BULETINUL

UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I"

Nr. 1/2024

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. 1/2024

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

Necesitatea unui model integrat de „război smart”

The need for an integrated model of smart warfare

Drd. Matei BLĂNARU*
*Școala Doctorală de Sociologie a Universității din București

Abstract

Din păcate, războiul din Ucraina și multe alte evenimente sau procese care au loc în întreaga lume ne arată că este posibil să nu poată exista o pace ”smart” decât dacă suntem gata să purtăm un ”război smart”. Atât împotriva unor inamici convenționali, cât și neconvenționali, atât în ceea ce privește războiul simetric, cât și cel asimetric. Și dacă începem să vedem societatea noastră în termeni de guvernare ”smart”, educație, economie sau oameni ”smart”, ceea ce înseamnă că o vedem în termeni de pace și societate ”smart” sau „inteligentă”, atunci este cu siguranță nevoie de a vedea și războiul, și conflictul într-o viziune integrată, compactă de „război smart”. Trebuie să înțelegem că ”smart” este și despre pace, dar și despre război, dacă vrem ca o pace „inteligentă” să dureze sau dacă vrem să o putem apăra, pentru că România are în mod categoric o strategie defensivă. Construim o pace „inteligentă”, dar trebuie să ne pregătim și pentru un „război smart”, „inteligent”.

Unfortunately, the war in Ukraine and many other events or processes taking place all over the world show us that perhaps there can be no smart peace unless we are ready to fight a smart war. Both against conventional or unconventional enemies, both regarding symmetrical or asymmetrical warfare. And if we are beginning to see our society in terms of smart governance, smart education, smart economy or smart people, which means we see it in terms of smart peace and smart society, then there is definitely the need to see war and conflict in an integrated, compact vision of smart war. We need to understand that ”smartness” is all about peace, but all about war as well, if we want a smart peace to last or if we want to be able to defend it, as Romania has a definitely defensive strategy. We are building a smart peace, but we have to prepare for a smart war as well.

Cuvinte-cheie:
smart; război; amenințări; societate; cyber; IA.

Keywords:
smart war; threats; society; cyber; AI.

Info articol
Primit: 30 ianuarie 2024; Evaluat: 19 februarie 2024; Acceptat: 14 martie 2024; Disponibil online: 5 aprilie 2024
Citare: Blănaru, M. 2024. „Necesitatea unui model integrat de „război smart”. *Buletinul Universității Naționale de Apărare „Carol I”*, 13(1): 7-25. https://doi.org/10.53477/2065-8281-24-01

Introducere

Evident, ca civili, războiul este ceva la care preferăm să nu ne gândim. Mai degrabă ne-am gândi la ”smart living”, la o pace ”smart”, la o societate ”smart” sau la o educație ”smart”[1] pentru copiii noștri, la orice altceva în afară de război. Ideologiile moderne și istoria recentă, în care societățile occidentale au evitat în mare parte războiul timp de mai bine de jumătate de secol, joacă și ele un rol important în această percepție a publicului. Dar, așa după cum vedem în Ucraina sau în Israel, acest mod de a gândi nu înseamnă că războiul nu este aici. Dimpotrivă, războiul este aici pentru a rămâne, dar poate că într-o nouă formă de „război smart”. Așadar, cum se duce un „război smart” sau ce este acesta?

Modul în care societatea noastră se schimbă, și războiul din Ucraina ne oferă multe indicii în această direcție. Guvernarea ”smart”, conducerea ”smart”, ”smart living”, educația ”smart” și așa mai departe, toate abordează preocupările societale și înseamnă o abordare integrativă a acestor preocupări, cu un impact semnificativ al noilor tehnologii. Dar dacă un viitor al societății este descris în acest fel, cu atribut ”smart”, atunci de ce nu ar trebui să privim războiul în același mod și de ce nu ar trebui să ne adaptăm mai devreme decât mai târziu la „războiul smart”? Nu vrem să spunem că războiul modern nu încorporează sau nu generează cele mai moderne tehnologii, războaiele întotdeauna au făcut asta de-a lungul istoriei, dar ceea ce spunem este că modul nostru de a gândi războiul nu a ținut pasul cu aceste noi realități. Chiar modul nostru de a gândi poate fi o vulnerabilitate, în contextul unor noi amenințări sau al unor actori ostili. Și asta trebuie să se schimbe. Astfel, avem neapărat nevoie de conceptul de „război smart”.

1. Literatura actuală pe tema „războiului smart”

La momentul la care scriem această lucrare (octombrie 2023), nu am putut găsi un concept de „război smart” (”smart war”), denumit ca atare în literatura științifică modernă și în modul în care vrem să-l abordăm noi – care este similar cu o educație ”smart”, o guvernare sau o societate „smart” –, ceea ce înseamnă că este o necesitate să profităm de toate inovațiile tehnologice într-o perspectivă strategică incluzivă și integrată. Există totuși un concept destul de similar de „război inteligent” (”intelligent warfare”), dezvoltat în special de cercetătorii chinezi.

În ceea ce privește conceptul de „război smart”, majoritatea mențiunilor disponibile publicului online se referă la „războiul smart” ca fiind echivalent cu un „război inteligent”, echivalent cu un război purtat într-o manieră inteligentă privind capacitatea mentală. Sau aceste mențiuni se referă la industria jocurilor de noroc. Alte relatări se referă la așa-numita politică de

[1] În cuprinsul acestei lucrări, vom folosi cu precădere cuvântul ”smart” în loc de traducerea în limba română a acestuia drept „inteligent/ă”, pentru că vrem să facem distincția dintre *smart* = bazat pe inovații și tehnologii de ultimă generație și *inteligent/ă* = înzestrat cu inteligență ca și capacitate mentală, deștept, ager la minte, pătrunzător.

„război smart” a administrației americane în diferite momente, între 2002 și în jur de 2015, ceea ce în cele din urmă făcea referire tot la smart = inteligent din punctul de vedere al capacității mentale. În politicile și strategiile SUA, a existat un așa-numit „război smart” (”the smart war”) ca fiind diferit de „războiul prost” (”dumb war”), diferență subliniată pentru prima dată de Obama într-un discurs din 2002 (Thrush 2011). Dar, din nou, acesta însemna doar un fel de război condus într-o manieră inteligentă din punctul de vedere al capacităților mentale. Care se spune că a și eșuat în Afganistan. În 2002, secretarul american al apărării, Donald Rumsfeld, a conceput și el o strategie de „război smart” pentru invazia Irakului și răsturnării de la putere a lui Saddam Hussein. Cu toate acestea, în ciuda folosirii intense a „bombelor smart”, „războiul smart” conceput de strategia lui Rumsfeld a însemnat doar un fel de război purtat și într-o manieră inteligentă.

Într-o altă analiză, există o mențiune foarte interesantă a „războiului smart”, chiar dacă din nou folosește „smart” ca însemnând o capacitate mentală de inteligență. Articolul ”Soft War = Smart War? Think Again” critică încrederea excesivă în soft power atunci când se urmăresc obiectivele de securitate, probabil referindu-se și la noile concepte de ”smart power”: *„În lumina acestui fapt, legarea securității noastre pe termen lung de ideea că putem să-i manipulăm și să îi depășim pe alții în domeniul persuasiunii interculturale și, astfel, să ducem un fel de război soft, inteligent, pare deosebit de imprudentă.”* (Simons 2012) Suntem de acord cu această concluzie. Războiul soft este extrem de important, dar doar atunci când este folosit împreună cu, sau are în spate, și hard power. Abilitățile de război soft, avansate din punct de vedere tehnologic, și capabilitățile militare avansate din punct de vedere tehnologic alcătuiesc împreună o parte importantă din conceptul de „război smart” pe care vrem să-l descriem. Va fi mai clar când vom evidenția mai jos caracteristicile pe care le-am atribui unui „război smart”. Totuși, nu ar trebui să existe nicio confuzie între conceptul de ”smart power” și ceea ce încercăm noi să analizăm drept ”smart war”. Războiul din Ucraina a dovedit importanța utilizării ”smart power” (Danylenko și alții 2022, 43-53), dar în cele din urmă ”smart power” este doar o combinație între *hard power* și *soft power* (Dargiel 2009). Dar „războiul smart” ar trebui să însemne mult mai mult decât atât și în feluri diferite. „Războiul smart” înseamnă, în primul rând, a gândi în afara tiparelor. De exemplu, toate tehnologiile pentru construirea și utilizarea dronelor maritime erau deja aici. Dar nimeni nu s-a gândit să le folosească în măsura în care Ucraina le folosește acum, provocând pagube uriașe marinei Federației Ruse. Și acesta este doar începutul. Curând, este posibil ca navele mari și portavioanele să înceapă să își piardă rolul dominant pe care îl au acum pe mare.

