, echipele pot aplica o gamă variată de metode și tehnici de analiză care încurajează și stimulează aplicarea gândirii critice în vederea identificării perspectivelor alternative la rezolvarea situației primite, sporind viabilitatea rezultatelor obținute (TRADOC G-2, Version 9.0 2022; UK Minstry of Defence 2021b; NATO ACT 2017). Cea mai simplă metodă care poate fi folosită în faza de lucru poate fi cea a brainstormingului, o tehnică larg acceptată pentru stimularea gândirii creative și identificarea de soluții inovatoare la probleme (NATO ACT 2017, 31).

Pentru a responsabiliza fiecare participant și pentru a intensifica gradul de implicare al participanților în cadrul studiului, se recomandă ca, pentru fiecare rundă, să fie desemnat un lider de echipă, responsabil pentru coordonarea activităților în timpul sesiunii de lucru, precum și pentru prezentarea concluziilor în sesiunea plenară. Totodată, după cum am precizat anterior, fiecare echipă trebui să aibă repartizat cel puțin un analist. Subliniem din nou importanța pregătirii acestora pentru a asigura un proces de colectare a datelor cât mai eficient.

Următoarea fază a fiecărei runde, **cea plenară**, se desfășoară în comun de către toate echipele de joc, sub atenta îndrumare a moderatorului desemnat, și durează aproximativ o oră. Menționăm că, în această fază, poate fi prezent și liderul de concept pentru a se asigura că răspunsurile oferite de echipe sunt înțelese corect și se încadrează în direcția teoretică a studiului. Figura 3 prezintă modul de organizare pentru această fază a fiecărei runde.

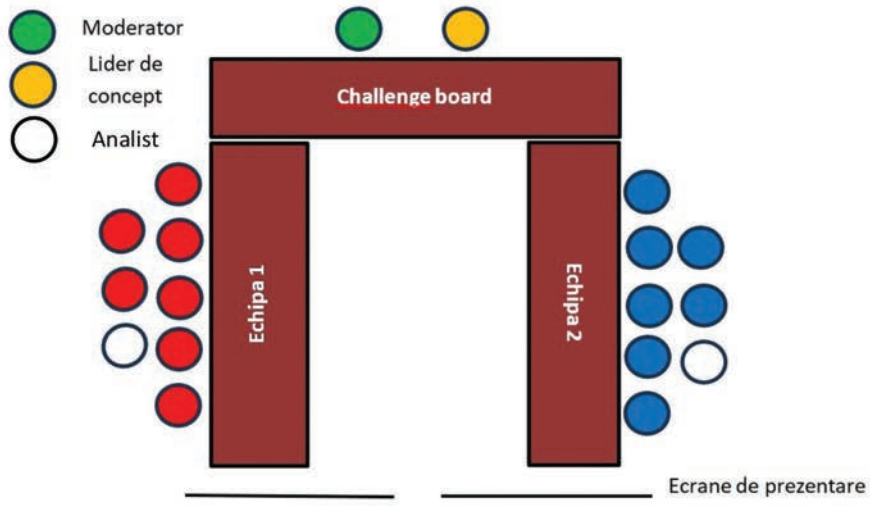


Figura 3 Cadrul de organizare a fazei planetare
Sursa: NATO ACT 2014, 19.

În cadrul acestei faze, fiecare lider de echipă stabilit pentru runda respectivă prezintă soluțiile identificate de echipa sa pentru rezolvarea situației primite. La sfârșitul prezentării sale, membrii celeilalte echipe, moderatorul, dar și liderul de concept pot adresa întrebări de clarificare a informațiilor susținute. În acest fel, se asigură o discuție constructivă între echipe, având potențialul de a dezvolta și de a rafina soluțiile prezentate.

Ultima fază a fiecărei runde poate presupune completarea unui **chestionar** de către toți participanții echipelor prin care se poate colecta feedbackul lor direct, pentru a înțelege mai bine cum au perceput desfășurarea jocului. Chestionarul are rolul de a identifica nivelul lor de înțelegere, eficiența, precum și relevanța cardului concept în rezolvarea provocărilor propuse. Dorim să reamintim că, din rațiuni care țin de eficiența temporală, metodologia de completare a acestor chestionare se realizează în cadrul primei zile a jocului, în timpul activităților administrative, ea fiind identică tuturor rundelor.

Argumente și considerații privind întrebuințarea CDAG în cercetarea militară

Există o multitudine de avantaje atunci când vine vorba de alegerea utilizării CDAG. Numai simplul fapt că este folosit de către cea mai mare alianță a lumii pentru dezvoltarea propriilor concepte operaționale reprezintă un argument solid în privința adoptării acestuia și integrării lui în cercetarea științifică. Alte **beneficii ale Jocului pentru dezvoltarea și evaluarea conceptelor (CDAG)** pot fi considerate următoarele:

- Asigurarea unui cadru de rezolvare creativă a problemelor operaționale, putând fi integrate și metode dovedite științific ca facilitatoare ale gândirii critice. Acest aspect asigură potențialul unor soluții inovative care să

contribuie la dezvoltarea eficientă a conceptelor testate (Feckler 2011, 2).
- Comunicarea deschisă dintre membrii echipelor asigură un cadru liber de exprimare a opiniilor avizate.
- CDAG reprezintă o soluție economică de testare a conceptelor, asigurând îmbunătățirea acestora fără costuri mari, înainte de a fi testate în cadrul unor exerciții de amploare (Collins și Hasberg 2018, 237).
- Poate reduce riscul de eșec al unui concept, deoarece permite testarea acestuia într-un mediu teoretic, cu risc scăzut, înainte ca acesta să fie testat în practică.
- Asigură potențialul de identificare și gestionare a eventualelor riscuri conexe conceptului testat.
- Creează un cadru de discuții între experți care facilitează posibilitatea dezvoltării conceptului analizat.
- Este un instrument extrem de flexibil care poate fi ajustat în raport cu conceptul testat sau cu obiectivele propuse, nu numai înainte, ci și în pe timpul desfășurării acestuia.
- Adițional, poate fi folosit ca metodă de învățare continuă pentru participanți. În cadrul său, pot fi integrate metode dovedite științific a dezvolta nivelul de gândire critică și creativă a participanților la joc (NATO ACT 2017, Foreward).
- Având în vedere nevoia de adaptare continuă a sistemului la provocările mediului actual de operare tot mai complex și volatil, CDAG poate asigura testarea noilor concepte militare. Evoluția tehnologică extrem de rapidă a societății contemporane influențează în mod covârșitor caracterul conflictelor, iar CDAG poate reprezenta o metodă economică și fără riscuri de a testa noi modalități, concepte sau moduri de operare ale forțelor armate în demersul de adaptare a acestora la mediul de operare curent.

Totuși, **avantajul major al CDAG** este faptul că facilitează posibilitatea de a colecta date prin mai multe metode, asigurând astfel **triangulația** acestora. Este și motivul pentru care am ales acest titlu al studiului.
Există trei metode științifice de colectare a datelor care pot fi folosite în diferite momente ale desfășurării CDAG. Acestea sunt: observarea, focus grupul și chestionarul.

Adunarea acestor informații se efectuează de analiști atât în timpul activității echipelor de joc, al sesiunii plenare aferente fiecărei runde, cât și în ultima fază, prin chestionarele administrate. După încheierea întregii activități, toți analiștii vor preda liderului de concept materialele colectate. Astfel, CDAG realizează un cadru coerent de colectare a datelor.

În faza de lucru a echipelor, analiștii desemnați colectează date folosind **metoda observației**. Aceasta este recunoscută ca fiind una dintre principalele metode pentru culegerea datelor în cercetarea calitativă (Creswell 2013, 166; Hennink, Hutter și Bailey 2020, 289; Saunders, Lewis și Thornhill 2019, 378). Această metodă poate asigura înțelegerea aprofundată a contextului, creând cadrul de culegere a unor

date diverse și detaliate. În cazul CDAG, pentru a facilita acest proces, este indicat ca analiștii să primească o fișă de observație din partea liderului de concept în prima zi a jocului, în timpul activităților administrative. Reiterăm, de asemenea, nevoia realizării unei sesiuni de pregătire a analiștilor la începutul activității pentru a spori eficiența procesului de colectare a datelor. Este, de asemenea, important să menționăm că fiecare fișă trebuie să fie însoțită de instrucțiuni metodologice de completare, concepute pentru a garanta eficacitatea procesului de colectare a datelor.

Datorită modului de desfășurare a jocului, metoda de colectare a datelor, folosită **în etapa plenară**, este **focus grupul**. Aceasta reprezintă o discuție de grup moderată, în care participanții își împărtășesc ideile cu privire la un anumit subiect (Crabtree și Miller 2023, 156). Din prezentarea organizațională a CDAG, realizată în secțiunea precedentă, se poate observa că această metodă se aliniază perfect modului în care este organizat jocul în faza plenară. Mai mult, alegerea focus grupului ca metodă de colectare poate fi justificată și din perspectiva numărului de participanți, literatura academică indicând o componență optimă a grupului de discuție, cuprinsă între 4 și 15 persoane (Krueger și Casey 2014, 33).

În plus, natura calitativă a jocului se aliniază perfect utilizării focus grupului, acesta fiind o metodă desfășurată aproape întotdeauna cu scopul principal de a colecta date calitative (Stewart și Shamdasani 2015, 42). În această fază, datele sunt colectate tot de analiștii fiecărei echipe, ideal prin înregistrarea întregii discuții pe un suport electronic, precum și prin consemnarea principalelor dezbateri în fișele de observație, folosite și în timpul etapei de lucru. Avantajul utilizării acestei metode de culegere a datelor este că poate genera un cadru de discuții interactiv, pe fondul rezultatelor obținute de fiecare echipă, facilitând posibilitatea emergenței unor soluții novatoare, datorită perspectivelor diversificate.

Cea de-a treia metodă de colectare care poate fi folosită în cadrul CDAG este **chestionarul**, recunoscută ca fiind pretabilă în strategiile de cercetare de tip calitativ (Charmaz 2014, 116). Rolul său este, de asemenea, acela de a înțelege fenomenul și conceptul studiat. Astfel, chestionarul poate urmări să colecteze date care să asigure înțelegerea gradului de claritate, dar și eficacitatea conceptului testat. Trebuie totuși acordată o atenție sporită modului de redactare a întrebărilor pentru a asigura coerența metodologică, în raport cu abordarea calitativă a jocului. Astfel, trebuie optat pentru întrebări de tip deschis, conform practicilor recunoscute în metodologia cercetării calitative, pentru a capta în detaliu perspectivele participanților la studiu, în raport cu obiectivele stabilite.

Organizarea chestionarului trebuie să constituie un element important care să fie luat în calcul la dezvoltarea acestuia. Întrebările trebuie să fie structurate într-o formă logică, de natură să faciliteze un parcurs coerent pentru respondenți, asigurând astfel potențialul de a crește calitatea răspunsurilor obținute. Îndrumările oferite de Ian Brace și Kate Bolton, în cartea lor *Questionnaire Design: How to plan, structure and write survey material for effective market research* (Brace și Bolton 2022, 38-42), pot

reprezenta un ghid oportun în vederea planificării activităților specifice colectării datelor prin metoda chestionarului.
Este de menționat că, în vederea eficientizării procesului de colectare a datelor, se pot alege ca instrumente de cercetare sisteme electronice de administrare a chestionarului, precum Google Forms, majoritatea acestor platforme asigurând automat diagrame și grafice ale rezultatelor obținute, facilitând astfel un mediu propice de culegere și de analiză facilă a datelor.

Trebuie, de asemenea, să admitem și anumite **limite** ale întrebuințării unui astfel de cadru structural de colectare a datelor. Ele reprezintă puncte slabe în cadrul studiului, care ar fi putut influența rezultatele și concluziile cercetării (Theofanidis și Fountouki 2018, 155). În primul rând, calitatea datelor este dependentă de experiența analiștilor în colectarea lor și de modul în care aceștia au reușit să surprindă elemente cu adevărat relevante pentru studiul întreprins. În acest sens, reiterăm necesitatea unei pregătiri prealabile a lor pentru a spori capacitatea acestora de a colecta date relevante obiectivelor cercetării. În plus, deși jocul nu poate răspunde anumitor trăsături psihologice intrinseci conflictelor armate, precum frica, oboseala sau stresul (Popa 2019, 46), la care sunt supuși militarii în situații reale, considerăm că acesta oferă un mediu propice colectării datelor calitative pentru a rafina diferite concepte militare. De asemenea, este important să se țină cont și de limitările metodologice, izvorâte din metodele de colectare întrebuințate. Astfel, datele obținute prin folosirea observației sunt dependente atât de influența observatorului, cât și de gradul de subiectivitate al acestuia, cele în urma focus grupului pot fi influențate de anumite presiuni de conformitate, pentru unii participanți, și de anumiți lideri de opinie, în timp ce datele colectate prin chestionar pot fi superficiale, având în vedere momentul final în cadrul jocului, când se aplică această metodă. Toate aceste limitări trebuie luate în considerare pentru a asigura interpretarea corectă a rezultatelor și pentru a face din jocul de dezvoltare și evaluare a conceptelor un cadru eficient de colectare a datelor în cercetările științifice specifice domeniului științe militare.

În plus, trebuie avută în vedere **respectarea coerenței metodologice** a cercetării științifice. Trebuie ținut cont de faptul că jocul de dezvoltare și evaluare a conceptelor se recomandă doar în studiile calitative, desfășurate pe baza unui raționament inductiv, care urmărește explorarea unor fenomene militare și identificarea de soluții noi la provocările mediului curent de operare. De asemenea, se recomandă alegerea unei strategii de cercetare calitative care să respecte natura jocului, aceea de a dezvolta anumite concepte aflate într-o fază incipientă. Din acest motiv, teoria fundamentată pe date (Grounded theory – GT) poate reprezenta cea mai adecvată strategie de cercetare. Esența acesteia se potrivește modului de organizare a CDAG, GT reprezentând un demers calitativ de colectare și analiză sistemică de date, de rafinare și comparare constantă a rezultatelor obținute cu cele anterioare până la dezvoltarea unei teorii (Charmaz și Thornberg 2021, 305). Astfel, CDAG poate sprijini acest demers de rafinare a teoriei/conceptelor.
Mai mult, având în vedere modul de desfășurare a jocului, trebuie acordată o atenție deosebită și **considerațiilor etice**. Toți participanții trebuie să fie informați

despre caracterul voluntar al implicării lor în acest studiu și să li se comunice dreptul necondiționat de a se retrage din cercetare, fără a suporta vreo repercusiune negativă. Astfel, se asigură un cadru oportun de colectare a unor date valoroase, care reprezintă premisa esențială a unor rezultate de calitate.

Concluzii

Jocul pentru dezvoltarea și evaluarea conceptelor (CDAG) reprezintă un instrument versatil, care poate contribui în mod esențial la cercetarea științifică în domeniul militar, oferind un cadru organizat și eficient pentru testarea conceptelor operaționale aflate în stadii incipiente de dezvoltare. Prin adaptabilitatea sa, CDAG asigură integrarea creativă a metodelor de colectare a datelor, precum observarea, focus grupul și chestionarul, promovând un demers științific calitativ, bazat pe triangulație și validarea rezultatelor.

Principalele avantaje identificate, inclusiv capacitatea de a facilita gândirea critică, de a economisi resurse și de a gestiona riscurile în mediul de testare, demonstrează valoarea semnificativă a CDAG ca instrument de dezvoltare a conceptelor militare. În plus, flexibilitatea și structura sa organizatorică permit experimentarea cu noi idei și soluții, reducând considerabil riscul asociat implementării directe a acestora în teren. Totuși, trebuie analizate și luate în calcul și o serie de limite metodologice, în special cele conexe metodelor de colectare a datelor, utilizate în timpul jocului.

În concluzie, consider CDAG a fi un instrument extrem de important în cercetarea și dezvoltarea conceptelor militare, în special pentru tinerii cercetători. Cu toate limitele sale, acesta oferă o abordare structurat etică și eficientă pentru colectarea datelor, constituind o resursă valoroasă pentru identificarea de soluții viabile de adaptare continuă a structurilor militare la provocările mediului de operare contemporan.

Referințe

Brace, Ian și Kate Bolton. 2022. *Questionnaire Design: How to plan, structure and write survey material for effective market research.* 5th. Londra: Kogan Page Limited.

Braun, Virginia și Victoria Clarke. 2013. *Successful qualitative research – a practical guide for beginners.* London: Sage Publications.

Charmaz, Kathy. 2014. *Constructing Grounded Theory.* 2nd edition. London: Sage Publications.

Charmaz, Kathy și Robert Thornberg. 2021. ”The pursuit of quality in grounded theory.” *Qualitative research in psychology* 18 (3).

Collins, Sue și Marcel-Paul Hasberg. 2018. ”Tabletop Assessment Games in Concept Development and Experimentation,.” În *Advances in Defence Analysis, Concept Development and Experimentation: Innovation for the Future*. Norfolk: NATO HQ Supreme Allied Command Transformation.

Crabtree, Benjamin F. și William L. Miller. 2023. *Doing Qualitative Research,.* 3rd. Los Angeles: Sage Publications.

Creswell, John C. 2013 . *Qualitative inquiry and research design: choosing among five approaches.* Londra: Sage Publications.

Dawson, Catherine. 2019. *Introduction to research methods: A practical guide for anyone undertaking a research project,* 5th edition. Robinson.

Feckler, D. 2011. ”ACT Employs Analitical War-Game.” *The Transformer, Bi-Annual Publication of Allied Command Transformation*, 2.

Hennink, Monique, Inge Hutter și Ajay Bailey. 2020. *Qualitative Research Methods.* London: Sage Publications.

Joint Doctrine Note 1-19. 2019. *Competition Continuum.* US Joint Chiefs of Staff. https://irp.fas.org/doddir/dod/jdn1_19.pdf.

Krueger, Richard A. și Mary Anne Casey. 2014. *Focus Groups: A Practical Guide for Applied Research.* 5th. Los Angeles: Sage Publications.

Leavy, Patricia. 2020. *The Oxford Handbook of Qualitative Research.* 2nd. Oxford: Oxford University Press.

—. 2023. *Research Design – Quantitative, Qualitative, Mixed Methods, Arts-Based, and Community-Based Participatory Research Approaches,* Ediția a doua. New York: The Guilford Press.

Mazarr, Michael J., Jonah Blank, Samuel Charap, Benjamin N. Harris, Timothy R. Heath, Niklas Helwig, Jeffrey W. Hornung și alții. 2022. *Understanding the Emerging Era of International Competition Through the Eyes of Others. Country Perspectives.* Santa Monica, California: RAND Corporation.

Mazarr, Michael J., Jonathan S. Blake, Abigail Casey, Tim McDonald, Stephanie Pezard și Michael Spirtas. 2018. *Understanding the Emerging Era of International Competition. Theoretical and Historical Perspectives.* Santa Monica, California: RAND Corporation.

MCDP 1-4. 2020. ”*Competing.*” https://www.marines.mil/News/Publications/MCPEL/Electronic-Library-Display/Article/2449338/mcdp-1-4/.

Merriam, Sharan B. și Robin S. Grenier. 2019. *Qualitative Research in Practice. Examples for Discussion and Analysis.* 2nd. San-Francisco: Jossey-Bass.

Moser, Albine și Irene Korstjens. 2018. ”Series: Practical guidance to qualitative research. Part 3: Sampling, data collection and analysis.” *European Journal of General Practice* 24 (1).

NATO ACT. 2011. *Transformer.* Norfolk: NATO Allied Command Transformation.

—. 2014. *NATO Concept Development Assessment Game “CDAG” Handbook.* Norfolk: NATO Allied Command Transformation.

—. 2017. *The NATO Alternative Analysis Handbook,* Ediția a doua. Norfolk: NATO Allied Command Transformation.

—. 2021. *NATO Concept Development and Experimentation Handbook: A concept developer’s toolbox.* Norfolk: NATO Allied Command Transformation.

Nistorescu, Claudiu Valer. 2024. „Adaptarea organizației militare – O condiție esențială pentru obținerea succesului pe câmpul de luptă." *Gândirea Militară Românească* (3): 194-209.

Popa, Marian. 2019. *Psihologie militară.* Ediția a doua. București: Editura Polirom.

Rassel, Gary, Suzanne Leland, Zachary Mohr și Elizabethann O'Sullivan. 2020. *Research methods for public administrators.* Routledge.

Ravitch, Sharon M. și Nicole Mittenfelner Carl. 2021. *Qualitative Research. Bridging the Conceptual, Theoretical, and Methodological.* 2nd. Londra: Sage Publications.

Salmons, Janet E. 2022. *Doing Qualitative Research Online.* Londra: Sage Publications.

Saunders, Mark N.K., Philip Lewis și Adrian Thornhill. 2019. *Research Methods for Business Students.* 8th edition. Pearson Education.

Stewart, David W. și Prem N. Shamdasani. 2015. *Focus Groups: Theory and Practice.* 3rd edition. Los Angeles: Sage Publications.

Theofanidis, Dimitrios și Antigoni Fountouki. 2018. "Limitations and delimitations in the research process." *Perioperative Nursing-Quarterly scientific, Online Official Journal of GORNA* 7 (3).

TRADOC G-2, Version 9.0. 2022. *The Red Team Handbook. The Army's guide to making better decisions.* 9. US Army Training and Doctrine.

UK Ministry of Defence. 2021a. "Defence Experimentation for Force Development Handbook." https://assets.publishing.service.gov.uk/media/6014030be90e07626914df3c/20210121-DEFD_Handbook_Version_2-O.pdf.

__. 2021b. "Red Teaming Handbook." 3rd. Edition. https://assets.publishing.service.gov.uk/media/61702155e90e07197867eb93/20210625-Red_Teaming_Handbook.pdf.

BULETINUL
UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I"
https://buletinul.unap.ro

Fundamentarea capabilității de asigurare a sprijinului prin foc întrunit, folosind modelul NATO

The foundation for a joint fire support capability using the NATO model

Lt.col.drd. Adrian MIREA*
*Universitatea Națională de Apărare „Carol I", București, România
e-mail: mirea.adrian82@gmail.com

Abstract

Asigurarea sprijinului prin foc la nivel întrunit reprezintă o capabilitate indispensabilă grupărilor de forțe care facilitează îndeplinirea obiectivelor stabilite în toate tipurile de operații. Pornind de la ideea că elaborarea unei doctrine a sprijinului prin foc, actualmente inexistentă la nivel național, nu este suficientă pentru realizarea acestei capabilități la nivelul grupării de forțe, am argumentat, prin lucrarea de față, și alte schimbări pe care le consider necesare, folosind modelul NATO de dezvoltare a unei capabilități, descris prin acronimul DOTMLPF-I. În prima parte a articolului, am prezentat succint elementele componente ale modelului NATO, pentru ca, ulterior, în cea de-a doua parte, să abordez capabilitatea de asigurare a sprijinului prin foc în ansamblul ei, sub aspectul doctrinei, al organizării structurilor de forțe, al modului de instruire, al nevoilor de revizuire a resurselor disponibile, al modului de pregătire profesională a liderilor militari și a personalului responsabil în domeniul sprijinului prin foc, al infrastructurii existente și al nivelului de interoperabilitate necesar, astfel încât capabilitatea menționată să fie real disponibilă structurilor de forțe armate. Acțiunile identificate pe cele opt direcții ale modelului NATO pot constitui o perspectivă de dezvoltare sau de consolidare a capabilității de asigurare a sprijinului prin foc întrunit la nivel național.

Providing joint fire support is an indispensable capability for joint forces that facilitates the achievement of set objectives in all types of operations. Starting from the idea that the development of a fire support doctrine, currently non-existent at the national level, is not sufficient to achieve this capability at the joint force level, I have argued in this paper, other changes that I consider necessary using the NATO capability development model, described by the acronym DOTMLPF-I. In the first part of the article, I have briefly presented the components of the NATO model and then, in the second part, I address the fire support capability as a whole, in terms of doctrine, force structure organization, training, the need to review the available resources, the training of military leaders and fire support personnel, the existing infrastructure and the level of interoperability required to make this capability truly available to the armed forces structures. The actions identified in the eight strands of the NATO model can provide a perspective for developing or enhancing the capability to provide nationally-led joint fire support.

Cuvinte-cheie:
sprijin prin foc întrunit; capabilități; model NATO; DOTMLPF-I.

Keywords:
fire support; joint fire support; capability; NATO model; DOTMLPF-I.

Info articol
Primit: 25 octombrie 2024; Evaluat: 21 noiembrie 2024; Acceptat: 3 decembrie 2024; Disponibil online: 17 ianuarie 2025
Citare: Mirea, A. 2024. „Fundamentarea capabilității de asigurare a sprijinului prin foc întrunit, folosind modelul NATO."
Buletinul Universității Naționale de Apărare „Carol I", 13(4): 129-139. https://doi.org/10.53477/2065-8281-24-43

https://doi.org/10.53477/2065-8281-24-43

Actualmente, la nivel național nu există cadrul normativ doctrinar comun care să implementeze unitar modul de asigurare a sprijinului prin foc la nivel întrunit, structurile de forțe aparținând componentelor unei grupări de forțe întrunite, având fiecare propriile doctrine și manuale de luptă care detaliază sprijinul prin foc. Alături de necesitatea de a avea elaborată și implementată, la nivelul tuturor categoriilor de forțe armate naționale, o doctrină a sprijinului prin foc întrunit, am considerat utilă identificarea unor modalități de fundamentare a acestei capabilități de asigurare a sprijinului prin foc întrunit (prin efort exclusiv național) în baza modelului NATO de dezvoltare a capabilităților, cunoscut sub acronimul DOTMLPF-I (Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities and Interoperability) – Doctrină, Organizare, Instruire, Înzestrare, Leadership, Personal, Facilități și Interoperabilitate (NATO 2021, 7). Pentru argumentarea alegerii acestui model, menționez faptul că inclusiv Strategia Militară a României din anul 2016 fundamenta, în capitolul IV *Capabilități de apărare și prioritățile de realizare a acestora*, acțiuni pe cele opt direcții, descrise de modelul NATO, pentru a realiza capabilități credibile și sustenabile de apărare (Portal legislativ 2016).

Analiza unei capabilități existente sau determinate ca fiind necesară pentru a răspunde unei noi cerințe, folosind modelul NATO menționat, poate demonstra nevoia unor schimbări de natură materială sau nonmaterială, sub forma unor acțiuni pe oricare dintre cele opt direcții, descrise de acronimul DOTMLPF-I.

Figura 1 Modelul NATO de dezvoltare a capabilităților
Sursa: MD Harris Institute 2013.

Întrucât elaborarea doctrinei sprijinului prin foc de nivel întrunit nu poate fi suficientă pentru constituirea capabilității de asigurare a acestuia, mi-am propus ca, prin lucrarea de față, să identific și să argumentez succint potențialele acțiuni pe toate cele opt direcții menționate, pentru a fundamenta sau a dezvolta la nivel național această capabilitate de asigurare a sprijinului prin foc întrunit.

În realizarea articolului, am explorat, în principal, surse deschise de informații de forma site-urilor și a lucrărilor de autor, la care am alăturat doctrine și manuale de luptă neclasificate, în vigoare la nivel național și la nivel NATO, care detaliază aspecte relevante privind asigurarea sprijinului prin foc de nivel întrunit și care

argumentează potențiale acțiuni, pentru fundamentarea unei capabilități după modelul NATO. Colectarea, analiza și interpretarea datelor din sursele explorate au fost realizate sistematic, având ca fundament analiza documentară, metodă care mi-a asigurat înțelegerea și sintetizarea principalelor aspecte privind obiectul de studiu al acestei lucrări (Okoko, Tunison și Walker 2023, 140).

Utilitatea DOTMLPF-I în fundamentarea unei capabilități

Cadrul de analiză, descris de acronimul DOTMLPF-I, reprezintă un instrument sau o metodologie (Willi 2016) utilă, din punctul meu de vedere, atât pentru fundamentarea unei capabilități noi, cât și pentru identificarea de sincope sau deficiențe în modul de abordare a unei capabilități existente – asigurarea sprijinului prin foc întrunit, în cazul de față. Utilitatea acestui instrument analitic rezidă în abordarea sistematică a tuturor aspectelor (interdependente) care pot influența disponibilitatea unei capabilități. Schimbările produse unui singur element – așa cum ar fi elaborarea unei doctrine a sprijinului prin foc întrunit – nu vor avea efectul operațional scontat, deoarece, în funcție de entitatea analizată, pot fi identificate ca fiind necesare și alte schimbări, ca, de exemplu, schimbări la nivel organizatoric sau în ceea ce privește interoperabilitatea componentelor forței întrunite, pentru ca acea capabilitate dorită să poată fi real obținută sau consolidată.
Scopul urmărit prin întrebuințarea unui astfel de instrument analitic, în cazul capabilității de asigurare a sprijinului prin foc întrunit, este creșterea nivelului de eficiență a grupărilor de forțe în valorificarea potențialului sistemelor de sprijin prin foc disponibile la nivelul componentelor sale.

Direcția de acțiune privind ***doctrina*** urmărește implementarea sau actualizarea principiilor fundamentale de întrebuințare a structurilor de forțe care, de regulă, sunt cuprinse în doctrinele naționale în vigoare. În cazul nostru, nu avem o doctrină a sprijinului prin foc întrunit la nivel național, însă dacă aceasta ar fi existat, analiza după modelul NATO ar fi urmărit o eventuală rafinare a ei, astfel încât elementele de conținut sau terminologia specifică în domeniul asigurării sprijinului prin foc întrunit să reflecte o abordare actualizată a capabilității urmărite.

Acțiunile în domeniul ***organizare*** au în atenție funcționalitatea structurală a forțelor pentru a identifica eventuale sincope sau nevoi de actualizare în modul de cooperare sistematică a indivizilor sau a componentelor structurilor de forțe pentru a îndeplini obiectivele încredințate. Accentul analizei pe această direcție este pus pe modul de valorificare a capabilității vizate, în contextul organizațional existent. Pot fi identificate astfel unele nevoi de ajustare organizatorică astfel încât capabilitatea vizată să se manifeste la potențial maxim.

În ceea ce privește ***instruirea,*** acțiunile pe această direcție se referă la modul de pregătire sau de antrenament al indivizilor, subunităților, unităților și statelor majore în implementarea prevederilor doctrinare, a manualelor de luptă sau a tacticilor,

tehnicilor și procedurilor existente, pentru îndeplinirea misiunii. Din perspectiva unei capabilități noi sau aflate în curs de dezvoltare (în proces de achiziție, de înzestrare, de implementare etc.) la nivelul structurilor de forțe, instruirea reprezintă un element central pentru a putea înțelege toată gama de implicații operaționale pe care le are disponibilitatea acestei capabilități emergente.

Direcția de acțiune ***înzestrare*** urmărește componenta materială a unei capabilități. Analiza în acest domeniu poate identifica eventuale nevoi de modificare a cantităților de echipamente existente sau poate scoate în evidență necesitatea unor noi achiziții, astfel încât capabilitatea urmărită să fie cu adevărat operațională din toate punctele de vedere.

Acțiunile pe linie de ***leadership*** urmăresc pregătirea profesională a liderilor militari – un produs al educației continue – care încorporează instruirea, expertiza, educația și dezvoltarea personală a acestora. De altfel, leadershipul fundamentează comanda – arta motivării și direcționării personalului. Se impun schimbări pe această direcție atunci când se constată unele sincope în valorificarea capabilității urmărite, datorate nivelului de competență profesională a indivizilor.

Analiza și identificarea de măsuri în domeniul ***personal*** au în vedere existența personalului calificat să valorifice capabilitatea ca obiect de studiu. Categoriile de personal care încadrează structurile de forțe și deprinderile elementare ale acestora pot avea un impact semnificativ asupra modului de exploatare a întregului potențial asigurat de o capabilitate disponibilă.

Din perspectiva domeniului ***facilități***, potențialele acțiuni au în atenție elementele de infrastructură necesare exploatării eficiente a capabilității urmărite. În această categorie de acțiuni, sunt vizate clădirile, structurile, utilitățile aferente, terenurile, dar și poligoanele necesare operativității capabilității analizate.

Potențialele acțiuni pe direcția ***interoperabilitate*** urmăresc cele trei domenii ale acesteia – tehnic potențialele, uman și procedural. Fiind vorba despre un model de dezvoltare a capabilităților de nivel NATO, putem afirma că interoperabilitatea unei capabilități este esențială, întrucât structurile de forțe puse la dispoziție de aliați trebuie să performeze într-un mediu de operare multinațional. Mai mult decât atât, din perspectivă NATO, interoperabilitatea este considerată chiar un multiplicator al forței (NATO 2023).

Aplicabilitatea modelului NATO (DOTMLPF-I) în fundamentarea unei capabilități

Așa după cum am menționat anterior, cadrul de analiză descris de acronimul DOTMLPF-I reprezintă un instrument util atât pentru fundamentarea unei capabilități noi, cât și pentru identificarea de sincope sau deficiențe în modul de

abordare a unei capabilități existente. Capabilitatea analizată prin prisma celor opt direcții de acțiune este asigurarea sprijinului prin foc la nivel întrunit.

Pornind de la ideea că, la momentul actual, există unele sincope în asigurarea sprijinului prin foc de nivel întrunit – așa cum este lipsa cadrului normativ doctrinar –, mi-am propus ca, în continuare, să prezint o perspectivă privind fundamentarea acestei capabilități la nivelul structurilor de forțe armate naționale, folosind modelul NATO în maniera în care am observat că este folosit la nivel de Alianță (NATO 2018).

Doctrină

Doctrina sprijinului prin foc întrunit este reglementarea de bază care fundamentează cadrul conceptual comun și terminologia specifică, necesare comandanților și statelor majore în planificarea și asigurarea sprijinului prin foc la nivel întrunit, conform concepției operației (NATO 2015, VII). Lipsa unui astfel de cadru normativ doctrinar la nivel național care să implementeze în mod unitar conceptele fundamentale privind sprijinul prin foc întrunit la toate categoriile de forțe armate m-a determinat să argumentez nevoia de eliminare a acestei sincope în articolul „Implementarea unei doctrine a sprijinului prin foc de nivel întrunit – cerință a operației întrunite". (Mirea și Stanciu 2024)

Prima și cea mai importantă acțiune privind doctrina pentru a fundamenta capabilitatea de asigurare a sprijinului prin foc la nivel întrunit este elaborarea unei astfel de reglementări de la cel mai înalt nivel ierarhic al autorității militare naționale. Doctrina sprijinului prin foc întrunit este cea care descrie fundamentele capabilității – ca obiect de studiu – însă ea constituie, totodată, și un ghid de bune practici, pentru comandantul grupării de forțe și pentru statul său major, în valorificarea sistemelor de sprijin prin foc, puse la dispoziție de categoriile de forțe componente. Elaborarea doctrinei va asigura implementarea coerentă a unor concepte esențiale, așa cum sunt misiunile tactice standard sau măsurile de coordonare a sprijinului prin foc, astfel încât valorificarea întregului potențial al capabilității de asigurare a sprijinului prin foc întrunit să se realizeze eficient și în condiții de siguranță pentru forțele proprii.

Organizare

Nevoia de acțiune pe această direcție este direct dependentă de implementarea programelor de achiziții derulate sau în perspectivă, care au ca obiect echipamentele militare componente ale sistemului de sprijin prin foc. De exemplu, înzestrarea structurilor de forțe terestre cu sisteme M142 HIMARS (High Mobility Artillery Rocket System) (Mureșan 2024) implică unele schimbări de natură organizatorică la nivelul unităților pentru a putea exploata astfel de sisteme, fiind, probabil, necesară o revizuire a funcțiilor servanților în cadrul grupelor/pieselor/instalațiilor, deoarece sistemele HIMARS necesită un număr mic de servanți, în comparație cu sistemele de artilerie pe care le înlocuiesc (Mureșan 2024).

Necesitatea schimbărilor de natură organizatorică sunt cu atât mai evidente, dacă avem în vedere asumarea la nivel național a cerințelor de capabilități în cadrul

NATO. Transformările implicate de dispariția sau de înlocuirea sistemelor de sprijin prin foc vechi, asociate cu implementarea graduală a programelor de achiziții, vin cu provocări inedite, inclusiv din punct de vedere organizatoric. Acestea, la rândul lor, trebuie să fie reflectate în actualizarea manualelor de luptă în vigoare, care reglementează și detaliază modul de cooperare sistematică a indivizilor, subunităților și unităților pentru eficiență operațională. O soluție temporară de asigurare a exploatării întregului potențial al capabilității de asigurare a sprijinului prin foc întrunit, indiferent de situația organizatorică de moment a forțelor armate naționale, poate fi, din punctul meu de vedere, implementarea și actualizarea permanentă a procedurilor operaționale standard – SOP (Standard Operating Procedure) – la nivelul comandamentelor pentru asigurarea standardizării și conservarea eficienței structurilor de forțe (James 2020).

Instruire

În lipsa unei doctrine a sprijinului prin foc întrunit, după cum am menționat anterior, categoriile de forțe armate naționale se ghidează după propriile doctrine și manuale de luptă care reglementează modul de asigurare a sprijinului prin foc. Instruirea în comun a factorilor responsabili de la nivelul componentelor grupării de forțe întrunite poate dezvolta și consolida capabilitatea de asigurare a sprijinului prin foc la nivel întrunit. Exercițiile militare au printre obiective și instruirea în comun a participanților, în special a celor proveniți din categorii de forțe diferite, pentru a consolida interoperabilitatea la nivel întrunit, dar și la nivel de alianță (SMFT 2019). Scenariile exercițiilor constituie cadrul instruirii în comun a cadrelor din comandamente pentru planificarea și desfășurarea de acțiuni, conform unei concepții unice.

În acest context, o direcție de acțiune pentru consolidarea capabilității de asigurare a sprijinului prin foc întrunit este identificarea și contracararea sincopelor generate de diferențele de perspectivă, la nivelul categoriilor de forțe, privind conceptele elementare din domeniul sprijinului prin foc. Aceste sincope sunt, din punctul meu de vedere, un efect al lipsei cadrului normativ doctrinar comun, menționat anterior, categoriile de forțe armate având propriile reglementări în acest domeniu. La acest moment, concepte, precum *misiuni tactice standard* sau *măsuri de coordonare a sprijinului prin foc*, nu sunt similar înțelese și implementate la nivelul tuturor categoriilor de forțe armate naționale. De exemplu, misiunea tactică standard *sprijin direct,* care poate fi atribuită unei structuri de sprijin prin foc, este detaliată diferit în forțele terestre față de forțele navale. Structurile de forțe terestre implementează prevederile doctrinei NATO pentru sprijinul prin foc AArtyP-5(B), NATO Fire Support Doctrine (NATO 2015, 3-2), iar structurile de forțe navale implementează prevederile doctrinei aliate pentru operații maritime AJP 3.1, Allied Joint Maritime Operations.

Instruirea responsabililor cu asigurarea sprijinului prin foc din structurile de forțe terestre, alături de ofițerii de legătură din celelalte categorii de forțe armate – componente ale grupării de forțe întrunite, asigură identificarea de sincope în exploatarea capabilităților de sprijin prin foc întrunit și poate determina implementarea de soluții pentru înlăturarea acestora, așa cum sunt SOP-urile.

***Înzestrar*e**
Programele naționale de înzestrare, derulate recent sau în curs de implementare, pot genera unele provocări în valorificarea noilor capabilități disponibile structurilor de forțe, alături de cele deja existente (MApN 2024). Astfel, înzestrarea cu tehnică de luptă modernă și înlocuirea celor învechite determină nu doar o revizuire a manualelor de luptă în vigoare, ci și o revizuire a cantității de echipamente militare disponibile în vederea asigurării eficienței structurii, în raport cu misiunea sa de bază.

O altă acțiune pe această direcție pentru consolidarea capabilității de sprijin prin foc întrunit vizează înțelegerea faptului că, modificările din domeniul înzestrării structurilor de forțe au impact asupra întregii structuri a operațiilor desfășurate de acestea. De exemplu, înzestrarea structurilor de forțe terestre cu sisteme HIMARS are impact asupra fiecărei componente a structurii operațiilor (*dispozitiv de luptă, sistem de lovire, amenajare genistică*) și implică o revizuire a volumului de resurse necesare forțelor astfel încât aceste noi capabilități de sprijin prin foc să poată fi real valorificate în operație. Dacă avem în vedere aspecte, precum necesitatea aprovizionării corespunzătoare cu muniții sau nevoia suplimentară de protecție antiaeriană și antirachetă (antidronă) a sistemelor HIMARS, putem concluziona că înzestrarea cu astfel de sisteme moderne impune o revizuire a cantității de echipamente militare de toate resorturile disponibile forței.

Leadership
Având în vedere că leadershipul este, așa după cum am menționat mai sus, un produs al educației continue care se constituie pe baza instruirii, expertizei și dezvoltării personale a indivizilor, consolidarea capabilității de asigurare a sprijinului prin foc întrunit poate fi obținută prin acțiuni în toate aceste domenii. Scopul final este dezvoltarea și menținerea nivelului optim de competențe profesionale, în primul rând, pentru responsabilii cu asigurarea sprijinului prin foc de la nivelul comandamentelor structurilor de forțe.

Un aspect important din punctul meu de vedere este că, în conformitate cu prevederile reglementărilor naționale în vigoare, responsabilii cu asigurarea sprijinului prin foc la nivel întrunit provin din rândul ofițerilor de armă artilerie și rachete terestre (SMFT 2018, I-2). În consecință, acțiunile de consolidare a capabilității de asigurare a sprijinului prin foc întrunit trebuie să fie focalizate pe pregătirea profesională optimizată a acestor responsabili pe parcursul întregii lor cariere, dezvoltându-le abilități de conceptualizare a sprijinului prin foc la nivel întrunit pe toate funcțiile ocupate și la toate cursurile de carieră la care participă.

O acțiune concretă pentru atingerea scopului propus poate fi, din punctul meu de vedere, ajustarea structurii curriculare a programelor tuturor cursurilor de carieră, pentru a integra în pregătirea acestor responsabili sisteme de sprijin prin foc din alte categorii de forțe armate naționale.
O altă acțiune concretă poate fi integrarea sistemelor de sprijin prin foc din alte categorii de forțe armate naționale în toate exercițiile desfășurate de responsabilii

cu asigurarea sprijinului prin foc în forțele terestre. De exemplu, coordonatorul sprijinului prin foc de la nivel brigadă, care este și comandantul batalionului de artilerie terestră organic, va avea la dispoziție în cadrul exercițiilor și unele sisteme de sprijin prin foc din forțele aeriene sau din forțele navale pentru a le integra în planul sprijinului prin foc al structurii sale.

Acțiunile pe această direcție a leadershipului care vizează pregătirea profesională adecvată a indivizilor – a liderilor militari – sunt o caracteristică a programelor de studii din Facultatea de Comandă și Stat Major a Universității Naționale de Apărare „Carol I", întrucât au stabilite, prin modelul absolventului, calitățile necesare liderilor militari de la toate nivelurile de comandă. Exercițiile de nivel întrunit, desfășurate în cadrul Universității Naționale de Apărare „Carol I" au, printre obiective, și dezvoltarea de deprinderi esențiale pentru ofițerii cursanți și studenți în conducerea acțiunilor militare. Responsabilii cu asigurarea sprijinului prin foc din forțele terestre beneficiază de expertiza colegilor din forțele aeriene și navale, stabiliți ca ofițeri de legătură la nivelul comandamentelor, pentru a planifica și a asigura pe timpul exercițiilor sprijinul prin foc de nivel întrunit.

Personal

Acțiunile pe această direcție sunt strâns legate de cele din domeniul *leadership*, însă au ca obiectiv asigurarea competențelor necesare tuturor categoriilor de personal implicat în exploatarea sistemului de sprijin prin foc de nivel întrunit. Personalul esențial, din punctul meu de vedere, pentru asigurarea sprijinului prin foc la nivel întrunit este cel care încadrează (sau augmentează, în cazul ofițerilor de legătură) comandamentele structurilor de forțe. Aceștia sunt principalii specialiști, dar și factorii responsabili care trebuie să dețină competențele necesare exploatării sistemului de sprijin prin foc întrunit într-o operație. Astfel, pregătirea profesională corespunzătoare tuturor cadrelor (indiferent de categoria de forțe din care provin, arma sau specialitatea de bază) care participă în cadrul celulelor/grupurilor de lucru în domeniul sprijinului prin foc este foarte importantă pentru valorificarea întregului potențial al capabilității de asigurare a sprijinului prin foc la nivel întrunit.

Facilități

Facilitățile existente la nivel național asigură, din punctul meu de vedere, condițiile minim necesare exploatării capabilității de asigurare a sprijinului prin foc întrunit, structurile de forțe armate naționale având la dispoziție o multitudine de elemente de infrastructură pentru instruire, antrenament și utilizare a sistemelor de sprijin prin foc. Nevoile punctuale de modernizare sau de îmbunătățire a condițiilor oferite de facilitățile disponibile sunt permanent analizate la nivelul fiecărei categorii de forțe, în parte.

O acțiune pe această direcție poate fi, din punctul meu de vedere, analiza oportunității existenței unui poligon la nivel național care să permită folosirea la distanțe mari a sistemelor de sprijin prin foc cu bătaie foarte mare, așa cum sunt sistemele HIMARS, care au muniții cu rază de acțiune de până la 300 km, sau dronele

de tip Bayraktar. Odată cu introducerea în înzestrarea structurilor de forțe armate naționale a unor noi sisteme de sprijin prin foc sau cu caracteristici superioare celor pe care le înlocuiesc, pot apărea și astfel de nevoi. Poligoanele de trageri existente la nivel național asigură folosirea acestor muniții, însă în anumite limite, poligoanele fiind dezvoltate și omologate pentru capabilități de generație mai veche.

Interoperabilitate

Acțiunile în acest domeniu vizează asigurarea interoperabilității tehnice, umane și procedurale pentru ca personalul și echipamentele care constituie sistemele de sprijin prin foc la nivelul categoriilor de forțe armate naționale să poată real fundamenta capabilitatea de asigurare a sprijinului prin foc la nivel întrunit.

Prin elaborarea doctrinei sprijinului prin foc întrunit și prin întrebuințarea procedurilor standard de operare, pe care le-am menționat mai sus, se acoperă nevoia de interoperabilitate procedurală necesară capabilității de asigurare a sprijinului prin foc întrunit.

Instruirea în comun a responsabililor cu asigurarea sprijinului prin foc din toate categoriile de forțe armate naționale în cadrul exercițiilor militare de nivel întrunit acoperă nevoia de interoperabilitate umană necesară capabilității de asigurare a sprijinului prin foc întrunit.

Interoperabilitatea tehnică este cea mai problematică, din punctul meu de vedere, deoarece realizarea acesteia implică achiziția de sisteme specializate, așa cum sunt sistemele automatizate de comandă și control sau sistemele automatizate de conducere a focului. De astfel de sisteme, depinde valorificarea întregului potențial al sistemelor de sprijin prin foc disponibile unei grupări de forțe. Un exemplu în acest sens este sistemul IFATDS (International Field Artillery Tactical Data System), disponibil structurilor înzestrate cu HIMARS, care trebuie integrat, din punctul meu de vedere, cu sisteme la fel de moderne de comandă și control sau de tip ISR (Intelligence, Surveillance and Reconnaissance/ Informații, Supraveghere și Cercetare) astfel încât valorificarea întregului potențial al sistemelor HIMARS să poată fi realizată.