În 2011, secretarul general al NATO de atunci, Anders Fogh Rasmussen, a vorbit despre un concept de strategie de ”smart defence”, care ar fi însemnat „ideea de a crea mai multe capabilități europene cu mai puțini bani” (Eugénio 2013) și de a reduce povara financiară și operațională a SUA cu privire la NATO. Deci, și NATO a considerat ”smart” ca o capacitate mentală. NATO pare să nu opereze cu conceptele de ”smart war” sau ”intelligent war”, dar în 2021 a adoptat prima strategie, raportată la IA, recunoscând că: „Inteligenta artificială (IA) schimbă mediul global de apărare și

securitate. Oferă o oportunitate fără precedent de a ne consolida avansul tehnologic, dar va crește și viteza amenințărilor cu care ne confruntăm. Această tehnologie de bază va afecta probabil întregul spectru de activități întreprinse de Alianță în sprijinul celor trei sarcini principale ale sale: apărare colectivă, managementul crizelor și securitate cooperativă." (NATO 2021) Recunoașterea vitezei noilor amenințări și a faptului că noile tehnologii (nu doar IA, în opinia noastră) vor afecta pe deplin toate activitățile Alianței este unul dintre principalele noastre argumente și în această analiză.

Totuși, conceptul de „război smart" folosit într-o manieră ușor similară cu cea pe care vrem să o abordăm noi este resimțit la nivelul solului. O mențiune despre „războiul smart" într-un mod puțin asemănător cu ceea ce vrem să analizăm noi aici (deși ei îl folosesc mai mult drept "smart" = capacitatea inteligentă de a gândi) nu a venit de la cercetători, ci de la nivelul solului, dintr-o sursă probabil neașteptată – mercenarii Wagner din Ucraina, care s-au plâns, în 2022, că Ucraina duce un „război smart" împotriva lor, în timp ce comandanții lor, cu precădere, erau încă blocați într-o mentalitate militară convențională (Comisarul 2022).

Chiar și unele volume de marcă, foarte recente, care abordează *„o perspectivă internațională și interdisciplinară asupra adoptării și guvernanței inteligenței artificiale (IA) și machine learning (ML) în domeniul apărării și inovării militare de către marile puteri și cele mijlocii"* (Raska și Bitzinger 2023, iii) nu promovează o abordare și o definiție integrată a „războiului smart" în modul în care ne propunem. De exemplu, în poate cel mai recent volum din domeniu, *The AI Wave In Defence Innovation. Assessing Military Artificial Intelligence Strategies, Capabilities, and Trajectories*, coordonat de Michael Raska și Richard A. Bitzinger, din care am citat mai sus, nu am putut găsi conceptul de „război smart" astfel denumit. Dar, în apărarea sa, nu acesta a fost scopul volumului. Volumul se ocupă de un aspect foarte important al „războiului smart", chiar esențial, adică inteligența artificială (IA) și *machine learning* (ML), dar nu a conceput și o imagine de ansamblu care să cuprindă toate caracteristicile și abordarea integrată a unui „război smart", pe care noi le vom puncta pe scurt mai jos.

Însă, după cum o arată și volumul menționat anterior, lucrurile diferă într-o oarecare măsură atunci când vine vorba despre China și Armata Populară de Eliberare (PLA), care folosesc de ceva timp conceptul de „război inteligent". De exemplu, există o analiză amănunțită, din 2021, scrisă de Centrul American pentru Analize Navale (CNA), denumită *The PLA and Intelligent Warfare: A Preliminary Analysis*, care încearcă să cerceteze semnificația și strategia chineză a „războiului inteligent", iar rezultatele sunt oarecum surprinzătoare. Se afirmă pe bună dreptate că *„adoptarea pe scară largă a inteligenței artificiale (IA) și a sistemelor de arme autonome prevestește o nouă revoluție în operațiunile militare"* (Pollpeter și Kerrigan 2021, i), ceea ce este un aspect foarte important legat de subiectul abordat în lucrarea de față. De asemenea, se spune că *„Armata Populară de Eliberare (PLA) conceptualizează acum un viitor teren de luptă dominat de IA și autonomie, pe care îl numește «război inteligent»"*

(Pollpeter și Kerrigan 2021, i), ceea ce este un avertisment clar pentru viitor, din perspectivă geopolitică și strategică.

În această analiză din 2021, există o afirmație foarte interesantă referitoare la faptul că analiștii chinezi au făcut *„evaluările conform cărora IA și autonomia vor permite armatelor mai slabe să învingă armatele mai puternice",* ceea ce *„sugerează că autorii pot privi IA și autonomia ca pe noi tehnologii care ar putea juca un rol semnificativ în înfrângerea armatei SUA."* (Pollpeter și Kerrigan 2021, iv) Nu suntem încă acolo în ceea ce privește inteligența artificială și sistemele autonome, dar putem vedea cum aproape inexistenta marină ucraineană a reușit să învingă puternica flotă rusă de la Marea Neagră, folosind doar câteva dispozitive "smart" de război, adică dronele navale.

În ceea ce privește caracteristicile acestui „război inteligent", descris de chinezi și PLA, analiza CNA, pe care am citat-o, subliniază că *„majoritatea autorilor din Republica Populară Chineză nu definesc în mod explicit războiul inteligent, ci îl descriu astfel: « o etapă nouă și avansată a războiului bazat pe IA și autonomie; o combinație de inteligență umană și artificială; utilizarea pe scară largă a IA în toate aplicațiile militare»."* (Pollpeter și Kerrigan 2021, i) De asemenea, analiștii chinezi au subliniat pe bună dreptate importanța datelor, algoritmilor și puterii de calcul pentru ceea ce ei numesc „război inteligent" (Pollpeter și Kerrigan 2021, i). În ceea ce privește cine va deține controlul asupra acestor capacități de „război inteligent", majoritatea analiștilor chinezi au prezis că, cel puțin la nivel strategic, oamenii vor deține controlul și, în general, va exista un sistem de control hibrid, format din oameni și mașini. O minoritate prezice că, în timp, mașinile vor înlocui complet oamenii și în această direcție.

Din punct de vedere oficial, în 2019 a apărut o *White Paper* privind Apărarea Națională a Chinei în Noua Eră, care descrie pe scurt ce vor să spună ei prin „război inteligent": „Există o tendință predominantă de a dezvolta arme și echipamente de precizie, inteligente, nedetectabile sau fără pilot. Războiul evoluează ca formă spre un război informatizat, iar războiul inteligent este la orizont." (State Council of The People's Republic of China 2019).

Una dintre cele mai recente lucrări-cheie referitoare la „războiul inteligent", din perspectiva chineză a conceptului, este *Intelligent Warfare. Prospects of Military Development in the Age of AI,* scrisă de Mingxi Wu, un cercetător chinez, care susține că: *„Războiul inteligent poate lua forme diversificate, în special confruntări cognitive cu IA în centrul lor și operațiuni integrate care utilizează «intelligence+» și «+intelligence».(...) Tehnologiile inteligente precum IA, big data, cloud computing, biologia interdisciplinară, sistemele fără pilot și parallel training avansează într-un ritm vertiginos și devin din ce în ce mai integrate cu tehnologiile consacrate, modificând epistemologia, metodologia și mecanismele operaționale ale oamenilor și sporind capacitatea oamenilor de a transforma lumea. După mecanizare și informatizare, «inteligentizarea» va fi a treia etapă a civilizației umane."* (Wu 2023, xv) Suntem pe deplin de acord cu tot ce a spus cercetătorul chinez mai sus, dar din nou, aceasta este într-un viitor relativ îndepărtat. Cu toate acestea, lucrurile nu vor mai fi niciodată la

fel în ceea ce privește războiul și ar fi bine să acceptăm asta mai devreme decât mai târziu. Autorul continuă, spunând că *„cine controlează avantajul inteligenței va avea inițiativa în viitorul război"*. (Wu 2023, xvi) Acesta pare să fie principalul obiectiv chinez privind o posibilă viitoare confruntare cu SUA.

2. Caracteristici și înțelesul conceptului de „război smart"

„Războiul smart" este un concept în curs de elaborare și i se pot adăuga mult mai multe dimensiuni (dintre care unele în mod cert nu au fost încă inovate), dar dorim să subliniem, în paragrafele următoare, câteva dintre principalele sale caracteristici *sine qua non*. Obiectivul acestei analize nu este acela de a investiga în detaliu următoarele trăsături sau componente ale ceea ce noi descriem drept „război smart", ci doar de a le enumera pe cele mai importante dintre acestea. Evident, lista nu este închisă, ci, la fel ca și „războiul smart", este în continuă evoluție și deschisă către inovație și pentru noi funcții.

2.1. Drone (vehicule fără pilot)

Una dintre principalele caracteristici ale oricărui „război smart", în accepțiunea actuală, așa cum îl vedem noi, înseamnă să te bazezi în mare măsură pe un număr foarte mare de drone moderne, relativ ieftine (Trofimov 2023), indiferent dacă sunt operate de oameni sau de IA, de sisteme autonome. Războiul din Ucraina, la fel ca și atacul terorist al Hamas împotriva Israelului, subliniază această considerație. Așa după cum a spus Oleksii Reznikov, fostul ministru al apărării din Ucraina, despre ruși: *„Nu avem nicio flotă sau capacitate navală serioasă. Dar îi putem lovi cu drone"* (Harding 2023). Și, apoi, mai este vorba și despre costul dronelor lor maritime, variind de la 10 la 100 de mii de dolari SUA, în comparație cu costul navelor Flotei Ruse, de sute de milioane de dolari SUA (Harding 2023). Am putea concluziona că „războiul smart" se merită.