Concluzii

Implementarea programelor de înzestrare actuale sau a celor de perspectivă, care presupun achiziția și introducerea în dotarea structurilor de forțe armate naționale a diverselor echipamente militare moderne, aduce cu sine și anumite provocări privind exploatarea și valorificarea optimizată a capabilităților astfel dobândite. Alături de avantajele directe, ușor sesizabile, pe care noile echipamente militare le aduc structurilor de forțe, trebuie luate în considerare toate implicațiile pe care acestea le au pentru a putea fi exploatate într-o operație la întregul lor potențial. Astfel, schimbările organizatorice, impuse de noile echipamente, reflectate în statele de organizare, trebuie însoțite de revizuiri ale unor domenii conexe care au legătură directă sau indirectă cu exploatarea lor, așa cum sunt pregătirea profesională a personalului responsabil cu

folosirea echipamentelor, facilitățile existente pentru instruirea indivizilor, a echipelor, a grupelor sau a unităților, volumul de resurse normate structurilor beneficiare, gradul de interoperabilitate al acestor echipamente etc.

Modelul de analiză, desfășurată pe cele opt direcții de acțiune ale acronimului DOTMLPF-I, este un instrument util pentru a înțelege toate implicațiile exploatării oportune a unei noi capabilități, dar și pentru a ne contura o perspectivă de optimizare a unei capabilități existente. În cadrul acestui articol, am folosit acest instrument pentru a aborda sistematic fiecare aspect sub care capabilitatea ca obiect de studiu – asigurarea sprijinului prin foc întrunit – poate fi consolidată prin acțiuni concrete pe cele opt direcții. Am ajuns astfel să identific unele sincope în modul actual de exploatare a sistemului de sprijin prin foc întrunit la nivel național și, totodată, să fundamentez acțiuni cu caracter de propuneri de îmbunătățire a capabilității de asigurare a sprijinului prin foc la nivel întrunit.

Capabilitățile asumate de țara noastră ca o contribuție la planificarea apărării colective a NATO, analizate inclusiv pe modelul DOTMLPF-I, sunt cele care fundamentează nevoile de achiziții sau nevoia de schimbare a anumitor aspecte pe cele opt direcții, astfel încât aceste capabilități asumate să fie real dezvoltate și consolidate la nivel național.

Referințe

James, Randy. 2020. ”Standard Operating Procedures: This is the way we’ve always done it.” *U.S. Army.* https://www.army.mil/article/238732/standard_operating_procedures_this_is_the_way_weve_always_done_it.

Ministerul Apărării Naționale [MAPN]. 2024. „Programe de înzestrare”. https://www.dpa.ro/programe-de-inzestrare/.

MD Harris Institute. 2013. ”DOTMLPF-P Analysis for War and Peace”. https://mdharrismd.com/2013/11/09/dotmlpf-p-analysis-and-military-medicine/.

Mirea, Adrian și Cristian-Octavian Stanciu. 2024. „Implementarea unei doctrine a sprijinului prin foc de nivel întrunit – cerință a operației întrunite.” *Colocviu Strategic*, Nr. 1: 1-6.

Mureșan, Darius. 2024. „Câte HIMARS are România și când ajung ultimele sisteme în țară. Armata deține inclusiv celebrele rachete ATACMS ce lovesc la 300 km distanță.” *Defense Romania.* https://www.defenseromania.ro/cate-himars-are-romania-si-cand-ajung-ultimele-sisteme-in-tara-armata-detine-inclusiv-celebrele-rachete-atacms-ce-lovesc-la-300-km-distanta_629999.html.

NATO. 2015. *NATO FIRE SUPPORT DOCTRINE AArtyP-5.* NATO: NATO Standardization Office.

—. 2018. ”NATO’s Joint Air Power Strategy”. https://www.nato.int/cps/en/natohq/official_texts_156374.htm?selectedLocale=en.

—. 2021. *NATO CD-E Handbook, A concept developer`s toolbox.* Norfolk: Allied Command Transformation.

—. 2023. ”Interoperability: connecting forces”. https://www.nato.int/cps/en/natohq/topics_84112.htm.

Okoko, Janet Mola, Scott Tunison și Keith D. Walker. 2023. *Varieties of Qualitative Research Methods.* Saskatoon, Saskatoon: Springer Texts in Education.

Portal legislativ. 2016. „Strategia militară a României din 28 septembrie 2016.” Publicat în Monitorul Oficial, nr. 789, din 7 octombrie 2016. https://legislatie.just.ro/Public/DetaliiDocument/182367.

Statul Major al Apărării [SMFT]. 2018. *Manualul sprijinului prin foc în operațiile grupării de forțe F.T.-6.* București: MApN.

—. 2019. „Noutăți SG19”. https://www.defense.ro/sg19/noutati.

Willi, Bernie. 2016. ”Assessing Nations for NATO Partnerships.” *Transforming Joint Air Power The journal of the JAPCC* 51-54.

BULETINUL
UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I"
https://buletinul.unap.ro

Profilul personalității liderilor performanți: o analiză BFI-2

Personality profile of high-performing leaders: a BFI-2 analysis

Lt.col.Dr. Cristian PANAIT*
*Academia Forțelor Aeriene „Henri Coandă", Brașov
e-mail: cristian.panait@afahc.ro

Abstract

În acest articol sunt studiate trăsăturile de personalitate ale unui grup de lideri cu performanțe într-un mediu militar. În cadrul studiului, a fost utilizat Inventarul Big Five-2 (BFI-2), analiza T-score și analiza dispersională (ANOVA) pentru a stabili configurațiile de personalitate care contribuie la un leadership eficient în mediul militar. Studiul confirmă importanța BFI-2 în identificarea trăsăturilor care indică un potențial ridicat de succes pentru exercitarea comenzii în medii tensionate, evidențiind diferențele dintre lideri și media populației. Rezultatele sugerează că promovarea acestor trăsături poate crește eficacitatea în leadership, oferind astfel o perspectivă utilă pentru programele de selecție și instruire.

The present study employs a Big Five Inventory-2 (BFI-2) analysis to investigate the personality traits of a group of high-performing leaders operating within a military context. The Big Five Inventory-2 (BFI-2), T-score analysis, and Variance analysis (ANOVA) were utilized to identify the personality configurations contributing to effective leadership in military environments. The study validates the utility of the BFI-2 in identifying personality traits that are predictive of success in exercising leadership in high-stress environments; it also highlights the distinction between leaders and the mean of the general population on these traits. The results indicate that the enhancement of these traits may result in increased leadership effectiveness, thus providing insights for the improvement of human resources selection and training programs.

Cuvinte-cheie:
lider militar; Inventarul Big Five-2 (BFI-2); conștiinciozitate; stabilitate emoțională; leadership; evaluarea personalității; selecția și formarea resurselor umane.

Keywords:
High-Performing Military Leaders; Big Five Inventory-2 (BFI-2); Personality Traits; Conscientiousness; Emotional Stability; Leadership; Personality Assessment; Human Resources Selection and Training.

Info articol
Primit: 14 noiembrie 2024; Evaluat: 29 noiembrie 2024; Acceptat: 10 decembrie 2024; Disponibil online: 17 ianuarie 2025
Citare: Panait, C. 2024. „Profilul personalității liderilor performanți: o analiză BFI-2".
Buletinul Universității Naționale de Apărare „Carol I", 13(4): 140-151. https://doi.org/10.53477/2065-8281-24-44

În acest articol sunt prezentate profilurile de personalitate ale unui grup de lideri cu performanțe, într-un context militar, utilizând Inventarul Big Five-2 (BFI-2), pentru a identifica trăsăturile de personalitate predominante, și rezultatele *T-score*, pentru a putea compara rezultatele la nivelul populației în general.

În cuprinsul articolului, termenul „lider performant" se referă la persoanele aflate în poziții de conducere și care dau dovadă de calități deosebite în atingerea obiectivelor organizaționale, în gestionarea responsabilităților și menținerea rezilienței sub presiune. Aceste caracteristici sunt esențiale și definesc activitatea unui ofițer care reușește să avanseze în carieră în funcții sensibile de conducere, din perspectiva responsabilităților. Lotul pentru cercetare este alcătuit din ofițeri care au fost admiși într-o școală militară de studii superioare, în urma unui proces riguros de selecție, care au demonstrat nu doar intenție, dedicare și spirit de sacrificiu, prin alocarea timpului personal pentru a finaliza o instruire riguroasă, ci și competență în îndeplinirea funcțiilor de conducere în diverse domenii militare. Specialitatea acestor ofițeri este de piloți de vânătoare, piloți de transport, controlori de trafic aerian și ofițeri de apărare antiriană. Aceste criterii de a identifica liderii cu performanțe sunt în concordanță cu studii ale unor cercetători, precum S. Singh (2003), conform căruia liderii cu rezultate superioare favorizează adaptabilitatea și coeziunea echipei, în contexte de înaltă performanță, D.M. Hutton (2018) care se referă la adaptabilitatea situațională și eficacitatea interpersonală în medii de risc ridicat, precum și P. Hawkins (2014), care subliniază că liderii care obțin performanțe excelează în formarea unor echipe eficiente și în îndeplinirea obiectivelor.

Înțelegerea trăsăturilor de personalitate care contribuie la un leadership eficient este un obiectiv de interes în cercetarea psihologică, modelul de personalitate Big Five evidențiindu-se ca un instrument de cercetare care oferă un cadru relevant, acceptat și validat științific (Cronbach Alpha = 0,86). Inventarul Big Five-2 (BFI-2), care reprezintă o evoluție a Inventarului original Big Five, oferind un instrument pentru măsurarea trăsăturilor de personalitate, asociate cu potențialul și performanța în leadership. Dezvoltat de Soto și John (2017a), BFI-2 extinde sfera evaluării personalității prin introducerea unui model ierarhic care include 15 factori sau trăsături la nivel de fațetă, în cadrul celor cinci metafactori majori: *extraversie*, *agreabilitate*, *conștiinciozitate*, *instabilitate emoțională* (emoționalitate negativă sau neuroticism) și *deschidere către experiențe* (Open-Mindedness). Prin realizarea unei analize atât generale, cât și detaliate, BFI-2 oferă o putere predictivă și o fiabilitate sporită, fiind relevant pentru evaluarea trăsăturilor de personalitate care susțin leadershipul.

Evaluarea personalității prin modelul Big Five și-a dovedit constant relevanța în mediile organizaționale, unde anumite trăsături de personalitate sunt corelate cu eficacitatea în leadership. Cercetările indică faptul că nivelurile ridicate de *conștiinciozitate* și *stabilitate emoțională* sunt asociate, în mod deosebit, cu eficiența în leadership, întrucât aceste trăsături favorizează comportamentul orientat spre îndeplinirea obiectivelor, reziliență și luarea deciziilor într-un mod stabil.

Conștiinciozitatea ridicată, caracterizată prin trăsături, precum *productivitate*, *organizare* și *responsabilitate*, permite liderilor să adopte o abordare disciplinată, esențială pentru a face față unor cerințe complexe. *Stabilitatea emoțională*, reprezentată prin scoruri scăzute ale factorilor *anxietate* și *volatilitate emoțională*, le permite liderilor să gestioneze eficient stresul, factor important în situațiile care necesită gândire rapidă și luarea deciziilor cu calm.

Capacitatea BFI-2 de a evalua trăsăturile, folosind *T-score* facilitează o măsurare standardizată a intensității trăsăturilor la diverse grupuri de indivizi, ajustează scorurile individuale, în comparație cu un eșantion normativ, permițând analiza comparativă a modului în care anumite trăsături pot varia în rândul liderilor, în raport cu marea masă a oamenilor. În domeniul de studiu al leadershipului, *T-score* oferă o perspectivă valoroasă asupra modului în care intensitățile factorilor, precum *conștiinciozitatea* și *stabilitatea emoțională,* pot indica potențialul de succes al unui lider în contexte diverse, în special în medii cu riscuri ridicate, cum ar fi cel militar, unde reziliența și disciplina sunt esențiale.

Cercetările anterioare subliniază importanța anumitor trăsături din modelul Big Five în îmbunătățirea performanței în leadership, Judge *și colab.* (2002) au descoperit că, deși *extraversia* poate fi mai puțin predominantă decât *conștiinciozitatea* și *stabilitatea emoțională*, aceasta contribuie totuși la leadership prin promovarea interacțiunilor sociale pozitive, asertivității și comunicării eficiente în echipă. *Agreabilitatea*, deși nu este asociată foarte des cu leadershipul, din cauza potențialului de a reduce autoritatea, fermitatea comenzii, poate totuși îmbunătăți încrederea și armonia în grup, mai ales la liderii care obțin scoruri ridicate la fațete, precum *încrederea* și *respectul*. Prin urmare, nivelurile moderate de *agreabilitate* pot crea o abordare echilibrată, care încurajează munca în echipă, fără a compromite autoritatea.

Prin analiza *T-score*, cercetarea oferă o perspectivă comparativă asupra intensității trăsăturilor, evidențiind rolul pe care îl au *conștiinciozitatea* și *stabilitatea emoțională* în cadrul lotului pentru cercetare. Aceste constatări contribuie la înțelegerea modului în care anumiți factori Big Five se aliniază cu leadershipul eficient, oferind o perspectivă detaliată asupra rolului personalității în predictibilitatea succesului în leadership. Această cercetare este relevantă și datorită faptului că organizațiile se bazează din ce în ce mai mult pe evaluări de personalitate, precum BFI-2, pentru selecția resursei umane și instruirea în diverse domenii de activitate.

Metodologia cercetării și obiective

Acest studiu utilizează o metodologie cantitativă și comparativă pentru a analiza trăsăturile de personalitate ale liderilor militari performanți, folosind instrumentul Big Five Inventory-2 (BFI-2). Scorurile brute au fost transformate în scoruri T, permițând comparații standardizate cu o populație normativă și facilitând înțelegerea trăsăturilor de personalitate predictive pentru succesul în leadership.

Orientarea studiului către leadershipul militar în medii cu stres ridicat a condus la formularea următoarelor întrebări de cercetare:

1. Care sunt cele mai pronunțate trăsături de personalitate ale liderilor militari cu performanțe semnificative, identificate prin BFI-2?
2. Cum se compară aceste trăsături cu cele ale celorlalți oameni, în general, utilizând scoruri normative T?

Prin abordarea acestor întrebări de cercetare, studiul își propune să identifice configurațiile de personalitate esențiale unui leadership eficient.

BFI-2 a fost ales ca instrument de cercetare datorită validității sale demonstrate, de a măsura atât trăsăturile de personalitate în multiple culturi și grupuri de indivizi, cât și cele specifice, cum este cel militar. Acest instrument de cercetare conține 60 de itemi, grupați în cinci metafactori: *extraversie, agreabilitate, conștiinciozitate, instabilitate emoțională și deschidere către experiențe,* împreună cu 15 factori care permit o analiză mai detaliată în cadrul fiecărui metafactor. Alegerea acestui instrument de cercetare este în concordanță cu cercetările care subliniază importanța perspectivelor la nivel de fațetă pentru predictibilitatea anumitor rezultate în leadership (Soto și John 2017b, 69-81). De exemplu:

- *conștiinciozitate*: factori, precum *productivitatea*, *responsabilitatea* și *organizarea,* sunt deosebit de relevanți, datorită asocierii lor cu comportamente orientate spre îndeplinirea obiectivelor (misiunilor), fiabilitate și atenție la detalii. Liderii care obțin scoruri ridicate la acești factori sunt mai predispuși să exceleze în roluri care necesită disciplină și consistență.
- *instabilitate emoțională*: scorurile scăzute la factori, precum *anxietatea*, *volatilitatea emoțională* și *depresia,* indică stabilitate emoțională, o trăsătură importantă pentru liderii care operează în medii stresante. Această stabilitate permite liderilor să rămână calmi și concentrați pentru luarea deciziilor raționale, în situații dinamice sau de criză.
- *extraversie* și *agreabilitate*: scorurile moderate la factori, precum *sociabilitatea*, *asertivitatea* și *încrederea,* au fost evaluate pentru a înțelege rolul lor în îmbunătățirea dinamicii echipei și în dezvoltarea relațiilor interpersonale. În leadership, aceste trăsături creează un echilibru între autoritate și abordabilitate, contribuind la coeziunea echipei și la moralul acesteia.
- *deschidere către experiențe*: *imaginația creativă* și *curiozitatea intelectuală* au fost evaluate ca indicatori ai adaptabilității și deschiderii către idei noi, trăsături benefice pentru liderii care trebuie să lucreze în medii complexe și în continuă schimbare.

Prezentarea lotului pentru cercetare

Lotul pentru cercetare a fost format din 29 de indivizi, dintr-un grup de 30 de ofițeri din cadrul Forțelor Aeriene Române care urmează Masterul de Conducere Interarme, specializarea Forțe Aeriene.

Acești ofițeri au fost admiși în urma unui proces riguros de selecție, demonstrând devotamentul și competența necesară pentru funcții de conducere, toți ofițerii aveau grade de ofițer superior, cu un minim de 15 ani experiență în actul de conducere militară. Specializările lor includ piloți de vânătoare, piloți de transport, controlori de trafic aerian și ofițeri de apărare aeriană, reflectând o gamă diversă de domenii militare în care adaptabilitatea, disciplina și capacitatea decizională sunt esențiale. Acest context asigură că lotul pentru cercetare reprezintă un grup orientat spre performanță și leadership, adecvat pentru examinarea trăsăturilor de personalitate, asociate cu un leadership eficient. Din punct de vedere psihologic, acest grup este, teoretic, un grup omogen, deoarece selecția în carieră s-a făcut inclusiv prin admiterea unor examene psihologice, care se susțin cu periodicitate. Pentru a investiga potențialele interacțiuni dintre trăsăturile de personalitate cheie, asociate cu leadershipul eficient, variabilele *conștiinciozitate* și *stabilitate emoțională*, a fost efectuată o analiză dispersională (ANOVA), având în vedere că, în cadrul lotului pentru cercetare, au existat două grupuri, ofițeri din primul și din al doilea an de studii. Această abordare a permis verificarea existenței unor efecte de interacțiune semnificative între aceste trăsături, pe diferite niveluri de formare, oferind o înțelegere mai detaliată a modului în care respectivele trăsături combinate pot influența performanța în leadership. Prin examinarea interacțiunii dintre *conștiinciozitate* și *stabilitate emoțională*, analiza a avut ca scop descoperirea diferențelor de efecte combinate ale acestor trăsături între cele două grupuri, contribuind astfel la evaluarea potențialului de leadership în diferite etape ale pregătirii ofițerilor.

Crearea unui grup de studiu, format doar din ofițeri militari limitează generalizarea constatărilor la alte contexte ocupaționale, cercetările viitoare ar putea extinde aceste constatări la alte profesii, care presupun funcționarea în situații tensionate, precum sănătate, aplicarea legii sau chiar corporativ, pentru a determina dacă profiluri de personalitate similare produc eficiență în leadership. În plus, examinarea schimbărilor longitudinale ale trăsăturilor de personalitate în rândul liderilor ar putea oferi perspective asupra modului în care trăsături, precum conștiinciozitatea și stabilitatea emoțională, se dezvoltă sau fluctuează de-a lungul carierei unui lider sau dacă sunt stabile, fixe.

Personalitatea este considerată ca fiind relativ fixă, în funcție de vârstă, după vârsta de 30 de ani schimbările survenite fiind nesemnificative. Într-un studiu (Srivastava și alții 2003, 1041-1053) efectuat pe un eșantion n = 132.515 de indivizi, s-a constatat că agreabilitatea și conștiinciozitatea au crescut pe parcursul vârstei adulte timpurii și mijlocii, iar stabilitatea emoțională a scăzut în rândul femeilor, nu și al bărbaților.

Procedura de evaluare

BFI-2 a fost administrat într-un mediu controlat, față în față, pentru a asigura consistența răspunsurilor și pentru a răspunde pe loc, în cazul unor nelămuriri. Fiecare participant a completat inventarul de 60 de itemi, traduși în limba română de

personal specializat, cu itemi concepuți pentru a evalua trăsăturile de personalitate, pe dimensiunile modelului Big Five. Participanții au evaluat afirmațiile pe o scală Likert, de la 1 (total dezacord) la 5 (total acord), care a fost apoi transformată în scoruri brute pentru fiecare metafactor și factor. Pentru standardizarea rezultatelor, scorurile brute au fost convertite în *T-score*, metodă psihometrică ce permite interpretarea normativă a scorurilor individuale, în comparație cu un grup mai larg de indivizi. Baza de date la care am comparat rezultatele obținute este prezentată în Tabelul 1 (Soto și John 2017a, 117-143).

TABEL NR. 1

Statistica descriptivă pentru BFI-2

	Internet sample				Student sample				
Domain or facet	Men *M* (*SD*)	Women *M* (*SD*)	Combined *M* (*SD*)	Gender *d*	Men *M* (*SD*)	Women *M* (*SD*)	Combined *M* (*SD*)	Gender *d*	Sample *d*
Extraversion	3.15 (.78)	3.31 (.80)	3.23 (.80)	.21	3.20 (.70)	3.31 (.73)	3.25 (.71)	.15	−.03
Sociability	2.80 (1.02)	3.10 (1.07)	2.95 (1.05)	.29	2.94 (.86)	3.06 (1.01)	3.00 (.94)	.12	−.05
Assertiveness	3.28 (.92)	3.28 (.93)	3.28 (.93)	.01	3.27 (.82)	3.28 (.85)	3.28 (.84)	.02	.01
Energy Level	3.37 (.88)	3.56 (.89)	3.47 (.89)	.22	3.40 (.80)	3.58 (.72)	3.49 (.77)	.24	−.03
Agreeableness	3.57 (.65)	3.79 (.60)	3.68 (.64)	.35	3.51 (.63)	3.82 (.56)	3.66 (.62)	.53	.03
Compassion	3.72 (.79)	3.97 (.76)	3.84 (.78)	.33	3.60 (.81)	3.98 (.69)	3.79 (.78)	.49	.07
Respectfulness	3.87 (.73)	4.08 (.68)	3.98 (.71)	.30	3.76 (.68)	4.05 (.64)	3.91 (.68)	.44	.10
Trust	3.13 (.83)	3.32 (.80)	3.23 (.82)	.24	3.15 (.77)	3.43 (.77)	3.29 (.78)	.36	−.08
Conscientiousness	3.35 (.74)	3.50 (.79)	3.43 (.77)	.20	3.34 (.60)	3.54 (.66)	3.44 (.64)	.31	−.03
Organization	3.33 (.99)	3.51 (1.03)	3.42 (1.01)	.19	3.46 (.88)	3.68 (.87)	3.57 (.88)	.26	−.16
Productiveness	3.31 (.87)	3.43 (.93)	3.37 (.90)	.13	3.24 (.75)	3.39 (.80)	3.32 (.78)	.19	.07
Responsibility	3.40 (.78)	3.57 (.83)	3.48 (.81)	.20	3.33 (.60)	3.55 (.71)	3.44 (.66)	.33	.05
Negative Emotionality	2.95 (.88)	3.18 (.84)	3.07 (.87)	.27	2.84 (.74)	2.95 (.79)	2.89 (.76)	.14	.21
Anxiety	3.28 (.95)	3.58 (.88)	3.43 (.93)	.33	3.20 (.78)	3.53 (.85)	3.37 (.83)	.40	.07
Depression	2.82 (1.03)	2.88 (1.02)	2.85 (1.02)	.06	2.65 (.92)	2.53 (.93)	2.59 (.93)	−.14	.26
Emotional Volatility	2.77 (1.04)	3.09 (1.04)	2.93 (1.05)	.31	2.66 (.91)	2.79 (.97)	2.73 (.95)	.13	.20
Open-Mindedness	3.93 (.64)	3.91 (.67)	3.92 (.65)	−.02	3.71 (.65)	3.62 (.63)	3.66 (.64)	−.15	.39
Intellectual Curiosity	4.18 (.69)	4.03 (.71)	4.10 (.70)	−.21	3.89 (.76)	3.80 (.70)	3.85 (.73)	−.12	.24
Aesthetic Sensitivity	3.71 (.90)	3.88 (.94)	3.80 (.92)	.19	3.57 (.95)	3.58 (.90)	3.58 (.92)	.02	.36
Creative Imagination	3.89 (.81)	3.82 (.80)	3.85 (.81)	−.09	3.68 (.75)	3.46 (.77)	3.57 (.77)	−.28	.36
Sample size	500	500	1,000		313	146	459		

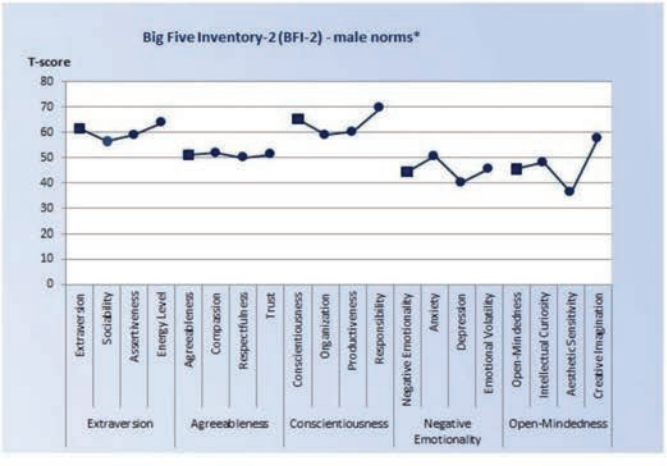
Rezultatele au fost introduse manual într-o bază de date comună, care, ulterior, au fost analizate în vederea obținerii datelor privind: media totală a fiecărei trăsături, deviația standard a răspunsurilor, media subgrupului de anul I, a celui de anul II și cea totală.

Pentru fiecare subiect în parte, a fost întocmit un profil al trăsăturilor de personalitate, așa după cum este exemplificat în tabelele 2 și 3.

TABEL NR. 2

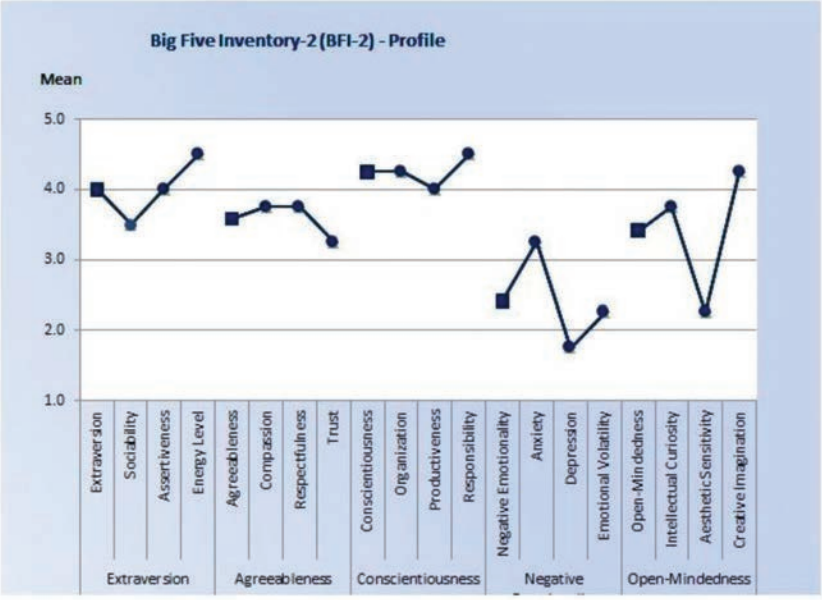
Profilul subiectului 10 (S10), în funcție de *T-score*

	Mean	*T-score**
Extraversion	4.0	61.4
Sociability	3.5	56.5
Assertiveness	4.0	58.9
Energy Level	4.5	63.8
Agreeableness	3.6	51.2
Compassion	3.8	51.9
Respectfulness	3.8	49.9
Trust	3.3	51.3
Conscientiousness	4.3	65.2
Organization	4.3	59.0
Productiveness	4.0	60.1
Responsibility	4.5	69.5
Negative Emotionality	2.4	44.3
Anxiety	3.3	50.6
Depression	1.8	40.2
Emotional Volatility	2.3	45.5
Open-Mindedness	3.4	45.5
Intellectual Curiosity	3.8	48.2
Aesthetic Sensitivity	2.3	36.1
Creative Imagination	4.3	57.6



TABEL NR. 3

Profilul subiectului 10 (S10) BFI-2



Analiza datelor

Datele au fost analizate prin calcularea scorurilor medii T pentru fiecare factor, pentru fiecare subiect, apoi au fost comparate cu datele normative pentru a determina gradul de abatere. Statistica descriptivă a fost utilizată pentru a identifica profilurile de personalitate ale lotului pentru cercetare, acordându-se o atenție deosebită scorurilor ridicate sau reduse, în comparație cu media normativă. Această abordare metodologică asigură că rezultatele studiului sunt atât valide din punct de vedere statistic, cât și aplicabile într-un context controlat de leadership.

TABEL NR. 4

Rezultatele BFI-2, subgrupa Anul I

Extraversion	57.9	54.3	69.8	59.0	46.0	63.8	54.3	56.7	50.7	52.6	53.7	56.7	44.6	54.3	56.7
Sociability	68.1	56.5	74.0	56.5	50.7	65.2	56.5	56.5	56.5	51.9	51.9	59.4	49.4	53.6	56.5
Assertiveness	43.7	46.7	62.0	58.9	43.7	62.0	52.8	52.8	46.7	58.5	52.6	55.9	46.7	52.8	55.9
Energy Level	57.5	57.5	63.8	57.5	45.0	57.5	51.3	57.5	48.1	45.4	55.8	51.3	38.5	54.4	54.4
Agreeableness	60.4	56.5	71.0	52.5	45.9	67.0	56.5	56.5	51.2	53.2	50.2	53.8	48.8	55.1	51.2
Compassion	58.0	51.9	67.3	48.8	45.7	64.2	54.9	51.9	48.8	53.9	50.3	48.8	43.0	51.9	45.7
Respectfulness	53.5	53.5	60.9	46.2	46.2	64.6	53.5	53.5	53.5	49.2	49.2	53.5	37.5	53.5	57.2
Trust	64.3	61.0	74.0	61.0	48.1	64.3	57.8	61.0	51.3	54.2	50.9	57.8	63.9	57.8	51.3
Conscientiousness	61.0	54.1	77.7	66.6	45.7	67.9	66.6	58.2	61.0	57.0	62.0	49.9	40.6	62.4	63.8
Organization	53.3	47.6	67.5	61.8	47.6	67.5	59.0	53.3	56.1	53.7	56.6	50.5	39.3	59.0	59.0
Productiveness	66.8	60.1	73.5	66.8	46.8	66.8	66.8	56.8	60.1	57.6	60.8	50.1	42.0	60.1	60.1
Responsibility	57.0	52.8	77.8	61.2	44.5	57.0	65.3	61.2	61.2	56.3	63.4	48.7	45.8	61.2	65.3
Negative Emotionality	46.5	47.7	26.3	45.4	46.5	37.5	34.1	47.7	44.3	40.1	40.1	46.5	50.6	45.4	44.3
Anxiety	41.0	47.4	25.0	50.6	44.2	28.2	34.6	44.2	41.0	37.9	37.9	47.4	52.6	44.2	37.8
Depression	51.1	48.4	32.1	37.5	51.1	45.7	37.5	48.4	48.4	44.3	47.0	45.7	52.4	48.4	45.7
Emotional Volatility	48.2	48.2	31.8	51.0	45.5	42.7	37.3	51.0	45.5	41.9	39.3	48.2	47.0	45.5	51.0
Open-Mindedness	51.9	44.2	59.6	46.8	44.2	46.8	42.9	37.8	41.6	54.7	57.4	50.6	46.8	48.1	48.1
Intellectual Curiosity	48.2	44.9	48.2	44.9	44.9	51.4	35.0	38.3	44.9	49.3	56.4	44.9	49.3	48.2	44.9
Aesthetic Sensitivity	51.9	44.0	57.2	49.3	44.0	36.1	44.0	38.7	41.4	51.9	54.7	51.9	43.6	46.6	46.6
Creative Imagination	54.3	47.6	67.6	47.6	47.6	57.6	54.3	44.3	44.3	60.3	57.0	54.3	50.5	50.9	54.3
	S15	S16	S17	S18	S19	S20	S21	S22	S23	S24	S25	S26	S27	S28	S29

Utilizarea T-score și a analizei la nivel de factor, oferită de BFI-2, contribuie la o înțelegere detaliată a profilurilor de personalitate prin standardizarea scorurilor în jurul unei medii de 50, cu o deviație standard de 10, permițând cercetătorilor să determine în ce măsură nivelul unei trăsături individuale se raportează la normă. În contextul acestui studiu, T-score a oferit perspective asupra trăsăturilor mai pronunțate sau reduse în rândul liderilor cu performanțe, în comparație cu restul indivizilor. Baza de date, rezultată în urma centralizării răspunsurilor, a fost realizată pentru analiza statistică a subgrupelor, așa după cum este prezentată în tabelele 4 și 5.

TABEL NR. 5

Rezultatele BFI-2, subgrupa Anul II

Extraversion	65.0	57.9	61.4	54.3	54.3	54.3	59.0	59.5	50.7	61.4	49.5	63.8	57.9	55.5
Sociability	65.2	56.5	59.4	47.8	47.8	53.6	62.3	59.3	53.6	56.5	47.8	62.3	62.3	50.7
Assertiveness	58.9	55.9	52.8	52.8	55.9	52.8	58.9	55.5	49.8	58.9	49.8	62.0	52.8	52.8
Energy Level	63.8	57.5	66.9	60.6	57.5	54.4	51.3	59.3	48.1	63.8	51.3	60.6	54.4	60.6
Agreeableness	52.5	40.6	67.0	55.1	44.6	56.5	53.8	50.2	52.5	51.2	57.8	63.1	55.1	57.8
Compassion	42.6	33.3	54.9	48.8	45.7	54.9	61.1	50.3	54.9	51.9	48.8	64.2	61.1	58.0
Respectfulness	53.5	38.8	64.6	53.5	38.8	53.5	46.2	49.2	42.5	49.9	53.5	53.5	49.9	53.5
Trust	61.0	54.5	74.0	61.0	51.3	57.8	51.3	50.9	57.8	51.3	67.5	64.3	51.3	57.8
Conscientiousness	70.7	63.8	76.3	61.0	63.8	45.7	55.4	63.3	61.0	65.2	69.3	69.3	48.5	62.4
Organization	64.7	64.7	67.5	56.1	59.0	36.3	53.3	56.6	59.0	59.0	59.0	56.1	41.9	56.1
Productiveness	66.8	56.8	73.5	60.1	60.1	53.5	56.8	63.9	60.1	60.1	66.8	66.8	56.8	63.5
Responsibility	69.5	61.2	73.7	61.2	65.3	52.8	52.8	63.4	57.0	69.5	73.7	77.8	48.7	61.2
Negative Emotionality	38.6	40.9	38.6	40.9	46.5	36.4	42.0	36.9	39.8	44.3	39.8	27.4	47.7	37.5
Anxiety	50.6	47.4	41.0	37.8	41.0	37.8	37.8	34.9	34.6	50.6	31.4	28.2	50.6	34.6
Depression	37.5	34.8	40.2	45.7	42.9	37.5	48.4	38.9	48.4	40.2	42.9	32.1	48.4	42.9
Emotional Volatility	34.5	45.5	40.0	42.7	56.5	40.0	42.7	41.9	40.0	45.5	48.2	31.8	45.5	40.0
Open-Mindedness	45.5	46.8	45.5	45.5	48.1	36.5	54.5	53.4	57.0	45.5	44.2	55.7	41.6	49.3
Intellectual Curiosity	48.2	35.0	48.2	51.4	44.9	28.4	48.2	49.3	58.0	48.2	44.9	54.7	31.7	44.9
Aesthetic Sensitivity	38.7	44.0	33.5	38.7	54.5	41.4	51.9	51.9	51.9	36.1	41.4	57.2	41.4	49.3
Creative Imagination	54.3	64.3	60.9	50.9	44.3	47.6	60.9	57.0	57.6	57.6	50.9	50.9	57.6	54.3
	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12	S13	S14

TABEL NR. 6

Media BFI rezultată în urma punctajelor obținute

Extraversion	56.4	57.5	55.4
Sociability	56.8	56.1	57.6
Assertiveness	53.8	55.0	52.8
Energy Level	55.4	57.9	53.0
Agreeableness	54.7	54.1	55.3
Compassion	52.3	52.2	52.3
Respectfulness	51.3	50.1	52.4
Trust	58.3	58.0	58.6
Conscientiousness	61.0	62.6	59.6
Organization	55.9	56.4	55.4
Productiveness	60.7	61.8	59.7
Responsibility	60.9	63.4	58.6
Negative Emotionality	41.4	39.8	42.9
Anxiety	40.4	39.9	41.0
Depression	43.6	41.5	45.6
Emotional Volatility	43.8	42.5	44.9
Open-Mindedness	47.9	47.8	48.1
Intellectual Curiosity	45.8	45.4	46.2
Aesthetic Sensitivity	46.0	45.1	46.8
Creative Imagination	53.8	54.9	52.8
	Medie	An II	An I

Având în vedere că grupul de studiu este format dintr-un număr mic de subiecți (<30), am comparat rezultatele obținute cu eșantionul prezentat în Tabelul 1, în Tabelul 6 fiind prezentată media rezultatelor obținute.

Interpretarea datelor

Dintre cei cinci metafactori Big Five: *extraversie, agreabilitate, conștiinciozitate, instabilitate emoțională și deschidere către experiențe,* se evidențiază la o primă vedere (cu verde valorile maxime, cu roșu valorile minime) scorurile la *conștiinciozitate* și *stabilitate emoțională* și scorurile moderate la *extraversie* și *agreabilitate*. Aceste constatări sugerează un profil de

personalitate aliniat caracteristicilor esențiale pentru un leadership eficient.
Pentru încadrarea rezultatelor obținute, am folosit următoarea scală, definită de o deviație standard, egală cu 10, scorurile T cuprinse în intervalul 20-34,99 sunt considerate foarte scăzute; scorurile T cuprinse în intervalul 35-44,99 sunt considerate scăzute; scorurile/cotele T cuprinse în intervalul 45-55 sunt considerate ca fiind medii; scorurile T cuprinse în intervalul 56,1-65,99 sunt considerate ridicate; scorurile/cotele T cuprinse în intervalul 66-80 sunt considerate foarte ridicate.
Scorul mediu T pentru *extraversie* (56,4) indică un nivel moderat de sociabilitate și energie în rândul lotului pentru cercetare. Subiecții din cadrul grupului de studiu au obținut scoruri mari la factorii *sociabilitate* (56,8) și *nivel de energie* (55,4), sugerând o înclinație naturală spre interacțiuni pozitive cu ceilalți și un entuziasm constant în cadrul grupurilor. Acești factori sunt benefici în leadership, deoarece contribuie la capacitatea unui lider de a ridica moralul unei echipe și de a menține o atitudine optimistă, care poate fi esențială în motivarea membrilor echipei. Scorul T pentru *asertivitate* (53,8), deși moderat, reflectă o tendință rezervată de impunere în fața celor din jur, ceea ce sugerează un leadership care echilibrează autoritatea cu abordabilitatea. Acest echilibru în asertivitate susține un stil de conducere care impune respect, fără a copleși subordonații, o caracteristică adesea asociată cu leadershipul eficient (Judge și alții 2002, 765-780).

Cu un scor mediu T de 54,7, *agreabilitatea*, în rândul grupului de studiu, este moderat ridicată. Încrederea se remarcă printr-un scor T ridicat (58,3), indicând că acești lideri sunt, în general, înclinați să vadă în mod pozitiv lumea din jur, o trăsătură care facilitează relațiile de cooperare și consolidarea încrederii în cadrul echipei. Această atitudine este valoroasă în contextele militare care se bazează pe respect reciproc și coeziune, unde încrederea în comandant este esențială, făcând diferența, de fapt, dintre un simplu comandant și un comandant care este și lider. *Compasiunea* (52,3) și *respectul* (51,3) au scoruri moderate, indicând că, deși acești lideri manifestă empatie, o fac într-un mod echilibrat, care nu compromite luarea deciziilor asertive. Acest profil se potrivește cu cercetările care sugerează că nivelurile moderate de *agreabilitate* îmbunătățesc dinamica în echipă și cooperarea, fără a afecta capacitatea unui lider de a acționa decisiv (Graziano și Eisenberg 1997).

Conștiinciozitatea s-a evidențiat ca fiind trăsătura cea mai pronunțată în rândul grupului de studiu, cu un scor mediu T de 61,0, marcând-o drept o caracteristică definitorie a lotului pentru cercetare. În cadrul acestui metafactor, *productivitatea* (60,7) și *responsabilitatea* (60,9) au înregistrat cele mai ridicate valori, subliniind un angajament puternic de a îndeplini sarcinile eficient. Acest nivel ridicat de *conștiinciozitate* este în concordanță cu cercetările anterioare care sugerează că, *conștiinciozitatea* este un predictor semnificativ al performanței la locul de muncă, în special în roluri care necesită organizare, atenție la detalii și responsabilitate (Barrick și Mount 1991, 1-26). Factorul *organizare*, cu un scor T de 55,9, consolidează profilul unui lider care apreciază structura și planificarea meticuloasă, trăsături esențiale pentru gestionarea sarcinilor complexe și menținerea unei performanțe constante sub presiune. Per ansamblu, valorile ridicate la factorii din domeniul *conștiinciozității*

subliniază tendința orientată spre obiectivele misiunilor încredințate și disciplina liderilor din acest lot pentru cercetare, indivizi care au depus un jurământ sfânt, de a-și apăra țara...chiar cu prețul vieții.

Scorul mediu T scăzut la *emoționalitate negativă* (41,4) indică faptul că liderii din acest lot pentru cercetare prezintă niveluri ridicate de stabilitate emoțională. *Anxietatea* (40,4) și *volatilitatea emoțională* (43,8) au fost deosebit de scăzute (nivel ridicat al deviațiilor standard), sugerând că acești lideri posedă un echilibru emoțional puternic, trăsătură esențială pentru menținerea calmului în situații critice. Scorurile scăzute la *depresie* (43,6) indică, de asemenea, o stare de spirit stabilă, esențială pentru luarea deciziilor și pentru performanță. Această stabilitate este în concordanță cu concluziile din psihologia leadershipului, care leagă un nivel scăzut de *nevrotism* sau *instabilitate emoțională* cu o gestionare eficientă a stresului și cu o atitudine stabilă în fața adversităților (Watson și Clark 1994, 486-498). Scorurile generale scăzute la factorii emoționalității negative sugerează că liderii din acest lot pentru cercetare sunt mai puțin predispuși la perturbări emoționale, favorizând astfel un stil de leadership potrivit pentru medii destinate rezolvării unor situații de criză, cum ar fi cele militare.

Deschiderea către experiențe a avut un scor mediu T moderat, de 47,9, indicând o deschidere către noi experiențe, echilibrată cu o preferință pentru abordări conservatoare și practice. Dintre factori, *imaginația creativă* a obținut cel mai ridicat scor, 53,8, sugerând că, deși acești lideri sunt capabili de gândire inovatoare, creativitatea lor este aplicată într-un mod stabil și strategic. În schimb, *curiozitatea intelectuală* (45,8) și *sensibilitatea estetică* (46,0) au fost ușor sub media populației, sugerând un accent pe obiective concrete și orientate spre rezultate, funcționarea în baza unor proceduri standard mai degrabă decât pe interese abstracte sau artistice. Acest model de deschidere moderată se aliniază, în general, cu abordarea sistemului militar față de inovație, unde adaptabilitatea este apreciată în limitele unor obiective practice și centrate pe misiune. Liderii din acest lot pentru cercetare demonstrează o abordare echilibrată între noutate și procedural, un avantaj în domeniile care necesită aplicarea strategică a creativității.

Analiza *T-score* relevă un profil de personalitate compatibil cu un leadership, caracterizat prin conștiinciozitate și stabilitate emoțională ridicată, extraversie și agreabilitate moderate și o deschidere echilibrată către experiențe, prin comparație cu restul indivizilor, în general. Scorurile ridicate la factorii *conștiinciozitate*, precum *productivitate* și *responsabilitate*, subliniază abordarea disciplinată și orientată spre obiective a acestor lideri. Scorurile scăzute la *instabilitate emoțională* subliniază capacitatea lor de a rămâne disciplinați și rezilienți, aspecte esențiale pentru menținerea performanței în medii stresante. Nivelurile moderate de *extraversie* și *agreabilitate* facilitează interacțiunile pozitive în echipă și construirea încrederii, fără a compromite fermitatea deciziilor. Împreună, aceste trăsături sugerează un profil de leadership care echilibrează importanța acordată îndeplinirii sarcinilor cu abilitățile interpersonale.

Din cauza limitelor acestui studiu, rezultatele obținute nu pot reprezenta o generalizare și concluzii la nivelul întregii categorii (delimitare) de ofițeri din Forțele Aeriene Române, din cauza imposibilității de a forma un eșantion reprezentativ, unele date privind numărul și experiența de comandă a ofițerilor având un caracter clasificat. O altă limitare care nu a putut fi controlată este legată de gradul de sinceritate a subiecților, precum și de înțelegerea corectă a întrebărilor din chestionarele distribuite. Altă limitare a studiului poate fi reprezentată de lotul supus cercetării la care s-au comparat datele obținute în calcularea T-score, concluziile și descrierea factorilor și metafactorilor presupun descrierea unui grup de indivizi, în comparație cu restul indivizilor, situațiile în care actul de conducere este exercitat pot presupune variabile care nu au fost luate în calcul.

Concluzii

Acest studiu a identificat configurația unui profil de lider militar, performant într-un mediu caracterizat printr-o ierarhie strictă, disciplină și conformitate, pregătire continuă, valori și coduri morale specifice, obligația de a respecta autoritatea unor grade superioare, procese decizionale rapide și cu repercusiuni potențial critice. Constatările rezultate subliniază importanța anumitor trăsături în cultivarea unei abordări procedurale, reziliente și eficiente în leadershipul militar.

Scorurile T ridicate la *conștiinciozitate*, în special la factori precum *productivitatea* și *responsabilitatea*, indică o abordare orientată spre obiective, disciplinată și axată pe detalii în rândul liderilor militari. *Conștiinciozitatea* ridicată este constant asociată cu performanța la locul de muncă în cercetările de leadership, presupunând un efort susținut în îndeplinirea sarcinilor. Liderii care manifestă o *conștiinciozitate* puternică sunt adesea capabili să mențină un mediu structurat, esențial pentru luarea deciziilor clare și atingerea obiectivelor în misiuni complexe. Acest studiu întărește ideea potrivit căreia *conștiinciozitatea*, cu factorii săi asociați, nu este doar un predictor al succesului orientat pe obiective, ci și o bază pentru cultivarea abilităților organizaționale de care liderii au nevoie.

Scorurile T scăzute la *instabilitate emoțională,* în special la *anxietate* și *volatilitate emoțională*, sugerează un grad ridicat de stabilitate emoțională, o trăsătură esențială pentru leadership. Stabilitatea emoțională permite liderilor să gestioneze eficient stresul, să își mențină calmul și să ia decizii bine fundamentate, fără a fi afectați de factori externi sau de tulburări interne. Constatările arată că stabilitatea emoțională a liderilor este importantă atât pentru reziliența individuală, cât și pentru încrederea echipei, deoarece liderii care prezintă o atitudine calmă și constantă sunt mai predispuși să inspire încredere și fiabilitate în cadrul echipelor lor. Astfel, *stabilitatea emoțională* apare ca o trăsătură esențială în leadership.

Cercetările viitoare ar putea să evidențieze diferențele culturale în manifestarea acestor trăsături, deoarece impactul personalității asupra leadershipului poate varia

în funcție de contextul cultural. Studiile interculturale care examinează profilurile BFI-2 ale liderilor în diverse contexte culturale ar putea dezvălui modul în care anumite trăsături sunt apreciate, contribuind la o înțelegere mai nuanțată a rolului personalității în leadershipul global.

Referințe

Barrick, M.R. și M.K. Mount. 1991. ”The Big Five Personality Dimensions and Job Performance: A Meta-Analysis.” *Personnel Psychology* 44 (1): 1-26.

Bono, J.E. și T.A. Judge. 2004. ”Personality and Transformational and Transactional Leadership: A Meta-Analysis.” *Journal of Applied Psychology* 89 (5): 901-910.

Graziano, W.G. și N. Eisenberg. 1997. ”Agreeableness: A Dimension of Personality.” În *Handbook of Personality Psychology*, de R. Hogan, J.A. Johnson și S.R. Briggs (Eds.), pp. 795-824. Academic Press.

Hawkins, P. 2014. *Leadership Team Coaching in Practice: Developing High-Performing Teams.* London: Kogan Page.

Hutton, D.M. 2018. ”Critical Factors Explaining the Leadership Performance of High-Performing Principals .” *International Journal of Leadership in Education* (Taylor & Francis) 21 (2): 150-170.

Judge, T.A., J.E. Bono, R. Ilies și M.W. Gerhardt. 2002. ”Personality and Leadership: A Qualitative and Quantitative Review. *Journal of Applied Psychology*.” 87 (4): 765-780.

Singh, S. 2003. *Leadership in High-Performing Organisations. In Leadership: Value Based Management for Indian Organisations.* AKWL Publications.

Soto, C. J. și O.P. John. 2017a. ”The Next Big Five Inventory (BFI-2): Developing and Assessing a Hierarchical Model With 15 Facets to Enhance Bandwidth, Fidelity, and Predictive Power.” *Journal of Personality and Social Psychology* 113 (1): 117-143.

__. 2017b. ”Short and Extra-Short Forms of the Big Five Inventory–2: The BFI-2-S and BFI-2-XS.” *Journal of Research in Personality* 68: 69-81.

Srivastava, S. O.P. John, S.D. Gosling și J. Potter. 2003. ”Development of personality in early and middle adulthood: Set like plaster or persistent change?” *Journal of Personality and Social Psychology* 84 (5): 1041–1053. https://doi.org/10.1037/0022-3514.84.5.1041.

Watson, D. și L.A. Clark. 1994. ”Emotions, Moods, and Traits.” *Journal of Personality and Social Psychology* 67 (3): 486-498.

BULETINUL
UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I"
https://buletinul.unap.ro

Tenchi warfare – operații militare moderne bazate pe filozofia ”tenchijin”

Tenchi warfare – modern military operations based on the "tenchijin" philosophy

Comandor (r) Dr. Sorin TOPOR*
*Expert în securitate cibernetică, Institutul Național de Cercetare-Dezvoltare în Informatică – ICI București/Membru asociat al Academiei Oamenilor de Știință din România
e-mail: sorin.topor@ici.ro

Abstract

În contextul desfășurării conflictului din Ucraina, protejarea resurselor materiale și umane reprezintă o condiție esențială pentru securitatea regională. Lucrarea analizează o serie de tendințe ale evoluției tehnologice, de lecții învățate din cadrul acestui conflict și de oportunități pentru aplicarea filozofiei japoneze ”tenchijin” în operațiile militare moderne. Propunem ca, sub denumirea de operații militare ”tenchi” (”tenchi warfare”), să evidențiem rolul tehnologiile militare avansate în operațiile militare, cu accent pe exploatarea spațiilor obscure și pe cunoaștere, pentru asigurarea unui puternic suport decizional în vederea sincronizării ritmului forțelor angajate cu ritmul evoluției adversarului. Similar modalităților de abordare a luptei de către luptătorii ninja, consider că o astfel de strategie ar putea fi utilă în ripostele ofensive, în diverse domenii, precum și pentru sporirea securității naționale și regionale.

In the context of the ongoing conflict in Ukraine, the protection of material and human resources is an essential condition for regional security. The paper examines a number of trends in technological development, lessons learned from this conflict, and opportunities for applying the Japanese tenchijin philosophy to modern military operations. We propose that under the name of "Tenchi warfare" we highlight the role of advanced military technologies in military operations, with an emphasis on the exploitation of obscure spaces and knowledge, to ensure strong decision-making support in order to synchronize the rhythm of the engaged forces with the rhythm of enemy evolution. Similar to how ninja fighters approach combat, we believe such a strategy could be useful in offensive reactions in various domains, as well as for enhancing national and regional security.

Cuvinte-cheie:
conflictul din Ucraina; tehnologii avansate; filozofie tenchijin; dispozitive tenchi; tenchi warfare; securitate națională; operații militare.

Keywords:
Ukraine conflict; advanced technologies; tenchijin philosophy; tenchi devices; tenchi warfare; national security; military operations.

Info articol
Primit: 11 noiembrie 2024; Evaluat: 29 noiembrie 2024; Acceptat: 3 decembrie 2024; Disponibil online: 17 ianuarie 2025

Citare: Topor, S. 2024. „Tenchi warfare – operații militare moderne bazate pe filozofia «tenchijin»". *Buletinul Universității Naționale de Apărare „Carol I"*, 13(4): 152-167. https://doi.org/10.53477/2065-8281-24-45

Conflictul din Ucraina a pus omenirea în fața unor operațiile militare care nu mai pot fi încadrate în prevederile legilor războiului tradițional și în alte convenții internaționale aferente. Chiar dacă în acest spațiu se desfășoară lovituri distructive asupra elementelor de infrastructură de către ambii actori implicați, după mai mult de 2 ani nu există o declarație de război. Mai mult decât atât, pe baza rețelei Internet, se desfășoară ample campanii de propagandă, de atac cibernetic și deep-fake, cu rol de formare și stimulare a unor curente de opinie, care susțin o ideologie, o politică sau altceva care să atragă sprijin din partea sponsorilor, care pot fi guverne, organizații militar-politice, ONG, asociații etc.

În acest context, tehnologiile emergente și disruptive dețin cea mai importantă poziție, fiind implementate în sistemele de arme și în alte echipamente militare, dar și în sisteme destinate monitorizării și managementului securității regionale și internaționale. Lecțiile învățate din Ucraina permit formularea unor observații generale care concură către realitatea că, pentru ca un actor să-și poată menține poziția strategică dominantă într-un anumit domeniu, acesta va trebui să utilizeze oricare tehnologie avansată, care să-i permită, în principal, exploatarea eficientă a resurselor informaționale.

Pe baza studiului efectuat, considerăm că identificarea elementelor obscure în diverse domenii strategice, prin exploatarea resurselor informaționale, pe lângă cunoașterea adversarului, înțelegerea intențiilor sale, ascunderea propriilor direcții strategice și operative etc., favorizează abordări care să îl surprindă pe adversar, lovind punctele sale slabe, cu un consum limitat de resurse. Apelând la filozofia japoneză ”tenchijin” și utilizând algoritmi ML/AI, ritmul desfășurării operației militare poate fi sincronizat cu cel al adversarului. Similar tacticilor ninja, se observă că un ritm mai lent uneori poate conduce la crearea unor spații obscure care să favorizeze executarea unui atac și surprinderea adversarului în poziții sau în domenii asupra cărora, la acel moment, nu poate realiza o guvernanță eficientă, atenția lui fiind concentrată pe alte elemente operaționale.

Despre filozofia japoneză ”tenchijin” și unele modalități de aplicare

Filozofia ”tenchijin” a stat la baza instruirii luptătorilor ninja în Japonia și în China antică. Originea conceptului provine din filozofia japoneză, care s-a inspirat din definiția arhetipală chineză și are în compoziție cele trei elemente din structura universului: Cer (”ten”), Pământ (”chi”) și Om (”jin”). El simbolizează echilibrul și unitatea dintre diferitele elemente ale universului și poate fi asociat conceptelor ”yin” și ”yang”, care reflectă dualitatea și interdependența dintre diferitele aspecte ale existenței. Originea sa se află în cele mai vechi timpuri, atunci când oamenii practicau agricultura și creșterea animalelor, viața fiind susținută de cunoașterea influențelor rotirii line a celor patru anotimpuri. Acest ritm influența producția, credința și politica. Rezolvarea unei crize, care putea conduce la război, era strict

determinată de momentul în care erau aliniate condițiile cerului, cu pământul și activitățile umane.

Astfel, a devenit un principiu al guvernării și al strategiilor militare, fiind formalizat și descris de către celebrul strateg militar Sun Tzu în lucrarea sa, „Arta războiului". Strategia de a „lupta fără luptă", descrisă de Sun Tzu, se bazează pe modalitățile de a utiliza tehnici de evitare a contactului direct acolo unde adversarul este puternic și conștient, prin acțiuni menite să-l dezorienteze, să-l desensibilizeze și, cel mai important, atacul să fie realizat în modalitățile în care inamicul nu se așteaptă (Tzu 2026, cap. 8). Pentru aceasta, cele trei elemente sunt aplicate pe trei niveluri (îndepărtat, mediu și apropiat), dintre cele 8 direcții cardinale. Cerul reprezintă poziția superioară care stabilește ordinea. Respectarea ordinii cerești asigură viața (adaptarea la calea cerească înseamnă creștere). Pământul reprezintă poziția inferioară, caracterizată prin forță și putere. Dacă există voință puternică, va fi pace. Omul deține poziția de mijloc. De aceea toate activitățile umane trebuie executate după reguli corecte și în armonie.

Practica artelor marțiale se bazează pe înțelepciune și pe puterea cognitivă a practicantului. Instruirea unui luptător ninja nu se limitează la exersarea tehnicilor de luptă, ci implică și dezvoltarea cunoașterii în astrologie și cosmos, în geografie și meteorologie. Toate acestea cunoștințe îi permiteau să înțeleagă care îi este poziția în spațiu față de adversar și cum să se plaseze față de acesta. Metodele sale de deghizare sunt o extensie a acestei cunoașteri. Un ninja era pregătit să joace diverse roluri, având o ținută adecvată, folosind un limbaj adecvat rolului îndeplinit, precum și un comportament specific care să-i permită îndeplinirea misiunii.
În afara înțelegerii condițiilor de spațiu, era deosebit de importantă încadrarea acțiunii sale în timp. Luptătorul ninja putea înțelege momentul în care focalizarea adversarului se schimbă. În funcție de acesta, va adopta un ritm lent, pentru a induce confuzie și pentru a nu fi sincronizat cu ritmul adversarului.

Pentru finalizarea contraatacului, o condiție esențială este revenirea la sincronizare cu ritmul adversarului. Mișcarea lui va fi rapidă și succesivă, având avantajul loviturii din spațiul neobservat de adversar. Ea poate fi directă sau indirectă, pentru sporirea confuziei. În plus, luptătorul ninja poate identifica noi vulnerabilități ale sistemului de protecție a adversarului, care apar, în mod inevitabil, din cauza mișcării lui în cadrul atacului. Astfel, luptătorul ninja întâmpină un atac prin eschive și riposte diverse. Pentru a deveni invizibil, el înțelegea când să utilizeze grenada fumigenă și în ce direcție să execute eschiva atunci când sabia adversarului lovea. El înțelegea că brațul care ține sabia va acoperi ochii atacatorului, mai ales dacă acesta lovea de sus în jos.

Dicționarul japonez sugerează, cu sens metaforic, că această tehnică reprezintă „plecarea în căutarea libertății" (Goo 2024). Dezvoltând această artă a luptei, întreaga teză lui Sun Tzu prezintă modalitatea în care poate fi atras un adversar către o iluzie, pe baza înșelării. Condiția de bază este ca cel care exploatează această știință

să dețină avantajul cunoașterii și înțelegerii vulnerabilităților adversarului. Dacă se impune, sunt lovite în mod direct elementele senzoriale ale adversarului (pentru un ninja, afectarea ochilor adversarului creează oportunitatea realizării de spații nesupravegheate).

Crearea de spații invizibile pentru adversar constituie o strategie care sporește șansa și siguranța propriei acțiuni. Dacă atenția adversarului este concentrată asupra locului care i s-a sugerat, i se deformează percepția asupra realității. Într-un mod extrem de simplu, apreciem că strategia conflictului bazat pe filozofia tenchijin reprezintă arta de a utiliza spațiile obscure și de adaptare a ritmului pentru ca o acțiune să fie eficientă, în concordanță cu obiectivul planificat.

Generalizând, observăm că practicanții artelor marțiale nu își manifestă în mod deschis intențiile de atac. Aceștia dețin abilități de exploatare a mediilor și spațiilor atipice, excentrice sistemului lor relațional. Astfel, permițându-i unui adversar să fie concentrat pe o iluzie, se va poziționa într-o zonă defavorabilă adversarului. Plecând de la aceste principii, au fost dezvoltate aplicații în numeroase domenii, precum medicină, economie, politică, urbanism, securitate etc. Chiar și în domeniul divertismentului, toți magicienii, în spectacolele lor, folosesc spațiile obscure și abaterea atenției publicului asupra altei mișcări, reușind trucuri în care dispar sau apar obiecte.

În prezent, numeroase entități economice din Japonia exploatează aceste tehnici bazate pe folosirea informațiilor spațiale, în vederea estimării spațiilor obscure și terenurilor. Se afirmă că aceste aplicații sunt utile în agricultură, pescuit, imobiliare, energie, logistică, turism etc. (Jaxa 2019). Spre exemplu, pe baza serviciului GIS și utilizând algoritmi de învățare automată (ML/AI), pot fi gestionate riscurile de scurgere la conductele de apă (Tokyo SME 2023). Yasutoshi Hyakusoku, cofondator al Start-up "Tenchijin" și șef al biroului R&D/ JAXA (Japan Aerospace Exploration Agency), afirma că, dacă s-a demonstrat că o mare parte din problemele economice pot fi rezolvate prin tehnologie, există și provocări sociale, a căror rezolvare, chiar dacă nu este ușoară, ar putea fi realizată astfel atât la nivel global, cât și local. Hyakusoku aprecia că „senzorii sau echipamentele de telecomunicații din spațiu care observă Pământul ar trebui să facă parte din infrastructurile planetei" (Spotlight 2023).

În cadrul ecosistemelor de afaceri, corporațiile se confruntă cu tot mai multe atacuri cibernetice, mai ales în relațiile cu parteneri terți și cu furnizorii. Pentru managementul riscului cibernetic, se apelează la soluții inovatoare și disruptive, în scopul furnizării de servicii de securitate cibernetică. Programul Scale Up Outliers, de la Endeavour (Tenchi 2024), are scopul de a reduce asimetria informațională în ceea ce privește securitatea informațiilor și riscurile de conformitate în ecosistemele corporative, într-o manieră cooperativă și scalabilă, pentru a maximiza rentabilitatea capitalului investit. Chiar dacă aceste dezvoltări au devansat multe domenii, serviciile de top de securitate cibernetică end-to-end, concentrate pe strategii de protecție, reziliență și o serie de servicii specifice

industriei, au atras atenția și unor armate, mai ales în ceea ce privește mediul cloud și guvernanța ecosistemului organizației.

Fiind un domeniu extrem de important, nu sunt informații publice referitoare la aceste servicii, situație în care analiza va fi limitată la principii de abordare a filozofiei tenchijin și la utilizarea eficientă a tehnologiilor emergente și disruptive. Acestea, având un potențial uriaș de a contribui la securitatea publică, pot deveni oricând ținte în diverse atacuri, în contextul existenței unei varietăți de intervenții militare în lume, dar și în alte tipuri de relații internaționale.

Tehnologii avansate în războiul ruso-ucrainean

În istoria umanității, mai ales în perioadele de schimbări ale balanței puterii și ordinii internaționale, există numeroase conflicte militare. Agresiunea Rusiei împotriva Ucrainei constituie o încălcare a tuturor regulilor, iar pericolul pe care îl reprezintă acest model rezidă în posibilitatea ca o situație similară să apară oriunde în lume. Astfel, riscurile la adresa securității regionale și globale, pe fondul presiunilor crescânde de schimbare a statu-quoului prin forță, sunt tot mai complexe și hibride, putând fi amplificate de vecinătatea unei țări care deține o armată puternică, arme nucleare și o veritabilă industrie de război.

Privind actualul context geopolitic, se observă că „războaiele înghețate" și situațiile de „zonă gri" a unor teritorii, extinderea altor „zone gri" ale războiului postmodern, cumulate cu atacuri cibernetice transfrontaliere asupra unor infrastructuri critice, controlul informațiilor, propaganda și deep-fake etc. estompează puterea normelor recunoscute ale stării de război față de cele de pace. Domenii ale securității naționale, considerate anterior nemilitare, au fost extinse asupra componentelor economice și tehnologice. Aceste abordări au ca rezultat o îngreunare excesivă a stabilirii limitei dintre conflictul militar și cel nemilitar.

Ironia privind starea de securitate internațională actuală este că toate măsurile și sancțiunile fără precedent luate împotriva Rusiei, chiar dacă urmăreau obligativitatea opririi luptelor, riscă sporirea distrugerilor materiale, creșterea numărului victimelor și a duratei conflictului. În plus, confruntările dintre regimuri (democratic vs. autocratic), amestecarea componentelor militare cu cele politice, lupta pentru obținerea dominației în oricare domeniu etc. au creat o incertitudine de stabilire a responsabilității agresorului, în situația izbucnirii unui război. Incidentele transfrontaliere, loviturile cu rachete și drone, sabotajele și incursiunile, distrugerile, cauzate de sabotaje, și pierderile de vieți omenești etc., mai ales în urma incursiunii Ucrainei, cu pătrundere în teritoriul Rusiei, au amplificat tensiunile regionale și au creat premisele unui război de lungă durată, cu noi riscuri asociate.
Aceste operații militare fără precedent nu puteau fi posibile fără utilizarea tehnologiilor avansate, care au revoluționat întregul ecosistem militar, care au influențat strategiile și rezultatele luptelor.

Prezentăm principalele tehnologii avansate utilizate în conflictul din Ucraina:

A. Drone

Înaintea debutului operației speciale ruse asupra Ucrainei, nici cei mai mari susținători în promovarea sistemelor aeriene fără pilot la bord (UVS) nu ar fi putut estima amploarea și diversitatea domeniilor de exploatare a dronelor. La numai doi ani și jumătate de la desfășurarea conflictului, utilizarea dronelor reprezintă o condiție esențială pentru executarea loviturilor de precizie și pentru recunoașterea/observarea tactică. Dronele sunt capabile să opereze în rețele informaționale formate din sisteme satelitare, rețele de comunicații terestre și agenți umani (HUMINT). Informațiile obținute cu aceste dispozitive au permis evaluarea rapidă a situație tactice și operative. Astfel, împotriva dronelor rusești, ucrainenii folosesc dispozitive miniaturizate ”tenchi” și sisteme portabile de război electronic. Reacția Rusiei a fost de extindere a atacurilor cu drone kamikaze Lancet, care identifică semnalele de recunoaștere a țintelor, generate de dronele Orlan-10 și SuperCam, în spectrul vizual și infraroșu (Battersby 2024). Prin aceste echipamente, Rusia a căutat să egaleze performanța loviturilor ucrainene cu sistemele HIMARS (puse la dispoziție de SUA), împotriva artileriei, tancurilor și altor ținte cu valoare ridicată (Farrell 2023).

B. Război electronic (EW)

Datorită particularităților determinate de condițiile de mobilitate și de cerințele sporite de schimb de informații, asigurarea securității resursei de frecvențe electromagnetice, atacarea resursei similare a adversarului reprezintă un obiectiv principal al operațiilor militare contemporane. Prin unde electromagnetice, se realizează coordonarea și sincronizarea acțiunilor, se asigură dreptul de informare a publicului și legăturile de comunicații sociale, se menține securitatea infrastructurilor critice și protecția populației civile din spațiile geografice aferente conflictului. În acest context, echipamentele de război electronic sunt esențiale pentru perturbarea comunicațiilor adversarului, pentru îngreunarea coordonării și scăderea eficienței acțiunilor sale, într-un mediu în care limitele spectrului de frecvențe electromagnetice nu pot fi extinse. Astfel, războiul electronic a trecut de la stadiul de rețea activă la cel de confruntare activă, constituind o condiție pentru câștigarea și menținerea inițiativei.

Rușii, spre deosebire de țările NATO, au operaționalizat războiul electronic la toate nivelurile ierarhice (strategic, operativ și tactic) și în toate componentele armatei sale (terestru, maritim, aerian și cosmic). EW formează baza doctrinei războiului informațional (Chiriac și Withingon 2024). De altfel, David T. Pyne, cercetător la EMP Task Force și fost director al Departamentului Apărării al SUA, afirma că Rusia deține „cel mai capabil sistem de război electronic din lume” (Giangiulio 2023), fiind impresionat de viteza de adaptare la performanțele celor mai noi sisteme de arme americane și ale NATO.

Echipamentele rusești de război electronic au reușit să facă ineficiente tehnologiile Excalibur, GLSDB și HIMARS, prin bruierea semnalelor din

satelit (Skove 2024). Au perturbat activitatea capabilităților de internet Starlink, oferite de Pentagon, complicând coordonarea forțelor și lansările de atacuri cu drone ucrainene (Mozur și Satariano 2024). În acest război, Ucraina nu ar fi rezistat atât de mult fără sprijinul companiilor tehnologice din SUA, Europa și Asia, care au oferit înaltă tehnologie electronică și cibernetică, necesară utilizării sistemelor de arme (Topor 2024).
De altfel și forțele militare ucrainene, în incursiunea de la Kursk (august, 2024), au beneficiat de un sprijin eficient EW, care a susținut crearea spațiilor obscure în apărarea rusă. Succesul nu ar fi fost posibil fără informații, sincronizare și suport decizional. Această forță militară a implicat sute de trupe ucrainene, unități de infanterie, unități de mecanizate și suport cu drone. Surpriza operațională a fost evidentă, riposta forțelor ruse fiind mult prea lentă pentru a opri ofensiva și pentru a-i împinge pe ucraineni dincolo de graniță. Dar războiul electronic nu trebuie confundat cu războiul cibernetic și cu alte tehnici de hacking (NATO 2023) ale dispozitivelor electronice.

C. Război cibernetic

Războiul cibernetic și în special componenta de apărare cibernetică au devenit o componentă critică a strategiei de securitate națională a Ucrainei. Spațiul cibernetic este recunoscut ca al cincilea domeniu al războiului, alături de cel terestru, aerian, maritim și spațial (Avanesova, Serhiienko și Lyubushin 2022, 25-40). În principal, dimensiunea cibernetică a războiului este o componentă dominantă în lupta pentru informațiile online, din campaniile de cucerire a inimilor și minților (Willett 2022, 7-26). În acest conflict, războiului cibernetic poate fi clasificat pe trei niveluri de abordare, anume: atacuri cibernetice distructive, penetrarea rețelelor pentru activități de spionaj și, nu în ultimul rând, operații de influențare psihologică, prin produse de sociologie cibernetică, a audienței internaționale. Față de acesta, Ucraina, fără sprijin occidental și din partea NATO, nu ar fi putut face față.

Prin internet, au fost stimulate emoțiile oricărui individ care era interesat de acest eveniment, prin mesaje ghidate în jurul termenilor cheie, precum război, victorie, moarte, distrugeri, frică, migrație etc. Astfel, s-a creat un spațiu semantic pentru aplicarea algoritmilor motoarelor de căutare AI/ML, precum și o serie de metaetichete în cadrul rețelelor de socializare, ca strategii de răspuns pentru radicalizarea audienței internaționale. Astfel, s-au format alianțe de state, coaliții de companii din sectoarele public sau privat și organizații neguvernamentale care au sprijinit pe unul dintre cei doi actori implicați. Narațiunile oficiale și neoficiale au variat semnificativ, în funcție de sursă, și au însoțit contactul direct dintre forțele armate. De regulă, componenta rusă caracteriza luptele ca o formă de apărare împotriva terorismului și altor mișcări de provocare, extrem de agresive, ale Ucrainei, ca o acțiune directă împotriva suveranității naționale, ca o măsură de sporire a securității față de nazificarea populației ruse de către regimul ucrainean. De cealaltă parte, Ucraina laudă curajul forțelor sale armate, face acuzații de

crime de război și solicită sprijin occidental pentru apărare.
Prin atacuri cibernetice, au fost manipulate alegerile prezidențiale, au fost lovite companii de distribuire a energiei, instituții financiare, servicii poștale, publicații de știri, servicii de transport și comerciale, au fost afectate pagini web guvernamentale și chiar servicii de telecomunicații care erau asigurate prin sistemul de sateliți al Starlink. Valoarea simbolică a apărării cibernetice a Ucrainei a depășit cu mult valoarea operativă a manevrelor militare, demonstrând hotărârea și menținerea capacităților de luptă ucrainene (Youvan 2024).

D. Sistemele de rachete și artileria de precizie

În domeniul armelor, tehnologii avansate au fost implementate în sistemele de lovire pentru sporirea preciziei loviturilor (mai ales asupra infrastructurilor cu valoare strategică), pentru reducerea daunelor colaterale, precum și pentru îmbunătățirea eficienței operaționale. La nivel tactic, sistemele de rachete și de artilerie, folosite de ambii actori, au condus la așa-zisul genocid al artileriei (70% din pierderile suferite de ucraineni sunt produse de artileria terestră rusă), forțele ucrainene făcând față doar cu artileria autopropulsată, primită ca ajutor (Buță și Manoliu 2023, 168-175). La nivel strategic, dezvoltarea și utilizarea rachetelor hipersonice de către Rusia au determinat revizuirea strategiilor de apărare și de evaluare a riscurilor, europene și NATO, fiind foarte posibil ca Rusia să continue dezvoltarea capacităților corespunzătoare, de mare viteză, cu extensie către cele nucleare (Wright 2022). Deși aceste provocări pot fi atenuate prin mecanisme tehnice și politice internaționale, potențialii producători pot să continue investițiile în cercetări științifice și testări tehnologice care să conducă către noi sisteme, a căror performanță să le depășească pe cele actuale.
Spre exemplu, Ucraina folosește rachete Switchblade (v. 300 și 600), o combinație tactică de rachetă-dronă-AI, cu capacități autonome, cu lansare de la sol și cu capacități de a localiza ținte în mod independent și de lovire, cu prioritate, a sistemelor de apărare antiaeriană, a tancurilor și a altor sisteme rusești de apărare (Cook 2024).

E. Inteligența artificială

Algoritmii IA au îmbunătățit analiza datelor, planificarea misiunilor și optimizarea resurselor. Astfel, au fost sporite viteza și precizia activităților decizionale în numeroase domenii militare și civile. Structurile de decizie militară pot folosi IA în domenii operative și tactice pentru a prevedea zonele de conflict, pentru a optimiza rutele de evacuare ori pentru a acorda prioritate tratamentului răniților (Kolesnikov și Kryzhevsky 2023, 80-83). La nivel strategic, IA poate fi folosită în sprijinul deciziilor de politică externă și a diplomației (Sirenko 2024, 122-128), pentru gestionarea situațiilor de urgență, pentru reconstrucția infrastructurilor și, chiar, pentru contracararea dezinformării (Kertysova 2018, 55-81). De reținut este faptul că războiul din Ucraina a determinat o dezvoltare foarte rapidă a sistemelor autonome bazate

pe IA, a căror implicare a schimbat dinamica manevrelor de luptă. Pe lângă drone, sistemele de război electronic, informațional și cibernetic utilizează IA pentru a colecta date, pentru a răspândi informații false (inclusiv manipularea imaginilor și videoclipurilor), pentru interceptarea comunicațiilor necriptate, pentru geolocație și analiza datelor open-source, în scopul identificării soldaților, armelor, sistemelor, unităților și manevrelor acestora (Marija și Vanja 2023, 59-76). Asta nu înseamnă că se ignoră rolul armelor convenționale. Esența utilizării IA în conflictele armate se reflectă prin economia resurselor umane și reducerea victimelor.

F. Comunicații securizate

Tehnologiile avansate de comunicație au îmbunătățit metodele de comunicare, în scopul coordonării manevrelor dintre unități și transmiterii rapide și sigure a informațiilor. În mod, evident, soluțiile tehnologice digitalizate au oferit oportunitatea creării de noi sisteme de guvernanță care au permis utilizarea optimă a resurselor, modernizarea politicilor și serviciilor specifice, precum și o interacțiune eficientă între toate unitățile structurale, militare și civile, la toate nivelurile ierarhice. În acest sens, protecția datelor și informațiilor a devenit nu doar o problemă tehnică, ci și una legislativă pentru guvernul ucrainean, și nu numai. Din punct de vedere tehnic, utilizarea sateliților Starlink a adus beneficii enorme păstrării nealterate a multor servicii de comunicație, mai ales pentru forțele angajate în luptă. În plus, au fost create și dezvoltate o serie de structuri administrative care să asigure securitatea serviciilor publice, sub formă electronică, precum portalul web iGov.org, aplicația Kiev Tsyfovii (pentru utilizarea diverselor servicii comunitare prin smartphone), alte aplicații care să asigure o serie de funcționalități legate de ostilitățile de pe teritoriul Ucrainei (harta adăpostului, harta unei afaceri în desfășurare, ajutor voluntar al armatei, asistență voluntară, linkuri către surse oficiale etc.), consolidând reziliența socială (Bojor, Petrache și Cristescu 2024, 185-194).

G. Apărarea antiaeriană

Războiul din Ucraina a devenit un teren de testare nu numai al dronelor, ci și pentru noile tehnologii de apărare antiaeriană. Acestea au fost esențiale pentru protejarea forțelor terestre de atacurile aeriene și cu rachete rusești. De altfel, aspectele privind modernizarea sistemelor de apărare antiaeriană ucrainene a reprezentat obiectul multor publicații, urmărind toată gama de sisteme, cu rază mare, medie, scurtă și apropiată a complexelor de echipamente militare (Spirin, Pogorilyi și Shynkarenko 2023, 75-81). Noile sisteme au inclus noi tehnologii optoelectronice, anume cele pentru determinarea cu precizie a coordonatelor țintei, pentru detectarea mai rapidă și reducerea timpului de reacție la schimbările în situația operativă, componente de protecție împotriva atacului electronic, capacități de mobilitate și de depășire a obstacolelor etc. Din cauza constrângerilor, apărute ca urmare a timpului asociat implementării și testării noilor sisteme în luptă, au fost identificate și o serie

de limite, care, în principal, sunt determinate de asigurarea compatibilității cu alte arme, cu sisteme de comunicații și cu drone. Pe fondul sprijinului cu echipamente moderne, acordat Ucrainei de către țările europene și NATO, Rusia nu și-a putut asigura superioritatea aeriană, fiind forțată să-și schimbe tactica de a folosi forțele aeriene, concentrându-și efortul asupra loviturilor cu rachete și cu drone. Din păcate, situația lipsei de control al atacurilor aeriene ale Federației Ruse, cu rachete de croazieră și drone, continuă să producă numeroase pierderi de vieți omenești în rândul populației ucrainene (Титаренко și Власенко 2024, 49-55).

H. Tehnologii de instruire și de antrenament

Tehnologiile avansate de simulare au permis antrenamente eficiente, o pregătire adecvată a militarilor, pentru a face față diverselor scenarii de luptă, și îmbunătățirea reacțiilor lor, în condiții de stres și incertitudine. Dintre numeroasele inovații tehnologice destinate pregătirii militarilor, amintim simulatoarele virtuale multimedia, jocurile educaționale, sistemele automate de evaluare a cunoștințelor, echipamentele de învățare la distanță etc. Folosirea acestor instrumente educaționale, pe lângă îmbunătățirea eficienței antrenamentelor și a motivației, au permis și reducerea timpului și a costurilor aferente. Astfel, se îmbunătățește educația militară aplicată, calitatea materialelor de învățare și modelele de evaluare. Această abordare se aliniază tendinței de integrare a tehnologiilor informaționale avansate în educația militară, devenind un instrument crucial pentru modernizarea instruirii și a antrenamentului. Sunt oferite soluții eficiente de utilizare a senzorilor, a armelor, a altor sisteme de luptă, pentru a răspunde nevoilor în evoluție ale forțelor armate, în contextul războiului în desfășurare. În plus, aceste soluții sunt utile și în ridicarea moralului trupelor ucrainene, susținând motivația de a răspunde amenințărilor hibride, în formarea specialiștilor militari și în dezvoltarea abilităților de utilizare a armelor, în conformitate cu standardele NATO (Kozubtsov și alții 2023).

În general, apreciem că operațiile militare desfășurate în cadrul acestui conflict demonstrează importanța colaborării și coordonării manevrelor componentelor structurilor de forțe armate, pentru obținerea avantajului tactic și operațional. Aceasta implică sincronizare, schimb eficient de informații și de resurse. Estimăm că, pe măsură ce tehnologiile avansate se vor dezvolta tot mai mult în direcția digitalizării și miniaturizării, sistemele de arme și echipamentele militare vor fi tot mai numeroase, mai precise, mai eficiente și integrate, în condițiile în care mediul electromagnetic și spațiul cibernetic vor deveni indispensabile oricărui tip de confruntare.

Analiză și discuții privind operațiile militare ”tenchi”

Actualele tehnologii avansate favorizează producerea unei multitudini de informații, analize și predicții pertinente, față de care învățarea și instruirea adecvată, în

scopul dezvoltării cunoașterii pot reprezenta baza unui management eficient într-o diversitate de domenii. Categoria dispozitivelor electronice tenchi cuprinde smartphone-uri, dispozitive inteligente de monitorizare a sănătății, ceasuri inteligente, alte tipuri de dispozitive electronice portabile, care utilizează baze mari de date și rețele de comunicații. Toate conțin tehnologii avansate de comunicații, precum Bluetooth sau Wi-Fi, senzori pentru măsurarea diverșilor parametri (de la sănătate la mediu), interfețe intuitive, algoritmi și alte aplicații care potențează o activitate umană. Dispozitive tenchi sunt incluse și în mașinile industriale care, în funcție de mediul de utilizare, pot executa activități diverse de la ambalare de produse la prelucrarea alimentelor (Tenchi Sangyo Co. 2021).

Conceptual, nu există o categorie de activități care să se identifice cu această denumire. ”Tenchi warfare” este un scenariu al filmului de animație ”War on Geminar”, un spin-off al serialului japonez ”Tenchi Muyo”! Apreciem că ipotezele abordate în acest film pot deveni realitate, în condițiile în care tehnologiile disruptive și emergente sunt tot mai prezente în viața cotidiană. Jocul video realizat pe baza acestui film transpune participanții în scenarii cu lupte între personaje, samurai și ninja, cu abilități speciale care navighează prin nivele complexe, evită inamicii, elimină ținte, fură informații și salvează ostatici, totul fără a fi detectați. Având o diversitate de arme, combinațiile de acțiuni strategice și tactici de camuflaj conduc la rezolvarea misiunilor de dezvăluire a conspirațiilor politice și de răzbunare a unor trădări, în mod evident, în atmosfera feudală japoneză. Jocul îi pune pe participanți în fața unor alegeri morale care pot afecta povestea și relațiile cu diverse personaje. Modul multiplayer permite ca jucătorii să concureze între ei, folosind abilitățile de ascundere, de camuflaj și dezinformare.

Aparent, un joc similar celor din clasa ”capture the flag” sau ”assassination” este destul de captivant în media digitală. Dar, similar altor jocuri strategice de război, poate forma percepții greșite a normelor etice și morale ale războiului, pentru un tânăr care nu are nicio pregătire militară.
Pentru analiștii și cercetătorii științifici militari, poate constitui un instrument util în înțelegerea unor aspecte ale filozofiei techijin. Exersarea tehnicilor de ascundere poate dezvolta abilități de identificare a spațiilor obscure și de reglare a ritmului executării unei misiuni, care, ulterior, pot fi aplicate și în viața reală, într-un mediu complex, cu riscuri și amenințări asimetrice și hibride.

Este bine cunoscut că noțiunea de război cibernetic a fost dezvoltată în jurul conceptului de spațiu cibernetic. Paternitatea îi revine romancierului Wiliam Gibson, care, în cartea sa Neuromancer (1984), stabilea prin cyberspace un spațiu virtual, dincolo de lumea fizică, accesibil prin rețelele de calculatoare, având un puternic impact asupra viziunii internetului actual. Odată cu introducerea internetului în operații militare, spațiul cibernetic a devenit un concept de bază care stabilește mediul de desfășurare a războiului informațional, cu persoane care pot ataca și/sau determina un nivel ridicat de securitate pentru computere și rețelele informatice (Van Haaster 2019).

În mod similar, stabilim prin conceptul de ”tenchi warfare” acele strategii și metode de desfășurare a unui război prin tehnologii avansate, emergente și disruptive asupra infrastructurilor critice ale inamicului, manipularea informațiilor, anticiparea evoluțiilor și proiectarea puterii, precum și asigurarea securității împotriva riscurilor și amenințărilor hibride. Sub aspect etic și moral, o mare problemă o reprezintă utilizarea manipulării pentru distrugerea unui sistem social, organizat în jurul unei anumite ideologii. Avem în vedere terorismul și executarea de lovituri la mare distanță pentru producerea de distrugeri materiale și pierderi de vieți umane, în conflicte care nu pot fi încadrate în legislația internațională sub conceptul recunoscut de război.

În prezent, oportunitatea exploatării tehnologiilor avansate într-un conflict asigură în mare măsură siguranța obținerii victoriei. Provocările privind protecția infrastructurilor critice și a populației civile captive în zona de conflict derivă nu din utilizarea tehnologiilor emergente și disruptive, ci din scopul în care sunt folosite. În acest context, considerăm că pot fi planificate și realizate operații militare bazate pe arta tenchijin, pe care le includem în conceptul ”tenchi warfare”.

Spre exemplu, chiar dacă este recunoscută falsitatea motivației ruse privind legalizarea războiului împotriva Ucrainei (Rusia a invocat menținerea păcii în regiunile Donețk și Lugansk, precum și oprirea genocidului comis în regiunea de est a Dombasului) și chiar dacă a fost determinat un mecanism internațional de stabilire a autorilor crimelor din timpul războiului, Rusia a folosit forța militară și a ocupat mai multe locații critice și strategice ucrainene (Khater 2022). Reacția Ucrainei, aflată sub un intens război informațional și sub lovituri care includ tehnologii avansate, poate fi considerată o operație tenchi, bazată pe strategii care au stabilit un nivel ridicat de colaborare și de coordonare eficientă forțelor, reglarea ritmului operațiilor de apărare pentru a face față ofensivei ruse, executarea ripostelor ofensive în zone și cu metode care i-au permis surprinderea adversarului.

Nimeni nu se aștepta ca la data de 6 august 2024, după doi ani și jumătate de la declanșarea războiului, trupele ucrainene să execute o incursiune cu succes pe teritoriul Rusiei, ajungând până la Kursk. Remarcabile sunt amploarea și viteza acestei operații militare, cunoașterea realității puterii de reacție a forțelor ruse în zona de rupere a apărării, precum și modul de pregătire a întregii operații militare, sub umbrela unor măsuri de securitate nemaiîntâlnite până în prezent. Astfel, Ucraina a stabilit o zonă tampon pentru a împiedica bombardarea teritoriului său din regiunea Kursk, o presiune suplimentară pentru Rusia (aceasta fiind obligată să transfere trupe din altă zonă de contact pentru oprirea ofensivei) și un câștig imagologic, esențial în restabilirea moralului trupelor și populației civile.

Mai mult decât atât, această strategie a permis obținerea rapidă și menținerea unor avantaje tactice și operaționale în numeroase domenii, dintre care enumerăm:

1. exploatarea punctelor slabe ale defensivei ruse, îmbunătățirea tacticilor de pătrundere și folosirea combinată a tehnologiei avansate, informații GIS,

drone, acțiuni de sabotaj, lovituri de precizie și strategii de manevră;
2. sprijin internațional cu echipamente și sisteme moderne, adaptarea și reformarea tacticilor, în funcție de capacitățile de luptă;
3. îmbunătățirea mobilității și a atacurilor concentrate pe punctele slabe ale inamicului;
4. demonstrarea utilizării eficiente a capacităților informaționale pentru demoralizarea trupelor rusești și mobilizarea opiniei publice pentru sporirea solidarității naționale;
5. extinderea apărării și a capacităților tactice de adaptare, în funcție de tipologia de luptă (urbană, în teren deschis, de război electronic etc.);
6. recucerirea unor teritorii care a permis realizarea unei retrageri controlate din alte zone, urmate de contraatacuri rapide și eficiente.

Apreciem că această incursiune poate fi similară contraatacului unui ninja care a înțeles cum să utilizeze, în favoarea sa, spații și domenii obscure, pe fondul unui ritm adaptat al apărării strategice, urmat de o reacție ofensivă rapidă, până în momentul atingerii obiectivelor planificate.

Concluzii

În contextul transformării digitale și dezvoltării tehnologiilor emergente și disruptive, al tendințelor în creștere ale pieței echipamentelor de apărare și securitate, al implementării progreselor tehnologice în sisteme tot mai complexe și capabile să stimuleze cercetarea științifică și producția de noi echipamente, cu investiții semnificative în domenii diverse, conceptul propus de ”tenchi warfare” poate caracteriza acest moment istoric al evoluției artei militare. În prezent, chiar dacă există numeroși factori care diferă, în funcție de contextul geopolitic și militar regional, fiecare țară caută să-și consolideze capacitățile de apărare și să-și îmbunătățească pregătirea militară.

Conceptul prezentat este o ipoteză de cercetare științifică, rezultată din analiza descriptivă a conceptului filozofic japonez, aplicată tehnologiilor avansate de impact pentru domeniul militar, pe baza căreia, printr-o serie de modelări, simulări și testări, se poate stabili cât de utilă este această tehnologie și care sunt condițiile sale de implementare în operațiile militare. O astfel de abordare poate fi utilă atât în faza de stabilire a designului platformelor de luptă, în stabilirea nivelului de dotare cu armament etc., cât și în stabilirea strategiilor de reorganizare a formațiunilor de luptă.

Mai mult decât atât, apreciem că o planificare strategică elaborată printr-o astfel de abordare poate contura direcții eficiente de dezvoltare a industriei militare, de consolidare a securității infrastructurilor critice, având ca principală cerință protecția resursei umane, în contextul unor atacuri hibride, sprijinite de un intens război informațional. Estimăm că pot fi dezvoltate și alte direcții aferente consolidării securității naționale, cu puternic impact pozitiv asupra economiei naționale.

Referințe

Avanesova, N.E., Y.I. Serhiienko și R.A. Lyubushin. 2022. ”Strengthening the State Cyber Defence and Creating of Cyber Troops: State, Problems and Organizational – Economic Measureas for Ukraine.” *Economic Innovations* 24 (1): 25-40. https://doi.org/10.31520/ei.2022.24.1(82).

Battersby, Blair. 2024. ”Russia Struggling to Integrate Its Most Effective Unmanned System, TRADOC G2.” https://oe.tradoc.army.mil/2024/04/18/russia-struggling-to-integrate-its-most-effective-unmanned-system/.

Bojor, Laviniu, Tudorică Petrache și Cristian Cristescu. 2024. ”Emerging Technologies in Conflict: The Impact of Starlink in the Russia-Ukraine War.” *Land Forces Academy Review* 29 (2): 185-194. https://doi.org/10.2478/raft-2024-0020.

Buță, Viorel și Răzvan Manoliu. 2023. „Noi tendințe în întrebuințarea diferitelor arme în războiul ruso-ucrainean.” *Conferința științifică internațională „Gândirea Militară Românească”, Teorie și Artă Militară.* doi:doi.org/10.55535/gmr.2023.4.09.

Chiriac, Olga R. și Thomas Withingon. 2024. ”Russian Electronic Warfare: From History to Modern Battlefield, Irregular Warfare Initiative.” https://irregularwarfare.org/articles/russian-electronic-warfare-from-history-to-modern-battlefield/.

Cook, Ellie. 2024. “US-Made «Tank-Killer» Switchblade Destroys Russian SAM System in Rare Video.” *Newsweek.* https://www.newsweek.com/ukraine-switchblade-drone-russia-tor-air-defense-system-video-1976448.

Farrell, Francis. 2023. ”How Russia’s homegrown Lancet drone became so feared in Ukraine, The Kyiv Independent.” https://kyivindependent.com/how-russias-homegrown-lancet-drone-became-so-feared-in-ukraine.

Giangiulio, Graziella. 2023. “#UKRAINERUSSIAWAR. For Kiev it is the last chance but Moscow last the numbers to win on paper.” *News AGC Communication.* https://www.agcnews.eu/ukrainerussiawar-for-kiev-it-is-the-last-chance-but-moscow-has-the-numbers-to-win-on-paper/.

Goo. 2024. ”Tenchi”. https://dictionary.goo.ne.jp/srch/jn/%E3%83%86%E3%83%B3%E3%83%81/m0u/.

Jaxa. 2019. “Introduction of JAXA ventures.” https://aerospacebiz.jaxa.jp/en/venture/tenchijin/.

Kertysova, Katarina. 2018. “Artificial Intelligence and Disinformation: How AI Changes the Way Disinformation is Produced, Disseminated, and Can Be Countered.” *Security and Human Right,* No. 29: 55-81. https://doi.org/10.1163/18750230-02901005.

Khater, Maya. 2022. “The Legality of Russian Military Operations Against Ukraine from the Perspective of International Law.” *Access to Justice in Eastern Europe Journal.* doi:10.33327/AJEE-18-5.3-a000315.

Kolesnikov, E.B. și V.V. Kryzhevsky. 2023. ”The use of Artificial Intelligence at the Stages of Evacuation, Diagnosis and Treatment of Wounded Soldiers in the War in Ukraine.” *Kharkiv Surgical School,* no. 4-5 (September): 80-83. https://doi.org/10.37699/2308-7005.4-5.2023.11.

Kozubtsov, Igor, Ihor Danyliuk, Andrii Krasnobokyi și Svitlana Voronaia. 2023. "Prospects for the use of Virtual Reality Technologies in the training of military specialists (Tactical level of Military Education) according to the compatible NATO Standards." *Bulletin of Science and Education* 11 (17). https://doi.org/10.52058/2786-6165-2023-11(17)-770-784.

Marija, Doric și Glisin Vanja. 2023."The use of artificial intelligence in the Russo-Ukarinian war." *Politika nacionale bezbednosti* 25 (2): 59-76. https://doi.org/10.5937/pnb25-47369.

Mozur, Paul și Adam Satariano. 2024. "Russia, in New Push, Increasingly Disrupts Ukraine's Starlink Service." *The New York Times*. https://www.nytimes.com/2024/05/24/technology/ukraine-russia-starlink.html.

NATO. 2023. "Electromagnetic warfare." https://www.nato.int/cps/en/natohq/topics_80906.htm.

Sirenko, A.S. 2024. "The Role of Artificial Intelligence in Making Foreign Policy Decision in the Ukrainian- Russian War." *European Socio-Legal & Humanitarian Studies,* No.1: 122-128. https://doi.org/10.61345/2734-8873.2024.1.13.

Skove, Sam. 2024. "Another US precision-guided weapon falls prey to Russian electronic warfare, US says, Defence One." https://www.defenseone.com/threats/2024/04/another-us-precision-guided-weapon-falls-prey-russian-electronic-warfare-us-says/396141/.