Această dimensiune se schimbă în prezent, dezvoltându-se foarte rapid, iar investiția în capacități interne pentru dezvoltarea și fabricarea de drone ieftine ar fi cea mai bună alegere. Ne amintim că, la începutul războiului din Ucraina, dronele turcești Bayraktar făceau prima pagină a ziarelor în toată lumea. Acum, aproape că nu mai auzim de ele. Aceasta înseamnă că armata rusă a dezvoltat contramăsuri eficiente. Din perspectiva unui „război smart", cineva ar putea argumenta că, exact acum, când s-au schimbat lucrurile în acest sens, armata română va primi drone Bayraktar relativ depășite, relativ scumpe, în valoare de sute de milioane de dolari SUA, în loc să fi început să-și extindă propriile capacități de producție și dezvoltare de drone, care merită toți acești bani în viitor. Alegerea direcției în care să investești și a volumului de fonduri necesar este cu siguranță un atribut al oricărei strategii bune și al războiului „smart".

2.2. Comunicarea și diplomația publică

O altă dimensiune esențială a oricărui „război smart" actual ar fi o campanie diplomatică și de comunicare foarte activă și bine pusă la punct, ceea ce sunt

capabilități de *soft power*. Având în vedere stadiul actual al globalizării, importanța opiniei publice, narațiunile și justificarea, mai ales pentru societățile occidentale, aceste lucruri nu pot fi subestimate. Putem vedea cum, pentru Israel, este din ce în ce mai dificil să ducă o confruntare, să gestioneze narațiuni și să justifice războiul în acest domeniu al comunicării și al percepției publice, chiar și pentru publicul intern și ciuda faptului că nu Israelul a început războiul cu Hamas.

Comunicarea a fost întotdeauna esențială pentru a câștiga un război. Dar există comunicare în interiorul lanțului de comandă militar și comunicarea către societatea civilă atât în țară, cât și în străinătate, adică narațiunile folosite și diplomația publică. O analiză foarte cuprinzătoare privind importanța diplomației publice actuale în războiul din Ucraina este lucrarea *Public diplomacy during military international conflicts. The Ukraine war case*, de Hlihor Ecaterina, care afirmă că *„diplomația publică însăși s-a transformat"* și *„bătălia dintre militarii ucraineni și cei ruși pentru imagine și legitimitate în opinia publică internațională"* este din ce în ce mai importantă, deoarece *„în era informațională în care trăim, activitățile și capacitățile diplomației publice pot avea un impact semnificativ asupra modului în care oamenii, organizațiile și guvernele percep acest război."* (Hlihor 2023, 19)

2.3. *Soft Power*

Este o dimensiune esențială a oricărei confruntări prezente și va fi ca atare în perioada următoare. Joseph Nye Jr. a dezvoltat pentru prima dată conceptul în 1990, iar în volumul său emblematic, din 2004, a spus: *„Soft power se bazează pe câteva valori comune. De aceea schimburile sunt adesea mai eficiente decât simpla difuzare. Prin definiție, soft power înseamnă să-i convingi pe alții să-și dorească aceleași rezultate pe care ți le dorești și tu, și asta necesită înțelegerea modului în care ei aud mesajele și ajustarea acestor mesaje în consecință. Este crucial să înțelegem publicul-țintă."* (Nye 2005, 111) Ni se pare că, acum mai mult ca niciodată, avem nevoie să-i înțelegem pe „ceilalți", oricine ar fi ei. Astfel, *soft power* înseamnă, de asemenea, folosirea culturii, înțelegere reciprocă și respect pentru alte culturi, economie, valori morale, seriozitate, încredere și alte aspecte. Analiștii chinezi tind să minimizeze importanța *soft power* atunci când vorbesc despre „războiul inteligent", în timp ce, uneori, cercetătorii și practicienii occidentali tind să supraestimeze și să se bazeze prea mult pe *soft power*. Sau, la fel cum s-a întâmplat în Afganistan, s-ar putea să o implementeze într-o manieră defectuoasă (de exemplu, s-au bazat pe elemente locale corupte care au înstrăinat în cele din urmă populația locală, în ciuda uriașelor investiții financiare și de *soft power* americane).

2.4. Războiul informațional

Am menționat pe scurt, anterior, importanța comunicării și a diplomației publice, ceea ce ne aduce la importanța războiului informațional în această eră a dezvoltării tehnologice „smart": *„Războiul informațional (IW), ansamblu complex de noi fenomene, asociate cu utilizarea tehnologiilor de informații și comunicații (TIC) în scenarii de luptă. IW redefinește modul în care este purtat războiul. (...) În zilele noastre, IW indică un fenomen eterogen ce privește desfășurarea armelor robotizate, a armelor cibernetice și utilizarea ITC pentru a stimula coordonarea dintre militari pe câmpul de luptă și pentru*

propagandă, așa-numitul C4ISR (comandă integrată, control, comunicații, computere, informații, supraveghere și recunoaștere)." (Taddeo și Floridi 2014, v).

2.5. Abordarea societală

Dacă am menționat importanța diplomației publice și a războiului informațional pentru „războiul smart", atunci cu siguranță trebuie să menționăm importanța amenințărilor societale. O abordare societală a războiului „smart" ar presupune *nation building* și o construire a coeziunii pe plan intern și diplomație publică, atrăgând atenția publicului și sprijinul publicului la nivel internațional. Într-o anumită măsură, exact ceea ce face Ucraina de când a fost invadată de Rusia.

O abordare societală și sprijinul societal pentru război au fost întotdeauna considerate și recunoscute drept importante, dar mijloacele și metodele actuale s-au schimbat la fel de mult ca și cele tehnologice și militare. După ce s-au învățat lecțiile din trecut, războiul societal modern este mult mai puternic și mai greu de contracarat. Mai ales atunci când se resimte o lipsă din ce în ce mai mare de încredere în instituții și în politicieni (care, pe de altă parte, poate fi exact rezultatul pe care o campanie de război societal și-ar dori să-l obțină într-o societate). În China există o *„forță de sprijin strategic a PLA, care are responsabilități pentru spațiul cosmic, războiul cibernetic, războiul electronic și operațiunile de război psihologic*" (Pollpeter și Kerrigan 2021, v).

2.6. Războiul psihologic și cognitiv

Sunt domenii secundare specifice abordării societale a războiului. În acest domeniu, PLA chineză a efectuat din ce în ce mai multe cercetări, încercând să vadă cum tehnologiile moderne, precum IA, pot oferi avantaje-cheie într-o confruntare modernă. Există un volum cuprinzător pe această problemă, *Chinese Next-Generation Psychological Warfare: The Military Applications of Emerging Technologies and Implications for the United States*, care afirmă că, *„pe scurt, China vede războiul psihologic ca fiind centrat pe manipularea informațiilor pentru a influența luarea deciziilor și comportamentul adversarului, ca fiind una dintre cele câteva componente-cheie ale războiului modern. Războiul psihologic chinez a evoluat, condus, în parte, de progresul tehnologic care a adus noi oportunități și, în parte, de lecțiile învățate de la alte armate, dar principiile și obiectivele de bază au rămas relativ constante. Importanța acordată războiului psihologic este din ce în ce mai legată de evaluările militare chineze, conform cărora domeniul cognitiv va fi un domeniu-cheie al războiului în viitor.*" (Beauchamp-Mustafaga 2023, iv-v) Despre tehnologiile moderne care pot fi utilizate în acest scop, același volum precizează cum *„comunitatea PLA responsabilă de războiul psihologic a discutat despre o gamă de tehnologii pe care își propune să le folosească pentru operațiunile viitoare, inclusiv trei categorii largi de tehnologii: informatică avansată, în special prelucrarea big data și a informațiilor; neuroștiințele, în special imagistica creierului; o serie de propuneri moștenite care rămân de interes, inclusiv arme sonice, arme laser, mesaje subliminale și holograme.*" (Beauchamp-Mustafaga 2023, v)

Despre propagandă și dezinformare și despre importanța ei astăzi, asociate cu avantajul tehnologiilor moderne, analiza CNA, pe care am citat-o mai devreme, afirmă că *„PLA poate pune accent pe războiul cognitiv, pe măsură ce integrează*

IA în lupte. Unii scriitori din RPC susțin că războiul cognitiv poate permite RPC să îndeplinească maxima lui Sun Tzu, de «a câștiga fără luptă» prin distrugerea moralului și a voinței adversarilor. PLA poate crește eforturile de a influența concurenții și potențialii adversari în domeniul cognitiv prin răspândirea propagandei și a dezinformării." (Pollpeter și Kerrigan 2021, v) Toate acestea arată din nou cât de importantă este această componentă societală pentru „războiul smart".
Și NATO operează cu acest concept de *război cognitiv* și oferă o definiție: „*Războiul cognitiv include activități desfășurate în sincronizare cu alte instrumente de putere, pentru a afecta atitudinile și comportamentele, prin influențarea, protejarea sau perturbarea cognitivă la nivel individual, de grup sau de populație. pentru a obține un avantaj asupra unui adversar. Conceput pentru a modifica percepțiile asupra realității, manipularea la nivel de întreagă societate a devenit o nouă normă, cunoașterea umană devenind un domeniu critic al războiului.*" (NATO fără an)

2.7. Sateliți și Starlink
Războiul actual din Ucraina tocmai a dovedit din nou importanța sateliților, a explorării spațiului, chiar și a sistemului de sateliți Starlink al lui Elon Musk, pentru un „război smart" modern.