Spirin, Denis, Olecsandr Pogorilyi și Olga Shynkarenko. 2023. "Justification of modernization paths for short-range air defense missile systems of land forces." *Scientific works
 Of State Scientific Research Institute of Armament and Military Equipment Testing and Certification* 16 (2): 75-81. https://doi.org/10.37701/dndivsovt.16.2023.11.

Spotlight, Japan. 2023. "The usages of Data from Space." https://www.jef.or.jp/journal/pdf/249th_Special_Interview.pdf.

Tenchi Sangyo Co., LTD. 2021. "Tenchi Sanhyo Packaging Machines." https://www.tenchi.jp/en/aboutus/.

Tenchi. 2024. "Tenchi Security raises a $7 million Series A from Bradesco, L4 Venture Builder, and Accenture." https://www.tenchisecurity.com/en/insights-news/tenchi-security-raises-a-7-million-million-series-a-from-bradesco-l4-venture-builder-and-accenture.

Tokyo SME. 2023. "Leakage Risk Assessment & Management Software: Tenchijin CMPASS KnoWaterleak." https://tokyo-smes.com/en/productservice/management-software/.

Topor, Sorin. 2024. "The importance of military sciences to ensure national survival in future conflicts ." *Journal: Annals – Series on Military Sciences*, No. 1. https://www.ceeol.com/search/article-detail?id=1248442.

Tzu, Sun. 2026. *Arta războiului.* București: Editura Art.

Van Haaster, Jelle. 2019. "On Cyber: The utility of military cyber operations during conflict." *[Thesis, fully internal, Universiteit van Amsterdam], UvA-DARE (Digital Academic Repository)*. p. 90. https://pure.uva.nl/ws/files/37093787/Thesis.pdf.

Willett, Marcus. 2022. "The Cyber Dimension of the Russia-Ukraine War." *Survival: Global Politics and Strategy* 64 (5): 7-26. doi:10.1080/00396338.2022.2126193.

Wright, Timoty. 2022. "Hypersonic Missile Proliferation: An Emerging European Problem?" *EU Non-Proliferation and Disarmament Consortium, Non-Proliferation and Disarmament Papers*, No. 80. doi:doi.org/10.55163/qvhv3959.

Youvan, Douglas. 2024. "The Shadow War in Kursk: Assessing the Potential Role of CIA Covert Operations in the Ukrainian Incursion int Russian Territory." doi:10.13140/RG.2.2.15318.46404.

Титаренко, Олександр şi Євген Власенко. 2024. „ПРОТИПОВІТРЯНА ОБОРОНА В РОСІЙСЬКО-УКРАЇНСЬКІЙ ВІЙНІ: УРОКИ ТА РЕКОМЕНДАЦІЇ" ("AIR DEFENSE IN THE RUSSIAN-UKRAINIAN WAR: LESSONS AND RECOMMENDATIONS")." *Повітряна міць України* 1 (6): 49–55. https://doi.org/10.33099/2786-7714-2024-1-6-49-55.

BULETINUL
UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I"
https://buletinul.unap.ro

Operațiile de informații, proiecte de rivalitate în Arena informațiilor

Information operations, rivalry projects in the information arena

Lect.univ.Dr. Cristinel-Marius AMZA*
*Universitatea Națională de Apărare „Carol I", București
e-mail: amza.marius@unap.ro

Abstract

Organizarea și desfășurarea operațiilor de informații în Arena informațiilor implică o rivalitate și o confruntare reală între serviciile de informații, pentru a câștiga unele avantaje în defavoarea celorlalte. Nu este deloc surprinzător faptul că acești rivali încearcă permanent, pe de-o parte, să-și împiedice reciproc eforturile de a se cunoaște unul pe celălalt, și, pe altă parte, să-l inducă în eroare, să-l dezinformeze sau să-l înșele.

The organization and conduct of intelligence operations in the Intelligence Arena involves a real rivalry and confrontation among the Intelligence Services, conducted in order to gain some advantages at the expense of others. Nothing is surprising in the fact that these rivals are constantly trying on the one hand to thwart each other's efforts to know the other, and, on the other hand, to mislead, misinform, or deceive.

Cuvinte-cheie:
operații de informații; factori de decizie; ISR; contrainformații; clandestin; secret.

Keywords:
intelligence operations; ISR; counterintelligence; clandestine; confidential; secret.

Info articol
Primit: 2 octombrie 2024; Evaluat: 1 noiembrie 2024; Acceptat: 13 decembrie 2024; Disponibil online: 17 ianuarie 2025
Citare: Amza, C.M. 2024. „Operațiile de informații, proiecte de rivalitate în Arena informațiilor".
Buletinul Universității Naționale de Apărare „Carol I", 13(4): 168-181. https://doi.org/10.53477/2065-8281-24-46

La acest moment, putem afirma că majoritatea strategiilor de securitate sau de apărare, elaborate de cele mai multe state ale lumii fac referire, în speță, la interesele naţionale, iar acestea sunt cele care determină acţiunile acestora pe scena internaţională, asigurându-se că supravieţuiesc.
Culegerea de informații referitoare la adversari a fost și este esențială pentru elaborarea acestor strategii militare încă de la apariția rivalităților. Cunoașterea capacităților adversarilor, a ordinii de luptă și a intenției poate face diferența dintre victorie și înfrângere. Fie prin intermediul senzorilor umani și interceptarea comunicațiilor, fie prin observarea de pe vârful unui deal sau, în epoca modernă, de la cel mai înalt nivel al spațiului, abilitatea de a cunoaște ceea ce face adversarul este esențială pentru înțelegere și, în cele din urmă, pentru victorie.
În contextul mediului actual de securitate, dependența puterii naționale de sfera informațiilor este evidentă și impune ca structurile de informații să fie capabile să sprijine politica externă dorită de factorii de decizie de la nivelul strategic. Statele dominante creează și își configurează serviciile de informații pentru a-și spori puterea în relațiile internaționale, iar din această perspectivă, acestea sunt, în esență, „arene de acțiune pentru relațiile de putere” (Morgenthau 2007; Evans și Wilson 1992, 330).

Informațiile înseamnă cunoașterea mediului de securitate, a actorilor și forțelor care reprezintă o amenințare la adresa unui stat (NATO AAP-6 2021). Cunoştinţele sunt în sprijinul factorului politic și militar care sunt parte componentă a procesului decizional și rezultatul culegerii, prelucrării, exploatării, integrării și interpretării informațiilor disponibile privind mediul actual de securitate și amenințările.
Informațiile au două mari obiective: primul este reducerea incertitudinii prin furnizarea de informații precise, oportune și relevante, a datelor referitoare la amenințări și mediul înconjurător, iar cel de-al doilea se referă la protejarea teritoriului național și a cetățenilor prin desfășurarea de activități și acțiuni de contrainformații.

Sfera intereselor și divergențele de geopolitică, geostrategie, economie și ideologie dintre actorii statali nu vor permite niciodată decidenților de la nivelul strategic să aibă o imagine clară asupra mediului de securitate, de aceea informațiile acoperă cel mai mare număr de necunoscute și trebuie să răspundă întrebărilor legate de acestea pentru cunoașterea adevăratelor intenții. Aproape întotdeauna vor exista lacune în informații și în datele furnizate și va lipsi gradul de detaliu dorit, deoarece informațiile nu pot oferi absolut totul cu certitudine, acestea utilizează probabilități, dar încearcă să reducă incertitudinea, înfruntându-l pe competitor prin culegerea de informații relevante, prin plasarea lor în context pentru a oferi cunoștințe și a le transmite pentru formarea imaginii complete și pentru a îmbunătăți înțelegerea acesteia, iar în acest sens, desfășurarea acțiunii de informații și de contrainformații de către serviciile de informații este relevantă.

O abordare a arenei informațiilor din punctul de vedere al operațiilor de informații constă în clasificarea acestora în trei mari categorii: prima categorie se referă la

culegerea de date și informații pentru procesarea, transformarea în produse finite de informații și diseminarea acestora către decidenți, cea de-a doua categorie se referă la acele operații de informații, întreprinse pentru a influența cursul unor evenimente, numite, uneori, operații clandestine sau secrete, iar cea de-a treia cuprinde operațiile de contrainformații, executate pentru a contracara operațiile de informații, indiferent de natura adversarului. Toate aceste trei tipuri de operații de informații vor avea impact asupra politicii externe a oricărui stat. Impactul va varia în ceea ce privește atât domeniul de aplicare, cât și gradul de implicare, pentru că factorul politic este cel care aprobă planificarea și executarea operațiilor de informații (Westwood 1977, 86).

O operație de informații este un proiect unic și complex, planificată și executată pe o perioadă de timp medie și îndelungată, cu resurse umane experimentate și cu un consum uriaș de resurse materiale și financiare pentru a îndeplini obiectivele. Un asemenea proiect constă într-un număr variabil de faze, subfaze, sarcini și acțiuni colective și individuale, executate într-o concepție unitară, iar realizarea este posibilă numai prin coordonarea și relaționarea de către un grup multidisciplinar, alcătuit din personal de informații (ofițeri operativi, analiști, personal tehnic, IT etc.), a fazelor, activităților și sarcinilor. Obiectivul principal al gestionării implementării proiectului operației este acela de a asigura performanța și calitatea tehnică necesară cu cel mai mic risc posibil și într-un timp cât mai rezonabil.

Operațiile de informații pentru culegerea de date și informații în scopul procesării și transformării acestora în produse finite de informații sunt necesare în acțiunile militare, deoarece aduc clarificarea mediului strategic, operațional și tactic, clarifică intențiile adversarului și sunt esențiale pentru deciziile comandantului. Informațiile includ organizațiile, capacitățile și procesele utilizate pentru sarcini, culegere, procesare, analiza și exploatarea informațiilor din mai multe surse, cu accent permanent pe satisfacerea cerințelor de informații ale comandantului grupării de forțe întrunire (JFC), iar acțiunile de informații se desfășoară în și din toate domeniile pe toată durata competiției (U.S. Air Force Doctrine 2023).
Informațiile le permit liderilor de la toate nivelurile să ia decizii pentru aplicarea puterii de luptă. Succesul în operații necesită decizii oportune și eficiente, bazate pe aplicarea logicii informațiilor și cunoștințelor disponibile. Prin urmare, comandanții și statele majore caută să construiască și să mențină înțelegerea permanentă a situației pe parcursul operației.

Operațiile de informații cuprind culegerea de informații din toate domeniile cu întregul spectru de capabilități al senzorilor, procesarea, exploatarea, analiza integrată și activități de furnizare de informații la nivel de mare unitate, centre de operații (aeriene, navale și terestre), distribuite beneficiarilor și centrelor naționale de producție. Aceste operații au ca rezultat diseminarea de informații către utilizatorii tactici, operaționali și strategici prin parcurgerea unui ciclu de informații: planificare și direcționare; culegere, procesare, analiză; diseminare; evaluare și feedback. Important este faptul că evaluarea și feedbackul sunt continue și facilitate pe tot parcursul ciclului prin colaborare și dialog cu toate părțile interesate.

Serviciile întrunite de informații, supraveghere și cercetare (JISR) sunt vitale pentru toate operațiile militare și oferă factorilor de decizie și statelor majore o mai bună cunoaștere a situației din mediul operațional. Pentru a permite culegerea informațiilor și pentru a se asigura că informațiile sunt analizate și sunt diseminate factorilor de decizie, există o serie de actori primari implicați, inclusiv mijloacele de culegere, supraveghere și cercetare (de exemplu, aeronavele de supraveghere Alliance Ground Surveillance și Airborne Warning & Control System, care utilizează radare, sateliți de observare, mijloace electronice și structuri de cercetare pentru a culege informații), analiștii de informații și factorii de decizie.

Cercetarea specială (special reconnaissance) reprezintă acțiunile de cercetare și supraveghere, efectuate ca o operație specială în medii ostile, greu accesibile sau sensibile din punct de vedere politic și/sau diplomatic pentru a culege sau a verifica informații de importanță strategică sau operațională, evitându-se descoperirea și lupta directă cu inamicul. Cercetarea specială se execută de subunități mici, cum ar fi un detașament sau o echipă de cercetare, formată din personal militar cu un nivel de pregătire ridicat, de obicei din unități de forțe speciale sau structuri de informații militare.

Ca scop și rol, cercetarea specială este diferită de acțiunile de comando, dar ambele sunt, de regulă, efectuate de aceleași tip de subunități. Rolul cercetării speciale include sprijinul direct al loviturilor operațiilor aeriene prin oferirea de imagini, permițând echipajelor să ajusteze atât strategia de zbor, cât și pe cele ale sistemelor de artilerie și de rachete terestre în zonele de operații din adâncimea dispozitivului inamicului, plasarea de senzori acționați și monitorizați de la distanță și pregătirile specifice pentru acțiunile altor structuri de forțe speciale sau informații militare. În multitudinea de misiuni pe care le pot executa subunitățile de cercetare specială, se regăsesc și acțiunile directe la obiective, precum și cele de război neconvențional, inclusiv operațiile de gherilă. Subunitățile de cercetare specială, pe lângă faptul că au un nivel înalt de pregătire, au și o echipare și dotare cu tehnică și armament calitativ superioară, deoarece trebuie să lupte în condiții dificile, adeseori cu un raport de forțe defavorabil, atunci când sunt descoperite, iar elementele de asigurare a extragerii vor avea nevoie de timp pentru a ajunge la ele.

În timpul primului Război din Golf din 1991, unitățile SAS britanice și forțelor aeriene ale SUA au fost trimise, inițial, în adâncimea dispozitivului de luptă irakian pentru a găsi lansatoarele de rachete Scud și pentru a direcționa loviturile executate de mijloacele aeriene. Atunci când acțiunile aeriene au întârziat, patrulele au atacat infrastructurile critice ale sistemelor Scud cu armamentul și cu tehnica din dotare.

În urma executării unei operații de cercetare specială, debriefingul structurilor poate fi făcut de ofițerii HUMINT, care sunt cel mai familiarizați cu tehnicile lor de culegere a informațiilor, deoarece este posibil ca informațiile rezultate să contribuie la culegerea informațiilor HUMINT, dar, în funcție de misiune, pot contribui și pentru IMINT, SIGINT, MASINT și TECHINT. Unele dintre aceste tehnici și proceduri sunt extrem de sensibile și confidențiale, fiind gestionate pe baza principiului „nevoii

de a cunoaște" în cadrul structurilor care coordonează operația de cercetare specială, inclusiv pentru membrii celulei de informații din toate sursele.

Operațiile de informații discrete, ascunse sau secrete ale unui guvern care urmărește influențarea evenimentelor în alte state nu sunt decât o mică parte a relațiilor internaționale, dar acestea există tocmai pentru a sprijini factorii de decizie. Planificarea și executarea acestui tip de operații au avantajul distinct al realizării politicii fără a pune în joc aspectul național și indiferent de natura lor, atunci când structurile de informații eșuează, nu lasă gustul amar al înfrângerii ca într-o confruntare.

Doctrina considerată multă vreme axiomatică, potrivit căreia șeful statului ar trebui să poată nega că a autorizat sau chiar că a avut cunoștință de o astfel de operațiune, chiar dacă implicarea unui stat într-o acțiune secretă devine cunoscută, este strâns legată de cele afirmate anterior. Acesta ar trebui să poată afirma, destul de plauzibil, că operația a fost îndeplinită de subordonații săi care au acționat fără știrea ori autorizarea lui (Shulski și Schmitt 2008, 151).

Operațiile de informații care urmăresc influențarea evenimentelor le putem clasifica în următoarele tipuri de operații: „discrete", „sub acoperire", „clandestine" și „sub steag fals". În acest articol, voi folosi termenul de operații „discrete" pentru a face diferența de operațiile „sub acoperire" și „clandestine".
O operație discretă (black operation) este o operație secretă a unei agenții guvernamentale, a unei entități militare sau a unei organizații paramilitare și poate include și activități ale entităților private, având ca obiectiv principal intrarea clandestină sau în secret în cadrul structurilor țintă ale unui competitor pentru a obține informații cu ajutorul surselor umane. Aceasta este în mod evident cea mai bună situație, în cazul culegerii de informații, din moment ce este dobândit accesul la documente secrete sau fragmente de informații, utile ori necesare. Caracteristicile de bază ale unei operații discrete constau în faptul că aceasta este confidențială și nu poate fi atribuită organizației care o desfășoară (Smith Jr. 2003). Acest tip de operație de informații a fost planificată și executată de majoritatea serviciilor specializate, precum MI6, MI5, Mossad, CIA, KGB, FSB, ISI, precum și de structuri de informații ale altor state (Intelnews 2008).

Diferența majoră dintre o operație discretă și una care este pur și simplu secretă este că o operație discretă implică un grad semnificativ de înșelăciune, pentru a ascunde identitatea organizatorului operației sau pentru a face să pară că o altă agenție ori entitate este implicată. Un exemplu cunoscut de astfel de operații este cel din luna mai 2007, atunci când ABC News și, mai târziu, The Daily Telegraph au afirmat că președintele Statelor Unite ale Americii George W. Bush a autorizat Agenția Centrală de Informații (CIA) să întreprindă „operații discrete" în Iran pentru a promova schimbarea regimului și pentru a sabota programul nuclear. Ulterior, ABC News a fost criticată pentru că a dezvăluit operația secretă, candidatul la președinția din 2008, Mitt Romney, declarând că a fost „șocat să vadă raportul ABC News privind

acțiunile secrete în Iran", dar ABC a spus că CIA și administrația George W. Bush știau de planurile lor, de a publica informațiile și nu au ridicat obiecții (Montopoli 2007). În luna iunie a aceluiași an, CIA a desecretizat o parte din documente și le-a făcut publice, în acestea detaliindu-se supravegherea ilegală, comploturi de asasinat, răpiri și alte operații „discrete", întreprinse în perioada anilor '50, '70, deoarece acestea ofereau o perspectivă asupra unei perioade foarte dificile și arăta profilul unei agenții de informații foarte diferit privind modul de acțiune pentru îndeplinirea sarcinilor.

O operație clandestină (clandestine operation) este o operație de informații sau militară, desfășurată în așa fel încât acțiunile și activitățile să fie neobservate de populația locală sau de structurile de informații și de contrainformații ale adversarului. Până în anii '70, operațiile clandestine au fost, în primul rând, de natură politică, vizate, în general, să sprijine grupuri sau națiuni pe care o altă entitate le favoriza. Exemplele includ implicarea serviciilor de informații americane cu criminali de război germani și japonezi după Cel de-Al Doilea Război Mondial sau acțiunea militară eșuată din Golful Porcilor din 1961. În prezent, aceste operații se regăsesc în metodele de acțiune ale multor structuri de informații de pe mapamond, sunt numeroase și se execută în funcție și de tehnologia avută la dispoziție.

Cea mai mare parte a operațiilor clandestine sunt legate de culegerea de informații, activitate desfășurată, de obicei, atât de către oameni, cât și de către senzori, amplasați în zone strategice sau camuflați în locuri importante. Amplasarea de cabluri de comunicații subacvatice sau terestre, de camere, microfoane, senzori de trafic, monitoare, precum snifferele, și de sisteme similare necesită ca misiunea să rămână nedetectată. Senzorii clandestini pot fi, de asemenea, montați pe vehicule subacvatice fără pilot, pe sateliți de cercetare, pe vehicule aeriene fără pilot (UAV) sau detectoare fără pilot, ori plasați manual de către surse umane clandestine.

Termenii clandestin și ascuns nu sunt sinonimi. După cum se menționează în definiție (care a fost folosită de Statele Unite și NATO încă din Cel de-Al Doilea Război Mondial), într-o operație sub acoperire, identitatea sponsorului este ascunsă, în timp ce într-o operație clandestină, operația în sine este ascunsă. Cu alte cuvinte, clandestin înseamnă „procedeu ascuns/stealth", atunci când se urmărește ca operația să nu fie descoperită. Termenul "stealth" se referă atât la un set larg de tactici, menite să ofere și să păstreze elementul surpriză, cât și la reducerea rezistenței inamicului la culegerea de informații. Ascuns înseamnă „să poată fi negat", astfel încât dacă operația este descoperită, aceasta să nu fie atribuită unui grup sau unei entități. Unele operații pot avea aspecte atât clandestine, cât și ascunse, cum ar fi utilizarea de senzori ascunși, amplasați la distanțe foarte mari sau de observatori umani, care sunt în măsură să direcționeze atacurile de artilerie și rachete terestre și loviturile acțiunilor aeriene. Atacul este evident, dar componenta folosită pentru a localiza ținta poate rămâne clandestină.

În Cel de-Al Doilea Război Mondial, țintele identificate și localizate prin criptoanaliza comunicațiilor radio au fost atacate doar dacă s-au executat și acțiuni

de cercetare aeriană a zonelor sau, în cazul doborârii avionului amiralului Isoroku Yamamoto, de observare, acțiune care a fost în sarcina Coastwatchers (Coast Watch Organization, Combined Field Intelligence Service, agenți aliați de informații militare, staționați pe insulele îndepărtate ale Pacificului). În timpul războiului din Vietnam, șoferii camioanelor atacate pe traseul Ho Chi Minh nu cunoșteau posibilitățile senzorilor deținuți de SUA, de tipul dispozitivului aeropurtat Black Crow, care identifica locația camioanelor după căldura motorului.

La acest moment, în Atanticul de Nord există o vastă infrastructură critică de rețele de cabluri submarine de comunicații între Europa și America de Nord, iar site-uri, precum TeleGeography, dețin hărți detaliate ale dispunerii cablurilor cu utilizări civile (energie, internet etc.), însă există și sisteme militare care nu fac obiectul unor asemenea postări, deoarece conțin date esențiale pentru toate formele de comunicare dintre membrii Alianței. Legat de aceasta, navele de cercetare electronică ale marinei ruse (de exemplu, nava Yantar, clasificată oficial ca navă auxiliară de cercetare generală oceanografică, cu capabilități de salvare subacvatică, care se subordonează unei structuri separate de marina militară a Ministerului rus al Apărării) acționează, uneori, pe ascuns (dezactivarea sistemului de identificare prin satelit), în apropierea cablurilor submarine vitale, determinând îngrijorarea oficialilor militari și de intelligence în legătură cu o eventuală interceptare a unor comunicări cu caracter secret.

O operație sub acoperire (covert operation) este o operație, executată de structurile militare sau de structurile de poliție, care implică un agent secret sau trupe care acționează sub o presupusă acoperire pentru a ascunde identitatea părții responsabile (Carson 2018). Conform legislației SUA, Agenția Centrală de Informații (CIA) este în măsură să conducă operații sub acoperire. Cadrul legislativ a definit acțiunea sub acoperire ca „activități speciale" atât politice, cât și militare, pe care guvernul SUA le poate refuza legal (Daugherty 2004). Efectul acestui cadru legislativ se regăsește într-o atenție deosebită pe care Congresul SUA o acordă CIA, în comparație cu celelalte structuri de informații.

Potrivit unui studiu, din 2018, al politologului, de la Universitatea din Chicago, Austin Carson, operațiile sub acoperire pot avea efectul benefic de a preveni escaladarea diferendelor în conflicte sau războaie. El susține că păstrarea secretului operațiilor militare poate limita dinamica escaladării, precum și izolarea liderilor de presiunile interne, permițându-le simultan să comunice adversarului interesul de a menține un război limitat (Carson 2018, 45).

Atunci când aceste operații sunt executate de structurile de poliție sintagma „sub acoperire" înseamnă a evita detectarea de către personalul monitor cu atribuții și mai ales a-și ascunde propria identitate (sau a folosi o identitate asumată), în scopul câștigării încrederii unui individ sau a unei organizații, pentru a afla ori a confirma informații confidențiale, ori pentru a câștiga încrederea persoanelor vizate în vederea culegerii de informații sau de dovezi. Operațiile sub acoperire, în mod tradițional, sunt executate de structurile de aplicare a legii, iar cei care îndeplinesc astfel de roluri sunt denumiți, în mod obișnuit, agenți sub acoperire.

Primele acțiuni au fost desfășurate în anul 1883 pe teritoriul Irlandei, au vizat combaterea acțiunilor de amplasare a bombelor pe care Frăția Republicană Irlandeză care le începuse cu câțiva ani mai devreme, iar agenții care au acționat au fost pentru prima dată instruiți în tehnici și tactici de combatere a terorismului. În 1906 pe teritoriul Statelor Unite a fost desfășurată o activitate similară, atunci când au fost înființate „echipele italiene" pentru a combate criminalitatea și a intimida elementele agresive din cartierele italiene sărace.

Există două probleme principale care pot afecta agenții sub acoperire. Prima este menținerea identității, iar a doua este reintegrarea în activitatea normală după îndeplinirea obiectivelor operației. A trăi o viață dublă într-un mediu nou prezintă multe probleme, deoarece munca sub acoperire este una dintre cele mai stresante activități pe care le poate întreprinde un agent special. Principala cauză a stresului este separarea agentului de prieteni, familie și de mediul său normal. Stilul de viață al agenților sub acoperire este foarte diferit de cel al polițiștilor obișnuiți și după încheierea misiunii, este dificil să se reintegreze în sarcinile cotidiene. După un astfel de stil de viață liber, agenții pot avea probleme de subordonare, de disciplină sau se simt inconfortabil și pot avea viziuni ciudate, uneori chiar paranoice despre lume și viață și pot fi permanent în stare de alertă.

De-a lungul istoriei, au fost desfășurate foarte multe operații de intelligence acoperite, care au avut ca scop obținerea de informații despre potențiali adversari, încă din perioada de pace. În acest context, se poate spune că astfel de operații fac parte din modul de acțiune al serviciilor de informații, în scopul avertizării timpurii a liderilor politico-militari (Piroșcă 2020, 2-3).

O operație sub steag fals (false flag) este un act comis cu intenția de a masca sursa reală a răspunderii și de a da vina pe o altă parte. Termenul a fost folosit pentru a descrie un truc în războiul naval prin care o navă arbora steagul unei țări neutre sau prietene pentru a-și ascunde adevărata identitate. Tactica a fost folosită, inițial, de pirați pentru a înșela alte nave, permițându-le astfel să se apropie de ele înainte de a le ataca. Mai târziu, a fost considerată o practică acceptabilă în timpul războiului naval, în conformitate cu legile maritime internaționale, cu condiția ca nava atacatoare să-și arate adevăratul pavilion, odată ce a început atacul (Ruis și Nilsson 2022, 18-35).

Astăzi, termenul mai reprezintă și organizarea de atacuri ale unor națiuni asupra lor, făcând ca acestea să pară a fi ale națiunilor inamice sau ale unor grupări teroriste, oferind astfel un pretext pentru represiune internă sau pentru declanșarea unei agresiuni militare. În acțiunile militare terestre, astfel de operații sunt, în general, considerate acceptabile în anumite circumstanțe, cum ar fi înșelarea inamicului, cu condiția ca înșelăciunea să nu fie perfidă și ca toate înșelăciunile să fie eliminate înainte de a deschide focul asupra inamicului.
Acest tip de operații de informații a fost utilizat ca pretext pentru declanșarea unor războaie. Astfel, incidentul Gleiwitz, din noaptea de 31 august 1939, l-a avut ca

protagonist pe Reinhard Heydrich, prin fabricarea dovezilor privind un atac polonez împotriva Germaniei, cu scopul de a mobiliza opinia publică germană la război și de a justifica războiul cu Polonia. Alfred Naujocks a fost un organizator cheie al operației, la ordinul lui Heydrich, care a dus la moartea câtorva deținuți din unele lagăre de concentrare naziste, care au fost îmbrăcați în soldați germani și apoi împușcați de Gestapo pentru a face să pară că au fost împușcați de soldații polonezi. Acest lucru, împreună cu alte operații sub steag fals din Operația Himmler, ar fi folosit pentru a mobiliza sprijinul populației germane pentru începutul Celui de-Al Doilea Război Mondial în Europa (Lightbody 2004). Operația nu a avut succes, deoarece nu a reușit să convingă opinia publică internațională de pretențiile germane, iar Marea Britanie și Franța au declarat război la două zile după ce Germania a invadat Polonia.

În februarie 2022, structuri de informații ale unor guverne occidentale au avertizat în legătură cu posibilitatea ca Federația Rusă să desfășoare o operație sub steag fals pentru a avea pretextul de a invada Ucraina. Aspectele premergătoare invaziei din 24 februarie au evidențiat o intensificare a campaniei de dezinformare și de inducere în eroare a Kremlinului și a mass-mediei ruse prin promovarea unor „steaguri false" aproape la fiecare oră, pretinzând că arată atacarea Rusiei de către forțele armate ucrainene, în încercarea de a justifica o invazie în Ucraina. Multe dintre videoclipurile postate pe canalele de socializare au fost pentru dezinformare, având o calitate slabă, metadatele nu s-au potrivit, deoarece au arătat date incorecte, iar dovezile și argumentele, prezentate de specialiștii de la Bellingcat și de alți jurnaliști independenți, au evidențiat că atacurile, exploziile și evacuările revendicate în Donbas au fost puse în scenă de Rusia.

În mod similar, în războiul naval o astfel de înșelăciune este permisă, cu condiția ca steagul fals să fie coborât și steagul adevărat să fie ridicat înainte de a se angaja în luptă (Squires 2008). Un exemplu notabil a fost crucișătorul german (fostă navă comercială) Kormoran, din Cel de-Al Doilea Război Mondial, care a surprins și a scufundat crucișătorul australian HMAS Sydney, în 1941, în timp ce era disimulat într-o navă comercială olandeză, provocând cele mai mari pierderi de vieți omenești pe o navă de război australiană. În timp ce Kormoran a fost grav avariat în timpul luptei și echipajul său a fost capturat, rezultatul a reprezentat o victorie morală considerabilă pentru germani.
În spionaj, termenul „steag fals" descrie recrutarea de agenți de către ofițerii de informații care se prezintă drept reprezentanți ai unei cauze față de care agenții potențiali îi simpatizează sau chiar propriul guvern al agenților.

Pentru a asigura succesul relațiilor internaționale ale unui stat și al operațiilor militare, factorii de decizie strategici trebuie să mai dispună și de măsurile necesare pentru a interzice posibilitatea adversarului de a executa acțiuni de terorism, spionaj, subversiune, sabotaj, crimă organizată sau de a ataca propriile rețele de comunicații și informatică. Pentru a realiza acest lucru, este necesară identificarea vulnerabilităților entităților proprii, iar rezultatele analizei vor fi trimise structurilor de contrainformații.

Contrainformațiile (CI) includ acele activități care se referă la identificarea și contracararea amenințării la adresa securității pe care o reprezintă serviciile sau organizațiile de informații ostile ori persoanele implicate în spionaj, sabotaj, subversiune sau terorism (NATO Standard AJP-2 2016; UK Ministry of Defence JP 2-00 2023), iar cea mai bună apărare împotriva atacurilor actorilor străini asupra teritoriului național, cetățenilor țării sau împotriva infiltrării serviciilor de informații constă în măsuri active și flexibile, cu posibilitatea de a alege cu rapiditate tehnicile de contrainformații, în funcție de evoluția situației, împotriva acelor servicii ostile, indiferent de apartenența lor. Această apărare este, de regulă, denumită contraspionaj, adică măsuri luate pentru a detecta spionajul inamicului sau atacurile fizice împotriva serviciilor de informații prietene, pentru a preveni deteriorarea și pierderea de informații și, acolo unde este posibil, pentru a întoarce tentativa împotriva inițiatorului său. Contraspionajul merge dincolo de a fi reactiv și încearcă în mod activ să submineze serviciul de informații ostil prin recrutarea de agenți în serviciul extern, prin discreditarea personalului efectiv loial propriului serviciu și prin luarea de resurse care ar fi utile serviciului ostil. Toate aceste acțiuni se aplică amenințărilor nonnaționale, precum și organizațiilor naționale.

Dacă acțiunea ostilă se desfășoară în propria țară sau într-una prietenă ori aliată, cu cooperarea structurilor de poliție, agenții ostili pot fi arestați sau, dacă sunt diplomați, declarați persona non grata. Din perspectiva unui serviciu de informații, exploatarea situației în avantajul părții este, de obicei, preferabilă arestării sau acțiunilor care ar putea duce la anihilarea amenințării. Prioritatea informațiilor intră, uneori, în conflict cu instinctele propriilor organizații de aplicare a legii, mai ales atunci când amenințarea străină combină personalul străin cu cetățenii țării.

În unele împrejurări, arestarea poate fi un prim pas în care deținutului i se oferă posibilitatea de a alege să coopereze sau să se confrunte cu consecințe grave până la condamnarea la moarte pentru spionaj. Cooperarea poate consta în a spune tot ce se știe despre celălalt serviciu, dar, de preferință, asistarea activă la acțiuni înșelătoare împotriva serviciului ostil.
Protecția serviciilor de informații se realizează prin organizarea contrainformațiilor defensive și implică evaluarea riscurilor asupra culturii, surselor, metodelor și resurselor acestora. Managementul riscurilor trebuie să reflecte în mod constant acele evaluări, deoarece operațiile eficiente de informații sunt adesea asumate de riscuri. Chiar și atunci când își asumă riscuri calculate, serviciile trebuie să atenueze riscul cu contramăsuri adecvate și, în mod special, pentru a descoperi metodele specifice artei schimbului de informații. Astăzi, serviciile de informații își dezvoltă capabilități pentru a explora alte entități de informații care se consideră deschise și pentru a putea submina persoane din interiorul comunității de informații. Contraspionajul ofensiv este cel mai puternic instrument de descoperire a intruşilor și de neutralizare a acestora, dar nu este singurul instrument.

În general, se subînțelege că guvernele se implică în acțiuni secrete (deoarece se implică în spionaj), acestea sunt de multe ori ilegale, conform legislației statului pe

teritoriul căruia se desfășoară. De asemenea, ele pot fi contrare legilor internaționale, la baza cărora stă principiul neamestecului în afacerile interne ale statelor suverane, deși acest principiu are din ce în ce mai multă greutate în jurisprudența internațională, după încheierea Războiului Rece (Shulski și Schmitt 2008).

Factorii de decizie au nevoie de informații care să nu fie controlate sau manipulate de forțe ostile. Deoarece fiecare disciplină de informații este supusă manipulării de către adversari, verdicitatea informațiilor și credibilitatea tuturor mijloacelor de culegere sunt esențiale. În consecință, fiecare organizație de contrainformații va valida fiabilitatea surselor și metodelor care se referă la misiunea de contrainformații, în conformitate cu standardele comune.

Atunci când o amenințare străină combină personalul străin cu cetățenii unei țări, avem de-a face cu operații de informații, sub denumirea de „coloana a cincea (fifth column)". În limbajul uzual, expresia îi desemnează pe cei care își trădează patria, care acţionează din interior, de obicei în favoarea unui grup inamic sau a unei alte naţiuni. De altfel, dicționarul Petit Robert definește sintagma prin „servicii secrete de spionaj inamice dintr-un teritoriu", iar Larousse, ca „element care lucrează pe un teritoriu în avantajul adversarului (sub această denumire au fost desemnaţi, în 1940, agenții serviciilor secrete germane care au acționat în Franţa)". Termenul se aplică și acțiunilor organizate de cadrele militare. Activitățile unei coloane a cincea pot fi la vedere sau clandestine. Toate persoanele și mijloacele materiale și financiare constituite în secret pot fi coordonate pentru a sprijini direct un atac din exteriorul țării. Activitățile clandestine, pentru o coloană a cincea, pot fi concretizate prin terorism, spionaj, sabotaj și dezinformare. Aceste acțiuni se execută exclusiv pe teritoriul național sau chiar în cadrul dispozitivului de luptă (pe timpul stărilor excepționale, instituite sau decretate) de către simpatizanții secreți ai unei forțe din afară.

Sintagma „coloana a cincea" își are originea în Spania (inițial quinta columna), datând din perioada premergătoare războiului civil spaniol. După cât se știe, a apărut, pentru prima dată, într-o telegramă secretă, din 30 septembrie 1936, trimisă la Berlin de către însărcinatul cu afaceri german la Alicante, Hans Hermann Völckers. În telegramă, el s-a referit la o „presupusă declarație a lui Franco" neidentificată, care se vehiculează (se pare că în zona republicană sau în zona levantină, deținută de republicani). Această „presupusă declarație" susținea că Franco a afirmat că existau patru coloane naționaliste care se apropiau de Madrid și o a cincea coloană care aștepta să atace din interior (termenul apare, pentru prima dată, într-o publicație spaniolă, după care, la 4 octombrie 1936, este preluată în publicația franceză *Le Journal*) (Le Journal 1936).

Public, termenul apare în numărul, din 3 octombrie 1936, al cotidianului comunist madrilen *Mundo Obrero*, iar până la jumătatea lunii octombrie, mass-media avertiza deja despre celebra coloană a cincea. Până la sfârșitul anilor '30, pe măsură ce implicarea americană în războiul din Europa a devenit mai probabilă, termenul de coloana a cincea a fost folosit în mod obișnuit pentru a avertiza despre potențiala

răzvrătire și neloialitate în interiorul granițelor SUA. Frica de trădare a fost sporită de căderea rapidă a Franței în 1940, pe care unii au pus-o pe seama slăbiciunii interne și a coloanei a cincea progermană, iar în Regatul Unit, într-un discurs adresat Camerei Comunelor, Winston Churchill i-a asigurat pe deputați că va acționa ca o mână de fier împotriva activităților coloanei a cincea.

Concluzii

Instrumentele de putere națională constau, de regulă, în ansambluri de surse de putere care trebuie să se adapteze permanent la schimbările care se petrec în mediul de securitate internațional sau chiar la cele din mediul intern al unui anumit stat. Instrumentul informațional este exercitat prin intermediul unor instituții specializate și are menirea de a furniza conducerii statelor, precum și celorlalte instituții care țin de alte instrumente de putere datele necesare adoptării celei mai potrivite decizii. Similar instrumentului diplomatic, instrumentul informațional este utilizat atât pe timp de pace, cât și în situații de criză sau în stare de război.
În acest sens, operațiile de informații sunt văzute de serviciile de informații ca metode și mijloace de folosire a agenturilor, de infiltrare a agenților în mediile de interes, din străinătate, în incursiuni pe teritoriul inamic, precum și în acțiuni de prevenire a unor acte de sabotaj sau de terorism pe teritoriul național.

Informațiile sunt vulnerabile nu numai la amenințările externe, ci și la cele interne. Trădarea și scurgerile de informații expun vulnerabilități, secrete guvernamentale și militare, surse și metode de informații. Amenințarea din interior este o sursă de daune extraordinare la adresa securității naționale, mai ales atuci când agenții au acces la informații referitoare la activități majore, discrete, sub acoperire sau clandestine.

Pentru planificarea, organizarea și desfășurarea operațiilor de informații, structurile de informații trebuie să își adapteze continuu activitățile la cerințele comandanților lor și la condițiile dure și des schimbătoare ale arenei informațiilor. Acest aspect implică în mod special agilitatea mentală și organizațională, susținută prin reziliență, adaptare și flexibilitate. Este normal ca succesul să apară mai târziu și de aceea este necesară perseverența în acțiuni, adaptarea rapidă și exploatarea oportunităților la momentul apariției lor. Pentru fiecare operație de informații, o agenție trebuie să elaboreze o metodologie specifică proiectului, asigurând astfel caracterul unic și complex al activităților, pentru a atinge scopul propus. Adaptarea rapidă a metodelor de lucru în domeniul informațiilor la mediul de acțiune și la ritmul de dezvoltare al tehnologiilor din domeniul informaticii și comunicațiilor obligă agenții secreți la o îmbunătățire a eficienței în culegerea informațiilor și la o flexibilitate a procedurilor de lucru, pentru a face față schimbării contextului și pentru a evita ideea că există doar o metodă de lucru.

La acest moment, putem spune că operațiile de informații sunt o acțiune uzuală care face parte din tacticile, tehnicile și procedurile de acțiune ale serviciilor de informații

din întreaga lume, în scopul cunoașterii permanente a intențiilor competitorilor sau ale statelor în care se manifestă ostilitate față de statul care inițiază astfel de operații, precum și pentru sprijinul acțiunilor militare și avertizării timpurii a liderilor politici și militari de la nivel strategic.

În concluzie, organizarea și desfășurarea operațiilor de informații în „Arena informațiilor" implică o rivalitate și o confruntare reală între serviciile de informații, pentru a câștiga unele avantaje în defavoarea celorlalte. Nu este surprinzător faptul că acești rivali încearcă permanent, pe de-o parte, să contracareze eforturile celuilalt de a-l cunoaște și, pe de altă parte, să-l inducă în eroare, să-l dezinformeze sau să-l înșele.

Referințe

Carson, Austin. 2018. *Secret Wars: Covert Conflict in International Politics.* Princeton University Press.

Daugherty, William J. 2004. *Executive Secrets: Covert Action and the Presidency.* University of Kentucky Press.

Evans, Tony și Peter H. Wilson. 1992. "Regime Theory and the English School of International Relations: A Comparison." *Millennium – Journal of International Studies* 21: 329 - 351.

Intelnews. 2008. "Tallinn government surveillance cameras reveal black bag operation." https://intelnews.org/2008/12/16/04-11/.

Le Journal. 1936. "La Passionaria prêche la terreur."

Lightbody, Bradley. 2004. *The Second World War: Ambitions to Nemesis.* Routledge.

Montopoli, Brian. 2007. "Știri CBS." http://www.cbsnews.com/8301-500486_162-2842625-500486.html.

Morgenthau, Hans J. 2007. *Politica între națiuni, Lupta pentru putere și lupta pentru pace.* Iași: Editura Polirom.

NATO AAP-6. 2021. "NATO Glossary of Terms and Definitions ."

NATO Standard AJP-2. 2016. "Allied Joint Doctrine for Intelligence, Counterintelligence and Security." Edition A Version 2. https://jadl.act.nato.int/ILIAS/data/testclient/lm_data/lm_152845/Linear/JISR04222102/sharedFiles/AJP2.pdf.

Piroșcă, Valerică. 2020. „Operații de intelligence." *Colocviu Strategic* 6 (173): 2-3. https://cssas.unap.ro/ro/pdf_publicatii/cs06-20.pdf.

Ruis, Carlos Diaz și Tomas Nilsson. 2022. "Disinformation and Echo Chambers: How Disinformation Circulates in Social Media Through Identity-Driven Controversies." *Journal of Public Policy & Marketing* (no. 42): 18-35.

Shulski, Abram N. și Gary J. Schmitt. 2008. *Războiul tăcut.* București: Editura Polirom.

Smith Jr., W. Thomas. 2003. *Encyclopedia of the Central Intelligence Agency.* New York: Facts on File Inc.

Squires, Nick. 2008. *HMAS Sydney found off Australia's west coast.* https://www.telegraph.co.uk/news/worldnews/australiaandthepacific/australia/1581972/HMAS-Sydney-found-off-Australias-west-coast.html.

U.S. Air Force Doctrine. 2023. "Air Force Doctrine Publication 2-0 - Intelligence." https://www.doctrine.af.mil/Doctrine-Publications/AFDP-2-0-Intelligence/.

UK Ministry of Defence JP 2-00. 2023. "Joint Doctrine Publication. Intelligence, Counter-intelligence and Security Support to Joint Operations." https://assets.publishing.service.gov.uk/media/653a4b0780884d0013f71bb0/JDP_2_00_Ed_4_web.pdf.

Westwood, James T. 1977. "A contemporary political dilemma: the impact of intelligence operations on foreign policy." *Naval War College Review* 29 (4): 86-92. https://www.jstor.org/stable/44641751.

BULETINUL
UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I"
https://buletinul.unap.ro

Explorarea competitive intelligence în România: înțelegerea perspectivelor și abordărilor corporative

Exploring competitive intelligence in Romania: understanding corporate views and approaches

Dr. Adina MIHĂESCU*
Lect.Dr. Raluca LUȚAI**
*Universitatea Babeș-Bolyai, Departamentul de Studii Internaționale și Istorie Contemporană – Facultatea de Istorie și Filosofie
e-mail: adina.mihaescu@ubbcluj.ro
**Universitatea Babeș-Bolyai, Departamentul de Studii Internaționale și Istorie Contemporană – Facultatea de Istorie și Filosofie
e-mail: raluca.lutai@ubbcluj.ro

Abstract

Conștientizarea și aplicarea inteligenței competitive (IC) în România sunt semnificativ mai puțin dezvoltate, în comparație cu pieţele internaționale. Această disparitate este evidentă în înțelegerea limitată a metodologiilor de IC și alocarea insuficientă de resurse, destinate cultivării unei culturi orientate spre IC în cadrul întreprinderilor românești. În plus, punctele de vedere ale participanților la piață cu privire la semnificația și utilizarea IC nu au fost analizate în profunzime, evidențiind o deficiență considerabilă în cercetarea sistematică pe această temă. Articolul intenționează să abordeze această lacună prezentă în literatura de specialitate prin explorarea percepțiilor firmelor românești asupra activităților legate de IC.

The awareness and application of Competitive Intelligence (CI) in Romania are significantly less developed than in international markets. This disparity is evident in the limited understanding of CI methodologies and the insufficient allocation of resources dedicated to fostering a CI-oriented culture within Romanian enterprises. Furthermore, the perspectives of market participants on the importance and use of CI have not been thoroughly examined, highlighting a considerable gap in systematic research on this topic. This study aims to address this gap in the existing literature by exploring the perceptions of Romanian firms regarding CI-related activities.

Cuvinte-cheie:
inteligență competitivă; România; companii; percepție.

Keywords:
competitive intelligence; Romania; companies; perception.

Info articol
Primit: 15 octombrie 2024; Evaluat: 8 noiembrie 2024; Acceptat: 6 decembrie 2024; Disponibil online: 17 ianuarie 2025

Explorarea competitive intelligence în România: înțelegerea perspectivelor și abordărilor corporativeManifestări religioase în spațiul virtual și implicațiile acestora față de securitatea cibernetică. *Buletinul Universității Naționale de Apărare „Carol I"*, 13(4): 182-196. https://doi.org/10.53477/2065-8281-24-47

Competitive intelligence – conceptualizare

Dacă, pentru serviciile de intelligence, informația reprezintă elementul principal pentru asigurarea securității naționale, le ajută să fie performante sau să mențină un nivel de securitate, pentru companiile private – indiferent de domeniu –, informația presupune profit și succes în fața competitorilor. Competitivitatea face ca firmele să fie din ce în ce mai preocupate cu colectarea și folosirea informațiilor, iar procesul în sine devine din ce în ce mai sofisticat. Societățile au o stringentă nevoie nu numai de a deține informații, ci mai ales de o selecție a acestora și de transformarea lor în cunoaștere care să susțină procesul decizional. „Cunoașterea lucrurilor potrivite la momentul potrivit și acționarea asupra lor este esențială pentru obținerea succesului." (Cook și Cook 2000) Accentul cade așadar nu doar pe informație brută, ci și pe cea relevantă din perspectiva utilității, momentul obținerii fiind la fel de important ca și informația în sine. În acest context, apare și se dezvoltă un concept deosebit de important pentru domeniul de afaceri – intelligence-ul competitiv.

Competitive intelligence (CI) este definit ca orice combinație de date, informații și cunoștințe care privesc mediul de afaceri în care operează o companie și care, atunci când sunt prelucrate, oferă un avantaj competitiv semnificativ sau permit luarea unor decizii fundamentate, bazate pe analize temeinice ale tuturor factorilor relevanți și ale opțiunilor disponibile (Larry 1996, 16). O altă definiție subliniază faptul că competitive intelligence este ,,procesul prin care companiile se informează cu privire la toate aspectele legate de activitatea și performanța rivalilor. Este un element esențial în care planificarea, nu doar campaniile de marketing, dar și programele de producție, resursele umane, financiare și celelalte activități ale competitorilor pot avea influență directă sau indirectă (Larry 1996).