2.8. Războiul spațial
Chiar dacă este posibil ca pandemia să fi întârziat unele procese de militarizare și de explorare a spațiului, tendința principală este aceea că „spațiul devine un mediu mai puțin stabil, chiar dacă oferă promisiunea de a deveni o nouă sursă de prosperitate umană". (Nagashima 2020) Comandamentul spațial al SUA a anunțat în urmă cu ceva timp, în 2020, că are dovezi că Rusia a efectuat recent teste de arme antisateliți (Patel 2020). Există pledoarii pentru mai multă reglementare în spațiu, pentru cooperare, în loc de concurență sau dominație, dar aceasta pare mai degrabă o iluzie, mai ales având în vedere situația internațională actuală. SUA au o forță militară, numită Forța Spațială: „*Ca serviciu militar, Forța Spațială are responsabilități, în temeiul Titlului 10 al Codului SUA, de a organiza, antrena, echipa, pregăti și menține forțe. Într-un conflict, acele forțe ar fi repartizate unui comandament de luptă.*" (Erwin 2020) În ceea ce privește China și Rusia, se pare că au deja arsenale, concepute pentru a fi folosite la distrugerea sateliților adversari în spațiu: „*Națiunile din întreaga lume – în special China și Rusia – construiesc arsenale de arme care pot distruge sau perturba sateliții în orbită.*" (Erwin 2021) Deci, că ne place sau nu, „războiul smart" este deja prezent și în spațiu și va avea o importanță din ce în ce mai mare.

2.9. Războiul electronic (EW)
Există mai multe relatări despre importanța și dezvoltarea echipamentelor eficiente de război electronic folosite în războiul din Ucraina. Federația Rusă pare să aibă un avantaj față de alți adversari în ceea ce privește capacitățile similare în acest moment.

2.10. Războiul cibernetic
Nu este nevoie să subliniem importanța uriașă a războiului cibernetic pentru orice „război smart". Hackingul, atacurile cibernetice și războiul cibernetic (de exemplu,

un eveniment destul de recent, în care CISA – Agenția de Securitate a SUA pentru Securitate Cibernetică și a Infrastructurii – a emis un avertisment referitor la un actor cibernetic din China, sponsorizat de stat, a cărui *„activitate afectează rețelele din sectoarele infrastructurii critice din SUA")* (CISA 2023) vor fi întotdeauna o parte esențială a oricărei strategii pentru orice fel de război de acum înainte, dar mai ales pentru un „război smart". „Războiul smart" pur și simplu nu poate fi definit fără atacuri cibernetice și capabilități de apărare cibernetică.

2.11. Semiconductori/cipuri

Orice război sau conflict militar în viitor va depinde de capacitatea de a furniza sau de a fabrica volumul și tipurile adecvate de microcipuri avansate pentru propriile capacități militare, instrumente IA și ML (machine learning). Există mai multe afirmații în acest sens (Hawkins 2023).

Una dintre cele mai recente și mai cuprinzătoare analize pe această temă este volumul *Chip War. The Fight for The World's Most Critical Technology*. Autorul subliniază că puterea de calcul din lume este în pericol, dacă măcar unul dintre pașii implicați în procesul de producție a semiconductorilor este întrerupt. Ne putem imagina cu ușurință impactul asupra inteligenței artificiale, dronelor, capacităților cibernetice, chiar și asupra bombelor „smart", avioanelor, în esență asupra a tot ceea ce face ca o societate să fie "smart", ca o pace să fie "smart" sau ca un război să fie "smart". Autorul continuă, spunând că, dacă mulți oameni cred astăzi că datele sunt noul *„petrol"*, de fapt puterea de procesare a computerelor care depinde de semiconductori este cea mai importantă și este în cantitate limitată, nu datele, care par nelimitate (Miller 2022). Inutil să mai argumentăm importanța esențială a semiconductorilor/cipurilor pentru orice război de astăzi, nu doar pentru un „război smart".

2.12. Inteligența artificială (IA)

Am menționat anterior două dintre cele mai recente și importante volume cu privire la cât de esențială este IA pentru războaiele viitoare (și poate și pentru pace în viitor). *The AI Wave In Defence Innovation. Assessing Military Artificial Intelligence Strategies, Capabilities, and Trajectories* și *The PLA and Intelligent Warfare: A Preliminary Analysis* încearcă să descrie posibilitățile imense (și riscurile) prezentate de tehnologiile IA. Depinde de mulți factori, dar, pe termen lung, IA poate fi *cea mai* importantă problemă în viitoarele războaie „smart".

Cu toate acestea, un aspect pe care trebuie să-l luăm în considerare este dependența excesivă de IA, mai ales în această etapă incipientă a dezvoltării IA. Pentru că, dacă eșecurile IA pot avea acum consecințe catastrofale la nivel individual (de exemplu, în China, dacă o persoană este desemnată ca „suspectă", „periculoasă" sau dintr-o anumită „rasă", conform sistemelor IA de recunoaștere facială și supraveghere și analizei IA a imaginilor camerelor de supraveghere, în fapt persoana respectivă ar putea fi nevinovată), consecințele pot fi catastrofale și la nivel colectiv, chiar național, dacă sistemele IA sunt defecte, vulnerabile și adoptate prematur în sfera de utilizare militară extinsă.

2.13. Internet of Things (IoT) în scopuri militare

Potrivit unei analize, „Internet of Things (IoT) descrie conceptul de conectare a oricărui dispozitiv la internet, rezultând o rețea gigantică de obiecte și oameni care colectează și partajează date. (...) O altă caracteristică definitorie a Internet of Things este că obiectele pot «vorbi» între ele, ca de exemplu senzorii dintr-o casă sau dintr-o fabrică «smart» care partajează informații pentru a controla luminile, temperatura sau nivelurile de inventar" (Mail.com 2023). Potrivit aceleiași analize, „Internet of Things este alcătuit din dispozitive «smart» – obiecte cu microcipuri și senzori încorporați care sunt conectate la o platformă bazată pe internet cu colectare de date și capacități de procesare". (Mail.com 2023) Armata SUA a continuat să cerceteze utilizarea militară a IoT, dar nu foarte convingător și nu într-o manieră hotărâtă. Cu toate acestea, a creat proiectul Internet of Battlefield Things (IoBT), iar în 2017, armata SUA a creat un proiect, numit Internet of Battlefield Things Collaborative Research Alliance (IoBT-CRA), menit să invite cercetătorii civili să aducă contribuții la IoBT. *Ceea ce reprezintă exact tipul de colaborare pe care am subliniat-o anterior ca fiind de o foarte mare importanță: cercetători, practicieni și educație.*

2.14. Construirea unei baze industriale adecvate și securizarea unui flux constant de materiale necesare și lipsit de piedici

Este limpede că se conștientizează importanța uriașă, pentru viitor, a acestor lucruri; menționăm doar faptul că Uniunea Europeană a adoptat în mod provizoriu un *Act european privind materiile prime esențiale „deoarece cererea de pământuri rare este de așteptat să crească exponențial în următorii ani"* (Consiliul European 2023). Iar în România se pare că erau în dezvoltare modele autohtone de drone, care vor fi esențiale în războiul de mâine și sperăm că vor exista mai multe programe interne, precum acesta, întreprins de *Agenția* de *Cercetare* pentru Tehnică *și Tehnologii Militare* (ACTTM) (Dumitrache 2023).

2.15. O schimbare în structura militară actuală de comandă și de execuție

Schimbările care au loc în prezent în întreaga societate atât din punct de vedere tehnologic, cât și la nivel societal profund trebuie să fie abordate în mod corespunzător, în viitor, de factorii de decizie militari. Structurilor militare actuale de comandă și de execuție pare să le fie greu să țină pasul cu inovațiile tehnologice în războiul din Ucraina.

În concluzie, "smart war" sau „războiul smart" ar însemna nu doar un nou mod de a duce războiul, ci și o strategie cu totul nouă, bazată pe o abordare integrată, dinamică, inovatoare și interdisciplinară a noilor evoluții tehnologice și societale, plus, cel puțin, toate caracteristicile menționate mai sus, precum și o schimbare dramatică a mentalității în ceea ce privește războiul, mai orientată spre viitor. Și putem, de fapt, începe „războiul smart" acționând chiar acum în lumina schimbărilor pe care le putem vedea deja întâmplându-se în societatea noastră, iar cuvântul-cheie este într-o manieră „integrată".

3. Diferențe între conceptul nostru de *„război smart” (”smart war”)* și conceptul chinezesc de „război inteligent” sau alte concepte asemănătoare

În primul rând, viziunea chineză tinde să vadă „războiul inteligent” ca pe ceva în viitor, în timp ce noi vedem „războiul smart” ca pe ceva ce poate fi făcut chiar acum. Din punct de vedere tehnologic, avem deja capacitățile necesare, din punct de vedere conceptual și organizatoric, nu le avem. În același timp, presate de politică, de considerente economice, de opinia publică, de salarii, de locuri de muncă, de lobby și de contracte uriașe, viziunile occidentale tind să conceapă „războiul inteligent” drept ceva care poate fi grefat încet pe vechiul și actualul mod tradițional de a purta războiul, așa cum se întâmplă în SUA. Dar, ca să-l citez pe amiralul american Selby, acest lucru pur și simplu nu este îndeajuns de bun (Lipton 2023).

În al doilea rând, noi nu vedem „războiul smart” doar ca pe un mod specific de a duce războiul, doar ca pe un act limitat în timp, mijloace, consecințe și scop, așa cum analiștii tind să perceapă „războiul inteligent” în China, ci privim „războiul smart” ca pe un întreg proces societal, aflat în desfășurare în toate dimensiunile societății, ca parte a societății. Dacă vorbim despre „administrație smart”, „economie smart”, „oraș smart”, „societate smart” etc., cum să nu vorbim despre „război smart” în aceiași termeni de schimbare radicală profundă a societății noastre? Desigur, îngrijorările oamenilor, nu puține, asociate cu acest viitor, trebuie abordate cât mai temeinic, sunt foarte serioase. Dar trebuie să vorbim despre ele și să începem să construim nu doar tehnologic, ci și conceptual viitorul cadru al „războiului smart”, cu accent pe apărare. Din acest punct de vedere, strategia de a duce și de a conceptualiza războiul a rămas cu mult în urma dezvoltării societății. Cercetătorii vorbesc deja despre a treia etapă a civilizației umane, așa după cum am arătat mai sus, iar acest lucru este valabil și pentru război.

În al treilea rând, actualele structuri militare de comandă, execuție și comunicare par să nu poată ține pasul cu dezvoltarea tehnologică. Așadar, trebuie să ne gândim serios la inovație în ceea ce privește structurile de comandă și execuție și în domeniul militar, dacă dorim ca factorul uman și decizia să prevaleze asupra IA în viitor. Acest aspect nu pare a fi abordat serios nici de partea occidentală, nici de partea chineză care inovează „războiul inteligent”, dar îl vedem ca pe o parte indispensabilă a „războiului smart” în viitor. Din nou, există o legătură indisolubilă a „războiului smart” cu dimensiunea societală, deoarece structurile umane de comandă și execuție fac și ele parte din societate. Având în vedere rigiditatea structurilor actuale de comandă militară, poate că această schimbare este și una dintre cele mai dificile de făcut. Dar asta nu înseamnă că trebuie făcută neapărat brusc, imediat, ci înseamnă că trebuie să începem să ne gândim la asta de astăzi.

O altă diferență-cheie între ceea ce înțelegem noi prin „război smart” și alte concepte similare este importanța acordată *soft power*. Cercetătorii chinezi se concentrează mai mult pe operațiunile psihologice și cognitive, mult prea puțin pe *soft power*,

cunoscându-și poate deficiențele în acest domeniu, în comparație cu Occidentul (deși, destul de târziu, cercetătorii chinezi au început să-și dea seama de greșeala lor de a neglija acest domeniu esențial al relațiilor internaționale actuale, în cazul lor, în ceea ce privește relația China-Asia Centrală), în timp ce conceptele occidentale tind să se bazeze prea mult pe *soft power,* atrăgând critici, precum cea pe care am citat-o la începutul analizei noastre (Toma și Ghinea 2023). *Soft power* este o parte esențială și foarte importantă a ceea ce înțelegem prin „război smart", dar într-o formulă echilibrată – nu prea puțin, ca în cazul Chinei, dar nici prea mult sau aplicat profund greșit, așa cum a făcut Occidentul în Afganistan – și ținând cont de particularitățile locale. Poate puțini oameni își dau seama, dar chiar și România are un potențial uriaș de *soft power* într-o regiune foarte vastă, care se întinde din Grecia până în Croația, Polonia și Cehia, iar acest potențial nu este exploatat deloc. Vom evidenția într-o analiză viitoare câteva elemente esențiale ale unei astfel de strategii de *soft power* pentru România.

Nu în ultimul rând, trebuie să ne gândim la „războiul smart" nu ca la ceva opțional sau conjunctural, sau ca la ceva ce putem lăsa pentru mai târziu. Trebuie să ne gândim la „războiul smart" ca la ceva obligatoriu, ceva ce trebuie făcut chiar acum și ceva care ar trebui luat în considerare ori de câte ori facem noi achiziții, în orice program nou de dezvoltare umană și tehnologică etc. Deci, este nevoie de o întreagă strategie pentru „războiul smart", începând chiar de acum. Și această strategie, așa după cum am arătat, nu se limitează doar la progresul tehnologic, ci și la modul în care încorporăm acest progres tehnologic conceptual, teoretic, în modul în care societatea noastră este organizată și funcționează și mai ales în forțele de apărare a societății noastre.
Este vorba despre modul în care ne modelăm toate acțiunile noastre prezente pentru a ieși în întâmpinarea viitorului, așa cum îl putem noi interpreta acum, pe baza a ceea ce se întâmplă deja concret astăzi. Despre asta este vorba într-un model integrat de „război smart".

4. Obstacole în calea implementării unui model integrat de „război smart"

De ce „războiul smart" nu este dezvoltat și implementat mai rapid? Unul dintre principalele obstacole în calea inovației și a acestei abordări integrate a „războiului smart", pe care o susținem, derivă, de fapt, din considerente politice și din partea unor diferite persoane sau entități aparținând actualului stabiliment civil sau militar, după cum observăm din diferitele achiziții militare, efectuate de oficialii români și după cum o dovedește cu siguranță și o analiză explicită din SUA pe care o citățm mai jos.
Așadar, câteva dintre motivele pentru care „războiul smart" nu este în prezent conceptualizat, analizat, dezvoltat și desfășurat, nici măcar în unele dintre cele mai puternice armate din lume, sunt aceleași cu motivele descrise în această analiză a *New York Times*, scrisă de Eric Lipton, despre marina militară a SUA și eforturile acesteia de modernizare. Ken Perry, fost căpitan de submarin nuclear din SUA

și *„care este acum director la ThayerMahan, o companie din Connecticut care a inventat un dispozitiv fără pilot care urmărește submarinele inamice cu o fracțiune din costul navelor mari pe care le folosește Marina”,* rezumă clar faptul că *„ei refuză să ia bani din programele moștenite, aflate în derulare. (…) Marina, marea industrie și alte părți-cheie implicate au interese în actualul proces de construcții navale”* (Lipton 2023). Mai mulți contractori pentru armata și marina americană așteaptă contracte mari pentru vehicule fără pilot, dezvoltate de ei, dar acest lucru pur și simplu nu se întâmplă. Nu încă.

De asemenea, autorul trage concluzia rațională că *„o nouă generație de nave mai ieftine și mai flexibile ar putea fi vitală în orice conflict cu China, dar Marina rămâne strâns legată de programe mari de construcții navale, generate de tradiție, influență politică și locuri de muncă”* (Lipton 2023). Tot acesta subliniază că obstacolele în calea implementării noilor tehnologii și moduri de gândire militară sunt următoarele: *„Marina militară, spun analiștii și actualii și foștii oficiali, rămâne strâns legată de forțele politice și economice care au produs politici de achiziții, concentrate pe locurile de muncă, ce produc nave de război puternice, dar greoaie, care pot să nu mai fie ideale pentru misiunea cu care se confruntă. O reticență față de asumarea de riscuri – și încălcarea tradițiilor –, amestecată cu bravada și încrederea în puterea flotei tradiționale au împiedicat grav progresul Marinei militare, au declarat, pentru The New York Times, câțiva oficiali de rang înalt plecați recent din Marina militară și Pentagon”* (Lipton 2023). Acestea sunt obstacolele în calea „războiului smart” pe care îl analizăm.

Un înalt ofițer al SUA, amiralul Selby, a încercat să implementeze mai bine aceste noi tehnologii în Marina SUA și *„a propus ca Marina să creeze un nou post de ofițer de rang înalt care să aibă autoritatea și finanțarea pentru a construi o așa-numită flotă hibridă în care noua generație de vehicule fără pilot ar opera, împreună cu navele de război tradiționale”* (Lipton 2023). Este o idee formidabilă, ar trebui să ne gândim foarte serios să o implementăm și noi.
Cu toate acestea, a fost refuzat, ceea ce l-a făcut să tragă concluzia că *„acum te confrunți cu mașinăria sistemului — oameni care vor doar să continue să facă ceea ce am făcut dintotdeauna. (...) Procesul de bugetare, procesele din Congres, eforturile de lobby din partea industriei. Totul este conceput pentru a continua să producem ceea ce avem deja și să le facem un pic mai bune. Dar asta nu este destul.”* (Lipton 2023)
Este exact ceea ce subliniem în această analiză: doar adaptarea tehnologiilor moderne la echipamentele de război convenționale și la modul de gândire convențional pur și simplu nu este destul pentru a rămâne în frunte în ceea ce urmează. Trebuie să dezvoltăm o viziune și o strategie integrate despre ce va fi viitorul „război smart” și să începem să le implementăm. Orice achiziție, orice inovație, orice dezvoltare, orice capacitate industrială pe care le vom face de acum înainte trebuie luate în considerare și puse în valoare, în funcție de elementele din cadrul unui plan strategic pentru „războiul smart” pe care trebuie să-l avem.