Acest domeniu este unul care a apărut în urma constatării unor nevoi sau lipsuri în activitatea de management, fiind transpus științific și metodologic în cercetare ulterior. Rezultă așadar că nu are o emergență din reflecțiile academice, ci mai degrabă bazată pe observații și necesitățile întreprinderilor. Rolul informațiilor economice a fost, evident, important de-a lungul istoriei, însă putem aborda această componentă a mediului de afaceri începând cu a doua jumătate a secolului XX. Primele lucrări științifice în acest domeniu au apărut în Statele Unite ale Americii. Una dintre lucrările care abordează complex și sistematic procesul de competitive intelligence a apărut în 1980 în Statele Unite ale Americii și îi aparține lui Michael Porter. Cu titlul *Competitive Strategy. Techniques for Analyzing industries and competitors*, cartea se adresează actorilor din mediul economic și își propune să rezolve o problemă indentificată în modul în care are loc procesul decizional la nivelul managementului. De asemenea, lucrarea prezintă o serie de tehnici generale de analiză a mediului concurențial și propune modele de stabilire a strategiilor (Porter 1980).

În lumea contemporană, anticiparea evoluțiilor și transformărilor rapide, apărute în cadrul pieților sau al diferitelor industrii, reprezintă provocări pe care managerii companiilor le gestionează din ce în ce mai greu. Pornind de la anumite situații date, formularea strategiilor (pe termen scurt, mediu și lung) reprezintă un pas

important, de care depinde însăși supraviețuirea companiei. Analiza de CI presupune un proces vast, prin care informațiile identificate sunt sortate, în funcție de utilitate, sunt evaluate, analizate și, în final, încredințate decidenților sub formă de analize complexe, destinate obținerii de avantaje concurențiale. Scopul esențial al fiecărui manager este obținerea profitului (sau a unui profit cât mai mare), iar acesta este unul dintre principalii indicatori economici care semnalează dacă strategiile alese sunt favorabile. Este important de precizat, aici, faptul că impactul unei analize CI nu este imediat și nu se poate observa numaidecât în creșterea profitului întreprinderii. Din perspectiva îmbunătățirii calității produselor, procesele CI aduc o multitudine de beneficii prin inovarea pe care o aduc atât companiilor, cât și sectoarelor și domeniilor în care acestea operează. Competitive intelligence presupune două direcții de lucru: una îndreptată înspre interior (mediul intern al companiei) și una îndreptată înspre exterior. Dacă cea dintâi vizează o analiză profundă a fiecărui departament în parte, cu structuri de lucru, procese și organigrame, cea de-a doua are ca obiectiv o cunoaștere fundamentală a concurenței (Cook și Cook 2000).
Toate companiile, indiferent de mărimea lor, au nevoie de competitive intelligence. Atât timp cât există conceptul de competiție, analiza acesteia este necesară. Tehnologia și posibilitatea consumatorilor de a face cumpărături online transformă concurența, internaționalizând-o, indiferent cât de mică sau mare este o companie. Pentru a rămâne pe o piață sau pentru a avea succes, companiile mici trebuie să fie conștiente de concurenții lor, să le identifice punctele forte și punctele slabe, precum și strategiile existente sau viitoare.

În România, nivelul de cunoaștere și utilizare a conceptului de competitive intelligence (CI) este încă slab dezvoltat, comparativ cu alte piețe internaționale. Lipsa unor cunoștințe și practici consolidate în jurul CI, alături de resursele limitate alocate acestui domeniu, contribuie la o integrare redusă a practicilor de intelligence în strategiile companiilor locale. Totodată, percepția agenților economici din piață față de importanța și utilitatea CI rămâne insuficient cunoscută, deoarece există puține studii sau cercetări care să exploreze sistematic modul în care actorii economici se raportează la acest proces strategic. Studiul nostru își propune să umple acest gol din literatura de specialitate, abordând într-un mod structurat analiza percepțiilor companiilor din România cu privire la utilizarea activităților specifice de competitive intelligence (CI). Prin intermediul unei metode calitative, cercetarea urmărește să exploreze în ce măsură organizațiile autohtone sunt conștiente de beneficiile CI, cum integrează aceste practici în procesele lor decizionale și ce bariere percep în adoptarea lor. Astfel, demersul nostru contribuie nu doar la înțelegerea mai profundă a subiectului, ci și la crearea unui cadru de referință, util pentru dezvoltarea și promovarea CI în contextul economic românesc.
În cele ce urmează, vom prezenta designul cercetării și principalele rezultate, reieșite în urma interviurilor realizate cu reprezentanți ai unor companii din România.

Designul cercetării

Pornind de la asumpțiile prezentate mai sus, lucrarea de față folosește metoda de cercetare calitativă care are la bază instrumentul interviului semistructurat, o metodă

care ne va ajuta să înțelegem modul în care companiile românești se raportează la practica intelligence-ului competitiv.
Domeniul competitive intelligence îmbină elemente din domeniul studiilor de intelligence și din cel al studiilor economice. Punctul de congruență al celor două domenii este incertitudinea, care poate fi eliminată din procesul decizional doar prin intermediul informației.

Selecția cazului
Studiul nostru urmărește percepția agenților economici din România cu privire la conceptul de competitive intelligence. Ne propunem deci o analiză a mediului economic românesc, pornind de la percepțiile actorilor economici, viziunea acestora și modalitățile lor de a rezista și de a se dezvolta. Importante pentru noi sunt atenția pe care acești agenți economici o acordă mediului concurențial și strategiile pe care le folosesc în această direcție. Cu alte cuvinte, încercăm să explorăm mecanismele cauzale care lucrează într-o relație generală (Jason 2008, 294-305). În acest sens, vom folosi metoda cazului unic, cazul României.

The Atlas of Economic Complexity, instrument de cercetare și explorare a fluxurilor comerciale globale pe pieţele internaționale, elaborat de Harvard Kennedy School of Government, în urma cercetărilor conduse de Harvard Growth Lab, plasează România pe locul 44 (dintr-un total de 133) în topul celor mai bogate economii ale lumii, cu o creștere de 3,9% în ultimii cinci ani. Se apreciază că țara noastră prezintă un mediu economic dinamic și complex, cu reale posibilități de creștere și de dezvoltare în următorii ani, considerându-se că perioada de tranziție postcomunistă, de la economie centralizată la economie de liber-schimb este finalizată (Growth Lab, fără an). Există, totodată, și o serie de particularități ale economiei românești care o diferențiază de celelalte state ale Uniunii Europene, printre care, cel mai de interes pentru studiul nostru, este faptul că nivelul de competitivitate și cel al indicatorilor de performanță sunt sub media europeană (Valentin 2017). Stat democratic de 34 de ani, membră a NATO de 19 ani și membră a Uniunii Europene de 17 ani, România este o țară capitalistă tânără. Este necesară o analiză a mediului economic prin prisma actorilor/companiilor care activează în cadrul acestuia, studiind, interpretând și analizând percepțiile acestora, raționamentele în baza cărora își desfășoară activitatea și, de asemenea, propriile metode de a interpreta complexitatea mediului economic în cadrul căruia funcționează și se dezvoltă.

Metoda de culegere a datelor
O analiză calitativă a mediului de afaceri din România prin prisma raportării la informații și concurență se poate face, cel mai cuprinzător, în viziunea noastră, cu ajutorul interviului semistructurat. Caracterul plurivalent al relației dintre economie și intelligence este dificil de cuantificat prin metode statistice, ceea ce a motivat alegerea interviului, care facilitează un dialog structurat, cu întrebări și răspunsuri, menite să dezvăluie viziunile companiilor asupra domeniului competitive intelligence.
Interviul semistructurat ne oferă flexibilitate și posibilitatea adaptării întrebărilor, în funcție de răspunsurile date de intervievat. Interacțiunea va fi una personalizată,

deschisă, oportună pentru studierea unui subiect, despre care nu sunt prea multe date disponibile. Acest climat ne va aduce mult mai multă înțelegere cu privire la percepțiile companiilor și ne va oferi ocazia să explorăm teme pe care, inițial, nu le-am luat în calcul.

Deoarece este imposibil de cercetat, în cadrul unei analize, întreaga populație, se stabilește un eșantion reprezentativ, iar intervievarea acestuia conduce la obținerea unor rezultate care pot fi mai apoi generalizate (Kalika, Mouricou și Garreaun 2009). Selecția respondenților s-a bazat pe diversitate, astfel că discuțiile s-au purtat cu reprezentanții unor companii din diferite arii și domenii de activitate, care activează (și) pe piața din România. Pentru că domeniul abordat, cel al informațiilor în afaceri, nu este unul ușor accesibil tuturor, s-au selectat întreprinderi mari, cu cifre de afaceri (în ultimii trei ani) de peste un milion de lei. Deși numărul companiilor contactate în vederea realizării interviului a fost considerabil mai mare, în final, numărul răspunsurilor obținute a fost de 23.

Discuțiile au fost purtate: față în față – cu 8 respondenți (35%), prin intermediul aplicațiilor informatice video – cu 11 respondenți (48%) și telefonic – cu 4 respondenți (17%). Perioada de desfășurare a interviurilor a fost de aproximativ 10 luni, din luna august 2022 până în luna mai 2023, iar durata medie a unei întâlniri a fost de 30 de minute. Din totalul celor 23 de respondenți, 19 au solicitat semnarea unui acord de confidențialitate NDA (non-disclosure agreement), care prevedea respectarea de către intervievator a păstrării confidențialității discuței în sine și a datelor și informațiilor oferite. Acesta a fost solicitat, deși fiecare respondent, în parte, a fost asigurat de respectarea anonimatului și a regulamentelor GDPR (General Data Protection Regulation) și de faptul că scopul acestei cercetări este pur academic și științific.

Din perspectiva conținutului, grila de interviu cuprinde trei părți: prima parte, în care se obțin date despre compania în cauză, se cercetează nivelul de înțelegere al subiectului CI, percepții asupra importanței informațiilor în mediul de afaceri; partea a doua – la care răspund cei care afirmă că întreprind acțiuni de CI – și partea a treia – la care răspund cei care declară că nu întreprind acțiuni de CI.

Profilul respondenților

Respondenții studiului nostru reprezintă persoane din cadrul managementului unor companii care au fost alese pe baza mai multor criterii. Astfel, în selectarea respondenților, au fost folosite următoarele criterii: cifra de afaceri, numărul de angajați și apartenența companiei (companie românească/companie multinațională). Cifra de afaceri este relevantă, în primul rând, întrucât ea indică totalitatea vânzărilor, a operațiunilor comerciale, în fapt, realizate de o companie într-o anumită perioadă de timp (de regulă un an). Ea evidențiază însăși desfășurarea activității unei firme, stabilind totalul vânzărilor (și totalul veniturilor) efectuate. Mergând mai departe, conform Legii 346, din 14 iulie 2004, privind stimularea înființării și dezvoltării întreprinderilor mici și mijlocii, cifra de afaceri clasifică companiile în (a) întreprinderi

mici și mijlocii (număr de angajați mai mic de 250 și cifra de afaceri netă de până la 50 de milioane de euro) care, la rândul lor, se împart în microîntreprinderi (până la 9 salariați și cifră de afaceri până la 2 milioane de euro), întreprinderi mici (între 10 și 49 de salariați și cifră de afaceri până la 10 milioane de euro) și întreprinderi mijlocii (între 50 și 249 de angajați și cifră de afaceri de până la 50 de milioane de euro). A doua mare categorie este cea a companiilor mari și corporațiilor (peste 250 de angajați și cifră de afaceri de peste 50 de milioane de euro). În funcție de aceste elemente legislative, profilul respondenților este următorul:

TABEL NR. 1

Clasificarea respondenților

Tip companii	Număr respondenți
Corporații	5
Întreprinderi mijlocii	8
Întreprinderi mici	8
Microîntreprinderi	2

O privire de ansamblu asupra respondenților poate să fie consultată în cadrul de mai jos.

TABEL NR. 2

Profilul respondenților

Cod atribuit	Cod CAEN*	Cifră de afaceri	Număr angajați	Companie multinațională	Companie românească
C 1	6419 – Alte activități de intermedieri monetare	6 miliarde lei	5 mii	Da	
C 2	4646 – Comerț cu ridicata - produse farmaceutice	3 miliarde lei	700	Da	
C 3	4120 – Lucrări de construcție a clădirilor rezidențiale și nerezidențiale	20 milioane lei	45		Da
C 4	4120 – Lucrări de construcție a clădirilor rezidențiale și nerezidențiale	20 milioane lei	20		Da
C 5	7311 – Activități ale agențiilor de publicitate	90 milioane lei	40	Da	
C 6	7022 – Activități de consultanță pentru afaceri și management	2,5 milioane lei	10		Da
C 7	7022 – Activități de consultanță pentru afaceri și management	1 milion lei	5		Da
C 8	4520 – Întreținerea și repararea autovehiculelor	50 milioane lei	50		Da
C 9	6201 – Activități de realizare a softului la comandă	200 milioane lei	600	Da	
C 10	6201 – Activități de realizare a softului la comandă	180 milioane lei	600	Da	
C 11	6201 – Activități de realizare a softului la comandă	170 milioane lei	500	Da	
C 12	9200 – Activități de jocuri de noroc și pariuri	90 milioane lei	50		Da
C 13	4711 – Comerț cu amănuntul în magazine nespecializate, cu vânzare predominantă de produse alimentare, băuturi și tutun	130 milioane lei	200		Da
C 14	4764 – Comerț cu amănuntul al echipamentelor sportive în magazine specializate	350 milioane lei	80	Da	
C 15	4791 – Comerț cu amănuntul prin intermediul caselor de comenzi sau prin Internet	25 milioane lei	15		Da
C 16	8559 – Alte forme de învățământ	10 milioane lei	50		Da
C 17	8559 – Alte forme de învățământ	5 milioane lei	10		Da
C 18	0150 – Activități în ferme mixte (cultura vegetală, combinată cu creșterea animalelor)	180 milioane lei	120		Da
C 19	0147 – Creșterea păsărilor	150 milioane lei	600		Da
C 20	0121 – Cultivarea strugurilor	150 milioane lei	100		Da
C 21	6920 – Activități de contabilitate și audit financiar, consultanță în domeniul fiscal	10 milioane lei	10		Da
C 22	6492 – Alte activități de creditare	33 milioane lei	100		Da
C23	2351 – Fabricarea cimentului	2 miliarde lei	1000	Da	

Metoda de analiză a datelor

Studiul nostru folosește, ca metodă de analiză a datelor, analiza tematică inductivă, care se concentrează pe înțelegerea și interpretarea practicilor și experiențelor, mai degrabă decât pe măsurarea variabilelor, folosind procese matematice. Pornind de la conceptele teoretice studiate, am considerat că analiza tematică inductivă se armonizează cel mai bine cu studiul percepției și înțelegerii avute de către companiile din România asupra domeniului competitive intelligence. Mai mult decât atât, aceasta permite o abordare intrinsecă în aflarea motivației din spatele deciziei și a felului în care companiile aleg să întreprindă acțiuni de CI. Astfel, în urma interviurilor conduse, s-au identificat teme mari recurente, pe care le vom discuta în secțiunea următoare.

Analiza

În lucrarea de față, se va face o abordare epistemologică a domeniului competitive intelligence în România. Din studiile efectuate, rezultă că acesta este insuficient cercetat la noi în țară, mai mult chiar, este insuficient cunoscut și înțeles de mediul privat.

Competitivitatea nu este exclusiv o preocupare a mediului privat, ci ea însumează interese ale mediului politic național și european. Aceste structuri înțeleg să acorde atenție sporită și implicare în această direcție, considerând competitivitatea un principiu sine qua non al dezvoltării economice durabile. Conform Comisiei Europene, competitivitatea este deosebit de importantă „întrucât în aceasta se reflectă creșterea susținută a standardului de viață al unei națiuni" (Comisia Europeană 2023). Mișu Negrițoiu, președintele Autorității de Supraveghere Financiară (ASF), afirma în cadrul unei conferințe a BNR: „competitivitatea se creează, în principal, la nivel microeconomic; prosperitatea sustenabilă este creată de către firme într-un mediu macroeconomic propice, iar factorii care determină nivelul productivității sunt: investițiile, capacitatea de a inova și concurența." Aceste trei aspecte menționate sunt deosebit de importante într-o economie de piață dezvoltată, iar în lucrarea noastră, îl vom aborda pe cel de-al treilea prin prisma competitive intelligence.

Nivelul de înțelegere a domeniului competitive intelligence

Literatura de specialitate oferă o serie de definiții și abordări complexe ale CI, însă lucrarea de față cercetează modul în care respondenții, companiile intervievate percep acest domeniu.

Din totalul de 23 de persoane intervievate, 8 (C3, C4, C8, C12,C13,C15,C16,C22), (34,8%), afirmă că nu au auzit niciodată, nu cunosc conceptul de CI, rezultând un procent de 65,2% al celor care au întâlnit pe parcursul activității lor acest concept. În timpul discuțiilor, cei care afirmă că nu sunt în temă încearcă să se lămurească, să obțină mai multe detalii sau chiar doresc, sub forma unor întrebări, lămurirea conceptului: „se referă la spionaj?" sau „este un domeniu nou adus de ceva firme de afară?". De cealaltă parte, se află categoria respondenților care declară că au întâlnit pe parcursul activității lor conceptul. Cei care sunt capabili să îl definească surprind

următoarele aspecte, de altfel, corecte: analiza informațiilor legate de competitori, colectarea și analiza de date existente pe piață, protejarea propriilor date sensibile, îmbunătățirea performanțelor: „Competitive Intelligence (CI) reprezintă procesul de colectare și utilizare a informațiilor relevante despre concurență – clienți, furnizori. Ne ajută să înțelegem mai bine mediul de business" (C2).

În categoria numărul trei, se află acei respondenți care declară că sunt familiarizați cu conceptul de CI, dar atunci când sunt rugați să-l definească, definiția formulată este incorectă. Un element frecvent întâlnit este acela că, în continuare, competitive intelligence este confundat cu spionajul și cu activitatea serviciilor de informații: „are legătură cu serviciile de informații și cu companiile care se spionează reciproc."(C20) Acest lucru se datorează suspiciunii din jurul domeniului de intelligence din România. Comunicarea instituțiilor de intelligence cu publicul nu a reușit să clarifice diferența dintre spionaj (de exemplu, industrial) și intelligence competitiv, care rămâne un domeniu puțin abordat.

Am încercat să descoperim dacă respondenții au cunoștințe despre companii din România sau din străinătate care utilizează CI și care sunt acestea. 12 respondenți au afirmat că au cunoștință de astfel de companii, dar nu au certitudini, motiv pentru care nu ni s-a oferit numele niciunei companii de acest tip. La fel, încercând să aflăm dacă respondenții au cunoștință de companii, din domeniul lor de activitate, care să utilizeze CI, am primit 7 răspunsuri afirmative. Întrebați în continuare dacă ar putea să ne spună care sunt acestea, au ales să răspundă evaziv. Interesant este faptul că tot această categorie de respondenți au cunoștință de cursuri de formare profesională în acest domeniu și de companii care oferă consultanță în CI. Am remarcat faptul că toate companiile de consultanță menționate sunt din afara României, niciuna nu este autohtonă. Respondenții au menționat lipsa companiilor românești în acest domeniu, fapt explicat de aceștia prin insuficienta dezvoltare a respectivului domeniu la noi în țară. Adițional, unii dintre ei au pomenit chiar că nu există o cultură în acest sens.

Percepția față de importanța informațiilor

Deloc surprinzător, dictonul „informația este putere" pare să fie interiorizat de toți respondenții interviului nostru. Întrebați care este importanța pe care o acordă informațiilor, respondenții, în proporție unanimă, au răspuns că se consideră a fi la curent cu dinamica pieței și a mediului concurențial în care își desfășoară activitatea – „în domeniul nostru de activitate cine nu este la curent cu ultimele informații, cu ultimele tehnologii apărute nu rezistă pe piață" (C4). Valoarea pe care o dau informațiilor pe care le dețin este subliniată și de faptul că toți cei chestionați menționează importanța pe care o dau protecției de date/informații. Indiferent de domeniul de activitate, toți sunt preocupați ca date despre companiile lor, rețete, patente să nu fie făcute publice („avem rețete de producție, valoroase pe care le protejăm, care sunt secrete" (C7)). Și la această categorie se păstrează confuzia dintre informațiile obținute din surse deschise, într-un mod legal și spionaj. Un respondent chiar ne spune -„nu ne ocupăm cu așa ceva (CI) pentru că spionajul este ilegal și

nu vrem să avem probleme". Cu alte cuvinte, așa cum pomeneam și mai sus, mulți dintre cei intervievați asociază acest termen absolut legal conotațiilor spionajului, făcând confuzii între cele două concepte sau neputând sesiza diferențe notabile între acestea.

Companii care întreprind acțiuni de competitive intelligence

Una dintre temele majore abordate, în funcție de care am scindat respondenții și am structurat interviurile, este cea care produce două categorii mari de abordări: companii care întreprind și companii care nu întreprind activități de CI.

În prima categorie, regăsim 7 companii, din totalul de 23 intervievate (30,4%): C1, C2, C5, C9, C10, C11, C23. În tabelul de mai jos, putem observa profilul respondenților companii care derulează activități de CI.

TABEL NR. 3

Profilul companiilor care deruleaza activități de CI

Companie	Cifra de afaceri (medie)	Număr angajați (mediu)	Tip companie
C1	6 miliarde de lei	5.000	Companie mare/corporație
C2	3 miliarde de lei	700	Companie mare/ corporație
C5	90 de milioane de lei	40	Întreprindere mijlocie
C9	200 de milioane de lei	600	Întreprindere mijlocie
C10	180 de milioane de lei	600	Companie mare/corporație
C11	170 de milioane de lei	500	Companie mare/corporație
C23	2 miliarde lei	1.000	Companie mare/corporație

După cum putem observa, profilul companiilor care întreprind acțiuni de CI sunt companii mari, cu cifră de afaceri de peste 18 milioane de euro, majoritatea corporații (adică cifra de afaceri mai mare de 50 de milioane de euro și peste 250 de angajați). De fapt, din totalul celor 7 companii, 5 sunt companii mari/corporații și doar 2 sunt companii mijlocii (cu cifră de afaceri mai mare de 10 milioane de euro, având peste 50 de angajați). Cei mai mulți dintre ei au demarat activități specifice domeniului studiat din momentul în care și-au început activitatea în România. Desigur, unul dintre motivele pentru care se întâmplă acest lucru este faptul că toate aceste companii au o structură organizațională veche, testată, care nu își are începuturile în România.

Câteva dintre companiile (2) care au introdus, ulterior, în activitatea lor și componenta de CI consideră că se observă diferențe notabile în ceea ce presupune îmbunătățirea activității societății. Acest lucru este întărit de aspecte care țin de (1) importanța anticipării surprizelor – „suntem mult mai conștienți de motivațiile deciziilor concurenței, acestea nu mai reprezintă surprize" –, de (2) nevoia de a inova – „am lansat pe piața din România produse noi, inexistente până atunci, studiind companiile străine" – sau de (3) desfășurarea unor activități pragmatice, profitabile – „pentru că înțelegem mai bine piața, negociem mai bine cu furnizorii, obținând avantaje".

Am fost interesați să aflăm dacă aceste companii au departamente/structuri de CI în interiorul companiilor sau externalizează aceste activități. Cinci (71,4%) dintre acestea au externalizat domeniul CI, în sensul în care de acest domeniu se ocupă companii specializate. Numele niciuneia dintre aceste companii nu mi-a fost

divulgat, 4 dintre respondenți menționând doar că nu sunt companii românești. Unul dintre respondenți a afirmat că a creat, în cadrul companiei, propriul departament responsabil cu CI, iar un alt respondent a precizat că, deși în momentul de față au proprii angajați care fac CI, la începutul activității au colaborat cu o firmă specializată, din afara țării (motivația fiind de ordin financiar).

Referitor la gradul de conștientizare, în cadrul companiei, de către angajați a demersurilor de CI exercitate, toți cei intervievați afirmă că majoritatea angajaților nu cunosc faptul că societatea în care ei lucrează desfășoară activități de CI. Sunt la curent doar persoanele direct interesate, factorii decizionali, top și macromanagementul. Referitor la motivul din spatele acestei decizii, răspunsurile sunt diverse, dar au o temă comună: „nu e nevoie să știe, nu vrem să se afle deschis, în piață, că facem asta". Pe de-o parte, societățile vor să își protejeze datele, pe de altă parte, există teama unor confuzii care ar putea apărea în rândul angajaților, majoritatea nefiind la curent cu domeniul de informații în afaceri. („datele pe care le obținem prin CI sunt foarte valoroase, dacă s-ar afla asta, e posibil ca procesul de obținere să fie îngreunat, iar în acest sens, numărul mare de angajați reprezintă o vulnerabilitate" – C1).

Referitor la utilitatea informațiilor obținute cu ajutorul CI, toți cei cu care am discutat concluzionează că datele/rapoartele obținute sunt deosebit de importante. În schimb, modalitățile de lucru par a fi diferite, pentru fiecare companie în parte. Astfel, am regăsit următoarele situații: se solicită rapoarte ori de câte ori este necesar (achiziții, fuziuni etc.) – C5, se primesc rapoarte anuale, conținând analize și previziuni pentru anul/anii următori – C2 sau departamentul de CI convoacă ședințe de lucru ori de câte ori consideră că este necesar – C10. Aceste rapoarte, analize par a fi utile în multe situații, enumerate de respondenți: profitabilitate, creșterea vânzărilor, credibilitatea companiei, cash-flow, relația cu furnizorii, rata de recuperare a investițiilor, imaginea companiei, relația cu clienții, valoarea de piață, resursa umană, cota de piață, cifra de afaceri, adaptarea/descoperirea de noi tehnologii.

Discuțiile purtate au condus și în direcția analizei viitorului domeniu CI în România, așa cum este văzut de societățile care se ocupă și sunt preocupate de acest aspect. Observăm că un procent de 71,4 dintre respondenți consideră că domeniul CI se va dezvolta în România. Ei pun pe seama acestui lucru dezvoltările tehnologice și gradul din ce în ce mai mare de deschidere a pieței românești. Tehnologii ca și IA (Inteligența Artificială) ar aduce noi beneficii în domeniul informației în afaceri, dar ar putea reprezenta și pericole pentru companiile care nu înțeleg, care nu sunt la curent cu aceste tehnologii sau care sunt incapabile de adaptare. De asemenea, dezvoltarea domeniului consultanței în afaceri în România ar putea aduce după sine și evoluții în ceea ce privește activitățile de CI.

Doi respondenți afirmă că nu preconizează o dezvoltare a domeniului CI în România. Ei pun acest lucru, pe de-o parte, pe seama resurselor bănești necesare unei companii să întreprindă acțiuni de CI, resurse mai greu de obținut de companiile mici. Pe de

altă parte, consideră că societatea românească, încă postcomunistă, este reticentă în a accepta ușor termeni ca intelligence, informații, contrainformații, având tendința de a le asocia cu spionajul și cu acțiunile ilegale.
Educația cu privire la cultura de securitate ar fi, în acest sens, necesară, cu atât mai mult cu cât acest domeniu nu este reglementat legislativ în România.

Companii care nu întreprind acțiuni de competitive intelligence
Majoritatea reprezentanților de companii cu care am avut dialog declară că nu întreprind acțiuni de CI. Profilul respondenților care au declarat acest lucru poate fi analizat în Tabelul 4.

TABEL NR. 4

Profilul companiilor care nu desfășoară activități de CI

Cod atribuit	Cifra de afaceri (medie)	Număr angajați (mediu)	Tip companie
C 3	20 de milioane de lei	45	Întreprindere mică
C 4	20 de milioane de lei	20	Întreprindere mică
C 6	2,5 milioane de lei	10	Microîntreprindere
C 7	1 milion de lei	5	Microîntreprindere
C 8	50 de milioane de lei	50	Întreprindere mică
C 12	90 de milioane de lei	50	Întreprindere mijlocie
C 13	130 de milioane de lei	200	Întreprindere mijlocie
C 14	350 de milioane de lei	80	Întreprindere mijlocie
C 15	25 de milioane de lei	15	Întreprindere mică
C 16	10 milioane de lei	50	Întreprindere mică
C 17	5 milioane de lei	10	Întreprindere mică
C 18	180 de milioane de lei	120	Întreprindere mijlocie
C 19	150 de milioane de lei	600	Întreprindere mijlocie
C 20	150 de milioane de lei	100	Întreprindere mijlocie
C 21	10 milioane de lei	10	Întreprindere mică
C 22	33 de milioane de lei	100	Întreprindere mică

Dintr-un total de 16 reprezentanți ai companiilor care au declarat că nu desfășoară acțiuni de CI, 2 dintre acestea (12,5%) sunt microîntreprinderi, 8 (50%) sunt întreprinderi mici și 6 (37,5%) sunt întreprinderi mijlocii. Cifra lor de afaceri este cuprinsă între 1 milion de euro și 120 de milioane de euro, iar numărul angajaților, între 5 și 600. Observăm că nu există nicio corporație în această categorie, toate cele care au acceptat să fie intervievate declarând că derulează operațiuni de CI.
Discuțiile purtate cu reprezentanții acestor companii au fost diferite față de cele purtate cu reprezentanții companiilor care afirmau că desfășoară activități de CI, încercându-se obținerea unor motivații și raționamente aflate în spatele deciziei.

În primul rând, din totalul respondenților (16) care au declarat că societățile pe care le reprezintă nu desfășoară acțiuni de CI, 37,5 % motivează decizia prin costurile ridicate („suntem o companie mică, nu ne permitem deocamdată investiții în așa ceva" – C6). Cu toate acestea, doar 3 respondenți afirmă că au cunoștință despre companii care oferă cursuri de specialitate și sunt la curent sau au primit ofere de preț; ceilalți 3 susțin că nu au cunoștință despre prețurile practicate de firmele de consultanță sau de formare pe acest domeniu, doar presupun că tarifele practicate ar fi mari („nu m-am interesat niciodată cât costă, pentru că deocamdată bugetul nu ne permite cursuri sau să mai angajăm personal"– C20). Acest aspect este important, întrucât relevă faptul că o decizie importantă, cum este aceasta, se bazează pe supoziții, fără ca ele să fie verificate.

Un alt argument adus în discuție este de natură morală, etică. Acesta se referă, de fapt, la confuzia dintre CI (și domeniul informațiilor în afaceri) și spionaj. Asemuind cei doi termeni, chiar confundându-i, respondenții afirmă că valorile etice, implementate în companiile lor, nu le permit astfel de acțiuni („spionajul este ilegal, astfel de practici ne-ar decredibiliza" – C12) și prin urmare, sunt irelevante pentru ei („compania noastră pune foarte mare accent pe valori morale și etice, și nu ne preocupă demersuri care nu se încadrează în aceste valori" – C18). Mai mult chiar, afirmă că nu ar avea încredere în companiile care desfășoară CI, dar, totodată, susțin că nu cunosc astfel de companii.

O motivație recurentă, regăsită pe parcursul discuțiilor, este cea care se bazează pe necunoașterea domeniului CI. Astfel că nu se demarează operațiuni de CI, pentru că nu se înțelege ce presupun acestea („nu știu cum am putea afla detalii despre concurență, unde am găsi aceste informații" – C15), cine și ce ar trebui să facă în cadrul companiei („departamentul de marketing studiază concurența și află ce promovează" – C4). În acest sens, 31,25 % dintre cei întrebați nu se ocupă cu domeniul informațiilor în afaceri sau cu cel al studierii competiției, pentru că nu cunosc detalii despre cum ar trebui să facă acest lucru.

Pentru mulți dintre respondenți, o explicație pentru lipsa de activități în acest domeniu se referă la lipsa resursei umane. Aceștia susțin că ar fi folositor, pentru firmele lor, ca anumite persoane/angajați să se ocupe cu CI, însă nu știu cum și unde ar putea găsi personal calificat. Ei consideră că acest domeniu nu s-ar preta în a fi externalizat unei terțe companii, ci ar trebui abordat de proprii angajați, cu competențe în domeniu. Se susține ideea conform căreia dacă ar exista o „școală" în acest sector de activitate, care să producă specialiști acreditați, atunci companiilor le-ar fi mai accesibil acest domeniu. De asemenea, respondenții nu văd utile cursurile în domeniu, pe care să le urmeze proprii angajați, ci ar fi nevoie de „meserii" („nu am încredere în cursuri rapide de calificare profesională, mai ales într-un domeniu așa de complex" – C3), întreprinderilor fiindu-le mai ușor să angajeze profesioniști în domeniu decât să-și formeze proprii specialiști. Cu alte cuvinte, acești respondenți nu consideră utilă o investiție în cursuri de formare/reconversie profesională, preferând să angajeze profesioniști pentru fiecare departament/poziție, și văd cursurile de specializare mai degrabă ca pe niște bonusuri care ar putea fi oferite angajaților. Pe de altă parte, nu se opun dacă angajații doresc să urmeze astfel de cursuri și să le plătească ei înșiși.

Limitele cercetării

Cercetarea pe care am desfășurat-o a fost una provocatoare din mai multe puncte de vedere, iar acest lucru are efect asupra rezultatelor cercetării. Bazată pe interpretări din datele obținute, cercetarea se axează pe stabilirea unor percepții, opinii sau motivații, prezente în spatele unor acțiuni, analiza în profunzime a unor decizii. Ea stabilește raportarea agenților din mediul economic la domeniul competitive

intelligence, propriile lor viziuni și percepții asupra fenomenului; însă nu este lipsită de limitări. Scopul a fost mai mult decât să se obțină niște informații, să se înțeleagă motivațiile existente în spatele unor comportamente, unele atitudini și fenomene existente în cadrul mediului de afaceri din România.

Una dintre limitele cercetării este cauzată de eșantionarea neprobabilistică, acest lucru făcând dificilă generalizarea concluziilor studiului la nivelul întregii țări. Pe de altă parte, sarcina găsirii unor companii dispuse să ofere informații a fost dificilă. Reticența manifestată de către acestea poate fi justificată prin faptul că, într-un mediu concurențial, companiile tind să își protejeze datele spre a nu fi făcute publice și cunoscute de concurenți.

Cu ajutorul interviului, se poate intra în profunzimea unei teme complexe, însă subiecții pot fi influențați, involuntar, de către intervievator (deși acesta este unul neutru) sau pot să ofere informații distorsionate. Comportamentul acestora poate fi disimulat, iar intervievatorul să nu observe asta, fapt care poate face ca informația să fie perimată, distorsionată sau incompletă. Pe parcursul derulării interviurilor, am acordat o atenție deosebită acestor aspecte, însă totuși limitarea de față există. O altă limită este reprezentată de noutatea domeniului competitive intelligence în România. Pe de-o parte, acest aspect creează o confuzie în rândul companiilor în ceea ce privește CI, el este puțin cunoscut și înțeles.

Tematica abordată fiind una sensibilă pentru subiecți și pentru companiile pe care le reprezintă, confidențialitatea și protejarea identității acestora sunt deosebit de importante atât din punct de vedere etic, cât și juridic. Asigurarea anonimatului și a confidențialității este un aspect dificil de coordonat.

Concluzii

Studiul pe care l-am făcut relevă faptul că toți respondenții consideră că informațiile sunt importante în mediul de afaceri, deși nu toți sunt preocupați activ și sistematic de obținerea lor. La fel, toți consideră că este importantă studierea concurenței, deși decid să nu facă acest lucru, sau nu într-un mod sistematic și științific. Companiile cu care am discutat știu puține lucruri despre oportunitățile de formare în acest domeniu sau despre companiile care pot să le ofere consultanță.

Un aspect important, recurent pe parcursul desfășurării prezentei cercetări este cel referitor la confuzia dintre CI și spionaj. Pe de-o parte, acest lucru poate fi înțeles, întrucât nu există o cultură a informațiilor în afaceri suficient de dezvoltată în țara noastră, economia capitalistă de aici fiind totuși una destul de nouă. Pe de altă parte, termenul intelligence, specific serviciilor de informații, poate fi mai dificil transpus în mediul privat astfel încât sensul acestuia să se modifice. Evident, CI lucrează cu surse deschise, dar și acest concept poate pune probleme de înțelegere unui neavizat/nespecialist. Asocierea cu spionajul se regăsește și în rândul unora

care susțin că cunosc sau au întâlnit conceptul de CI, fapt care arată că este ușor să fie confundat sau că cei care îl uzitează nu sunt specialiști ori nu s-au informat din surse specializate, credibile. În această lucrare, am explicat în detaliu diferențele dintre aceste două concepte și consider că este utilă promovarea CI, menționându-se tocmai acele aspecte care îl deosebesc și îl separă de spionaj.

Din totalul respondenților, un număr de șapte au afirmat că desfășoară activități de CI (aproximativ 30%), iar profilurile lor sunt de companii mari, multinaționale. Acestea susțin că, de la debutul intrării pe piața din România, desfășoară operațiuni de CI, ceea ce ne conduce înspre concluzia că această practică este una obișnuită și că societățile multinaționale sunt la curent și folosesc acest domeniu. Aceasta creează un dezavantaj pentru companiile românești care, în majoritate, nu întreprind astfel de acțiuni, nu acordă o atât de mare importanță mediului concurențial sau, chiar mai mult, nu sunt conștiente că alte firme fac asta. Astfel, o companie mare, cunoaște în detaliu o piață ori concurența existentă aici, pe când o companie mică nu beneficiază de acest atu.

Cei care întreprind acțiuni de CI sunt pe deplin satisfăcuți și pot preciza avantajele pe care le aduc acestea companiilor. Totuși, această informație preferă să o țină ascunsă, nu doar de ochii publicului, ci și de proprii angajați. În ceea ce privește locul în care se desfășoară activitățile de CI, putem spune că majoritatea respondenților apelează la serviciile companiilor externe. Putem deduce că aceste firme nu sunt românești, datorită faptului că respondenții, atunci când au fost întrebați, nu au putut da exemple de firme de consultanță decât din afara țării. Dintre cei care au propriile departamente de CI, unul a afirmat că acesta este relativ nou construit, întrucât, la început, se colabora cu o firmă de consultanță. Dificultatea în a găsi specialiști în acest domeniu a fost, din nou, un aspect recurent. Se constată o lipsă a personalului calificat în domeniul informațiilor în afaceri în România, de unde preferința de a selecta companii străine în vederea colaborării din state în care există o tradiție mai lungă în acest domeniu.

Microîntreprinderile și companiile mici intervievate declară că nu desfășoară acțiuni de CI, la fel și majoritatea companiilor mijlocii. Cum precizam și mai sus, observăm că aceasta este mai degrabă o preocupare a companiilor mari, extinse și în afara granițelor țării. Percepția companiilor mai mici este aceea că fie CI presupune alocarea unor sume consistente, fie nu se pretează companiilor mici și deci nu ar prezenta o utilitate care să justifice efortul financiar.
Deși se discută despre o alocare semnificativă de fonduri, aceasta este mai degrabă o prezumție, pentru că cei intervievați nu cunosc detalii despre cât ar costa un curs, o expertiză sau colaborarea cu societăți specializate. Fiind un domeniu mai puțin cunoscut, mai degrabă nou, există supoziția că expertiza sau consultanța ar presupune costuri mari. Dar companiile necunoscând aceste costuri, nu se poate aprecia dacă avantajele obținute le-ar surclasa sau care ar fi raportul cost/beneficiu.
Cu toate acestea, reprezentanții companiilor care afirmă că nu desfășoară activități de CI nu exclud această posibilitate. Ei se prezintă fie deschiși spre această modalitate

de lucru, afirmând că ar putea face demersuri în acest sens în viitor, fie sunt încă sceptici cu privire la capacitatea de alocare a fondurilor în această direcție. Nivelul de scepticism este ridicat, în principal pentru că percepția este aceea că necesitățile financiare ar fi crescute.

Referințe

Comisia Europeană. 2023. „Glosar de Politică Regională." https://ec.europa.eu/regional_policy/whats-new/newsroom/27-03-2023-how-competitive-is-your-region-commission-publishes-the-regional-competitiveness-index_ro.

Cook, Michelle și Curtis Cook. 2000. *Competitive Intelligence. Create an intelligence organization and compete to win.* Kogan Page.

Growth Lab. fără an. "The atlas of economic complexity." Accesat 15 noiembrie 2024. https://atlas.hks.harvard.edu/.

Jason, Seawright. 2008. "Case selection techniques in case study research: a menu for qualitative and quantitative options." *Political Science Research Quarterly* 294-305.

Kalika, Michel, Philippe Mouricou și Lionel Garreaun. 2009. *La méthodologie, le mémoire de master.* The free press.

Larry, Kahaner. 1996. *Competitive Intelligence. How to gather, analyze and use information to move your business to the top.* Simon&Schuster Inc.

Porter, Michael. 1980. *Competitive Strategy: Techniques for analyzinf industries and competitiors.* The Free Press.

Valentin, Vlad Ioan. 2017. *Strategia de dezvoltare a României în următorii 20 de ani.* București: Editura Academiei Române.

BULETINUL
UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I"
https://buletinul.unap.ro

Riscuri, amenințări și vulnerabilități legate de platformele social media și motoarele de căutare. Reglementări și cadre juridice naționale

Risks, threats, and vulnerabilities related to social media platforms and search engines. Regulations and national legal frameworks

Dr. Dănuț MAFTEI*
Masterand Lorin Nicolae BOGDAN-DUICĂ**
*Directoratul Național de Securitate Cibernetică, București, România
e-mail: dn.maftei@gmail.com
**Directoratul Național de Securitate Cibernetică, București, România
e-mail: bogdanduicalorin@yahoo.com

Abstract

Platformele de socializare online și motoarele de căutare sunt utilizate din ce în ce mai mult de persoane violente, infractori, infractori cibernetici și alți actori răuvoitori statali sau nonstatali, implicați în activități specifice amenințărilor hibride și interferenței străine, generând provocări pentru copii, fete, femei, cetățeni, societăți, economii, servicii critice, democrație și securitatea națională. Neglijarea proliferării online a activităților ilegale nu numai că erodează încrederea în aceste platforme, ci și pune în pericol securitatea și viața privată a utilizatorilor. Pentru a contracara eficient toate provocările, sunt necesare urgent noi măsuri legale. Reglementările ar trebui aplicate platformelor social media, motoarelor de căutare și serviciilor care permit utilizatorilor să posteze conținut online sau să interacționeze între ei.

Online social media platforms and search engines are used more and more by violent people, criminal offenders, cybercriminals, and other state or non-state malicious actors, who are involved in activities connected to hybrid threats and foreign interference, causing challenges for children, girls, women, citizens, societies, economies, critical services, democracy, and homeland security. Neglecting the proliferation of illegal activities not only erodes trust in online platforms but also places at risk the security and privacy of its users. To counter efficiently all the challenges, urgent new regulatory frameworks are needed. The regulations should be applied to social media platforms, search engines, and services that allow users to post content online or to interact with each other.

Cuvinte-cheie:
platforme social media; securitate națională; democrație; actori rău intenționați; interferențe străine; informații false; violență; fraude.

Keywords:
social media platforms; national security; democracy; malicious actors; foreign interference; false information; violence; frauds.

Info articol
Primit: 14 noiembrie 2024; Evaluat: 2 decembrie 2024; Acceptat: 6 decembrie 2024; Disponibil online: 17 ianuarie 2025
Citare: Maftei, D. și L.N. Bogdan-Duică. 2024. „Riscuri, amenințări și vulnerabilități legate de platformele social media și motoarele de căutare. Reglementări și cadre juridice naționale". *Buletinul Universității Naționale de Apărare „Carol I"*, 13(4): 197-214. https://doi.org/10.53477/2065-8281-24-48

Apariția social media a marcat o nouă eră, facilitând evoluția umanității. În prezent, există diverse platforme de social media (PSM), motoare de căutare și servicii care permit utilizatorilor să interacționeze rapid între ei sau să posteze conținut online. Acestea includ o varietate de pagini web, de aplicații și de alte servicii, inclusiv de social media, platforme de partajare video, site-uri de stocare și partajare în cloud a fișierelor de consum, forumuri online, servicii de mesagerie instantanee online și de întâlniri. Ele pot fi utilizate pentru a viziona videoclipuri, pentru a dobândi noi cunoștințe, pentru a împărtăși momente speciale ori pentru a relua legătura cu prietenii.

Pe de altă parte, aceste servicii populare online și platforme social media au și o latură negativă, deoarece pot fi un focar pentru înșelăciuni, fraude, violențe, propagandă și vehicularea de informații false. Platformele online și noile tehnologii au facilitat, au ieftinit și au accelerat mai mult ca oricând punerea în practică a activităților malițioase de către diverși actori statali și nonstatali, naționali și străini. În plus, anonimatul, lipsa controlului și a mecanismelor eficiente de verificare facilitează răspândirea conținutului dăunător și identificarea atacatorilor. În paralel, frecvența și complexitatea tacticilor, tehnicilor și procedurilor (TTP), utilizate de actorii rău intenționați pentru a exploata vulnerabilitățile platformelor și pe cele ale utilizatorilor, cresc neîncetat.

Platformele social media permit diseminarea rapidă și pe scară largă a informațiilor false și a altor forme de interferență străină care amenință principiile și valorile democratice. Se poate observa că acestea sunt utilizate inclusiv pentru a planifica și a afișa acte violente sau pentru a răspândi știri false și mesaje dăunătoare. Activitățile desfășurate prin folosirea PSM pot afecta democrația, pot polariza opiniile, pot incita la violență, pot submina încrederea în instituții, pot alimenta discriminarea și marginalizarea și pot eroda coeziunea socială, impactul asupra societății fiind profund și complex. De exemplu, în cazul persoanelor care nu folosesc social media în scopuri violente, acestea vor fi implicate și ele în violențe diverse, din cauza algoritmilor care sunt setați să promoveze acest tip de conținut și să încurajeze acte care conduc la violență în viața reală.

Fraudele realizate prin anunțurile false, postate pe rețelele sociale, au crescut, de asemenea, în mod dramatic. Chiar și anunțurile legale sunt clonate și utilizate în scopuri malițioase, iar utilizatorilor finali le este dificil să afle dacă anunțul este legal fără a-l accesa (Alexander 2024).
Numărul preluărilor de conturi de social media este în creștere, iar conținutul nu este neapărat verificat, motiv pentru care nimeni nu poate fi sigur că interacționează cu cineva cunoscut. Utilizatorii ar trebui să abordeze toate interacțiunile din social media cu o doză adecvată de scepticism, indiferent dacă este vorba despre un tweet, o postare sau un mesaj direct, fiind dificil să recunoască dacă o aplicație poate fi sau nu de încredere. De exemplu, întrucât **escrocheriile online** (Stathis 2024a) și **fraudele din Facebook Marketplace** sunt atât de răspândite (Alexander 2024), ar fi indicat ca utilizatorii să învețe cum să identifice un escroc (Stathis 2024b).

Actorii rău intenționați, în special cei statali, folosesc platformele social media ca mijloace de desfășurare a operațiunilor de război hibrid. Cercetătorii au remarcat în special evoluția doctrinei rusești privind războiul informațional, împreună cu „rădăcinile sale adânci în practica sovietică de lungă durată” (Giles 2016; Snegovaya 2015). Gândirea militară rusă recentă pune accent pe războiul hibrid, pe care îl consideră ca fiind o nouă realitate persistentă, cu „sfera informațională” și „războiul informațional” ca un spațiu de luptă critic.