5. De ce un „război smart" ar fi o alegere foarte bună pentru capacitățile defensive ale României?

În primul rând, capacitățile militare ale României sunt în urmă față de ceea ce este necesar chiar în acest moment pentru o apărare și o prezență încrezătoare la Marea Neagră. România nu își poate permite sumele mari de bani necesare pentru actualizarea echipamentelor vechi și pentru achiziționarea cantităților mari de echipamente militare convenționale necesare construirii unei forțe militare de apărare foarte puternice. Mutarea centrului atenției către capabilități militare „smart" poate însemna cheltuieli mai mici, în același timp păstrând un avans în dezvoltarea și implementarea echipamentelor moderne de top pentru un „război smart". *Dacă suntem atât de mult în urmă, înseamnă că trebuie să gândim înainte.*

Eric Lipton, autorul analizei foarte interesante de la *New York Times,* citată anterior, subliniază, de asemenea, marea diferență de cost între războiul convențional de astăzi și „războiul smart" de mâine, ceea ce reprezintă și unul dintre argumentele noastre cheie: *„Funcționând cu un buget care a fost mai mic decât costul combustibilului pentru una dintre marile nave ale Marinei, personalul din Marină și contractorii au realizat bărci-dronă, nave submersibile fără pilot și vehicule aeriene capabile să monitorizeze și să intercepteze amenințările de pe sute de mile din Golful Persic, cum ar fi bărci rapide iraniene care caută să deturneze petrolierele."* (Lipton 2023)

În al doilea rând, România beneficiază de un număr considerabil de mare de oameni implicați în domeniul inovator al cercetării IT, programării, securității cibernetice, așadar are un capital uman în această direcție. Un alt motiv bun pentru ca România să implementeze un „război smart" ar fi că acesta pare să dea roade pe câmpul de luptă, mai ales pentru armatele mai slabe sau mai mici împotriva adversarilor mai mari. Ucraina a reușit să reziste și chiar să contraatace armata rusă, folosind un amestec complex de caracteristici de „război smart", neconceptualizate în acest mod, dar variind de la o diplomație publică foarte bună la inovație și la utilizarea eficientă a dronelor navale, ceea ce a culminat cu o înfrângere pentru Flota Mării Negre a Federației Ruse.

Ținând cont de toate cele de mai sus, sub nicio formă nu vrem să spunem că armele și munițiile convenționale nu ar mai trebui să fie achiziționate, fabricate sau folosite, ori că nu sunt importante. Bineînțeles că sunt încă foarte importante, bineînțeles că ar trebui să existe investiții în fabricarea și achiziționarea de arme convenționale și muniție și, în special, în instalații de fabricare a prafului de pușcă, dar ar trebui să schimbăm treptat perspectiva spre „războiul smart" care va urma, și investițiile mari în termeni financiari, dar mai ales în termeni de timp și efort, ar trebui făcute având în vedere aceasta, având în vedere ceea ce urmează.

România are o oportunitate unică în acest sens, similară modului în care a decurs dezvoltarea infrastructurii de internet în România cu ceva timp în urmă. Întrucât

țara noastră nu avea infrastructură anterioară de internet, atunci când această infrastructură a fost implementată în România s-au folosit tehnologii și echipamente moderne și de aceea avem acum una dintre cele mai fiabile, rapide și mai ieftine conexiuni la internet din lume (Dumitrescu 2022). *Ar trebui să facem și acum exact același lucru cu capacitățile și echipamentele noastre actuale de război – din moment ce ne lipsesc suficiente echipamente defensive de război convenționale, ar trebui să sărim peste câteva etape și să investim mult în cele mai noi și mai eficiente echipamente «smart» de război, care sunt viitorul.* Războiul din Ucraina nu poate fi mai clar în această privință.

Din perspectiva războaielor viitoare, raportat la rămânerea în urmă atât în ceea ce privește gândirea strategică, cât și echipamentele, poate că un exemplu bun ar fi noua achiziție, pentru Marina Română, a două nave de deminare second hand din Marea Britanie, care le înlocuiește pe acestea cu drone maritime (Jipa 2023). Este greu de explicat de ce se întâmplă acest lucru, de ce se achiziționează echipamente atât de vechi, având în vedere faptul că, încă de dinainte de izbucnirea războiului din Ucraina, au existat pledoarii explicite din partea militarilor români profesioniști cu privire la importanța investiției, dezvoltării și implementării dronelor maritime și aeriene cu diverse utilizări (Eremia 2020). Poate este doar un exemplu de lipsă de strategie cu privire la noul „război smart".

Un alt exemplu ar fi achiziționarea foarte scumpă de aeronave F16 second hand din Norvegia și a deja parțial depășitelor drone Bayraktar din Turcia. Bineînțeles că România are nevoie de avioane moderne și în număr chiar mai mare decât în prezent, dar oficialii români ar fi trebuit poate să se concentreze pe achiziționarea de avioane și drone mai avansate tehnologic (și, de ce nu, noi?). Există din ce în ce mai multe voci care susțin că până și F35-urile sunt considerate a fi unele dintre ultimele avioane de luptă de acest tip. În ciuda excentricităților sale, Elon Musk are o anumită viziune pentru viitor și, în 2020, la un simpozion despre războiul aerian în SUA, a afirmat explicit în fața înalților comandanți ai forțelor aeriene americane faptul că *„era avioanelor de vânătoare a trecut"* și că *„viitorul aparține războiului bazat pe drone cu autonomie locală"* (Cohen 2020). Nu ar putea fi mai clar decât atât. Ca să nu mai vorbim despre timpul și resursele necesare pregătirii unui singur pilot de avion de vânătoare, de exemplu, în comparație cu antrenamentul și resursele necesare pregătirii unui operator de dronă.

Cuvintele lui Elon Musk l-au făcut să cadă pe gânduri chiar și pe generalul Mike Holmes, șeful US Air Combat Command, care ar fi spus că *„următoarea decizie pe care trebuie să o fac este atunci când... Block 30 și F-16 mai vechi, când vor trebui să fie înlocuite, cu ce le voi înlocui? Vreau să lucrez cu alternative pentru a răspunde la această întrebare". „Voi mai vrea să le înlocuiesc pe toate cu F-35 sau voi începe să fac altceva, așa cum a vorbit Elon sau așa cum discut eu cu Will Roper [șeful de achiziții al Forțelor Aeriene]?"* (Cohen 2020) Iar aceasta este exact ceea ce toată lumea ar trebui să se întrebe serios înainte de a adopta strategii reale de „război smart" pentru viitor. Și este exact ceea ce ar trebui să facă și România.

Concluzii

Înțelegem problemele complexe din spatele unor puternice companii tradiționale producătoare de echipamente pentru apărare, înțelegem problemele politice, cu locurile de muncă și cu oamenii, la fel cum s-a arătat și în articolul din *New York Times*, dar, atunci când vorbim despre securitate și război modern, recalibrarea la un „război smart” este obligatorie. Putem vedea cum chinezii fac deja asta. Și recalibrarea la un alt mod de a gândi este și ea o necesitate. Ucraina învață deja asta pe calea cea mai grea. Noi ar trebui să fim inteligenți și să învățăm acest lucru pe calea mai ușoară și să ne pregătim dinainte pentru orice ar putea veni. Pentru strategia de securitate națională a României, care a fost întotdeauna una defensivă, investițiile majore în cercetare și în producția națională de drone, precum și în capabilități de război electronic, în loc de echipamente masive învechite (sau care vor fi în curând depășite) și foarte scumpe, ar trebui să fie o necesitate. Aceasta ar fi o gândire „smart”.

Desfășurarea cu succes a unui „război smart” nu trebuie privită în termeni de tehnologii „smart” individuale, aplicate în diferite structuri ale armatei și în moduri diferite, deoarece acest lucru nu va fi suficient. „Războiul smart” modern trebuie să fie conceptualizat într-o manieră cuprinzătoare, integrată și interdisciplinară, încorporând contribuții atât din partea profesioniștilor militari, cât și a celor civili, menite să ofere poate chiar acel salt în tehnologie și gândire pe care generalul ucrainean Zalujnîi îl deplângea de curând că lipsește.

Referințe

Beauchamp-Mustafaga, Nathan. 2023. ”Chinese Next-Generation Psychological Warfare: The Military Applications of Emerging Technologies and Implications for the United States”. https://www.rand.org/pubs/research_reports/RRA853-1.html.

CISA [The Cybersecurity and Infrastructure Security Agency]. 2023. “People’s Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection.” https://www.cisa.gov/news-events/cybersecurity-advisories/aa23- 144a#_Toc135639517.

Cohen, Rachel S. 2020. “The Fighter Jet Era Has Passed.” *Air and Space Forces Magazine.* https://www.airandspaceforces.com/article/the-fighter-jet-era-has-passed/.

Comisarul. 2022. „Ucrainenii duc un «smart war», iar noi ne ghidăm după hărți/Furie în rândul Mercenarilor Wagner față de generalii ruși”. https://www.comisarul.ro/articol/ucrainenii-duc-un-smart-war-iar-noi-ne-ghidam-dupa_1370939.html.

Consiliul European. 2023. ”Infographic – An EU critical raw materials act for the future of EU supply chains”. https://www.consilium.europa.eu/en/infographics/critical-raw-materials/.

Danylenko, Serhiy, Nina Averianova, Tatiana Voropayeva, și Mykola Drobotenko. 2022. ”The Strategy of “Smart Power” As a Key Prerequisite For Ukraine’s Victory in The Russian-Ukrainian Neo-Imperial War.” *Almanac of Ukrainian Studies* 30: 43-53. doi:10.17721/2520-2626/2022.30.6.

Dargiel, Jessica. 2009. "'Smart Power': A change in U.S. diplomacy strategy". https://www.e-ir.info/2009/06/21/smart-power-a-change-in-us-diplomacy-strategy/.

Dumitrache, Ciprian. 2023. "În plin război al dronelor, Armata română va avea un UAV de concepție proprie. La anul ajung și primele drone Bayraktar TB2". https://m.defenseromania.ro/in-plin-razboi-al-dronelor-romania-anunta-cand-ajung-in-tara-primele-bayraktar-bonus-mapn-lucreaza-la-prima-drona-de-concepție-proprie_624823.html#google_vignette.

Dumitrescu, Radu. 2022. "Romania among EU countries with highest internet speed for households". https://www.romania-insider.com/romania-eu-countries-highest-internet-speed-households.

Eremia, Cristian. 2020. „A sosit timpul marilor investiții în drone navale militare." *Monitorul Apărării și Securității.* https://monitorulapararii.ro/a-sosit-timpul-marilor-investitii-in-drone-navale-militare-1-33035.

Erwin, Sandra. 2020. "U.S. Space Force to expand presence inside the Pentagon." *Space News.* https://spacenews.com/u-s-space-force-to-expand-presence-inside-the-pentagon/.

—. 2021. "Report: Space weapons are a fact of life, but there are many ways to counter them." *Space News.* https://spacenews.com/report-space-weapons-are-a-fact-of-life-but-there-are-many-ways-to-counter-them/.

Eugénio, António. 2013. "Smart Defense: Overcoming Hurdles and Passing Batons." *Marshall Center Occasional Paper,* no. 25. https://www.marshallcenter.org/en/publications/occasional-papers/smart-defense-overcoming-hurdles-and-passing-batons.

Harding, Luke. 2023. "A new form of warfare':how Ukraine reclaimed the Black Sea from Russian forces." *The Guardian.* https://www.theguardian.com/world/2023/oct/05/how- ukraine-reclaimed-black-sea-from-russian-forces.

Hawkins, Amy. 2023. "China's war chest: how the fight for semiconductors reveals the outlines of a future conflict." *The Guardian.* https://www.theguardian.com/world/2023/may/22/chinas-war-chest-how-the-fight-for-semiconductors-reveals-the-outlines-of-a-future-conflict.

Hlihor, Ecaterina. 2023. "Public diplomacy during military international conflicts. The Ukraine war case." *Bulletin of "Carol I" National Defence University,* no. 1. https://revista.unap.ro/index.php/bulletin/article/download/1672/1623/5597.

Jipa, Florin. 2023. "România a cumpărat două nave «vânător de mine» britanice, la mâna a doua, HMS Blyth şi HMS Pembroke. Preţul este trecut la «secret comercial»." *Monitorul Apărării și Securității.* https://monitorulapararii.ro/romania-a-cumparat-doua-nave-vanator-de-mine-britanice-la-mana-a-doua-hms-blyth-si-hms-pembroke-pretul-este-trecut-la-secret-comercial-1-51693?fbclid=IwAR1kNJliuHZIcP0GD_JQXefbM8-hfKZS1qoUjJBtQx5JlEvAwC51M2MDy04.

Lipton, Eric. 2023. "Faced With Evolving Threats, U.S. Navy Struggles to Change." *The New York Times.* https://www.nytimes.com/2023/09/04/us/politics/us-navy-ships.html.

Mail.com. 2023. "What is the Internet of Things (IoT)?" https://www.mail.com/blog/posts/the-internet-of-things/75/#.7518-stage-mmmm2-2.

Miller, Chris. 2022. *Chip War: The Fight for the world's Most Critical Technology.* Scribner Books Co.

Nagashima, Jun. 2020. "The Militarization of Space and its Transformation into a Warfighting Domain". https://www.spf.org/iina/en/articles/nagashima_02.html.

NATO. fără an. "Cognitive Warfare". https://www.act.nato.int/activities/cognitive-warfare/.

—. 2021. "Summary of the NATO Artificial Intelligence Strategy". https://www.nato.int/cps/en/natohq/official_texts_187617.htm.

Nye, Joseph S., Jr. 2005. *Soft Power: The Means to Success in World Politics.* New York: PublicAffairs Books.

Patel, V. Neel. 2020. "The US says Russia just tested an «anti-satellite weapon» in orbit." *MIT Technology Review.* https://www.technologyreview.com/2020/07/23/1005568/us-space-command-russia-test-anti-satellite-weapon-orbit-kosmos-2543/.

Pollpeter, Kevin, și Amanda Kerrigan. 2021. "The PLA and Intelligent Warfare: A Preliminary Analysis". https:// www.cna.org/reports/2021/10/The-PLA-and-Intelligent-Warfare-A-Preliminary-Analysis.pdf.

Raska, Michael și Richard A. Bitzinger. 2023. *The AI Wave In Defence Innovation. Assessing Military Artificial Intelligence Strategies, Capabilities, and Trajectories.* New York: Routledge.

Simons, Anna. 2012. "Soft War = Smart War? Think Again". https://www.researchgate.net/publication/286929221_ Soft_War_Smart_War_Think_Again.

State Council of The People's Republic of China. 2019. "China's National Defense in the New Era". https://english.www.gov.cn/archive/whitepaper/201907/24/content_WS5d3941ddc6d08408f502283d.html.

Taddeo, Mariarosaria și Luciano Floridi. 2014. *The Ethics of Information Warfare.* Springer.

Thrush, Glenn. 2011. "'Smart' war loses logic for Obama." *Politico.* https://www.politico.com/story/2011/06/smart-war-loses-logic-for-obama-057603.

Toma, Paula și Diana Ghinea. 2023. „Strategia Chinei pentru Asia Centrală (II). China la zi". *Adevărul.* https://adevarul.ro/blogurile-adevarul/strategia-chinei-pentru-asia-centrala-ii-china-2311194.html.

Trofimov, Yaroslav. 2023. "Drones Everywhere: How the Technological Revolution on Ukraine Battlefields Is Reshaping Modern Warfare." *The Wall Street Journal.* https://www.wsj.com/world/drones-everywhere-how-the-technological-revolution-on-ukraine-battlefields-is-reshaping-modern-warfare-bf5d531b.

Wu, Mingxi. 2023. *Intelligent Warfare. Prospects of Military Development in the Age of AI.* New York: Routledge.

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

Perspectiva SSSCIP asupra atacurilor cibernetice derulate în contextul conflictului militar dintre Federația Rusă și Ucraina (ianuarie 2022 – ianuarie 2024)

SSSCIP's Perspective on the cyber-attacks unfolded in the context of the military conflict between Russia and Ukraine (January 2022 – January 2024)

Drd. Mihai OLTEANU*

*Universitatea Națională de Apărare „Carol I", București, România

Abstract

Lucrarea de față evaluează raportările SSSCIP privind atacurile cibernetice derulate asupra Ucrainei în perioada ianuarie 2022 – ianuarie 2024. De la exploatarea malware-ului CaddyWiper, atribuit de SSSCIP către APT SANDWORM, la campaniile sofisticate ale FSB și atacul cibernetic asupra Kyivstar, lucrarea prezintă o perspectivă a atacurilor cibernetice de origine rusă derulate asupra Ucrainei, așa cum au fost raportate de autoritatea ucraineană în domeniu. Scopul articolului este acela de a identifica modul în care SSSCIP (principala instituție responsabilă pe componenta de securitate cibernetică) a raportat atacurile cibernetice asupra infrastructurilor IT&C ucrainene, completitudinea datelor publicate, precum și modalitatea în care sunt prezentate campaniile. Pentru realizarea acestui scop, au fost evaluate toate raportările SSSCIP din perioada de referință și au fost incluse în studiu doar acelea care s-au materializat și au afectat infrastructuri IT&C. În concluzii, vor fi evidențiate, în principal, limitările raportărilor SSSCIP și, secundar, perspectiva SSSCIP privind domeniile care au fost cel mai des vizate de atacuri cibernetice și capabilitățile actorilor ruși.

This paper evaluates the reports of the SSSCIP regarding cyber-attacks carried out against Ukraine from January 2022 to January 2024. From the exploitation of the CaddyWiper malware, attributed by SSSCIP to APT SANDWORM, to the sophisticated campaigns of the FSB and the cyber-attack on Kyivstar, the paper provides an insight into Russian-origin cyber-attacks against Ukraine, as reported by the main Ukrainian authority in the field, SSSCIP.
The purpose of the article is to identify how SSSCIP reported cyber-attacks on Ukrainian IT&C infrastructures, the completeness of the published data, and the way the campaigns are presented. To achieve this goal, all SSSCIP reports from the reference period were evaluated, and only those that materialized and affected IT&C infrastructures were included in the study. In conclusion, the paper will primarily highlight the limitations of SSSCIP reports and, secondarily, SSSCIP's perspective on the domains most frequently targeted by cyber-attacks and the capabilities of Russian actors.

Cuvinte-cheie:
SSSCIP; Ucraina; APT; securitate cibernetică; Federația Rusă; conflict militar.

Keywords:
SSSCIP; Ukraine; APT; cyber security; Russia; military conflict.