Așa-numiții „trolli” și „roboți” par să joace un rol-cheie în răspândirea știrilor false și a dezinformării prin intermediul platformelor social media. Trollii profesioniști gestionează conturi pe rețelele sociale pentru a provoca sau pentru a răspândi dezinformări și știri false. Pe de altă parte, roboții sunt implicați în gestionarea unor conturi automate care combină conținutul generat de oameni cu postările computerizate. Pentru a-și atinge obiectivele, sunt create și utilizate rețele mari de conturi false, acestea jucând un rol central în promovarea știrilor false.

Metodele utilizate de companiile de social media pentru identificarea conturilor automate și a campaniilor coordonate de știri false, conduse de actori statali, sunt diferite, iar rezultatele sunt, de asemenea, diverse. Deși platformele au implementat unele măsuri de moderare a conținutului, acestea sunt, adesea, insuficiente și întârzie să răspundă cererilor de eliminare a conținutului dăunător. Situația prezentată este cauzată parțial atât de volumul mare de conținut, generat de utilizatori, cât și de lipsa de stimulente suficiente pentru a acționa rapid și eficient. De exemplu, în pofida resurselor imense și a abilităților tehnologice, *Meta for Business* a fost criticată pentru răspunsul său inadecvat la proliferarea paginilor de phishing pe Facebook. Algoritmii companiei și mecanismele de moderare a conținutului sunt, adesea, considerate deficitare în identificarea și eliminarea acestor pagini înșelătoare în timp util, răspunzând în mod repetat, la solicitarea utilizatorilor, cu mesaje stereotipe, precum *„conținutul nu contravine standardelor comunitare”* sau *„conținutul este sigur”*. Această situație expune milioane de utilizatori riscurilor asociate cu escrocheriile de tip phishing și ridică întrebări serioase cu privire la angajamentul Meta față de siguranța utilizatorilor (Qureshi 2023).

Efecte negative ale mesajelor malițioase, postate pe platformele de socializare

Cercetarea științifică a evidențiat că mesajele malițioase de diverse tipuri, postate pe platformele de socializare, au, în general, un impact negativ atât asupra utilizatorilor individuali, cât și asupra securității naționale, democrației și stabilității societale.
Actorii străini intenționează să creeze condițiile necesare pentru manipulare sau pentru alt gen de interferență prin erodarea încrederii publice, prin destabilizarea sistemelor politice, prin subminarea normelor democratice și slăbirea rezilienței statelor democratice. Pe termen lung, acest lucru poate deteriora capacitatea democrațiilor de a rezista amenințărilor externe sau de a menține o guvernanță eficientă.

Unul dintre cele mai dăunătoare efecte ale *Manipulării și Interferenței Informațiilor Străine* (FIMI)[1] este erodarea încrederii publice în instituțiile democratice. Dezinformarea, știrile false și discursul instigator la ură, care vizează inclusiv minoritățile etnice, religioase și sexuale, amplifică diviziunile sociale, conduc la creșterea discriminării și a violenței împotriva minorităților, alimentând polarizarea politică și culturală.
În paralel, este erodată încrederea în instituții și în mass-media tradițională, acest fapt conducând la creșterea scepticismului și la apariția unor dificultăți în a distinge între informațiile reale și cele false.

[1] Foreign Information Manipulation and Interference.

Prin exacerbarea diviziunilor existente în societate, campaniile FIMI amplifică polarizarea discursului politic, făcând mai dificil, pentru societățile democratice, angajarea lor în dezbateri constructive sau identificarea într-un numitor comun cu privire la problemele critice cu care se confruntă. Această polarizare slăbește capacitatea instituțiilor democratice de a funcționa eficient, procesul legislativ fiind transformat în blocaj partizan și în extremism politic.

Platformele social media, dezinformarea, discursul instigator la ură, știrile false și atacurile cibernetice, utilizate pentru a manipula opinia alegătorilor, dar și pentru a crește tensiunile sociale și nivelul actelor violente înainte, în timpul și după alegerile electorale pot influența rezultatul acestora. Astfel de activități pot avea consecințe profunde, deoarece pot conduce la alegerea unor candidați care sunt mai favorabili intereselor străine sau, dimpotrivă, pot afecta perspectivele candidaților considerați ostili acestor interese.
Femeile și adolescentele cad pradă diferitelor forme de violență sexuală online (hărțuire cibernetică, videoclipuri care prezintă violuri, amenințări și distribuirea de imagini sexuale fără consimțământ). Aceste forme de violență pot deveni reale și pot interfera cu capacitatea femeilor de a se simți în siguranță la locul de muncă sau în public.

Pe de altă parte, popularitatea și ușurința de a utiliza PSM au facilitat accesul extremiștilor la alte persoane cu viziuni similare, crearea de rețele teroriste, recrutarea de noi membri, răspândirea ideologiilor extremiste și incitarea la violență. Algoritmii PSM pot amplifica conținutul extremist, expunându-i pe utilizatori la mesaje periculoase care contribuie la radicalizarea lor.
Interferența străină prin dezinformare care vizează sănătatea (de exemplu, referitor la vaccinuri, pandemii etc.) are un impact negativ asupra sănătății publice, crescând riscul de îmbolnăvire și de deces prematur.
Totodată, dezinformarea și știrile false pot afecta negativ economiile naționale și internaționale prin manipularea piețelor financiare, prin generarea de prejudicii financiare, prin subminarea încrederii întreprinderilor și răspândirea panicii. Provocări deosebite sunt generate și de traficul de persoane în scopuri de muncă sau sexuale, victimele traficului fiind cel mai adesea copiii și chiar adolescenții și tinerii.

Tactici, tehnici și proceduri utilizate online de actorii rău intenționați pentru a desfășura activități frauduloase

Zi de zi pot fi observate TTP atât vechi, cât și noi, utilizate de escroci pentru a înșela oamenii. Cu tot mai multe fraude online realizate zilnic, fiecare nouă fraudă este și mai complexă, mai inteligentă și mai puțin detectabilă decât ultima (Stathis 2024a). În prezent, utilizatorii PSM sunt victimele mai multor tipuri de amenințări, acestea fiind prezentate succint în continuare.

Atacurile de tip phishing (Adrien 2023) sunt atacuri efectuate online. Scopul lor este de a fura date personale sau de a obține controlul asupra conturilor de social media. Phishingul este o formă de criminalitate informatică în care actorii rău intenționați pretind a fi entități demne de încredere, adesea pentru a atrage utilizatorii prin promoții false, concursuri frauduloase sau știri inventate, ori pentru a-i determina să acceseze linkuri rău intenționate sau să dezvăluie informații sensibile, cum ar fi date personale, credențiale de conectare, informații despre carduri de credit, date financiare etc. Activitățile de phishing reprezintă la momentul actual una dintre cele mai frecvente forme de inginerie socială, cu peste 3 miliarde de e-mailuri spam, trimise zilnic.

Potrivit statisticilor, milioane de conturi de afaceri Facebook din întreaga lume sunt vizate de mesaje de phishing, cu o rată de succes de aproape una din 70 de victime infectate (Petkauskas 2023). Escrocii impersonalizează diverse PSM în atacurile de phishing, acestea fiind menite să instaleze pe ascuns programe software malițioase (spyware sau ransomware) pe calculatoarele personale, să fure credențiale și, eventual, date personale (Rosenkrantz 2024).

Deși phishingul rămâne popular, în prezent putem observa noi tehnici, precum *spear-phishing, whaling, compromiterea e-mailurilor de afaceri, smishing, https phishing, phishing cu clone, pop-up phishing, angler phishing, evil twin phishing, search engine phishing, watering hole phishing, vishing* etc. (Chin 2024). În plus, infractorii cibernetici folosesc instrumente generative de inteligență artificială pentru a-și redacta mesajele electronice, ceea ce le îmbunătățește rata de succes în phishing.

Hackerii folosesc o rețea masivă de conturi false și compromise pentru a transmite milioane de mesaje de phishing în platforma Messenger, acestea vizând conturile de afaceri Facebook cu programe malware care fură parole (Toulas 2023b). Potrivit rapoartelor, specialiștii avertizează că aproximativ unul din șaptezeci de conturi vizate este, în cele din urmă, compromis, ceea ce se traduce prin pierderi financiare masive (Zaytsev 2023).

Aplicațiile frauduloase pot fi reprezentate de reclame pentru aplicații sau funcții pe PSM, care pretind că permit utilizatorilor să verifice cine le-a vizualizat profilul (Budgar 2024).

În cazul fraudelor de pe **Facebook Marketplace** (Alexander 2024), se poate observa că un număr foarte mare de utilizatori cumpără și vând bunuri în fiecare zi, dar și

că escrocii folosesc această platformă de cumpărături online pentru a înșela oamenii și a le fura banii. Escrocii le pot solicita utilizatorilor să plătească sau să discute detalii suplimentare, dar prin utilizarea unor terțe canale de comunicare, în timp ce alții ar putea lista închirieri false, cadouri sau diverse produse.

În cadrul **fraudelor bancare**, mulți escroci oferă cadouri false pentru a-i determina pe utilizatori să divulge diverse informații personale (card de credit, numere de asigurări sociale etc.) sau să acceseze linkuri prin care ar putea descărca viruși pe calculatorul personal (Bradford 2024).

În cazul **atacurilor de tip spoofing**, hackerii pot accesa ilegal contul unei persoane și pot trimite mesaje sau postări false prietenilor acesteia, solicitându-le bani sau cadouri (Alexander 2023). Mesajele au rolul de a-l emoționa ori panica pe utilizator și apoi de a-l determina să ofere bani, fără a analiza bine situația. În plus față de utilizarea profilului unui prieten pentru a efectua un atac de tip spoofing, escrocii ar putea să impersonalizeze persoane sau organizații cunoscute.

Sextortion este o înșelătorie de inginerie socială, în care o victimă (de obicei, de sex masculin) se împrietenește cu o escroacă de sex feminin. Victima este convinsă să furnizeze imagini sau clipuri video cu caracter sexual explicit persoanei false, care amenință apoi că va publica în direct materialul compromițător, dacă nu i se transferă o anumită sumă de bani (Schappert 2024).

Atacatorii pot folosi și **scheme de tip "Secret Santa"**, prin care oamenii trebuie să trimită unei persoane un cadou de 10 $, urmând să primească și ele unul de la alte trei persoane. Nu există însă nicio garanție că victima va primi banii înapoi în aceste fraude, realizate pe Facebook, deoarece, dacă nimeni nu dă curs trimiterii cadoului, ar putea să nu primească nimic în schimb. Actorii malițioși ar putea folosi adresa de domiciliu a victimei pentru a efectua atacuri de tip *doxxing*[2] (Alexander 2022), iar partajarea altor informații personale ar putea dezvălui răspunsurile la întrebările de securitate ale parolelor, conturile personale fiind astfel vulnerabile în fața hackerilor.

Informațiile eronate (*"misinformation"*[3]) sunt informații false, înșelătoare sau extrase din context, diseminate de o persoană *care crede că sunt adevărate*, fără intenția de a provoca prejudicii. *Misinformation* are puterea „dovezii sociale" în a convinge persoanele să dea credibilitate acestor informații false. Oamenii vor accepta mai rapid știrile ca fiind adevărate atunci când sunt difuzate de prieteni, cunoștințe și de surse presupus credibile, dar și dacă aceste știri sunt mai populare (Hindman 2018).

[2] Doxxing sau doxing reprezintă furnizarea în mod public de informații personale identificabile despre persoane sau organizații, de obicei online și fără consimțământul acestora, ca formă de pedeapsă sau răzbunare.
[3] Denumire preluată din limba engleză.

Dezinformarea se referă la informații false (sau narațiuni ori fapte manipulate, propagandă) despre care *propagatorul știe că sunt false*. Este o minciună deliberată, intenționată, menită să manipuleze, să provoace daune și să îndrume oamenii, organizațiile și statele într-o direcție greșită, să genereze neîncredere în instituțiile statului democratic pentru a provoca prejudicii ori pentru a obține câștiguri politice, personale sau financiare (PakVoices 2023).

Dezinformarea implică mai multe părți interesate, este coordonată și dificil de urmărit. Acțiunile specifice dezinformării pot include videoclipuri modificate, articole de știri false sau postări amplificate artificial pe rețelele de socializare. Acestea conțin, adesea, calomnii sau discursuri instigatoare la ură împotriva anumitor grupuri de persoane și sunt adesea polarizante, incitând la furie și alte emoții puternice, putând determina oamenii să promoveze idei extremiste, teorii ale conspirației, fără loc de compromisuri.
Noile tehnologii emergente sunt utilizate din ce în ce mai mult pentru a discredita informațiile factuale. Inteligența artificială (IA) și IA generativă pot fi utilizate pentru a răspândi informații false și înșelătoare, cum ar fi ”*deepfake*”.

”Mal-information”[4] se referă la *informații bazate pe realitate*, folosite pentru a afecta persoane, grupuri sociale, organizații sau națiuni (ITU 2021). *Mal-information* implică fapte, deci nu falsuri. Datele personale și scurgerile de e-mailuri, dezvăluite prin *doxxing*, sunt exemple de mal-information. Hărțuirea, discursul instigator la ură și pornografia din răzbunare fac parte, de asemenea, din această categorie.

[4] Denumire preluată din limba engleză.

Știrile false sunt *informații intenționat elaborate*, senzaționale, încărcate emoțional, înșelătoare sau total fabricate, care imită tiparul știrilor importante (Saint Francis University 2023). Acestea sunt legate de distribuirea online de informații false, deghizate în știri legitime. Motivațiile din spatele știrilor false pot fi personale (pentru a afecta reputația unei persoane sau a unei organizații), financiare (pentru a mări traficul pe internet și/sau veniturile din publicitate) ori politice (pentru a influența punctul de vedere/ideologia publicului).

***

Desigur, există o mulțime de alte variante ale provocărilor cu care se pot confrunta oamenii pe PSM, precum ar fi *atacuri malware, mesaje spam, conturi clonate, colectări de fonduri medicale false, escrocherii de tip „clickbait”, fraude cu coduri de cupon false, cu chestionare Facebook, escrocherii romantice, cu locuri de muncă, strângeri de fonduri false, hărțuire cibernetică, ”internet banging”, abuz sexual asupra copiilor, control sau comportament coercitiv, violență sexuală extremă, pornografie extremă, vânzare de droguri sau de arme ilegale, exploatare sexuală, fraudă, infracțiuni de ordine publică, agravate din motive rasiale sau*

religioase, imigrație ilegală și trafic de persoane, promovarea sau facilitarea sinuciderii, abuz de imagini intime (pornografie din răzbunare), terorism etc.

Se impune ca factorii de decizie să înțeleagă cu claritate că toate aceste tipuri de TTP prezintă enorm de multe variante de acțiune care pot fi folosite cu succes de către diverși actori malițioși pentru desfășurarea complexă de atacuri online cu rezultate grave. În urma unor scanări detaliate a victimelor pentru identificarea vulnerabilităților lor specifice, atacurile vor fi, ulterior, organizate, adaptate și personalizate în funcție de specificul fiecărei ținte, combinat cu alte metode și tehnologii de vârf, astfel încât șansele de succes să fie maxime. Ca atare, în condițiile menționate, statele au nevoie să se adapteze rapid prin modificarea cadrului legal și să dezvolte strategii de lucru eficiente pentru contracararea unor astfel de provocări complexe.

Măsuri specifice, adoptate de autoritățile naționale, pentru combaterea activităților ilegale, desfășurate prin utilizarea platformelor social media

UE și diferite state de pe mapamond acordă, de ani de zile, atenție activităților rău intenționate desfășurate online și impactului pe care acestea îl au asupra securității naționale, democrației, instituțiilor statului, infrastructurii critice, societății, întreprinderilor și cetățenilor. Cercetarea științifică actuală a evidențiat și unele măsuri, luate de autoritățile naționale, împotriva provocărilor reprezentate de actorii rău intenționați prin utilizarea PSM, prezentate în continuare.

Platforma TikTok:

Începând cu anul 2020, **Platforma TikTok** a fost blocată/restricționată în state precum Afganistan, Armenia, Azerbaidjan, Bangladesh, India, Iran, SUA, motivele care au stat la baza acestor decizii fiind legate de securitatea națională, de nivelul ridicat al terorismului, de conflictele de la graniță etc. (Gordon 2024). În baza Regulamentului privind Serviciile Digitale[5], Comisia Europeană a inițiat proceduri împotriva TikTok privind lansarea *TikTok Lite* în Franța și în Spania (Comisia Europeană 2024).

În 2023, TikTok a fost interzisă pe dispozitivele deținute de instituțiile de stat în Austria, Belgia, Canada, Estonia, Franța, SUA, din cauza riscului pentru securitate și confidențialitate, precum și din cauza presupuselor legături existente între Partidul Comunist Chinez și companie, TikTok fiind acuzată de colectarea și partajarea de date personale cu serviciile de informații chineze (Lakshmanan 2024).

În mai 2023, în România, Directoratul Național de Securitate Cibernetică – DNSC (organism specializat al administrației publice centrale, aflat sub

[5] Regulamentul privind Serviciile Digitale impune platformelor digitale să își asume o mai mare responsabilitate pentru conținutul partajat pe platformele lor. Această legislație urmărește să limiteze răspândirea dezinformării dăunătoare, asigurând, în același timp, respectarea libertății de exprimare.

autoritatea Guvernului și responsabil cu asigurarea securității cibernetice a spațiului cibernetic civil național), a emis o recomandare instituțiilor statului și organismelor publice să nu descarce, să nu instaleze sau utilizeze TikTok pe rețelele și sistemele lor informatice (DNSC 2023b).
În Taiwan, TikTok fusese interzisă pe dispozitivele guvernamentale încă din decembrie 2022. Motivul deciziei a fost legat de preocupările privind utilizarea informațiilor de către China pentru desfășurarea unui „război cognitiv" împotriva Taiwanului.

Rapoartele tehnice despre TikTok menționează existența multor *riscuri și vulnerabilități de securitate cibernetică specifice instalării și utilizării acestei aplicații* (**colectarea de date personale, dispozitive utilizate, sistem de operare, IP, SSID Wi-Fi, număr de serie, ID SIM, IMEI, citirea SMS-urilor, adresă MAC, localizare GPS, conturi de utilizator, acces la clipboard, istoric, inutilitatea setării Do Not Track, servicii/aplicații utilizate, profilarea personală a utilizatorului, partajarea datelor colectate cu alți „parteneri", control la distanță etc**.) (Baiaș 2023).

Totodată, a fost luată în considerare și legislația chineză, aceasta obligând cetățenii și entitățile să coopereze cu serviciile de informații și cu instituțiile de stat pentru furnizarea de date și informații în scopuri „naționale" (***Legea Securității Statului*, 2015; *Legea Securității Cibernetice*, 2016; *Legea Activităților de Informații de Stat*, 2017; *Legea Activităților de Contrainformații de Stat*, 2023**).

***Platforma Facebook**:*
Încă din 2015, platforma Facebook a fost blocată în Etiopia, Bangladesh, Myanmar și Sri Lanka pentru a preveni răspândirea dezinformării și discursurilor de ură, pentru a controla fluxul de informații și a suprima disidența, pe motive de securitate națională ori din cauza conținutului, considerat ofensator pentru islam.
Pe de altă parte, Facebook a fost supus restricțiilor și cenzurii în China, Iran și Coreea de Nord, unde accesul la platformă este fie complet blocat, fie strict restricționat.

***Instagram**:*
Platforma Instagram a fost blocată în China din 2014 ca parte a eforturilor guvernului chinez de a controla fluxul de informații și de a limita accesul la platformele de socializare occidentale. De asemenea, platforma a fost blocată intermitent în Iran, în timpul unor tulburări politice și proteste, pentru a preveni și a stopa răspândirea informațiilor și coordonarea demonstrațiilor. Și Turcia a blocat temporar accesul la Instagram și la alte rețele sociale după o tentativă de lovitură de stat, pentru a preveni răspândirea dezinformării și panica (2016).

În 2020, India a interzis Instagram și alte aproximativ 60 de aplicații chinezești, invocând motive de securitate națională și confidențialitatea datelor. În același an, Federația Rusă a blocat Instagram, ca răspuns la decizia Meta de a permite utilizatorilor din anumite țări să posteze mesaje de incitare la violență împotriva soldaților ruși, în contextul războiului din Ucraina.

Totodată, Instagram a fost supus restricțiilor și cenzurii în Coreea de Nord și Turkmenistan, unde accesul la internet este strict controlat de guvernul național.

Cadrul legal actual al UE/statelor membre ale UE și al celor non-UE, emis pentru reglementarea platformelor de social media

Uniunea Europeană și mai multe state din întreaga lume au acordat atenție cadrului legal și de reglementare astfel încât utilizarea serviciilor de internet să fie mai sigură pentru cetățeni, organizații și companii, dar și pentru a face mai responsabile platformele sociale. Aceste legi impun obligații privind transparența, moderarea conținutului și răspunsul la solicitările autorităților. În plus, au fost înființate autorități responsabile cu activitățile rețelelor sociale. În contrast, în alte țări, legislația necesară reglementării platformelor de social media este inadecvată sau inexistentă. În aceste condiții, autoritățile nu dețin instrumente eficiente prin care să constrângă platformele să își asume responsabilitatea pentru conținutul găzduit și să răspundă prompt solicitărilor de eliminare a conținutului dăunător.

În **Uniunea Europeană**, Serviciul European de Acțiune Externă lucrează, încă din 2015, la combaterea FIMI, inclusiv a dezinformării, precum și la consolidarea comunicărilor strategice în ceea ce privește Parteneriatul Estic, Vecinătatea Sudică și Balcanii de Vest (EEAS 2024). În acest scop, au fost elaborate *Regulamentul General privind Protecția Datelor (GDPR)* din 2016 (EUR-Lex 2016), *Regulamentul privind Serviciile Digitale (DSA)* din 2020 (EUR-Lex 2022b)[6], precum și *Regulamentul privind Piețele Digitale (DMA)* din 2020 (EUR-Lex 2022a)[7].

Și **Germania** a manifestat interes pentru adaptarea legislației la provocările curente. În acest scop, în 2017 a fost adoptată *Legea privind Aplicarea Rețelelor (NetzDG)* (bundesjustizamt.de 2018). Legea NetzDG este una dintre cele mai stricte reglementări din Europa pentru combaterea discursului de ură online și a dezinformării. Aceasta conține prevederi care obligă platformele de socializare, care au peste două milioane de utilizatori în Germania, să elimine conținutul ilegal în termen de 24h, în caz contrar, riscând amenzi de până la 50 de milioane de euro. Deși nu este axată exclusiv pe dezinformarea de origine străină, NetzDG joacă un rol esențial în prevenirea răspândirii conținutului manipulator străin.

Totodată, Germania a înființat *Centrul Național de Apărare Cibernetică*. Această instituție are în componență reprezentanți din agențiile federale, inclusiv *Oficiul Federal pentru Securitatea Informațiilor* (BSI), *Serviciul Federal de Informații* (BND) și *Oficiul Federal pentru Protecția Constituției* (BfV),

[6] Regulamentul (UE) 2022/2065 privind o piață unică pentru serviciile digitale.
[7] Regulamentul (UE) 2022/1925 privind piețele contestabile și echitabile din sectorul digital.

acesta fiind serviciul intern de informații german. Centrul coordonează răspunsul Germaniei la amenințările cibernetice, care includ FIMI și utilizarea instrumentelor cibernetice pentru răspândirea dezinformării.
Pe de altă parte, BfV a dezvoltat programe specializate pentru monitorizarea FIMI în alegeri, concentrându-se în special pe campaniile de dezinformare din Rusia și China. Înaintea alegerilor federale din 2021, BfV a emis avertismente și și-a intensificat monitorizarea rețelelor sociale și a grupurilor finanțate din străinătate, implicate în răspândirea dezinformării.

Franța a adoptat, în 2018, *Legea contra manipulării informațiilor (Loi contre la manipulation de l'information)*, ca răspuns la creșterea îngrijorărilor legate de interferența FIMI în alegeri. Cunoscută sub denumirea de „*Legea Fake News*", aceasta permite judecătorilor să acționeze rapid în timpul alegerilor prin eliminarea/blocarea dezinformării din sursele media, dacă se poate demonstra că acestea difuzează informații în mod deliberat pentru a manipula rezultatele alegerilor. De asemenea, legea impune rețelelor sociale să dezvăluie sponsorii în campaniile electorale, pentru a evita manipularea finanțată din străinătate.

Totodată, *Consiliul Superior al Audiovizualului (CSA)*, organism de reglementare media din Franța, a primit puteri sporite pentru a supraveghea platformele media și diseminarea conținutului. În perioadele electorale, CSA poate acționa împotriva platformelor care permit răspândirea dezinformării sau manipularea provenind de la actori străini. De asemenea, CSA poate impune sancțiuni asupra surselor care nu respectă standardele de transparență privind publicitatea politică.
Pentru reglementarea platformelor de social media, **SUA** fac uz de *Secțiunea 230 din Legea privind Decența în Comunicații a SUA*, promulgată în 1996 (LLI 1996).

În **Australia**, începând cu anul 2021, funcționează *Codul de Negociere a Presei de Știri*.

În **Regatul Unit al Marii Britanii și Irlandei de Nord** a fost promulgată *Legea Siguranței Online 2023* (GOV.UK 2023a). Această lege complexă protejează copiii și adulții în mediul online, include reglementări stricte pentru platformele de social media și motoarele de căutare, impunându-le obligații de a proteja utilizatorii de conținut dăunător, de a elimina rapid conținutul ilegal și de a implementa sisteme și procese necesare reducerii riscurilor asociate cu activități ilegale sau malițioase. Legea mai conține și prevederi referitoare la *Ofcom* (*Autoritatea de reglementare independentă pentru Siguranța Online*), care elaborează recomandări pentru respectarea normelor și care are competențe extinse pentru a evalua și aplica conformitatea platformelor.

Obligațiile legii se aplică serviciilor/motoarelor de căutare și serviciilor care permit utilizatorilor să posteze conținut online sau să interacționeze între ei. Aceasta include o serie de site-uri, servicii de mesagerie instantanee online, aplicații și alte servicii, servicii de social media, site-uri de stocare și partajare în cloud a fișierelor

pentru consumatori, forumuri online, platforme de partajare video și servicii de întâlniri. Legea tratează serviciile legate de Regatul Unit, chiar dacă societățile care le furnizează sunt din afara țării (GOV.UK 2023b). Infracțiunile penale introduse de lege se aplică direct persoanelor care se fac vinovate și acoperă încurajarea sau sprijinirea autovătămării grave, cyberflashing, comunicări amenințătoare, transmiterea de informații false, menite să provoace un prejudiciu care nu este de mică importanță, abuzul de imagini intime, trollingul epileptic.

Conținutul ilegal specific și activitățile de care platformele trebuie să protejeze utilizatorii includ abuzul sexual asupra copiilor, violența sexuală extremă, comportamente de control sau constrângere, pornografie extremă, fraudă, incitarea la violență, infracțiuni de ordine publică agravate rasial sau religios, imigrația ilegală și traficul de persoane, promovarea sau facilitarea sinuciderii, vânzarea de droguri sau de arme ilegale, abuzul de imagini intime (revenge porn), exploatarea sexuală și terorismul. Legea impune, de asemenea, platformelor să elimine rapid conținutul ilegal legat de sinucidere și de autovătămare și să protejeze proactiv utilizatorii împotriva conținutului ilegal, conform *Legii sinuciderii* din 1961.

În Regatul Unit a fost înființată, în 2019, *Unitatea de Combatere a Dezinformării* (CDU), aceasta având scopul de a monitoriza conținutul online care prezintă riscuri pentru sănătatea publică, siguranța publică și securitatea națională, precum și de a răspunde la riscurile de dezinformare, inclusiv pe tema Covid-19. CDU analizează tentativele de dezinformare și poate acționa pentru a dezminți informațiile false pe social media, pentru a desfășura campanii de conștientizare și pentru a încuraja platformele să promoveze surse autoritare de informații. În prezent, CDU se concentrează pe dezinformarea legată de invazia ilegală a Rusiei în Ucraina și a contracarat deja dezinformarea rusă cu privire la Ucraina. CDU a fost convocată de peste 200 de ori în Parlamentul britanic.

În **Canada** funcționează *Legea privind daunele online*, aceasta având în atenție combaterea conținutului online dăunător, inclusiv discursul care incită la ură, dezinformarea și abuzul sexual asupra copiilor.

Singapore a promulgat, în 2019, *Legea pentru protecția împotriva informațiilor false și manipulării online* (POFMA), în baza căreia guvernul poate ordona corectarea sau eliminarea informațiilor false/dăunătoare de pe platformele sociale (Singapore.gov 2019).

Și **Brazilia** are în atenție activitatea online prin *Legea cadru pentru drepturile civile pe internet* din 2014, care stabilește principiile de utilizare a internetului în Brazilia, inclusiv neutralitatea rețelei și protecția datelor personale (Secretaria-Geral 2014).

În **India** regulile privind tehnologia informației (*Orientări privind intermediarii și Codul de etică pentru mediile digitale*) sau „*Regulile IT*" au intrat în vigoare în 2021, în acest context fiind stabilite cerințe specifice de conformitate pentru intermediarii din mediile sociale (Indian.gov 2021). *Regulile IT* au fost introduse pentru a verifica

răspândirea știrilor false, a discursului instigator la ură, a hărțuirii online, unele dintre aspectele semnificative fiind următoarele:

- PSM/alți intermediari trebuie să dea dovadă de diligență, depunând eforturi rezonabile pentru a determina utilizatorii să nu găzduiască, să nu afișeze, să nu încarce, să nu modifice, să nu publice, să nu transmită, să nu stocheze, să nu actualizeze sau să nu partajeze informații care (1) sunt dăunătoare copiilor (2), care încalcă marca comercială, drepturile de autor, brevetul sau alte drepturi de proprietate (3), care sunt defăimătoare, obscene, invazive pentru viața privată a unei alte persoane, care sunt inacceptabile din punct de vedere rasial sau etnic (4), care se dau drept o altă persoană (5), care încalcă orice alte legi.
- Regulile oferă un mecanism eficient de despăgubire prin care utilizatorii/ victimele pot depune o plângere împotriva încălcării normelor IT. Responsabilul cu reclamațiile trebuie să acționeze în timp util după primirea unei plângeri prin care se solicită eliminarea unei informații sau a unei legături de comunicare.
- Este obligatoriu ca toate PSM semnificative să numească un *Chief Compliance Officer* și un *Nodal Officer*, disponibili 24*7, pentru coordonarea cu agențiile de aplicare a legii.

În **România** DNSC a emis, în mai 2023, o recomandare către instituțiile statului și organismele publice, potrivit căreia acestea nu trebuie să descarce, să instaleze sau să utilizeze TikTok în rețelele și sistemele lor informatice. Totodată, autoritățile române au în atenție noi prevederi legale care vizează reglementări mai stricte pentru rețelele sociale, crearea unui mediu online mai sigur și mai responsabil, desemnarea de puncte de contact/reprezentanți naționali pentru rețelele sociale din România, introducerea unor sancțiuni pentru nerespectarea obligațiilor de moderare a conținutului.

Concluzii

Platformele online și motoarele de căutare le permit utilizatorilor să dezvolte rețele globale, acestea reprezentând, la momentul actual, cel mai popular mediu în rândul creatorilor de conținut. Conceptul din spatele lor pare inofensiv, însă accesibilitatea facilă și oportunitățile oferite implică și unele riscuri. Abuzul de proprietate intelectuală, furtul de date personale și bancare, dezinformarea, răspândirea de știri false, conținutul obscen, violența sau discursurile instigatoare la ură sunt câteva dintre provocări.

Atât activitățile malițioase, desfășurate, pe platformele social media, de către actorii statali și nonstatali, cât și alte forme de interferență străină constituie o amenințare la adresa principiilor și valorilor democratice, având un impact negativ asupra securității naționale, democrației, instituțiilor statului, infrastructurii critice, societății, mediului de afaceri și cetățenilor. Unii dintre cei mai expuși la conținutul online dăunător și inadecvat sunt copiii, femeile, fetele, dar și persoanele vârstnice.
Prezenta cercetare științifică atestă că atât utilizatorii obișnuiți, cât și autoritățile naționale se confruntă cu probleme legate de lipsa cadrului legal de reglementare

a procedurilor formale sau a posibilității de a-i contacta direct pe reprezentanții platformelor de social media atunci când este nevoie, pentru a lua măsuri în vederea blocării/eliminării/modificării în timp util a unor astfel de activități ilegale sau mesaje inadecvate. Studiul atestă inclusiv existența mai multor plângeri referitoare la lipsa unei reacții adecvate din partea PSM la rapoartele și cererile utilizatorilor pentru blocarea/eliminarea vectorilor de atac.

Pe de altă parte, platformele de social media se confruntă cu provocări continue în moderarea conținutului online dăunător. Unele dintre platforme au implementat diverse măsuri pentru a contracara provocările cu care se confruntă (moderarea conținutului, creșterea transparenței cu privire la moderarea conținutului, îmbunătățirea algoritmilor pentru a detecta automat conținutul dăunător, clasificarea conținutului, colaborarea cu fact-checkeri), însă acestea sunt adesea insuficiente și lente. Situația prezentată se datorează parțial volumului mare de conținut generat de utilizatori, dar și lipsei unor stimulente și sancțiuni suficiente pentru a acționa rapid și eficient.

A sosit momentul ca platformele de social media să își asume responsabilitatea, să investească în măsuri de securitate robuste, să abordeze proactiv această problemă și să prioritizeze siguranța utilizatorilor în era digitală. Obligațiile legale ar trebui aduse în atenția tuturor radiodifuzorilor și platformelor de social media pentru a oferi publicului informații imparțiale și obiective, prezentând faptele și evenimentele corect și cu respect pentru libertatea de exprimare.

În urma acestui studiu, se poate concluziona că **statele au nevoie de cadre și de politici de reglementare eficiente pentru a face utilizarea serviciilor de internet mai sigură**. Acestea ar trebui **să fie aplicate platformelor de social media, motoarelor de căutare și serviciilor care permit utilizatorilor să posteze conținut online sau să interacționeze între ei**: o gamă de site-uri, mesagerie instant online, forumuri online, aplicații de servicii și alte servicii, inclusiv cele de social media, site-uri de stocare și partajare de fișiere cloud pentru consumatori, platforme de partajare video, servicii de întâlniri etc. Legislația ar trebui să fie echilibrată, să protejeze libertatea de exprimare, dar și să se asigure că platformele online își asumă responsabilitatea pentru conținutul găzduit și contribuie la un mediu online mai sigur și mai sănătos, pentru a proteja utilizatorii de conținutul dăunător, pentru a elimina rapid conținutul ilegal, pentru a implementa sisteme și procese necesare reducerii riscurilor legate de serviciile oferite, atunci când sunt utilizate pentru activități malițioase.

Având în vedere contextul actual și experiența internațională, țările din întreaga lume ar putea reflecta asupra adoptării de măsuri legislative în următoarele domenii, pentru a reglementa mai eficient platformele social media, motoarele de căutare și serviciile care permit utilizatorilor să posteze conținut online social, dar și pentru a-i proteja pe aceștia. Analizând cadrul actual, **transparența și responsabilitatea** platformelor online reprezintă un element esențial. Acestea ar trebui să numească un reprezentant național în statele în care funcționează, care să răspundă de comunicarea cu autoritățile și de asigurarea conformității cu legislația locală. De asemenea, este

necesar ca utilizatorii să aibă la dispoziție mecanisme simple și accesibile pentru a raporta conținutul dăunător și/sau a contesta deciziile de moderare. În același timp, se impune ca platformele online să publice periodic rapoarte detaliate privind măsurile luate pentru a modera conținutul, numărul de plângeri primite și modul în care au fost soluționate.

În ceea ce privește, **moderarea conținutului**, platformele social media, motoarele de căutare și serviciile care permit utilizatorilor să posteze conținut online sau să interacționeze între ei ar trebui să fie obligate să elimine conținutul ilegal într-un termen scurt de la notificare. Totodată, este necesar ca acestea să colaboreze mai bine cu organizații independente de fact-checking și cu experți în drepturile omului pentru a îmbunătăți moderarea conținutului. Pe de altă parte, platformele ar trebui încurajate să utilizeze tehnologii avansate, precum inteligența artificială, pentru a identifica și a elimina cu celeritate, în mod automat, conținutul dăunător.

Referitor la **protecția utilizatorilor**, este important să se implementeze măsuri speciale pentru protejarea copiilor de conținutul dăunător, precum restricții de vârstă și instrumente de control parental. Platformele de social media ar trebui să ia măsuri eficiente pentru a limita răspândirea dezinformării, punând accent pe etichetarea conținutului fals sau înșelător și promovarea surselor de informații credibile. Este necesar ca legislația privind protecția datelor personale să fie respectată strict, iar utilizatorii să dețină controlul asupra modului în care datele lor sunt colectate și utilizate.

În vederea sprijinirii acestor măsuri, **se impune înființarea unor organisme de supraveghere și reglementare**. Astfel de organisme sunt necesare pentru a supraveghea activitatea platformelor social media, motoarelor de căutare și serviciilor care permit utilizatorilor să posteze conținut online sau să interacționeze între ei. De asemenea, entitățile în cauză ar trebui să aibă atribuții pentru a putea lua măsuri împotriva companiilor sau platformelor care permit realizarea online a acțiunilor de tip FIMI ori a altor activități ilegale, iar totodată, să impună sancțiuni, în cazul încălcării legilor și normelor stabilite.

În ceea ce privește **sancțiunile**, platformele online care nu respectă obligațiile legale ar trebui sancționate cu amenzi proporționale cu gravitatea încălcării și cu cifra de afaceri a companiei. În situații deosebite, se impune ca autoritățile naționale să aibă posibilitatea de a suspenda temporar sau de a bloca serviciile furnizate de platformele online și motoarele de căutare, oricând când situația o va cere.

Referințe

Adrien, Claudia. 2023. "Phishing Attacks Target Facebook, Microsoft, Making Them Most Impersonated Brands". https://www.channelfutures.com/security/phishing-attacks-target-facebook-microsoft-making-them-most-impersonated-brands.

Alexander, Brooke Nelson. 2022. "What Is Doxxing, and How Does It Set You Up to Be Hacked?" https://www.rd.com/article/what-is-doxxing/.

—. 2023. "What Is Spoofing, and How Can You Spot It?". https://www.rd.com/article/spoofing/.

—. 2024. "14 Facebook Marketplace Scams to Watch Out For". https://www.rd.com/article/facebook-marketplace-scams/.

Baiaș, Ionuț. 2023. „Directoratul Național de Securitate Cibernetică recomandă interzicerea TikTok pe dispozitivele instituțiilor publice". https://hotnews.ro/directoratul-national-de-securitate-cibernetica-recomanda-interzicerea-tiktok-pe-dispozitivele-institutiilor-publice-64785.

Bradford, Alina. 2024. "8 Common Bank Scams to Watch Out For". https://www.rd.com/list/bank-scams/.

Budgar, Laurie. 2024. "Can You Really See Who Viewed Your Facebook Profile Recently?". https://www.rd.com/article/who-viewed-my-facebook-profile/.

bundesjustizamt.de. 2018. "Network Enforcement Act Regulatory Fining Guidelines". https://www.bundesjustizamt.de/SharedDocs/Downloads/DE/NetzDG/Leitlinien_Geldbussen_en.pdf?__blob=publicationFile&v=3.

Chin, Kyle. 2024. "19 Most Common Types of Phishing Attacks in 2024". https://www.upguard.com/blog/types-of-phishing-attacks.

Comisia Europeană. 2024. "Commission opens proceedings against TikTok under the DSA regarding the launch of TikTok Lite in France and Spain". https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2227.

DNSC. 2023a. „ALERTA: Tentative de fraudă promovate prin anunțuri sponsorizate pe rețelele sociale". https://www.dnsc.ro/citeste/alerta-tentative-de-frauda-promovate-prin-anunturi-sponsorizate-social-media.

—. 2023b. "Press release." https://dnsc.ro/vezi/document/comunicat-de-presa-dnsc-recomanda-autoritatilor-si-institutiilor-publice-din-romania-interzicerea-descarcarii-instalarii-si-utilizarii-a-aplicatiei-tiktok-pe-dispozitivele-de-serviciu-pdf.

EEAS. 2024. "Tackling Disinformation, Foreign Information Manipulation & Interference". https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en.

EUR-Lex. 2016. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data". https://eur-lex.europa.eu/eli/reg/2016/679/oj.

—. 2022a. "Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector". https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32022R1925.

—. 2022b. "Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services". https://eur-lex.europa.eu/eli/reg/2022/2065/oj.

Giles, Keir. 2016. "Handbook of Russian Information Warfare". https://www.ndc.nato.int/news/news.php?icode=995.

Gordon, Anna. 2024. "Here's All the Countries With TikTok Bans as Platform's Future in U.S. Hangs In Balance". https://time.com/6971009/tiktok-banned-restrictions-worldwide-countries-united-states-law/.

GOV.UK. 2023a. "Online Safety Act 2023." https://www.legislation.gov.uk/ukpga/2023/50/enacted.

—. 2023b. "What the Online Safety Act does." https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer#:~:text=The%20Online%20Safety%20Act%202023,users'%20safety%20on%20their%20platforms.

Hindman, Matthew. 2018. "Disinformation, 'Fake News' and Influence Campaigns on Twitter." https://knightfoundation.org/reports/disinformation-fake-news-and-influence-campaigns-on-twitter/.

Indian.gov. 2021. "The Information Technology (Intermediary Guidelines and Digital Media Ethics Code)." https://www.meity.gov.in/writereaddata/files/Information%20Technology%20%28Intermediary%20Guidelines%20and%20Digital%20Media%20Ethics%20Code%29%20Rules%2C%202021%20%28updated%2006.04.2023%29-.pdf.

ITU. 2021. "Session 5: Disinformation, misinformation, malinformation and Infodemics: Ways to handle". https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Pages/Events/2021/ASP%20Regional%20Dialogue%20on%20Digital%20Transformation/Session%20Pages/RD-Session-5.aspx.

Justia. 2021. "Gonzalez v. Google, LLC, No. 18-16700 (9th Cir. 2021)." https://law.justia.com/cases/federal/appellate-courts/ca9/18-16700/18-16700-2021-06-22.html.

Lakshmanan, Lavie. 2024. "Canada orders TikTok to shut down Canadian operations over security concerns". https://thehackernews.com/2024/11/canada-orders-tiktok-to-shut-down.html?m=1.

LLI. 1996. "47 U.S. Code § 230 – Protection for private blocking and screening of offensive material." https://www.law.cornell.edu/uscode/text/47/230.

PakVoices. 2023. "Disinformation impacts on digital sphere in Pakistan (May-July 2023)." https://pakvoices.pk/?p=13745.

Petkauskas, Vilius. 2023. "Facebook Messenger phishing attack pumps out 100K+ weekly messages". https://cybernews.com/news/facebook-messenger-phishing-attack/.

Qureshi, Anees. 2023. "Meta Neglecting the Proliferation of Phishing Scam Pages on Facebook, Leaving Millions of Users Vulnerable". https://www.linkedin.com/pulse/meta-neglecting-proliferation-phishing-scam-pages-facebook-qureshi-dsizf/.

Rosenkrantz, Holly. 2024. "What Is Phishing, and How Can You Prevent This Cyberattack?". https://www.rd.com/article/what-is-phishing/.

Saint Francis University. 2023. "Misinformation, Disinformation, and Fake News". https://libguides.francis.edu/fake-news.

Sasnauskas, Mantas. 2023. "We uncovered a Facebook phishing campaign that tricked nearly 500,000 users in two weeks". https://cybernews.com/security/we-uncovered-a-facebook-phishing-campaign-that-tricked-nearly-500000-users-in-two-weeks/.

Schappert, Stefanie. 2024. "Meta deletes 63K sextortion scam accounts from Instagram, Facebook".https://cybernews.com/news/meta-deletes-63k-sextortion-scam-accounts-instagram-facebook/.

Secretaria-Geral. 2014. "LEI Nº 12.965, DE 23 DE ABRIL DE 2014." http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

Singapore.gov. 2019. "Protection from Online Falsehoods and Manipulation Act 2019." https://sso.agc.gov.sg/Act/POFMA2019.

Snegovaya, Maria. 2015. "Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare, Institute for the Study of War." https://www.understandingwar.org/report/putins-information-warfare-ukraine-soviet-origins-russias-hybrid-warfare.

Stathis, Jaime. 2024a. "14 Online Scams You Need to Be Aware Of—and How to Avoid Them". https://www.rd.com/list/how-to-avoid-online-scams/.

—. 2024b. "9 Red Flags You're About to Click on a Fake Social Media Ad". https://www.rd.com/list/fake-ads-on-social-media/.

Toulas, Bill. 2023a. "Facebook disrupts new NodeStealer information-stealing malware." https://www.bleepingcomputer.com/news/security/facebook-disrupts-new-nodestealer-information-stealing-malware/.

—. 2023b. "Facebook Messenger phishing wave targets 100K business accounts per week". https://www.bleepingcomputer.com/news/security/facebook-messenger-phishing-wave-targets-100k-business-accounts-per-week/.

Zaleznik, Daniel. 2021. "*Facebook and Genocide: How Facebook contributed to genocide in Myanmar and why it will not be held accountable*". https://systemicjustice.org/article/facebook-and-genocide-how-facebook-contributed-to-genocide-in-myanmar-and-why-it-will-not-be-held-accountable/.

Zaytsev, Oleg. 2023. "«MrTonyScam» — Botnet of Facebook Users Launch High-Intent Messenger Phishing Attack on Business Accounts". https://labs.guard.io/mrtonyscam-botnet-of-facebook-users-launch-high-intent-messenger-phishing-attack-on-business-3182cfb12f4d.

BULETINUL
UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I"
https://buletinul.unap.ro

Creșterea rezilienței cibernetice a IMM prin soluții open-source și colaborare internațională

Increasing the cyber resilience of SMEs through open-source solutions and international collaboration

Dr. Ionica ȘERBAN*
Masterand Florentina-Mihaela CURCĂ**
Masterand Robert-Ștefan ȘANDRU***
*Directoratul Național de Securitate Cibernetică
e-mail: ionica.serban@dnsc.ro
**Directoratul Național de Securitate Cibernetică
e-mail: mihaela.curca@dnsc.ro
***Directoratul Național de Securitate Cibernetică
e-mail: robert.sandru@dnsc.ro

Abstract

Într-o lume tot mai digitalizată, întreprinderile mici și mijlocii (IMM) sunt expuse amenințărilor cibernetice semnificative, din cauza resurselor limitate pentru securitate. Acest articol explorează rolul soluțiilor open-source și al colaborării internaționale în creșterea rezilienței cibernetice a IMM. Soluțiile open-source oferă accesibilitate financiară, flexibilitate și securitate sporită, fiind susținute de comunități globale care contribuie la îmbunătățirea continuă a acestora. De asemenea, partajarea descentralizată a informațiilor referitoare la amenințări, combinată cu inteligența artificială, permite o detectare și o prevenție mai eficientă a atacurilor cibernetice. Prin inițiative colaborative, cum ar fi HackOlympics, IMM pot învăța din practică și pot beneficia de soluții testate în scenarii reale. În concluzie, soluțiile open-source și utilizarea tehnologiilor avansate, precum IA, le oferă întreprinderilor mici și mijlocii o strategie eficientă pentru a răspunde provocărilor cibernetice moderne, îmbunătățindu-le reziliența și protecția împotriva amenințărilor.

In an increasingly digitalized world, small and medium-sized enterprises (SMEs) are exposed to significant cyber threats due to limited security resources. This article explores the role of open-source solutions and international collaboration in enhancing the cyber resilience of SMEs. Open-source solutions offer financial accessibility, flexibility, and increased security, supported by global communities that contribute to their continuous improvement. Moreover, decentralized sharing of threat information, combined with artificial intelligence, enables more efficient detection and prevention of cyberattacks. Through collaborative initiatives such as HackOlympics, SMEs can learn through hands-on experience and benefit from solutions tested in real-life scenarios. In conclusion, open-source solutions and the use of advanced technologies, such as AI, provide SMEs with an effective strategy to address modern cyber challenges, improving their resilience and protection against threats.

Cuvinte-cheie:
securitate cibernetică; IMM; soluții open-source; colaborare internațională; inteligență artificială; HackOlympics.

Keywords:
cybersecurity; SMEs; open-source solutions; international collaboration; artificial intelligence; HackOlympics.

Info articol
Primit: 14 octombrie 2024; Evaluat: 15 noiembrie 2024; Acceptat: 2 decembrie 2024; Disponibil online: 17 ianuarie 2025
Citare: Șerban, I., F.M. Curcă și R.Ș. Șandru. 2024. „Creșterea rezilienței cibernetice a IMM prin soluții open-source și colaborare internațională". *Buletinul Universității Naționale de Apărare „Carol I"*, 13(4): 215-236. https://doi.org/10.53477/2065-8281-24-49

În era digitalizării accelerate, securitatea cibernetică a devenit o provocare globală, afectând toate tipurile de organizații, indiferent de dimensiune. Cu toate acestea, întreprinderile mici și mijlocii (IMM) sunt în mod deosebit vulnerabile, deoarece adesea nu dispun de resursele necesare pentru a investi în tehnologii avansate de protecție și pentru a implementa sisteme robuste de securitate. Aceste companii reprezintă un segment esențial al economiei globale, având o contribuție semnificativă la dezvoltarea economică, la inovare și ocuparea forței de muncă. În ciuda acestui fapt, numeroase întreprinderi mici și mijlocii sunt ținte atractive pentru atacatorii cibernetici, deoarece, de multe ori, dispun de date valoroase, dar au infrastructuri de securitate insuficient dezvoltate.

Întreprinderile mici și mijlocii se confruntă cu o serie de provocări unice în ceea ce privește protecția cibernetică. În primul rând, lipsa resurselor financiare și umane limitează capacitatea lor de a investi în soluții comerciale scumpe de securitate cibernetică, accesibile mai mult pentru companiile mari. În al doilea rând, IMM nu dispun de echipe dedicate sau de expertiză în domeniul securității informatice, ceea ce le face să fie mai puțin pregătite să detecteze și să răspundă rapid la amenințările cibernetice.

De asemenea, întreprinderile mici și mijlocii sunt adesea concentrate pe creșterea afacerilor și nu percep riscurile cibernetice ca fiind prioritare, ceea ce duce la o lipsă de măsuri proactive pentru prevenirea atacurilor. Acest lucru le plasează într-o poziție vulnerabilă, fiind frecvent afectate de atacuri, precum ransomware, phishing și breșe de date, care pot provoca pierderi financiare substanțiale, afectând reputația și încrederea clienților.

Soluțiile open-source sunt o alternativă accesibilă, oferă o opțiune viabilă pentru IMM în consolidarea securității cibernetice. Acestea oferă acces gratuit la tehnologii avansate, care pot fi adaptate și personalizate, în funcție de nevoile fiecărei organizații. În plus, comunitățile open-source sunt extrem de active în remedierea vulnerabilităților și îmbunătățirea continuă a acestor soluții, oferind întreprinderilor mici și mijlocii oportunitatea de a beneficia de cele mai recente inovații și practici din domeniul securității cibernetice.
Adoptarea acestor soluții nu necesită costuri inițiale mari, iar IMM pot alege să implementeze treptat măsuri de securitate, pe măsură ce își dezvoltă capacitățile și resursele. De asemenea, soluțiile open-source beneficiază de un nivel ridicat de transparență și flexibilitate, ceea ce permite o personalizare mai profundă și o integrare ușoară în sistemele existente ale IMM.

Colaborarea internațională este cheia pentru success, o altă dimensiune crucială în creșterea rezilienței cibernetice a IMM. Atacurile cibernetice au o natură globală, iar pentru a combate aceste amenințări complexe, întreprinderile mici și mijlocii trebuie să participe la rețele de partajare a informațiilor, să colaboreze cu alte companii și instituții din domeniul securității și să învețe din experiențele altor entități de pe plan internațional.

Colaborarea dintre IMM și organisme internaționale permite schimbul de bune practici și accesul la resurse educative, la conferințe, hackathoni și simulări de atacuri. Aceasta creează un ecosistem de sprijin reciproc, în care noile amenințări sunt rapid identificate și soluțiile sunt dezvoltate și distribuite comunității, crescând astfel capacitatea întreprinderilor mici și mijlocii de a răspunde rapid la riscuri și de a-și îmbunătăți sistemele de apărare. Întreprinderile mici și mijlocii, deși vulnerabile din cauza resurselor limitate, au posibilitatea de a-și îmbunătăți reziliența cibernetică prin adoptarea soluțiilor open-source și prin participarea la inițiative de colaborare internațională. Aceste măsuri, împreună cu educarea continuă și conștientizarea importanței securității cibernetice, vor permite IMM să facă față provocărilor din mediul digital actual, asigurându-și protecția pe termen lung și contribuind la stabilitatea și dezvoltarea economiei globale.

Metodologie

Metoda științifică utilizată în această lucrare se concentrează pe o abordare integrată și multidisciplinară pentru a evalua eficacitatea soluțiilor open-source în creșterea rezilienței cibernetice a IMM. Metodologia a fost structurată pe mai multe etape, pentru a asigura o analiză cuprinzătoare și riguroasă a subiectului. Prima etapă a fost o revizuire sistematică a literaturii existente, pentru a înțelege peisajul actual al securității cibernetice și utilizarea soluțiilor open-source de către IMM. Au fost folosite surse academice și rapoarte din industrie pentru a identifica provocările și nevoile întreprinderilor mici și mijlocii în materie de securitate cibernetică. Baze de date, precum IEEE Xplore, Google Scholar și Scopus, au fost folosite pentru a extrage articole relevante privind tehnologiile de securitate, inteligența artificială și partajarea informațiilor despre amenințări.

În continuare, a fost efectuată o analiză comparativă a soluțiilor open-source disponibile pentru IMM, cum ar fi OpenVAS, Suricata, și PfSense. Respectiva etapă a implicat evaluarea acestor soluții pe baza criteriilor esențiale, inclusiv costurile, ușurința de utilizare, flexibilitatea și eficiența în detectarea și prevenirea amenințărilor.

Această lucrare se distinge prin prezentarea unui studiu aprofundat privind impactul soluțiilor open-source asupra securității cibernetice a IMM, un subiect de interes tot mai mare în era digitalizării. În acest context, soluțiile, precum OpenVAS, Suricata și PfSense, joacă un rol crucial, fiind adoptate din ce în ce mai mult de întreprinderile mici și mijlocii care caută alternative eficiente și accesibile la soluțiile comerciale.

Conform unui raport recent al Ponemon Institute (2023), peste 45% dintre întreprinderile mici și mijlocii la nivel global utilizează cel puțin o soluție open-source pentru securitatea cibernetică. Dintre acestea, 60% consideră că accesibilitatea financiară este principalul motiv pentru adoptarea acestor soluții. În mod specific, OpenVAS, o platformă pentru evaluarea vulnerabilităților, este utilizată

de aproximativ 35% dintre întreprinderile mici și mijlocii care implementează soluții open-source. Această platformă permite companiilor să identifice rapid punctele slabe din infrastructura IT, reducând riscul exploatării vulnerabilităților critice.
De asemenea, Suricata, o soluție avansată pentru detectarea și prevenirea intruziunilor, este integrată în sistemele de securitate ale IMM din întreaga lume. Conform unui studiu, publicat de OWASP (2023b), utilizarea Suricata a crescut cu 50% în ultimii doi ani, IMM apreciind capacitatea acesteia de a oferi monitorizare în timp real și adaptabilitate la diverse tipuri de atacuri cibernetice.

PfSense, o soluție firewall open-source extrem de populară, s-a dovedit a fi un instrument esențial pentru IMM. Datele furnizate de proiectul PfSense arată că peste 70% dintre utilizatorii săi sunt organizații mici și mijlocii, iar implementările au condus la economii de până la 80%, comparativ cu soluțiile comerciale. Mai mult, un raport Gartner (2023) subliniază că întreprinderile mici și mijlocii care utilizează PfSense observă o îmbunătățire semnificativă a securității rețelei, datorită flexibilității și personalizării ușoare pe care această soluție o oferă.

În cadrul studiului de caz prezentat în acest articol, o întreprindere din categoria IMM din sectorul IT din România a implementat PfSense pentru a face față provocărilor de securitate. În urma acestei implementări, compania a reușit să reducă atacurile cibernetice cu 80% și să asigure o continuitate operațională robustă, menținând în același timp costurile la un nivel minim. Aceste rezultate susțin tendințele globale și demonstrează că întreprinderile mici și mijlocii pot valorifica soluțiile open-source pentru a-și consolida reziliența cibernetică, fără a fi constrânse de bugete mari.
Integrarea acestor statistici și date evidențiază relevanța practică a soluțiilor open-source în protejarea IMM împotriva riscurilor cibernetice și subliniază contribuția semnificativă a acestei lucrări în promovarea utilizării unor astfel de tehnologii. Astfel, lucrarea nu doar că demonstrează aplicabilitatea acestor soluții, ci oferă și un cadru concret de analiză și implementare, bazat pe tendințele actuale și pe nevoile reale ale întreprinderilor mici și mijlocii.

Provocările de securitate pentru IMM în era digitală

IMM (întreprinderile mici și mijlocii) reprezintă coloana vertebrală a economiilor europene, fiind responsabile de aproximativ 99% dintre întreprinderi, generând două treimi din locurile de muncă în Europa (Comisia Europeană 2023). Cu toate acestea, ele se confruntă cu provocări majore în materie de securitate cibernetică, pe măsură ce digitalizarea devine esențială pentru funcționarea afacerilor moderne. Lipsa resurselor financiare și a expertizei interne limitează capacitatea IMM de a investi în tehnologii avansate de securitate, lăsându-le vulnerabile în fața atacurilor cibernetice (ENISA 2023c).

Într-o eră în care criminalitatea cibernetică evoluează rapid, întreprinderile mici și mijlocii devin tot mai frecvent ținta atacurilor. Studiile arată că peste 60% dintre

atacurile cibernetice vizează întreprinderile mici și mijlocii (Verizon 2023), care sunt văzute ca ținte mai ușoare, din cauza lipsei de măsuri de protecție, comparativ cu marile corporații.

Phishingul este una dintre cele mai răspândite amenințări. Angajații IMM primesc e-mailuri frauduloase care pretind a fi de la organizații legitime, încercând să obțină date sensibile. Acest tip de atac reprezintă aproape 57% din totalul incidentelor de securitate raportate în rândul IMM.

Ransomware-ul a devenit o amenințare omniprezentă, întreprinderile mici și mijlocii fiind frecvent vizate, din cauza lipsei unor soluții de backup adecvate. Ransomware-ul criptează datele companiei și solicită o răscumpărare pentru deblocarea accesului. Se estimează că 43% dintre atacurile ransomware au drept țintă întreprinderile mici și mijlocii.

Atacurile DDoS (Distributed Denial of Service) blochează serviciile online ale unei companii prin inundarea serverelor cu trafic fals, ceea ce poate afecta serios operațiunile întreprinderilor mici și mijlocii, în special cele care depind de funcționalitatea online (Arbor Networks 2023).
Breșele de date reprezintă o amenințare majoră, în special pentru IMM care gestionează date sensibile. Studiile arată că 60% dintre IMM care suferă breșe majore de securitate își închid activitatea în termen de șase luni. Impactul financiar al unei breșe poate fi devastator, având în vedere costurile de recuperare și sancțiunile legale care pot apărea în urma nerespectării reglementărilor de protecție a datelor, precum GDPR.

Unul dintre principalii factori care contribuie la vulnerabilitatea întreprinderilor mici și mijlocii este lipsa resurselor financiare. Soluțiile avansate de securitate sunt adesea costisitoare, iar întreprinderile mici și mijlocii au bugete limitate pentru a le achiziționa și implementa. Conform unui raport din 2023, 60% dintre întreprinderile mici și mijlocii nu își permit să investească în soluții comerciale de securitate.
Lipsa expertizei interne reprezintă un alt obstacol semnificativ. Majoritatea întreprinderilor mici și mijlocii nu au personal pentru securitate cibernetică și se bazează pe echipe IT mici sau chiar pe personal non-tehnic pentru a gestiona problemele de securitate. Această lipsă de expertiză duce la o pregătire insuficientă în fața atacurilor și la o reacție lentă, în cazul unor incidente (NIST 2022a).

Infrastructurile învechite sunt o altă problemă majoră pentru întreprinderile mici și mijlocii. Multe dintre acestea folosesc tehnologii vechi și nesecurizate, fără a implementa patch-uri de securitate regulate. Această situație lasă portițe deschise pentru atacatori, care exploatează vulnerabilitățile cunoscute.
Conștientizarea redusă a riscurilor este, de asemenea, un factor important. Mulți manageri de IMM subestimează riscurile cibernetice, crezând că afacerea lor nu este suficient de mare sau de valoroasă pentru a atrage atacuri. Această percepție eronată împiedică întreprinderile mici și mijlocii să ia măsuri proactive pentru a preveni atacurile.

Atacurile cibernetice pot avea consecințe devastatoare asupra IMM, care nu dispun de resursele necesare pentru a se recupera rapid. Pierderile financiare, generate de aceste atacuri, pot include plăți de răscumpărare, pierderi de afaceri, din cauza întreruperii serviciilor, și costuri suplimentare pentru recuperarea datelor.
În plus, impactul unui atac asupra imaginii poate fi la fel de dăunător. O breșă de securitate poate afecta grav încrederea clienților și partenerilor de afaceri, mai ales în cazul în care datele acestora sunt compromise. Într-o eră în care protecția datelor personale este o prioritate, un astfel de incident poate duce la pierderi de clienți și la sancțiuni financiare, impuse de reglementările de tipul GDPR.

Una dintre provocările fundamentale pentru IMM în asigurarea securității cibernetice este accesibilitatea soluțiilor și scalabilitatea acestora. Spre deosebire de marile corporații, care își permit să aloce bugete semnificative pentru implementarea unor soluții avansate de securitate, IMM funcționează cu resurse financiare și umane limitate. Din acest motiv, soluțiile de securitate tradiționale și comerciale sunt adesea inaccesibile din punct de vedere financiar, iar complexitatea acestora poate depăși capacitățile echipelor tehnice care, la nivelul acestor companii, sunt limitate.

Soluțiile de securitate comerciale de tip enterprise, cum ar fi firewall-uri avansate, sisteme de prevenire a intruziunilor (IPS), soluții de backup și recuperare, în caz de dezastru, sau sisteme de gestionare a identității și accesului (IAM), sunt dezvoltate, în general, pentru organizații mari, care au resursele necesare pentru a le implementa și întreține. Aceste soluții implică, pe lângă costuri inițiale ridicate, și cheltuieli recurente pentru licențe, suport tehnic și actualizări regulate. Pentru IMM, aceste cheltuieli reprezintă o povară semnificativă, ceea ce face ca multe dintre ele să nu-și permită astfel de investiții (Verizon 2023).

De asemenea, multe soluții comerciale sunt concepute pentru infrastructuri complexe și organizații cu nevoi diversificate, ceea ce le face dificil de adaptat la nevoile unei IMM. Personalul tehnic redus și, adesea, lipsa unui departament IT face ca multe IMM să nu aibă capacitatea de a gestiona soluții complicate, ceea ce le face vulnerabile atacurilor cibernetice.

În acest context, soluțiile open-source au câștigat teren ca o opțiune viabilă pentru IMM. Soluțiile open-source, care sunt dezvoltate și susținute de comunități globale de dezvoltatori și specialiști în securitate, sunt gratuit disponibile, permit o flexibilitate ridicată și oferă întreprinderilor mici și mijlocii posibilitatea de a le adapta la nevoile lor specifice (OWASP 2023a).

Exemple de soluții open-source care sunt utilizate în securitatea cibernetică includ:

- OpenVAS (Open Vulnerability Assessment System), pentru scanarea vulnerabilităților;
- Suricata și Snort, pentru detectarea și prevenirea intruziunilor;
- PfSense, pentru firewall-uri și routere;
- ClamAV, pentru protecția împotriva virușilor și malware-ului.

Aceste soluții sunt accesibile întreprinderilor mici și mijlocii nu doar datorită costului redus (majoritatea fiind gratuite), ci și datorită suportului larg, oferit de comunitățile din jurul acestor proiecte, care contribuie la actualizări frecvente și la corectarea vulnerabilităților.
Un alt avantaj major al soluțiilor open-source este scalabilitatea. În cazul întreprinderilor mici și mijlocii, care sunt în continuă evoluție, este esențial ca soluțiile de securitate să poată crește odată cu afacerea. Soluțiile open-source pot fi configurate, inițial, pentru a acoperi nevoile de bază ale securității, iar pe măsură ce afacerea crește, aceste soluții pot fi extinse fără costuri semnificative.

De exemplu, un firewall open-source, precum PfSense, poate fi implementat, inițial, la scară mică pentru a gestiona traficul de rețea și poate fi, ulterior, extins pentru a acoperi rețele mai mari sau pentru a include funcționalități avansate, cum ar fi VPN-uri sau QoS (Quality of Service), fără a implica costuri suplimentare majore pentru licențiere sau hardware (PfSense Project 2023). În plus, soluțiile open-source permit întreprinderilor mici și mijlocii să își personalizeze configurațiile pentru a răspunde nevoilor lor specifice, ceea ce le face mult mai flexibile, comparativ cu soluțiile comerciale (NIST 2022b).
Un alt aspect important care face ca soluțiile open-source să fie atractive pentru IMM este sprijinul activ al comunităților globale. Platformele open-source beneficiază de contribuții constante din partea dezvoltatorilor și experților în securitate din întreaga lume, care îmbunătățesc continuu funcționalitățile și identifică noi vulnerabilități.

Pe lângă contribuțiile tehnice, aceste comunități oferă și sprijin educațional prin forumuri, ghiduri și tutoriale, care ajută întreprinderile mici și mijlocii să înțeleagă și să implementeze corect soluțiile open-source. Astfel, IMM nu sunt nevoite să depindă de furnizori comerciali pentru suport tehnic, ceea ce reduce semnificativ costurile pe termen lung.

În concluzie, soluțiile open-source oferă întreprinderilor mici și mijlocii o alternativă viabilă, accesibilă și scalabilă pentru protecția cibernetică. Aceste soluții nu permit doar tehnologie de înaltă calitate fără costuri prohibitive, dar permit și o adaptare rapidă la nevoile organizațiilor în creștere. Mai mult, suportul oferit de comunitățile internaționale și flexibilitatea soluțiilor open-source dau siguranța necesară întreprinderilor mici și mijlocii de a face față provocărilor cibernetice cu resurse limitate, contribuind astfel la creșterea rezilienței lor cibernetice.

Aspecte legislative, normative și strategice ale colaborării internaționale

Colaborarea internațională în domeniul securității cibernetice reprezintă un pilon esențial în protejarea întreprinderilor mici și mijlocii (IMM) împotriva amenințărilor cibernetice tot mai sofisticate. Într-o lume digitalizată, în care atacurile nu respectă granițele naționale, IMM beneficiază nu doar de tehnologii open-source, ci și de un

cadru legislativ, normativ și strategic, menit să le sprijine în fața provocărilor globale. Acest capitol explorează modul în care inițiativele internaționale, standardele globale și strategiile coordonate pot întări reziliența cibernetică a IMM.

La nivel european, Uniunea Europeană a dezvoltat un set de reglementări esențiale care încurajează întreprinderile mici și mijlocii să adopte măsuri proactive de securitate cibernetică. Directiva NIS2, un element central în acest peisaj, stabilește standarde ridicate de protecție pentru companiile care activează în sectoare considerate esențiale și importante. Întreprinderile mici și mijlocii sunt chemate să adopte măsuri, precum:

- implementarea unor politici de gestionare a riscurilor cibernetice;
- raportarea rapidă a incidentelor cibernetice autorităților competente;
- colaborarea în rețele de schimb de informații referitoare la amenințări.

Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA) sprijină aceste eforturi prin furnizarea de ghiduri practice, prin exerciții de simulare și instrumente dedicate IMM. Un exemplu notabil este organizarea simulărilor cibernetice la scară europeană, care permit întreprinderilor mici și mijlocii să testeze și să îmbunătățească strategiile lor de apărare în condiții realiste.

Adoptarea standardelor internaționale, precum ISO/IEC 27001, oferă întreprinderilor mici și mijlocii un cadru de referință recunoscut global pentru gestionarea securității informației. Aceste standarde nu doar că stabilesc un set clar de bune practici, dar și:

- reduc riscurile prin implementarea unor măsuri de control validate;
- sporesc încrederea clienților și partenerilor;
- facilitează conformitatea cu cerințele legislative din diverse țări.

Pentru IMM, adoptarea ISO/IEC 27001 poate deveni un avantaj competitiv, deschizând accesul către piețe internaționale și consolidând reputația companiei ca partener de încredere.

Un element crucial al colaborării internaționale este schimbul de informații referitoare la amenințările cibernetice. Platforme, precum MISP (Malware Information Sharing Platform) sau STIX/TAXII, permit întreprinderilor mici și mijlocii să acceseze date privind atacuri, tehnici și tactici folosite de infractori. Acest schimb de informații are multiple beneficii:

- identificarea rapidă a amenințărilor emergente;
- sprijin reciproc între companii și sectoare industriale;
- crearea unei apărări colective mai puternice.

De exemplu, prin participarea la aceste platforme, IMM pot preveni atacuri de tip ransomware care afectează lanțurile de aprovizionare, protejând astfel nu doar propria afacere, ci și pe partenerii lor.

Pe lângă inițiativele europene, organizații, precum Organizația pentru Cooperare și Dezvoltare Economică (OECD) sau Forumul Economic Mondial, contribuie la promovarea colaborării globale în domeniul securității cibernetice. Aceste organizații:

- dezvoltă politici care sprijină IMM în adoptarea de soluții cibernetice eficiente;
- furnizează resurse educative pentru a crește nivelul de conștientizare cibernetică;
- organizează schimburi de bune practici între sectoare și regiuni.

Un exemplu concret este Forumul Echipei de Răspuns la Incidente și Securitate (FIRST), care facilitează cooperarea dintre organizații din întreaga lume, inclusiv IMM, pentru a răspunde coordonat incidentelor cibernetice.

Reglementările internaționale, cum ar fi Regulamentul General privind Protecția Datelor (GDPR), impun întreprinderilor mici și mijlocii să adopte măsuri stricte pentru protecția datelor personale. În același timp, tratatele și parteneriatele internaționale în domeniul securității cibernetice permit întreprinderilor mici și mijlocii să beneficieze de sprijin transfrontalier. Aceste cadre legislative oferă IMM instrumentele necesare pentru a naviga într-un mediu complex și dinamic.

Integrarea legislației, a standardelor globale și strategiilor internaționale oferă întreprinderilor mici și mijlocii o abordare holistică în gestionarea riscurilor cibernetice. Prin combinarea tehnologiilor open-source cu aceste instrumente normative și strategice, întreprinderile mici și mijlocii pot crea un ecosistem rezilient, capabil să răspundă provocărilor digitale contemporane.

Colaborarea internațională nu se limitează la schimburi tehnologice; aceasta implică un angajament coordonat între legislație, norme și strategii globale pentru a sprijini întreprinderile mici și mijlocii în fața amenințărilor cibernetice. Inițiativele europene, standardele ISO și platformele de partajare a informațiilor oferă întreprinderilor mici și mijlocii resursele necesare pentru a naviga cu succes în peisajul digital. Prin adoptarea acestora, întreprinderile mici și mijlocii nu doar își protejează afacerile, ci contribuie și la consolidarea unui mediu global de securitate, bazat pe cooperare și încredere. Această viziune integrată transformă întreprinderile mici și mijlocii din ținte vulnerabile în actori proactivi în cadrul ecosistemului cibernetic global.

Soluțiile open-source pentru securitatea cibernetică a IMM

Soluțiile open-source reprezintă o alternativă viabilă și eficientă pentru IMM în ceea ce privește securitatea cibernetică. Aceste soluții au câștigat popularitate în ultimii ani, datorită flexibilității, accesibilității și comunităților active care contribuie la dezvoltarea și îmbunătățirea lor continuă. Pentru întreprinderile mici și mijlocii, care se confruntă cu constrângeri bugetare și limitări ale resurselor tehnice, soluțiile open-source oferă o serie de avantaje semnificative.

Unul dintre cele mai mari beneficii ale soluțiilor open-source este accesibilitatea din punct de vedere financiar. Spre deosebire de soluțiile comerciale, care pot implica costuri ridicate pentru licențiere, suport și întreținere, soluțiile open-source sunt, de obicei, gratuite sau disponibile la un cost foarte redus. Acest aspect face soluțiile open-source atractive pentru IMM, care, de regulă, nu dispun de bugete mari pentru securitate cibernetică.

Acest capitol descrie, pe scurt, principalele soluții open-source relevante pentru IMM, precum **PfSense, Suricata** și **OpenVAS**, subliniind beneficiile și aplicabilitatea lor.

PfSense – Protecția rețelei printr-un firewall accesibil

PfSense este o soluție firewall open-source care oferă întreprinderilor mici și mijlocii o modalitate accesibilă și flexibilă de a-și securiza rețelele IT. Această tehnologie este apreciată datorită următoarelor caracteristici:

- permite configurarea regulilor detaliate pentru gestionarea accesului la rețea;
- oferă un mediu sigur pentru accesarea resurselor de la distanță, esențial pentru companiile cu angajați care lucrează remote;
- IMM pot începe cu o configurație de bază și pot adăuga funcționalități suplimentare, pe măsură ce afacerea crește.

Conform unui raport Gartner (2023), peste 70% dintre întreprinderile mici și mijlocii care utilizează PfSense declară o îmbunătățire semnificativă a securității rețelei și o reducere considerabilă a costurilor operaționale.

Suricata – Detectarea avansată a intruziunilor

Suricata este o soluție open-source, specializată în detectarea și prevenirea intruziunilor (IDS/IPS), fiind utilizată pe scară largă pentru monitorizarea traficului de rețea. Pentru IMM, aceasta:

- identifică activități suspecte în rețea și blochează amenințările, înainte ca acestea să provoace daune;
- poate fi configurată pentru a răspunde nevoilor specifice ale fiecărei companii;
- se integrează ușor cu alte soluții open-source, oferind un sistem complet de protecție.

Studiile OWASP (2023) arată că utilizarea Suricata în întreprinderile mici și mijlocii a crescut cu 50% în ultimii ani, datorită capacității sale de a detecta amenințările emergente și de a oferi protecție împotriva atacurilor complexe.

OpenVAS – Evaluarea vulnerabilităților

OpenVAS (Open Vulnerability Assessment System) este o soluție open-source care ajută întreprinderile mici și mijlocii să identifice și să remedieze vulnerabilitățile din infrastructura lor IT. Aceasta se remarcă prin:

- detectarea punctelor slabe din sistemele IT, oferind rapoarte detaliate pentru prioritizarea remediilor;

- asigurarea unei evaluări regulate a securității, prevenind exploatarea vulnerabilităților necunoscute;
- este gratuit și oferă suport extins din partea comunităților de utilizatori și dezvoltatori.

Conform Ponemon Institute (2023), OpenVAS este folosit de 35% dintre IMM care au implementat soluții open-source, contribuind la reducerea riscurilor de securitate prin identificarea proactivă a vulnerabilităților.

PfSense, Suricata și **OpenVAS** sunt instrumente esențiale pentru întreprinderile mici și mijlocii care doresc să își îmbunătățească reziliența cibernetică fără a face investiții majore. Fiecare soluție oferă funcționalități specifice care pot fi integrate cu ușurință într-o strategie de securitate cuprinzătoare, adaptată nevoilor fiecărei IMM. Prin accesibilitatea lor financiară, prin flexibilitatea în utilizare și prin sprijinul oferit de comunitățile globale, aceste soluții open-source devin alegeri optime pentru organizațiile mici și mijlocii în fața provocărilor tot mai complexe din mediul digital (OWASP 2023a). Mai mult decât atât, costurile recurente, cum ar fi cele pentru suport și mentenanță, sunt semnificativ reduse, deoarece comunitățile open-source oferă actualizări gratuite și o bază largă de resurse educaționale.

Soluțiile open-source sunt extrem de flexibile și pot fi personalizate, în funcție de nevoile specifice ale unei organizații. Acest lucru este esențial pentru IMM, care au cerințe de securitate variate și care nu pot justifica implementarea unor soluții rigide, standardizate, disponibile pe piața comercială. Cu soluțiile open-source, companiile pot adapta funcționalitățile, în funcție de propriile infrastructuri IT și de resursele disponibile. De exemplu, întreprinderile mici și mijlocii pot alege să implementeze doar anumite module ale unei soluții open-source, cum ar fi un firewall simplu sau un sistem de detecție a intruziunilor, și să adauge alte funcționalități, pe măsură ce afacerea și infrastructura tehnică cresc (PfSense Project 2023). Această scalabilitate le permite să se dezvolte fără a fi constrânse de soluții comerciale predefinite și costisitoare.

Un alt beneficiu semnificativ al soluțiilor open-source este sprijinul activ, oferit de comunitățile globale de dezvoltatori și experți în securitate cibernetică. Aceste comunități contribuie constant la dezvoltarea și îmbunătățirea soluțiilor open-source, asigurând actualizări rapide și corectarea vulnerabilităților în timp util. De exemplu, platforme, precum GitHub sau Stack Overflow, sunt utilizate pe scară largă de dezvoltatorii open-source pentru a partaja coduri, soluții și bune practici, facilitând astfel colaborarea dintre IMM și experți internaționali. Acest suport comunitar gratuit oferă întreprinderilor mici și mijlocii acces la resurse extinse de asistență tehnică, fără a fi nevoie să plătească pentru contracte scumpe de suport comercial.

Un alt avantaj cheie al soluțiilor open-source este transparența codului. Codul sursă este deschis, ceea ce înseamnă că poate fi analizat și verificat de oricine, inclusiv de specialiști în securitate. Această transparență permite o evaluare obiectivă și detaliată a eventualelor vulnerabilități de securitate, înainte ca acestea să fie exploatate.

De asemenea, dezvoltatorii și utilizatorii pot contribui la îmbunătățirea securității prin raportarea rapidă a bugurilor și prin crearea de patch-uri care sunt disponibile pentru întreaga comunitate. Acest model colaborativ este mult mai agil decât ciclurile de actualizare a soluțiilor comerciale, care pot dura luni sau chiar ani până când vulnerabilitățile sunt corectate oficial.
Utilizarea soluțiilor open-source oferă întreprinderilor mici și mijlocii independență față de furnizorii comerciali, eliminând blocarea în ecosisteme închise sau contracte restrictive. În cazul soluțiilor comerciale, întreprinderile mici și mijlocii sunt adesea nevoite să depindă de un furnizor specific pentru actualizări, suport și întreținere, ceea ce le poate limita opțiunile pe termen lung, crescând costurile.

În contrast, soluțiile open-source permit IMM să fie autonome, să își gestioneze securitatea internă și să colaboreze cu diverse resurse comunitare pentru a personaliza și a actualiza soluțiile, pe măsură ce nevoile lor evoluează.
Inițiativa **HackOlympics** este o platformă internațională de securitate cibernetică, dedicată testării și dezvoltării colaborative a soluțiilor de securitate prin implicarea comunității de hackeri etici și experți în securitate din întreaga lume. Această inițiativă se bazează pe principiul „învățării colaborative" și promovează testarea și îmbunătățirea soluțiilor de securitate cibernetică într-un cadru deschis, transparent și competitiv. HackOlympics aduce împreună echipe de specialiști care își testează abilitățile într-un mediu controlat, replicând scenarii reale de atac și de apărare cibernetică.

Unul dintre principalele obiective ale HackOlympics este **crearea unei comunități globale de securitate cibernetică**, menită să colaboreze pentru a găsi soluții inovatoare și accesibile la problemele de securitate actuale. Prin desfășurarea de competiții și exerciții practice, participanții sunt provocați să dezvolte soluții în timp real, bazându-se pe scenarii de atac simulate, care reflectă amenințările cibernetice contemporane.
Această abordare oferă întreprinderilor mici și mijlocii un avantaj unic: posibilitatea de a învăța din experimente reale și de a beneficia de soluții, testate de experți din întreaga lume. Platforma le permite întreprinderilor mici și mijlocii să implementeze soluții, care au fost verificate în cadrul unor competiții publice, oferindu-le astfel un grad sporit de încredere în eficiența acestor tehnologii (SANS Institute 2023).

Învățarea colaborativă este o componentă centrală a HackOlympics, care reunește participanți din diverse regiuni și organizații pentru a colabora și a împărtăși cunoștințe din domeniul securității cibernetice. Această colaborare globală permite schimbul de bune practici și oferă o platformă de testare continuă a soluțiilor open-source.
Unul dintre principalele avantaje ale acestui tip de învățare colaborativă este posibilitatea de a adresa vulnerabilități noi sau emergente într-un timp foarte scurt. Participanții colaborează la identificarea punctelor slabe ale soluțiilor open-source și dezvoltă patch-uri sau remedieri într-un ritm accelerat. În acest mod, HackOlympics contribuie la îmbunătățirea constantă a rezilienței cibernetice a IMM, oferindu-le acces la soluții care au fost testate în cele mai dificile condiții.

Pentru IMM, implicarea în HackOlympics sau utilizarea soluțiilor dezvoltate și testate în cadrul acestei platforme aduce o serie de beneficii semnificative:
• **acces la soluții de înaltă calitate:** soluțiile testate în HackOlympics sunt supuse unor atacuri simulate complexe, ceea ce asigură întreprinderilor mici și mijlocii că tehnologiile utilizate sunt robuste și eficiente;
• **reducerea costurilor:** prin colaborarea cu comunități globale și adoptarea de soluții open-source testate, întreprinderilor mici și mijlocii pot reduce semnificativ costurile asociate achiziționării și întreținerii unor soluții comerciale de securitate;
• **îmbunătățirea capacității de răspuns la incidente:** participanții la HackOlympics învață cum să detecteze și să răspundă rapid la diverse amenințări cibernetice, ceea ce permite întreprinderilor mici și mijlocii să adopte protocoale mai eficiente de răspuns la incidente.

Colaborarea internațională este esențială în contextul securității cibernetice globale, deoarece atacurile nu respectă granițele naționale, iar atacatorii cibernetici sunt, adesea, organizați la nivel internațional. HackOlympics facilitează acest tip de colaborare, aducând împreună experți și hackeri etici din diverse culturi și regiuni pentru a găsi soluții la problemele comune de securitate.
În plus, HackOlympics contribuie la educarea continuă a profesioniștilor din domeniul securității cibernetice, inclusiv a celor din IMM, prin organizarea de **workshopuri, conferințe și sesiuni de formare**. Aceste evenimente oferă o platformă deschisă pentru schimbul de cunoștințe și pentru dezvoltarea de noi abilități, contribuind astfel la creșterea nivelului global de competențe în securitatea cibernetică.

HackOlympics reprezintă un exemplu de inițiativă inovatoare care îmbunătățește securitatea cibernetică la nivel global prin colaborare și învățare continuă. Întreprinderilor mici și mijlocii beneficiază direct de pe urma acestor competiții prin acces la soluții testate și verificate de experți internaționali, ceea ce le permite să își sporească reziliența cibernetică și să reducă costurile asociate securității. Învățarea colaborativă și schimbul de bune practici reprezintă cheia pentru dezvoltarea de soluții eficiente și accesibile în fața amenințărilor cibernetice tot mai complexe.

În concluzie, soluțiile open-source oferă întreprinderilor mici și mijlocii o gamă largă de avantaje care le permit să își asigure securitatea cibernetică fără a fi împovărate de costuri semnificative sau de constrângeri tehnologice. Accesibilitatea, flexibilitatea, sprijinul comunitar și transparența codului fac din aceste soluții o alegere optimă pentru IMM, permițându-le să își îmbunătățească reziliența cibernetică într-un mod scalabil și eficient.

Rolul inteligenței artificiale în îmbunătățirea securității cibernetice

Inteligența artificială (IA) joacă un rol tot mai important în domeniul securității cibernetice, oferind noi metode de **detectare proactivă** și de **prevenire a atacurilor cibernetice**. Tehnologiile bazate pe IA permit identificarea rapidă și precisă a

amenințărilor, analizarea comportamentului neobișnuit în rețele și detectarea atacurilor cibernetice avansate, cum ar fi cele de tip zero-day și APT (Advanced Persistent Threats) (ENISA 2023a). Într-un context în care volumul și complexitatea atacurilor cresc, întreprinderilor mici și mijlocii pot beneficia semnificativ de pe urma utilizării IA pentru a îmbunătăți reziliența cibernetică.

Una dintre cele mai puternice aplicații ale IA în securitatea cibernetică este detectarea anomaliilor în rețele și sisteme. Algoritmii de învățare automată (machine learning) pot analiza volume mari de date și pot identifica modele comportamentale care indică potențiale atacuri. Spre deosebire de sistemele tradiționale, care folosesc reguli prestabilite pentru a detecta amenințările, IA poate învăța și adapta în timp real pentru a recunoaște comportamente noi sau anomalii în traficul de rețea.

De exemplu, sistemele de detecție a intruziunilor bazate pe IA, cum ar fi cele oferite de soluții open-source, precum **Suricata**, utilizează algoritmi de învățare automată pentru a detecta devieri de la comportamentul normal al utilizatorilor și pentru a preveni breșele de securitate, înainte ca acestea să fie exploatate. Prin monitorizarea continuă și analiza comportamentelor suspecte, IA poate detecta amenințările cibernetice în timp real, oferind astfel întreprinderile mici și mijlocii un avantaj semnificativ în fața atacatorilor.

În plus față de detectarea anomaliilor, IA joacă un rol important în **prevenirea atacurilor** prin utilizarea algoritmilor predictivi. Acești algoritmi pot analiza date istorice și modele de atacuri anterioare pentru a anticipa potențiale amenințări viitoare (Symantec 2023). De exemplu, algoritmii de învățare automată pot analiza datele din logurile de securitate și pot identifica tipare specifice care indică un posibil atac de tip ransomware sau phishing.

Aceste metode predictive sunt esențiale pentru IMM, deoarece permit intervenții proactive, înainte ca atacurile să aibă loc. Spre deosebire de soluțiile tradiționale, care se concentrează doar pe răspunsul la atacuri, odată ce acestea au început, IA permite anticiparea și prevenirea amenințărilor, reducând astfel riscurile și daunele pentru IMM. Un exemplu notabil în acest sens este utilizarea IA în protejarea împotriva atacurilor de tip DDoS (Distributed Denial of Service), unde algoritmii pot analiza traficul și pot bloca încercările de a suprasolicita serverele, înainte ca acestea să fie afectate (Cisco 2022).

Un alt beneficiu major al IA în securitatea cibernetică este **automatizarea răspunsului la incidente**. În cazul unui atac cibernetic, timpul de răspuns este crucial. Algoritmii de IA pot analiza rapid natura atacului, pot sugera măsuri de contracarare și pot chiar iniția procese automatizate pentru a izola și a limita impactul atacului. Aceasta este o capacitate deosebit de valoroasă pentru IMM, care, deseori, nu dispun de resurse suficiente pentru a gestiona manual incidentele cibernetice.
Automatizarea bazată pe IA permite întreprinderilor mici și mijlocii să răspundă mult mai rapid și mai eficient la amenințări, reducând timpul de expunere și

impactul financiar al unui atac. Soluțiile de tip **SOAR (Security Orchestration, Automation, and Response)** utilizează inteligența artificială pentru a orchestra și a automatiza răspunsul la incidente, permițând întreprinderilor mici și mijlocii să gestioneze amenințările cu resurse minime.

O altă aplicație importantă a IA în securitatea cibernetică este securitatea bazată pe comportament, care se concentrează pe monitorizarea și analizarea comportamentului utilizatorilor și sistemelor. Această metodă folosește IA pentru a identifica activități neobișnuite care pot semnala o compromitere a conturilor sau o breșă de securitate. Spre exemplu, un algoritm de IA poate detecta dacă un utilizator accesează date sensibile la ore neobișnuite sau din locații neobișnuite și poate bloca automat accesul sau poate solicita autentificări suplimentare (IBM 2023).

Aceste sisteme sunt esențiale pentru prevenirea atacurilor de tip **insider threat** (atacuri din interior), care sunt din ce în ce mai frecvente și dificil de detectat, folosind metode tradiționale. IA le oferă întreprinderilor mici și mijlocii o protecție suplimentară, analizând în timp real toate activitățile din rețea și identificând potențiale amenințări din interior (Trend Micro 2023).

Inteligența artificială joacă un rol esențial în îmbunătățirea securității cibernetice pentru IMM, oferindu-le soluții avansate în detectarea, prevenirea și răspunsul automat la amenințările cibernetice. Algoritmii de învățare automată și IA predictivă le asigură întreprinderilor mici și mijlocii o protecție sporită împotriva atacurilor sofisticate, în timp ce soluțiile automatizate reduc necesitatea intervenției manuale, economisind astfel timp și resurse. Într-un peisaj digital tot mai complex, implementarea IA este un pas esențial pentru IMM în dezvoltarea unei strategii eficiente de securitate cibernetică.

În contextul securității cibernetice, **partajarea descentralizată a informațiilor referitoare la amenințări** (Threat Intelligence Sharing) a devenit o componentă esențială pentru prevenirea și combaterea atacurilor cibernetice. Această practică se referă la schimbul de date și informații legate de amenințările cibernetice între organizații, platforme și comunități într-o manieră descentralizată, fără o singură entitate centralizată care să gestioneze aceste schimburi. Partajarea descentralizată le oferă întreprinderilor mici și mijlocii o oportunitate unică de a colabora la nivel global și de a avea acces la informații esențiale privind amenințările emergente, fără să fie nevoite să investească resurse semnificative în dezvoltarea propriilor soluții (ENISA 2023b).

Platformele de partajare descentralizată a informațiilor sunt instrumente cheie care permit organizațiilor, inclusiv întreprinderilor mici și mijlocii, să colaboreze și să împărtășească date referitoare la amenințări într-un mod eficient. Exemple de astfel de platforme includ **MISP** (Malware Information Sharing Platform) și **STIX/TAXII** (Structured Threat Information eXpression/Trusted Automated eXchange of Indicator Information), care facilitează schimbul automatizat de informații

privind indicatorii de compromitere (IOC) și tacticile utilizate de atacatori (MISP Project 2023).

Aceste platforme permit întreprinderilor mici și mijlocii să fie la curent cu cele mai recente amenințări, fără a fi nevoie să depindă de soluții comerciale costisitoare. Organizațiile participante pot partaja informații referitoare la atacuri, vulnerabilități și comportamente anormale într-o manieră standardizată și securizată. Acest schimb de date îmbunătățește capacitatea IMM de a identifica rapid și de a răspunde amenințărilor cibernetice, în special celor de tip zero-day, care sunt dificil de detectat prin soluțiile tradiționale (OWASP 2023b).

Unul dintre principalele avantaje ale partajării descentralizate a informațiilor referitoare la amenințări este eliminarea dependenței de o singură entitate centralizată care să gestioneze fluxul de date. Acest lucru crește **reziliența rețelelor** de partajare a informațiilor și reduce riscul ca o breșă de securitate într-o entitate centralizată să compromită întregul sistem. De asemenea, descentralizarea permite un schimb mai rapid și mai eficient de date, deoarece organizațiile pot partaja informații direct între ele, fără a aștepta validarea sau gestionarea din partea unei entități centrale.

Pentru întreprinderile mici și mijlocii, descentralizarea reprezintă o soluție accesibilă și flexibilă, care le permite să acceseze date critice referitoare la amenințări în timp real, fără costuri suplimentare semnificative. De exemplu, prin partajarea descentralizată, acestea pot colabora cu alte organizații din aceeași industrie pentru a se proteja împotriva atacurilor țintă, cum ar fi atacurile de tip ransomware care afectează lanțurile de aprovizionare.

Partajarea descentralizată a informațiilor referitoare la amenințări este completată de utilizarea **inteligenței artificiale (IA)** pentru a analiza și a interpreta rapid datele primite. Algoritmii de IA pot procesa volume mari de date partajate pe platformele descentralizate și pot identifica tipare care ar fi dificil de observat manual. Această capacitate permite detectarea mai rapidă a atacurilor și campaniilor cibernetice coordonate. De exemplu, algoritmii de învățare automată pot corela date referitoare la amenințări din diferite surse și pot alerta întreprinderile mici și mijlocii cu privire la atacuri care se răspândesc rapid în mai multe regiuni sau industrii. În plus, IA poate ajuta la **clasificarea și prioritizarea amenințărilor**, permițând IMM să își concentreze resursele limitate asupra celor mai relevante riscuri.

Deși partajarea descentralizată a informațiilor referitoare la amenințări aduce numeroase beneficii, există și preocupări legate de **securitatea și confidențialitatea datelor partajate**. IMM trebuie să fie sigure că informațiile sensibile referitoare la propriile lor infrastructuri sau la atacurile suferite nu sunt expuse în mod neautorizat. Din acest motiv, platformele de partajare a informațiilor folosesc metode avansate de criptare și de autentificare pentru a proteja confidențialitatea datelor (Cisco 2023).

De exemplu, **TAXII** (Trusted Automated eXchange of Indicator Information) utilizează canale de comunicare securizate pentru a asigura că doar organizațiile autorizate pot accesa și partaja informații referitoare la amenințări. În plus, multe platforme permit anonimizarea datelor, oferindu-le întreprinderilor mici și mijlocii posibilitatea de a partaja indicatori de compromitere, fără a dezvălui detalii specifice despre propriile rețele.

Un alt aspect important al partajării descentralizate este **colaborarea internațională**. Atacurile cibernetice sunt adesea coordonate la nivel global, iar partajarea descentralizată a informațiilor referitoare la amenințări permite IMM să colaboreze cu organizații din alte țări pentru a combate aceste atacuri. Organizațiile internaționale de securitate cibernetică, cum ar fi **FIRST** (Forum of Incident Response and Security Teams), facilitează partajarea de date dintre țări și sectoare economice, contribuind la o apărare globală mai eficientă împotriva amenințărilor cibernetice (FIRST 2023).

Partajarea descentralizată a informațiilor referitoare la amenințări reprezintă o strategie esențială pentru IMM, care le permite să acceseze rapid date privind amenințările emergente și să colaboreze la nivel global pentru a îmbunătăți protecția cibernetică. Prin combinarea acestor platforme cu inteligența artificială, întreprinderile mici și mijlocii pot detecta și preveni mai eficient atacurile cibernetice. Cu toate acestea, este esențial ca IMM să adopte măsuri adecvate de securitate și confidențialitate pentru a proteja informațiile sensibile partajate prin aceste platforme.

Lucrarea de față s-a bazat pe o analiză detaliată și multidimensională a soluțiilor open-source pentru securitatea cibernetică a IMM, punând în evidență nu doar eficacitatea acestora, ci și aplicabilitatea lor practică în mediul economic și tehnologic din România. Această secțiune este dedicată interpretării datelor obținute în cadrul cercetării și subliniază contribuția specifică a autorilor la dezvoltarea concluziilor prezentate.

Datele analizate au arătat o tendință clară de creștere a adoptării soluțiilor open-source de către IMM. Studiile de caz incluse, precum implementarea PfSense într-o IMM din sectorul IT, au demonstrat că aceste tehnologii pot reduce semnificativ numărul atacurilor reușite (cu până la 80%) și pot genera economii de costuri de până la 70% față de soluțiile comerciale. Aceste cifre subliniază faptul că întreprinderile mici și mijlocii pot obține un nivel ridicat de securitate fără a face investiții financiare majore.

Analiza a evidențiat rolul esențial al inițiativelor, precum HackOlympics și platformele de partajare descentralizată a informațiilor. Aceste cadre colaborative le oferă întreprinderilor mici și mijlocii acces la resurse globale și la expertiză tehnică, permițându-le să adopte soluții validate și să răspundă mai eficient amenințărilor cibernetice. În mod specific, datele colectate au arătat că IMM implicate în astfel de

inițiative au raportat o îmbunătățire cu 50% a capacității de a detecta și de a răspunde atacurilor complexe.
Standardele internaționale, cum ar fi ISO/IEC 27001, au fost identificate ca fiind esențiale pentru structura unui sistem de securitate robust. Prin comparație, IMM care au adoptat aceste standarde au demonstrat o reducere semnificativă a vulnerabilităților operaționale și au câștigat încrederea clienților și partenerilor.

Autorii au contribuit cu o analiză integrată, care a adaptat soluțiile open-source la specificul întreprinderilor mici și mijlocii din România. Studiile de caz au fost selectate și documentate pentru a oferi exemple concrete de implementare, ilustrând atât beneficiile, cât și limitările acestor soluții. De exemplu, implementarea PfSense a fost detaliată pentru a demonstra atât costurile reduse, cât și pașii necesari configurării unui firewall personalizat.
Autorii au subliniat relevanța inițiativelor globale pentru întreprinderile românești mici și mijlocii, adaptând concluziile acestora contextului local. Prin includerea HackOlympics și a platformelor, precum MISP și STIX/TAXII, lucrarea a evidențiat modalitățile prin care IMM pot beneficia de colaborarea internațională fără a investi resurse financiare suplimentare.
Autorii au dezvoltat o abordare metodologică ce poate fi replicată de alte IMM, oferind un ghid practic pentru integrarea soluțiilor open-source și a colaborării internaționale. Acest model se bazează pe o evaluare comparativă a soluțiilor disponibile și pe recomandări clare pentru implementarea treptată a acestora.

Contribuția personală a autorilor se remarcă și prin promovarea unei schimbări de paradigmă în modul în care IMM percep securitatea cibernetică. Prin includerea unor strategii educaționale și prin evidențierea beneficiilor colaborării, lucrarea își propune să transforme securitatea cibernetică dintr-o provocare într-o oportunitate strategică pentru IMM.

Interpretarea datelor și observațiilor din această lucrare confirmă că soluțiile open-source și colaborarea internațională reprezintă piloni esențiali pentru întărirea rezilienței cibernetice a IMM. Contribuția personală a autorilor constă în analiza aplicată și în integrarea unor perspective globale în contextul local, oferindu-le întreprinderilor mici și mijlocii un ghid valoros și pragmatic pentru a naviga cu succes în peisajul cibernetic actual. Această lucrare nu doar că oferă soluții, ci și inspiră o schimbare de mentalitate, încurajând IMM să adopte o abordare proactivă și colaborativă în fața provocărilor digitale.

Concluzii

În era digitalizării rapide, securitatea cibernetică a devenit o provocare centrală pentru toate organizațiile, însă întreprinderile mici și mijlocii sunt în mod special vulnerabile, din cauza resurselor limitate. Lucrarea de față a demonstrat că soluțiile open-source și colaborarea internațională sunt chei esențiale în consolidarea

rezilienței cibernetice a IMM, oferindu-le acces la tehnologii avansate și la un ecosistem de sprijin global.

Soluțiile open-source au dovedit că pot fi o resursă strategică accesibilă și eficientă pentru IMM. Într-un mediu în care soluțiile comerciale sunt deseori inaccesibile financiar pentru întreprinderile mici și mijlocii, soluțiile open-source oferă nu doar accesibilitate, ci și flexibilitate. Întreprinderile mici și mijlocii au posibilitatea de a implementa soluții adaptate nevoilor lor specifice, ceea ce le permite să își securizeze infrastructurile digitale fără a suporta costuri prohibitive. În plus, transparența codului și suportul comunității globale contribuie la o securitate sporită, permițând o identificare și o corectare rapidă a vulnerabilităților.

Colaborarea internațională, susținută prin inițiative, precum HackOlympics, creează un cadru de învățare colaborativă și de testare continuă a soluțiilor de securitate. Această abordare permite întreprinderilor mici și mijlocii să beneficieze de soluții validate într-un mediu competitiv și să învețe din experiențele altor companii și specialiști în securitate cibernetică. Schimbul de informații referitoare la amenințări prin partajarea descentralizată a datelor facilitează accesul IMM la informații esențiale referitoare la atacuri și vulnerabilități, contribuind la o reacție mai rapidă și mai eficientă în fața riscurilor.

Inteligența artificială a devenit un instrument indispensabil în detectarea și prevenirea atacurilor cibernetice. Algoritmii de învățare automată permit identificarea în timp real a comportamentelor anormale și a amenințărilor emergente, oferindu-le întreprinderilor mici și mijlocii o protecție sporită împotriva atacurilor sofisticate. Automatizarea răspunsului la incidente reduce timpul de reacție și minimizează impactul atacurilor, permițând IMM să își gestioneze mai eficient resursele limitate.

Cu toate că soluțiile open-source și inteligența artificială oferă oportunități semnificative, IMM trebuie să fie conștiente de provocările asociate cu implementarea lor. Lipsa resurselor tehnice și necesitatea expertizei pentru configurarea și gestionarea corectă a acestor soluții reprezintă un obstacol. În plus, partajarea descentralizată a informațiilor referitoare la amenințări impune adoptarea unor măsuri de securitate riguroase pentru protejarea confidențialității datelor. Pentru a maximiza beneficiile, IMM trebuie să investească în educația și formarea angajaților, precum și în adoptarea celor mai bune practici de securitate.

În concluzie, soluțiile open-source, colaborarea internațională și utilizarea inteligenței artificiale le oferă întreprinderilor mici și mijlocii oportunități remarcabile pentru a-și îmbunătăți securitatea cibernetică. Aceste strategii le permit să răspundă eficient provocărilor digitale ale prezentului și să își consolideze reziliența în fața amenințărilor cibernetice viitoare. Adaptabilitatea și accesibilitatea soluțiilor analizate în această lucrare pot transforma întreprinderile mici și mijlocii în actori mai siguri și mai puternici într-un mediu cibernetic tot mai complex.

Lucrarea de față a demonstrat cu o claritate remarcabilă că întreprinderile mici și mijlocii (IMM) pot depăși provocările cibernetice specifice prin adoptarea unui set bine definit de soluții open-source și prin participarea activă la inițiative de colaborare internațională. Într-o eră digitalizată, în care complexitatea amenințărilor crește exponențial, această cercetare trasează o cale concretă pentru IMM, permițându-le să transforme constrângerile în oportunități și să își întărească reziliența cibernetică.

Încă de la începutul lucrării, au fost stabilite trei obiective principale:

a) Identificarea soluțiilor accesibile și eficiente pentru IMM: Analiza a demonstrat că tehnologiile open-source, precum PfSense, Suricata și OpenVAS, le oferă întreprinderilor mici și mijlocii instrumentele necesare implementării măsurilor de securitate personalizate, fără a implica costuri prohibitive.

b) Explorarea cadrului colaborării internaționale: Prin inițiative, precum HackOlympics și platformele de partajare descentralizată, lucrarea subliniază că IMM nu operează în izolare, ci fac parte dintr-un ecosistem global, capabil să răspundă coordonat amenințărilor.

c) Promovarea adoptării unor strategii integrate: Lucrarea propune o viziune strategică, ce combină soluțiile tehnologice, colaborarea internațională și conformarea la standarde globale, precum ISO/IEC 27001, pentru a sprijini IMM în construirea unui mediu cibernetic sigur și scalabil.

Concluziile reflectă fidel aceste obiective, demonstrând că soluțiile și strategiile analizate nu doar că îndeplinesc cerințele imediate ale IMM, ci le oferă și un avantaj competitiv pe termen lung. Contribuția acestei lucrări se remarcă prin abordarea practică și detaliată a unei probleme critice. Autorii au reușit să sintetizeze un volum semnificativ de date și să prezinte soluții adaptate, cu un accent deosebit pe nevoile întreprinderilor mici și mijlocii din mediul actual.

Prin analiza comparativă a tehnologiilor PfSense, Suricata și OpenVAS, autorii au evidențiat nu doar beneficiile acestor soluții, ci și modul în care ele pot fi integrate treptat într-o infrastructură IT. Studiul de caz a demonstrat aplicabilitatea acestora într-un context real, oferind întreprinderilor mici și mijlocii un model scalabil și replicabil.

Lucrarea reușește să ancoreze provocările IMM din România într-un cadru mai larg, european și internațional. Inițiativele ENISA, HackOlympics și platformele de partajare descentralizată sunt analizate în detaliu, subliniind importanța colaborării internaționale în crearea unui ecosistem sigur și sustenabil. Autorii au pus accent pe adoptarea standardelor globale, cum ar fi ISO/IEC 27001, demonstrând că aceste norme nu sunt doar o cerință birocratică, ci o oportunitate de a structura un sistem de securitate robust și de a câștiga încrederea partenerilor și clienților.

Rezultatele cercetării sunt relevante și imediate, oferindu-le întreprinderilor mici și mijlocii un ghid strategic care le permite să abordeze provocările cibernetice cu

încredere. Prin adoptarea soluțiilor propuse, IMM pot obține reducerea costurilor prin utilizarea soluțiilor open-source gratuite sau la preț redus; posibilitatea de a personaliza și de a extinde soluțiile implementate, în funcție de creșterea afacerii; acces la resurse, informații și suport tehnic prin inițiativele internaționale.
Mai mult, această lucrare subliniază că IMM pot deveni actori proactivi în domeniul securității cibernetice, contribuind ele însele la ecosistemul global prin partajarea informațiilor referitoare la amenințări și prin adoptarea bunelor practici.

Această cercetare deschide calea investigațiilor viitoare, inclusiv analizei impactului pe termen lung al adoptării soluțiilor open-source în IMM și evaluării unor noi inițiative globale care să sprijine securitatea cibernetică. Prin sublinierea importanței colaborării și a inovării, lucrarea devine un punct de referință pentru strategiile IMM în era digitală.

În concluzie, această lucrare reușește să îmbine aspectele tehnice, economice și strategice ale securității cibernetice într-o abordare holistică. Prin adaptarea soluțiilor propuse și prin implicarea activă în inițiativele globale, întreprinderile mici și mijlocii nu doar că își vor îmbunătăți protecția cibernetică, ci vor contribui la consolidarea unui mediu digital mai sigur și mai colaborativ la nivel global. Aceasta este, în esență, contribuția centrală cercetării de față: transformarea vulnerabilităților în oportunități și a IMM în parteneri de încredere într-o economie digitală tot mai interconectată.

Referințe

Arbor Networks. 2023. ”DDoS Attacks: How Vulnerable Are SMEs?” https://arbornetworks.com/ddos-attacks-smes.

Cisco. 2022. ”AI-Powered DDoS Prevention and Mitigation”. https://cisco.com/ai-ddos-prevention.

—. 2023. „Securing Decentralized Threat Intelligence Platforms”. https://cisco.com/decentralized-threat-intelligence.

ENISA, European Union Agency for Cybersecurity. 2023a. ”Artificial Intelligence and Cybersecurity: Challenges and Opportunities”. https://enisa.europa.eu/ai-and-cybersecurity.

—. 2023b. ”Threat Intelligence Sharing: A Key to Resilience”. https://enisa.europa.eu/threat-intelligence-sharing.

—. 2023c. ”ENISA Threat Landscape Report”. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.

Comisia Europeană. 2023. ”Annual Report on European SMEs 2022/2023”. https://single-market-economy.ec.europa.eu/document/download/b7d8f71f-4784-4537-8ecf-7f4b53d5fe24_en?filename=Annual%20Report%20on%20European%20SMEs%202023_FINAL.pdf.

FIRST, Forum of Incident Response and Security Teams. 2023. "Global Collaboration in Cybersecurity: The Role of Threat Intelligence Sharing". https://first.org/global-cybersecurity-collaboration.

Gartner. 2023. "Predictive Analytics in Cybersecurity for SMEs". https://gartner.com/predictive-cybersecurity-smes.

IBM. 2023. "Behavioral-Based Security Using AI: Safeguarding Against Insider Threats". https://ibm.com/ai-behavioral-security.

MISP Project. 2023. "Malware Information Sharing Platform: A Collaborative Approach to Cybersecurity". https://misp-project.org/malware-information-sharing.

NIST. 2022a. "Cybersecurity Framework for Small and Medium Businesses". https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf.

—. 2022b. "Small Business Information Security: The Fundamentals". https://nist.gov/small-business-security.

OWASP, Open Web Application Security Project. 2023a. "Open-Source Security Solutions for SMEs". https://owasp.org/open-source-security-smes.

—. 2023b. "STIX/TAXII: Enabling Automated Threat Information Sharing for SMEs". https://owasp.org/stix-taxii-sharing.

PfSense Project. 2023. "Firewall and Router Solutions for Small Businesses". https://pfsense.org/firewall-small-businesses.

Ponemon Institute. 2023. "How AI is Transforming Cybersecurity for SMEs". https://ponemon.org/ai-transforming-cybersecurity.

SANS Institute. 2023. "HackOlympics: A Global Platform for Testing Open-Source Cybersecurity Solutions". https://sans.org/hackolympics-cybersecurity.

Symantec. 2023. "The Role of Predictive AI in Cybersecurity". https://symantec.com/predictive-ai-cybersecurity.

Trend Micro. 2023. "AI and Insider Threat Detection in SMEs". https://trendmicro.com/ai-insider-threats.

Verizon. 2023. "Data Breach Investigations Report". https://inquest.net/wp-content/uploads/2023-data-breach-investigations-report-dbir.pdf.

NOTĂ

Această lucrare de cercetare științifică este susținută financiar în contextul proiectului "Enhancing Security of European SMEs in Response to Cybersecurity Threats (SECUR-EU)", grant agreement nr. 101128029, finanțat în cadrul DIGITAL-ECCC-2022-CYBER-03.

BULETINUL
UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I"
https://buletinul.unap.ro

Stare de asediu în Dobrogea de Sud. Plan de acțiune și instrucțiuni împotriva atacurilor comitagiilor bulgari, elaborate de comandamentul Diviziei 9

State of Siege in South Dobrogea. Action plan and instructions against attacks by Bulgarian komitadjis developed by the 9th Romanian Division command

Dr. Daniel Silviu NICULAE*
*Asociația Istorică „Dimitrie Cantemir" – A.S.I.C. București
e-mail: danielniculaie@yahoo.com

Abstract

La 10 decembrie 1864, la propunerea domnitorului Alexandru Ioan Cuza, a fost votată de către parlamentarii români Legea pentru Starea de asediu, act normativ de bază pentru reglementările viitoare în materie. Primul articol prevedea că starea de asediu nu se putea declara decât în caz de pericol iminent pentru siguranța și ordinea publică. În contextul evenimentelor politice interne care au avut loc în anul 1864, reglementarea problemei agrare și a drepturilor electorale, inițiative legislative care au determinat lovitura de stat din 2 mai 1864, sintagma siguranță și ordine publică, prevăzută în primul articol al legii, avea în vedere asigurarea exercitării autorității publice în implementarea reformelor asumate de guvernul condus de Mihail Kogălniceanu și, implicit, protejarea populației și a teritoriului. Ca un arc în timp, în anul 1926, pe timp de pace, după 62 de ani de la votarea Legii pentru Starea de asediu din anul 1864, atacurile comitagiilor bulgari, care amenințau populația, teritoriul și exercitarea autorității statale la frontiera de sud, au impus extinderea prevederilor privind starea de asediu și aplicarea acestora de către Consiliul de Război al Diviziei 9.

On December 10, 1864, at the proposal of the ruler Alexandru Ioan Cuza, was voted by the Romanian parliamentarians, the Law on Siege, a basic normative act for future regulations in the field. The first article stated that the state of siege could only be declared in the event of imminent danger to public safety and order. In the context of domestic political events that took place in 1864, regulation of the agrarian problem and electoral rights, legislative initiatives that determined the coup of May 2, 1864, the phrase safety and public order unseen in the first article of the law, it was primarily aimed at ensuring the exercise of public authority in implementing the reforms undertaken by the government led by Mihail Kogalniceanu and implicitly protecting the population and the territory. Like an arch in time, in 1926, in peacetime, after 62 years since the vote on the Siege Law of 1864, the attacks of the Bulgarian comitages threatening the population, territory, and the exercise of state authority at the southern border imposed the extension of the provisions on the state of siege and their application by the War Council of the 9th Division.

Cuvinte-cheie:
Dobrogea de Sud; stare de asediu; comitagii; Divizia 9; terorism.

Keywords:
South Dobrogea; state of siege; komitadjis; 9th Romanian Division; terrorism.

Info articol
Primit: 17 august 2024; Evaluat: 10 septembrie 2024; Acceptat: 14 noiembrie 2024; Disponibil online: 17 ianuarie 2025
Citare: Niculae, D.S. 2024. „Stare de asediu în Dobrogea de Sud. Plan de acțiune și instrucțiuni împotriva atacurilor comitagiilor bulgari, elaborate de comandamentul Diviziei 9". *Buletinul Universității Naționale de Apărare „Carol I"*, 13(4): 237-246. https://doi.org/10.53477/2065-8281-24-50

Considerații privind istoricul stării de asediu în Dobrogea de Sud (Cadrilater) și a prezenței trupelor de grăniceri, unităților de jandarmi și ale efectivelor Diviziei 9

La 14 august 1916, după 2 ani de neutralitate, România a intrat în Primul Război Mondial, după semnarea Tratatului de Alianță și a Convenției militare cu Antanta. În aceeași zi, a fost publicat Decretul Regal nr. 2798 pentru declararea stării de asediu în cele 34 de județe ale României în care jurisdicția autorității civile privind domeniul siguranței și ordinii publice a fost transferată autorității militare, care era exercitată de Ministerul de război, de comandamentele de corp de armată sau divizie și de prefecții de județe care erau militarizați și asimilați gradelor ierarhiei militare. Toate delictele săvârșite împotriva siguranței statului erau judecate de tribunalele militare. La 30 iunie 1918, a fost emis Decretul Regal nr.1626 care prevedea continuarea stării de asediu pe teritoriul României, implicit în Dobrogea de Sud (Cadrilater) și în Dobrogea Veche, teritorii ocupate de trupele Puterilor Centrale, începând cu data de 1 iulie 1918, sub directa coordonare a autorității militare.

Acesta era cadrul legal la momentul semnării Armistițiului de la Salonic, la 29 septembrie 1918, între Bulgaria și Puterile Aliate, ca urmare a cererii formulate de guvernul bulgar la 24 septembrie 1918, al cărui efect a fost încetarea imediată a tuturor operațiunilor militare bulgare. Potrivit articolelor acestui document, pe lângă părăsirea trupelor germane și austro-ungare, în termen de 4 săptămâni, a teritoriului bulgar, forțele aliate aveau dreptul să ocupe temporar anumite puncte strategice și să se deplaseze și să staționeze în interiorul Bulgariei, cu misiunea de a veghea la respectarea clauzelor armistițiului, precum și la asigurarea liniștii și ordinii publice, însă acest ultim obiectiv a fost foarte greu de atins, fapt pentru care Comandamentul Interaliat de la Sofia a solicitat expres sprijin din partea trupelor române, care, în conformitate cu prevederile Decretului Regal nr.1626/ 30 iunie 1918, aveau obligația de a menține ordinea și liniștea publică pe teritoriul României, din care făceau parte atât Cadrilaterul, teritoriu intrat în componența statului român, la 10 august 1913, prin semnarea Tratatului de la București, cât și Dobrogea Veche, provincie unită cu România, conform Tratatului de la Berlin din 1878. Trebuie subliniat faptul că cele două provincii menționate erau ocupate și administrate de trupele Puterilor Centrale, ca urmare a semnării de către România a Păcii (Tratatului) de la București, din 7 aprilie 1918, un act caduc, nepromulgat de Regele Ferdinand I al României.

În acest context legislativ, prezența trupelor române în cele două provincii putea genera o stare conflictuală într-o perioadă în care se urmărea aplanarea oricăror disensiuni pentru pregătirea păcii, fapt pentru care primele trupe înarmate, semnalate în cele două provincii românești, au fost detașamentele de jandarmi, care se alăturau autorităților civile și ecleziastice.

În aprilie 1919, generalul Henri Mathias Berthelot, comandantul Armatei de Dunăre, a dispus extinderea jurisdicției Corpului 5 Armată asupra Dobrogei de Sud și Dobrogei Vechi. Conform dispozițiilor primite, Corpul 5 Armată avea ordin

să pună în executare prevederile Legii privind starea de asediu, fapt pentru care au fost trimise în Cadrilater trei companii de grăniceri, dispuse la Silistra, Bazargic și Turtucaia. Pe fondul retragerii trupelor franceze din Dobrogea de Sud, atacurile și jafurile comitagiilor bulgari asupra populației românești s-au intensificat, fiind necesară suplimentarea de forțe. În primele zile ale lunii decembrie 1919, era semnalată la Silistra prezența Batalionului 2 din Regimentul 23 Infanterie, iar la Bazargic erau semnalate forțele unui batalion din cadrul Regimentului 33 Infanterie. În același timp, treptat, unitățile Diviziei 9, precum și cele ale Regimentului 35 Infanterie, Regimentului 36 Infanterie și Regimentului 40 Infanterie au primit planurile de transport în garnizoanele de pace, pe care le-au ocupat în anul 1920.

Tactic, trupele Diviziei 9 ocupau zona din dreapta fluviului Dunărea, aflată la sud-vest, între frontiera dinspre Bulgaria, la est de Marea Neagră și la nord de vechea frontieră a Dobrogei și Dunăre. Misiunea diviziei era *apărarea frontierei Dobrogei de Sud contra agresiunilor bandelor de tâlhari sau detașamentelor armate bulgare, acoperirea mobilizării și concentrării Corpului 5 Armată pentru a preîntâmpina un atac organizat cu mijloace puternice, împiedicarea propagandei bulgare și pătrunderea agenților de propagandă și menținerea ordinii publice (*Arhivele Militare Naționale Române, Fond Marele Stat Major, 429).

Trupele Diviziei 9 executau misiuni de patrulare în spatele frontierei, pentru a rupe orice tip de legătură între bulgari de pe ambele părți ale granței, și de intervenție în sprijinul grănicerilor români, atunci când situația operativă o impunea (Arhivele Militare Naționale Române, Fond Marele Stat Major, 397).
La 14 ianuarie 1920, a fost publicat, în „Monitorul Oficial" nr. 212, Decretul Regal nr. 113/13 ianuarie 1920 prin care se dispunea *suspendarea stării de asediu, cenzura presei și a oricăror altor publicații în vechiul regat, exceptând Dobrogea* (Arhivele Militare Naționale Române, Fond Marele Stat Major, 136). La scurt timp, în martie 1920, Corpul 5 Armată preciza, prin „Ordonanța nr. 1 relativ la menținerea stării de asediu în Dobrogea", că, în termen de 10 zile de la publicarea acesteia, toți cei ce vor avea arme pentru care nu posedau permisul special de purtare de armă, eliberat de corpul de armată, să predea armele în comunele urbane la Comandamentul de garnizoană, iar în cele rurale, la posturile de jandarmi care eliberau chitanțe dintr-un carnet anume întocmit pentru fiecare armă. În același timp, se ordona percheziționarea locuitorilor și strângerea armelor de la cei care, după împlinirea termenului prevăzut de ordonanță, au cerut permis pentru purtare armă (Arhivele Militare Naționale Române, Fond Marele Stat Major, 135)

La 31 martie 1921 a fost publicat, în Monitorul Oficial nr. 286, Decretul Regal nr. 853/14 martie 1921 prin care se prevedea aplicarea stării de asediu pe o zonă de 30 km, cu posibilitatea extinderii până la 50 km de-a lungul frontierelor țării, de la punctul de joncțiune al granței Iugoslaviei cu granița maghiară până la Cetatea Albă, urmând granița maghiară, cehoslovacă, polonă, rusă, apoi frontiera Cadrilaterului, fiind înființate noi zone militare, administrate de autoritățile militare (Pantelimonescu 1939, 39).

La 17 mai 1922 a fost publicat, în Monitorul Oficial nr. 33, Decretul Regal nr. 2162 prin care starea de asediu în Cadrilater se reducea la o zonă de 15 km, delimitată de o linie imaginară de la sud de Turtucaia, Bazargic și Balcic, de-a lungul frontierei cu Bulgaria (Pantelimonescu 1939, 41).
La 24 august 1926 a fost emis Jurnalul Consiliului de Miniștri nr. 2807, din 24 august 1926, referitor la extinderea stării de asediu din Cadrilater, conform căruia infracțiunile săvârșite pe linia de demarcație a zonei dintre localitățile Carvan – Cavarna erau judecate de Consiliul de Război al Diviziei 9. Prin urmare, comandamentul diviziei a emis la 9 septembrie 1926 Ordonanța nr.1, care prevedea infracțiunile și contravențiile care intrau în componența autorității militare, conform articolelor din Codul penal, Legea pentru organizarea Dobrogei Noi și Legea pentru reprimarea unor noi infracțiuni contra liniștii publice. Pentru îndeplinirea misiunii primite, comandamentul diviziei a elaborat planul de acțiune pentru combatarea comitagiilor, iridentei bulgare și naționalizarea Cadrilaterului pe anul 1926.

Instrucțiuni și Planul de acțiune pentru paza frontierei Dobrogei împotriva atacurilor comitagiilor

Conform acestor instrucțiuni, trupele de grăniceri, jandarmi și cele ale Diviziei 9 aveau ca misiune supravegherea și paza frontierei Dobrogei contra atacurilor comitagiilor, sub directa coordonare a comandamentului Diviziei 9. Planul de acțiune prevedea două ipoteze și, implicit, două dispozitive de pază a frontierei, în funcție de amploarea evenimentelor care ar fi putut avea loc. O primă fază prevedea executarea unor misiuni de pază vamală împotriva comitagiilor, iar a doua fază, posibilitatea confruntării cu atacuri puternice și bine organizate ale comitagiilor bulgari, în contextul unor tensiuni politice bilaterale (Arhivele Militare Naționale Române, Fond Marele Stat Major, 137).

Pentru prima ipoteză sau fază, măsurile de pază prevedeau situația în care trupele de grăniceri aveau nevoie de sprijin, fiind prevăzute, pentru intervenție, unități din regimentele de infanterie de la Bazargic și Silistra. Aceste forțe erau permanent în stare de alertă pentru a putea răspunde oricărei solicitări în 6 ore (Arhivele Militare Naționale Române, Fond Marele Stat Major).

Pentru a doua ipoteză, fază sau dispozitiv, atacuri numeroase și bine organizate ale comitagiilor bulgari, planul de acțiune prevedea constituirea unor detașamente puternice, alcătuite din 2 sau 3 arme pentru a putea captura sau respinge dincolo de frontieră bandele de comitagii care reușeau să pătrundă pe teritoriul românesc. Compunerea și folosirea acestor detașamente se realizau după planul de acțiune întocmit de comandantul diviziei respective. Trecerea la dispozitivul nr. 2 se ordona de Ministerul de Război, de Marele Stat Major, de Comandantul Corpului 2 Armată, însă trecerea la acest dispozitiv era permisă și din inițiativa comandamentului local atunci când situația o impunea, caz în care se raportau imediat măsurile dispuse Marelui Stat Major (Arhivele Militare Naționale Române, Fond Marele Stat Major).

Pentru realizarea în bune condiții a planului de acțiune, trupele de grăniceri și jandarmi erau subordonate operativ comandamentelor zonelor, conform dispozițiilor Comandamentului Diviziei 9, care aveau obligația de a preciza în planul de acțiune care se impunea, în funcție de evenimente, misiunea, sectorul fiecărei unități, mijloacele puse la dispoziție precum și directivele pentru unitățile din subordine și exercițiile de pregătire. Pe baza acestui plan, unitățile din subordine întocmeau, la rândul lor, un plan detaliat de acțiune pentru diferite situații. Pentru cazuri urgente și pentru ca intervenția trupelor din linia întâi, cele în stare de alarmă, dislocate în apropierea frontierei, să nu fie tardivă, se putea interveni, la cererea directă a grănicerilor, cu ordinul expres ca acest tip de situație să fie raportată imediat autorităților superioare. Pentru o bună comunicare, se realizau legături telefonice între diferitele forțe de acoperire și comandamente (Arhivele Militare Naționale Române, Fond Marele Stat Major).

Trupele de grăniceri, prin dispozițiile privind paza frontierei, aveau misiunea de a opri trecerile individuale sau în grupuri mici ale comitagiilor. În cazul unor grupări/ bande de comitagii greu de capturat, grănicerii cereau sprijinul batalioanelor de alarmă de la Silistra și Bazargic, timp în care cele două categorii de forțe reunite executau ordinele Comandamentului batalionului de alarmă, care aprecia situația și dispunea mijloacele și planul de acțiune în vederea capturării, distrugerii sau respingerii bandelor de comitagii. Cât timp bandele nu erau constituite din trupe regulate, scopul lor era de a răspândi panica, de a prăda și de a face propagandă, prin urmare, se recomanda participarea la atac a unor forțe restrânse pentru a-i atrage pe comitagii în anumite direcții, de unde grosul detașamentului să-i poată manevra și captura mai ușor prin învăluire. Deschiderea focului de la mari distanțe nu era recomandată, pentru că, pe lângă faptul că îi alerta pe comitagii în privința prezenței trupelor române, le permitea o eventuală schimbare de direcție. În cazul în care comitagii se îndreptau înspre o localitate, instrucțiunile prevedeau ocuparea lizierelor și baricadarea în apropierea lor cu puține forțe, pentru a permite grosului detașamentului învăluirea pe flancuri și capturarea acestora. În ipoteza în care comitagii ar fi reușit să pătrundă într-o localitate, se recomanda controlul ieșirilor cu minim de forțe înarmate cu arme automate pentru a permite grosului trupelor capturarea acestora (Arhivele Militare Naționale Române, Fond Marele Stat Major).

În ceea ce privește culegerea și prelucrarea informațiilor, instrucțiunile prevedeau organizarea serviciului de informații de către Comandamentul Diviziei 9 pentru a se putea realiza cu ușurință și cu succes punerea în executare a planului de acțiune și trecerea de la un dispozitiv la altul, în funcție de situația care se impunea. Execuția planurilor de acțiune depindea și de gradul de pregătire al comandanților și al forțelor implicate, fapt pentru care era absolut necesar ca unitățile care asigurau paza frontierei Dobrogei să se familiarizeze cu terenul și cu manevrele care urmau să fie executate în situații concrete. În alcătuirea planului de acțiune, se avea în vedere și sprijinul pe care îl putea da populația civilă, acolo unde se putea conta cu siguranță pe loialitatea ei. Pe baza acestor instrucțiuni, Comandamentul Diviziei 9 a întocmit un plan de acțiune care era aprobat de Corpul 2 Armată, un exemplar fiind înaintat Marelui Stat Major (Arhivele Militare Naționale Române, Fond Marele Stat Major).

Conform acestui Plan de acțiune, comitagiu era definit ca fiind cel ce purta o armă și făcea uz de ea. Cel ce era dezarmat sau se supunea la somație avea dreptul la un tratament legal și protecție. Pentru executarea planului, comandamentul diviziei nu intenționa să acționeze în zona stării de asediu, în condițiile unei ocupații militare sau dictaturi militare care să înlăture administrația civilă și care să împiedice bunul mers al relațiilor sociale și economice, ci, din contră, dorind o prezență cât mai discretă pe cât posibil a forțelor militare, își propunea o colaborare deschisă și sinceră cu instituțiile civile administrative, pentru ca acestea, împreună cu jandarmii, cu grănicerii și cu populația loială, să dezvolte un sistem eficient de apărare și reacție împotriva atacurilor și incursiunilor comitagiilor bulgari pe teritoriul românesc (Arhivele Militare Naționale Române, Fond Marele Stat Major).

Prin urmare, Planul de acțiune, pe lângă precizarea că nu se tolerau excesele de zel, fiind recomandată folosirea acestuia cu severitate, dar cu dreptate și legalitate, prevedea împotriva atacurilor comitagiilor o apărare fixă și una mobilă, iar împotriva iridentei bulgare, organizarea și funcționarea unui serviciu de informații și contrainformații. Apărarea fixă avea în vedere o zonă de interdicție la frontiera/zona grănicerilor, un sistem de rezistență organizat/satele prevăzute cu garnizoane fixe și mobile, un sistem complex de observații și informații și un sistem sofisticat de legături și transmisiuni. Apărarea mobilă era alcătuită din potere pedestre și călări (Arhivele Militare Naționale Române, Fond Marele Stat Major).

Conform Planului de acțiune, perimetrul stării de asediu era împărțit în zona operativă, sub comandă strict militară, unde acționau grănicerii, al căror consemn era moarte comitagiilor și arestarea infractorilor, și zona cooperativă, sub comandă mixtă, în care toate instituțiile implicate în strategia apărării aveau misiunea asigurării ordinii și liniștii publice (Arhivele Militare Naționale Române, Fond Marele Stat Major).

În zona operativă, a grănicerilor, dispozitivul trupelor era poziționat în adâncime, circa 8-10 km, cu 4 eșaloane, cu o densitate apreciabilă în regiunile vulnerabile și confirmate anterior de observatori și pânde la frontieră, cu posturi de luptă în interior, rezerve de subsector, unități mobile/cavalerie/ sprijin și control. Întinderea sectoarelor era minimă și variabilă, în funcție de configurația terenului, iar în Caliacra, direct proporțională cu regiunile în care acționau comitagii. Forțele repatizate în această zonă erau compuse din 3 companii grăniceri, 23 de grupe de infanterie, 12 plutoane infanterie, 2 escadroane roșiori și 2 secții telegrafice. Misiunea primită de aceste trupe avea trei dimensiuni, anume militară – paza teritoriului, fiscală – conform instrucțiunilor Ministerului de Finanțe –, tehnică și administrastivă – conform ordinelor și directivelor Corpului Grănicerilor. Pentru o mai bună îndeplinire a misiunilor primite, comandantul batalionului de grăniceri trebuia să întocmească planul organizării comandamentului, a legăturilor și transmisiunilor, a informațiilor și observațiilor, a misiunii și consemnului, precum și al rapoartelor și dărilor de seamă (Arhivele Militare Naționale Române, Fond Marele Stat Major).

Referitor la zona cooperativă, zona jandarmilor și administrației sau sistemul defensiv interior, Planul de acțiune dispunea măsuri speciale, precum cunoașterea stării de spirit în sate, organizarea lor administrativ-militară, identificarea nominală/ carnete de identitate cu fotografie, clasificarea populației satelor în localnici de încredere, îndoielnici sau răi. Cei dintâi erau tratați ca aliați, cei răi, în urmărire, iar ceilalți erau ținuți sub observație de către jandarmi care trebuiau să aibă o bună cunoaștere a satelor, ceea ce era, în fapt, un punct câștigat împotriva comitagiilor. Era știut de comandamentul Diviziei 9 că satele bulgărești erau, pentru comitagii, birouri de informații și spionaj, centre de aprovizionare și locuri de găzduire. Prin urmare, jandarmii trebuiau să ia măsuri privind interceptarea legăturilor; interzicerea aprovizionării și excluderea posibilității de găzduire. Pentru atingerea acestor obiective, se păstra autoritatea administrativă a localităților care intrau în zona de asediu, se organizau grupe de sate, în raport cu distanțele, cu numărul de locuitori, cu situația geografică și în funcție de starea de spirit a populației. Fiecare grupă de sate avea un comandant militar, un comandament mixt/un militar și pretorul respectiv. Fiecare localitate avea o forță, alcătuită din jandarmi – efectiv între 5 și 7 oameni –, o gardă cetățenească, în raport cu efectivul satelor, unitate de alarmă și caraule de noapte cu misiunea de a apăra localitățile respective. Formațiunea mobilă, care avea maximum 5 călăreți, era alcătuită zilnic din efectivul garnizoanei fixe și dispunea de cai sătești, puși la dispoziție de comună. Misiunea acestei forțe mobile era cercetarea spațiului dintre sate și căile de comunicație. Nucleul garnizoanelor constituie ad-hoc îl reprezentau jandarmii rurali patrule sau călări, iar comandamentele de grup de sate aveau o mică garnizoană, jandarmi și cetățeni călare și pe jos, iar comandamentele de plășii dispuneau de o rezervă călare de jandarmi rurali, un serviciu de informații și un serviciu de aprovizionare a unităților, cu reședința pe teritoriul plășii (Arhivele Militare Naționale Române, Fond Marele Stat Major).

În ceea ce privește împărțirea zonei de asediu în sectoare aflate în responsabilitatea regimentelor Diviziei 9, Planul de acțiune prevedea 2 sectoare, respectiv Sectorul Mircea, unde acționa Regimentul 38 Infanterie, și Sectorul Vlad, unde acționa Regimentul 40 Infanterie. Comanda mixtă a sectoarelor se exercita în adâncime de comandanții regimentelor, în colaborare strânsă cu prefecții. Divizia 9 intra în acoperire cu 16 plutoane din Regimentul 38 Infanterie și din Regimentul 40 Infanterie (câte 8 de fiecare regiment). Efectivele unui pluton, numai din contingentul 1925, selecționați și perfect încadrați, aveau în componență un comandant cu 2 ajutoare, 25 de soldați de trupă, dintre care 18 combatanți și 7 pentru patrulări, observatori și informații. Armamentul era alcătuit dintr-o mitralieră, 2 pistoale-mitralieră cu servanți, puștile din dotarea celor 10 pușcași, iar muniția consta în 10 grenade, 5 rachete, 100 de cartușe armă, 500 de mitraliere, 250 de pistoale-mitralieră (Arhivele Militare Naționale Române, Fond Marele Stat Major).

În ceea ce privește mijloacele de comunicație și legătură, Planul de acțiune prevedea câte o camionetă și secție de telegraf la fiecare sector. Camionetele erau repartizate

pentru uzul de serviciu al comandanților de sectoare și transport de trupe operative. La cerere și în anumite condiții, erau date în folosință comandantului batalionului de grăniceri din sectorul fiecărui regiment (Arhivele Militare Naţionale Române, Fond Marele Stat Major).

În privința posturilor detașate și patrulărilor în puncte prea izolate și configurații prea sălbatice sau împădurite, se prevedea ca cele din zona grănicerilor să fie hotărâte de comandantul batalionului de grăniceri, în zona de interior de comandanții sectoarelor, în colaborare și la indicațiile comandamentelor mixte de plăși. Patrulările erau ordonate de șefii locali, fiecare în comandamentul său, după teren, împrejurări și informații zilnice (Arhivele Militare Naţionale Române, Fond Marele Stat Major).

Serviciul de informații, format din observatori și informatori, era organizat în fiecare sector, subsector, cartier – grupare, unitate și armă și era condus exclusiv de către comandamentul respectiv, după un plan bine chibzuit. În zona grănicerilor, erau organizate 4 centre și un birou, stabilite de comandantul batalionului de grăniceri. În zona interioară – centru la fiecare plasă. În zona cavaleriei – centru la fiecare escadron. La sectoarele de regiment – birourile de informații existente. În ceea ce privește orele de raport și dări de seamă, se prevedea ca, în sectoare și subsectoare, să se realizeze conform dispozițiilor șefilor respectivi, cu Divizia 9 de la sectoare, telefonic, în fiecare zi, la ora 18, buletine, rapoarte sau dări de seamă, în fiecare duminică, cu evenimentele săptămânale; pentru cazuri urgente, imediat și pe orice cale (Arhivele Militare Naţionale Române, Fond Marele Stat Major).

În ceea ce privește aprovizionarea trupelor, se avea în vedere ca aceasta să se facă cu respectarea drepturilor persoanei și avutului acesteia, iar unitățile militare nu aveau permisiunea să facă apel la resursele locale decât în situația imposibilității asigurării materiilor prime prin sursă directă. Se prevedea expres, sub sancțiuni severe, ca sub niciun motiv să nu fie permisă aprovizionarea personală sau a trupei direct de la localnici, ci numai prin administrația locală. Plata se efectua de către administrație prin emitere de bonuri, semnate exclusiv de comandanții unităților, al căror nume era comunicat din timp prefecturilor. Încasarea bonurilor se făcea la 15 sau 30 zile cu forme legale, certificate de autoritățile adminitrative. Comandanții unităților trimiteau anticipat Aministrației Plășilor tabele cu necesitățile lunare, cu indicarea zilelor de ridicare. Grănicerii se aprovizionau conform dispozițiilor administrative ale Corpului, rămânând însă sub aceleași sancțiuni, dacă comiteau încălcări ale drepturilor sau dispozițiilor administrative ale Comandamentului (Arhivele Militare Naţionale Române, Fond Marele Stat Major).

Planul de acțiune avea și dispoziții finale care prevedeau ca cei ce erau arestați să fie însoțiți de un detașament de protecție. Dacă era un număr mare de reținuți, aceștia erau legați unul de altul, iar în cazul în care încercau să fugă, era interzis să se tragă asupra lor, dacă nu fuseseră judecați și condamnați.
Deși planul de acțiune arăta perfect pe hârtie, în teren, realitatea era alta. Posturile grănicerilor și autoritățile românești erau atacate de către comitagii, fiind raportate

zilnic jafuri, tâlhării, rănirea sau uciderea soldaților și jandarmilor români. Cu toate acestea, concepția comandantului Diviziei 9, generalul Ioan Vlădescu, privind respingerea atacurilor de tip terorist al comitagiilor bulgari era una revoluționară, în condițiile în care doctrina militară a anului 1926 nu prevedea măsuri specifice împotriva unor acțiuni asimetrice.

Concluzie

Instituirea stării de asediu pe timp de pace în Dobrogea de Sud în anul 1926 a fost o măsură excepțională, dispusă ca urmare a atacurilor comitagiilor bulgari, care amenințau siguranța statului român. Pe fondul politicii revizioniste a guvernului bulgar care întreținea o stare tensionată la frontiera cu România, prin susținerea acțiunilor de tip terorist ale comitagiilor, decidenții politici și militari de la București, loiali principiilor tratatelor încheiate la sfârșitul Primului Război Mondial, au gestionat starea conflictuală de la frontiera de sud într-o manieră mai puțin abordată în istoriografia conflictelor asimetrice. Prin învestirea autorității militare și prin măsurile dispuse, comandanții unităților dispuse în garnizoanele de reședință din Cadrilater au scris o pagină de istorie militară mai puțin cunoscută. Acest articol este un omagiu adus jandarmilor, trupelor de infanterie și autorităților civile românești care au contribuit la promovarea valorilor principiilor europene, asumate de România în secolul XX.

Referințe

Analele Dobrogei. 2005. „Serie nouă, an VIII". Constanța.

—. 2019. „Seria III, an III". Constanța.

Arhivele Militare Naționale Române. Fond Marele Stat Major.

Assan, B.G. 1912. *Quadrilaterul Dobrogean, Rusciuc, Varna, Șumla, Silistra.* București: Editura Minerva.

Buletinul Arhivelor Militare Române. Anul XX. „Document. nr. 3/2017".

Ciorbea, Valentin. 2008. *Dobrogea 1878-2008. Orizonturi deschise de mandatul european.* Constanța: Editura Ex Ponto.

Filotti, Alexandru Gabriel. 2007. *Frontierele Românilor.* vol. I și vol. 2. Brăila: Editura Istros a Muzeului Brăilei.

Ghițescu, Mihai. 2021. „Despre starea de asediu în România, Schiță istorico-juridică, 1918-1938." *Revista Bibliotecii Academiei Române* Anul 6, nr. 12, iulie-decembrie.

Grecul, Gr. D. 1928. *Starea de asediu actuală.* București: Editura Curierul Judiciar S.A.

Kurkina, Ana-Teodora. 2013. *The problem of the appurtenance of Dobruja region, 1913-1940: Bulgarian and Romanian methods of claming rights over territory.* Budapest, Hungary: Central European University, History Departament.

Muzeul Militar Național Regele Ferdinand I. 2020. *Tradiție, Istorie, Armată.* Ediția a V-a, 29 octombrie 2019. Târgoviște: Editura Cetatea de Scaun.

Neagoe, Sever. 1985. *Teritoriul și frontierele în istoria românilor.* București: Editura Ministerului de Interne.

Negoiță, Cătălin. 2009. *Între stânga și dreapta. Comunism, iredentism și legionarism în Cadrilater (1913-1940).* Craiova: Editura Fundației Scrisul Românesc.

Pantelimonescu, V. 1939. *Starea de asediu, Doctrină, Jurisprudență și Legislație.* București: Editura Ziarului Universul.

Roman, Ioan N. 2008. *Despre Dobrogea și dobrogeni.* Constanța: Editura Ex Ponto.

—. 1905. *Dobrogea și drepturile politice ale locuitorilor ei.* Constanța: Editura Ovidiu.

Ungureanu, George. 2009. *Problema Cadrilaterului în contextul relațiilor româno-bulgare (1919-1940).* Brăila: Editura Istros a Muzeului Brăilei.

Ziarul Înfrățirea Românească. 1926. Anul II, nr. 23-24, 1-15 octombrie.


AGENȚIA ROMÂNĂ DE ASIGURARE A CALITĂȚII ÎN ÎNVĂȚĂMÂNTUL SUPERIOR
ROMANIAN AGENCY FOR QUALITY ASSURANCE IN HIGHER EDUCATION
Membră ENQA – Full member of ENQA
Înregistrată în EQAR – Registered in EQAR

CERTIFICAT
CERTIFICATE

Universitatea Națională de Apărare „Carol I" din București

a obținut, în urma evaluării instituționale, calificativul
GRAD DE ÎNCREDERE RIDICAT
pentru perioada 2021-2026
following institutional evaluation, attained the HIGH DEGREE OF CONFIDENCE rating for the period 2021-2026

BIROUL EXECUTIV AL CONSILIULUI ARACIS

EDITOR
Editura Universității Naționale de Apărare „Carol I"
(Editură cu prestigiu recunoscut de Consiliul Național de Atestare a Titlurilor, Diplomelor și Certificatelor Universitare)
Adresa: Șoseaua Panduri, nr. 68-72, sector 5, București
e-mail: buletinul@unap.ro
Tel. 319.48.80 / 0365; 0453

Bun de tipar: 17.01.2025
Lucrarea conține 248 de pagini.