Info articol
Primit: 1 februarie 2024; Evaluat: 26 februarie 2024; Acceptat: 13 martie 2024; Disponibil online: 5 aprilie 2024
Citare: Olteanu, M. 2024. „Perspectiva SSSCIP asupra atacurilor cibernetice derulate în contextul conflictului militar dintre Federația Rusă și Ucraina (ianuarie 2022 – ianuarie 2024)". *Buletinul Universității Naționale de Apărare „Carol I"*, 13(1): 26-43. https://doi.org/10.53477/2065-8281-24-02

Pe parcursul ultimelor decenii, evoluția continuă a tehnologiei și extinderea semnificativă a proceselor de digitalizare de la nivelul statelor și companiilor private au determinat o creștere constantă a importanței domeniului securității cibernetice. Această creștere a determinat modificări substanțiale ale celor mai importante sectoare ale societății, notabile în domeniile politic, economic și militar. Concomitent, amenințările cibernetice au crescut în complexitate, gama de ținte existente fiind mult mai variată, compromiterea acestora oferind oportunități financiare, politice și militare (Furstenau și alții 2020).

În context politic, atacurile cibernetice au devenit una dintre principalele preocupări la nivelul statelor și organizațiilor internaționale, deoarece compromiterea unor infrastructuri IT&C poate genera dezavantaje strategice. Aspecte, precum influențarea proceselor electorale, manipularea deciziilor politice și subminarea stabilității instituțiilor guvernamentale, au devenit amenințări la adresa domeniului politic. Instrumentalizarea atacurilor cibernetice s-a cristalizat într-un mijloc strategic de atingere a obiectivelor geopolitice atât pentru actorii statali, cât și pentru cei nonstatali (Visvizi și Lytras 2020, 333-336). Un exemplu în acest sens este actorul cibernetic APT28, care, conform raportărilor companiilor din industria de securitate cibernetică, acționează pentru a susține interesele Federației Ruse (FR) și a reușit compromiterea unor ținte de interes strategic de la nivelul unor state (precum Georgia, Polonia și Ungaria) sau organizații (precum NATO și OSCE) (Mcwhorter 2014).

În domeniul economic, digitalizarea extensivă a mediului de afaceri a generat inerent o serie de amenințări cibernetice, care pot afecta nu doar confidențialitatea informațiilor, ci și integritatea financiară și reputația organizațiilor. Furtul de date, spionajul industrial și diversele forme de șantaj cibernetic reprezintă elemente de risc la nivelul mediului public și al celui privat, care pot afecta buna funcționare a entităților economice (Hernandez-Castro și Cartwright 2020). Incidente notabile, precum campania cibernetică WannaCry, au ilustrat potențialul distructiv al amenințărilor cibernetice, având un impact direct asupra sectoarelor economice și industriale (Hernandez-Castro, Cartwright și Stepanova 2017).

În sfera militară, dependența sporită de sisteme informatice avansate a expus infrastructura militară la riscuri cibernetice semnificative. Complexitatea operațiunilor militare moderne impune o interconectivitate crescută între sistemele de comunicații și control, amplificând astfel vulnerabilitățile la atacurile cibernetice. De asemenea, atacurile cibernetice au devenit un instrument folosit de state, inclusiv ca parte a conflictelor militare, notabil în acest sens fiind conflictul dintre FR și Ucraina (UA), început în februarie 2022. Literatura de specialitate existentă până în acest moment oferă analize

[1] WannaCry a reprezentat o campanie cibernetică de tip ransomware, care a avut loc în mai 2017. Odată infectat un sistem, WannaCry cripta fișierele utilizatorilor și solicita plata unei răscumpărări în moneda virtuală Bitcoin, pentru eliberarea acestora. Atacul a avut impact global, afectând organizații importante, inclusiv sistemul de sănătate din Marea Britanie, companii din sectoarele energetic și financiar, generând alarmă cu privire la vulnerabilitatea infrastructurilor critice în fața amenințărilor cibernetice (Mohurle și Patil 2017).

privind atacurile cibernetice asupra unor domenii specifice, fără a exista evaluări extinse cu privire la cele mai importante campanii cibernetice, indiferent de ținta acestora, derulate împotriva UA, începând cu anul 2022. În context, scopul acestui studiu este acela de a analiza raportările oficiale, realizate de autoritățile ucrainene cu privire la cele mai importante atacuri cibernetice din perioada ianuarie 2022 – ianuarie 2024, care au afectat diverse sectoare de activitate. După analizarea acestora, vor fi formulate o serie de concluzii, în principal cu privire la modul de raportare al SSSCIP și, în plan secund, cu privire la atacurile cibernetice, în contextul conflictului dintre FR și UA.

Pentru derularea acestui studiu, vor fi folosite, cu precădere, raportările realizate de SSSCIP[2] UA, principalul serviciu ucrainean privind securitatea cibernetică, aflat sub controlul Președintelui, care desfășoară atât activități pentru stabilirea politicilor în domeniul protecției infrastructurilor IT&C (inclusiv rețelele clasificate ale UA) (Cyber Security Intelligence 2022), cât și intervenții, în cazul unor atacuri cibernetice (prin intermediul CERT-UA) (Temple-Raston 2023). Motivul axării pe raportările SSSCIP este acela că lucrarea își propune să analizeze atacurile cibernetice din perspectiva UA.

[2] Державна служба спеціального зв'язку та захисту інформації України – Serviciul de Stat pentru Comunicații Speciale și Protecția Informațiilor.

Este important de precizat faptul că atacurile cibernetice din cuprinsul rapoartelor SSSCIP variază în complexitate și relevanță din două puncte de vedere: (1) impactul pe care l-au produs asupra infrastructurilor IT&C atacate și (2) nivelul capabilităților tehnice deținute de atacator (Agrafiotis și alții 2018). În acest sens, este relevant că cele mai comune tipuri de atacuri cibernetice sunt cele de *phishing*, care presupun utilizarea unor tehnici de inginerie socială pentru a încerca să convingă ținta să acceseze un conținut cu potențial malware (Khonji, Iraqi și Jones 2013, 2091-2121). Cele mai multe atacuri de tip phishing nu au succes, aspect determinat de factori multipli, printre care capabilitățile reduse ale atacatorilor și utilizarea unor tehnici de inginerie socială documentate insuficient sau a unor programe malware cu nivel redus de complexitate, ușor de detectat de către soluțiile de securitate cibernetică (Patil și alții 2022). Astfel, din punct de vedere metodologic, pentru ca rezultatele din cadrul acestui articol să fie relevante, vor fi excluse acele raportări ale SSSCIP care fac referire doar la campanii de tip phishing despre care nu se menționează că au avut un impact la adresa infrastructurilor IT&C țintite. În acest sens, este important de menționat că, în intervalul de referință, au fost întocmite 435 de rapoarte publice de către SSSCIP, însă, în urma analizei preliminare, 394 dintre acestea fac referire strict la campanii cibernetice de tip phishing. Despre acestea, nu este menționat că ar fi reușit să compromită oricare dintre țintele urmărite, motiv pentru care nu au fost incluse în cadrul articolului. Pe baza acestor criterii, au fost selectate 41 de articole, care vor fi evaluate pentru evidențierea unor concluzii privind securitatea cibernetică, în contextul conflictului dintre FR și UA.

Literatura de specialitate în domeniu

În ceea ce privește analiza asupra componentei atacurilor cibernetice, în contextul conflictului dintre FR și UA, lucrările existente urmăresc impactul atacurilor asupra anumitor domenii sau în perioade de timp reduse. Davydiuk și Zubok fac o evaluare a domeniului energetic din UA din perspectiva rezilienței la atacuri cibernetice și a posibilității generării unor efecte în cascadă asupra altor sectoare de activitate, aspecte care dezavantajează UA în cadrul conflictului (Davydiuk și Zubok 2023, 121-139). Au fost publicate analize similare, inclusiv, asupra sectorului financiar din UA, cu privire la caracteristicile atacurilor și amenințărilor cibernetice, în contextul conflictului FR-UA. Astfel, sunt analizate tendințele atacurilor cibernetice asupra industriei financiare, fiind identificată utilizarea activă a mesajelor SMS și a e-mailurilor cu linkuri sau coduri malware (Kloba și Kloba 2022, 19-28). CERT-EU a publicat constant evaluări asupra unor atacuri cibernetice, derulate împotriva UA și identificate de diverse entități publice sau private (CERT-EU 2023). Totuși, aceste lucrări adoptă o perspectivă focalizată strict pe anumite domenii de activitate (precum cele centrate pe sectoarele energetic și financiar) sau urmăresc o evaluare, din perspectiva entităților externe conflictului. Comparativ, această lucrare vizează strict raportările realizate de UA prin instituțiile abilitate.

Marcus Willet analizează posibilitatea escaladării conflictului dintre FR și UA la nivelul comunității internaționale, prin implicarea NATO (pe baza dreptului internațional), ca urmare a unor atacuri cibernetice mai ample (Willett 2022, 7-26). Evoluția conflictului, din perspectiva securității cibernetice, este analizată inclusiv considerând implicarea unor actori nonstatali neanticipați în februarie 2022, dar care au avut un rol semnificativ (Lonergan, Smith și Mueller 2023, 85-102). Richard Wilson include, în lucrarea sa, posibilitatea ca atacurile cibernetice, în contextul conflictului FR-UA, să conducă la declanșarea unor evenimente de natură nucleară, în mod intenționat sau incidental (Wilson și Fitz 2023, 440-448). De asemenea, există lucrări care au încercat să construiască o strategie pe componenta de securitate cibernetică, menită să permită asigurarea rezilienței, concluzionând că îmbunătățirea sistemului de securitate cibernetică se află într-o fază incipientă (Tarasenko și alții 2022, 583-599).

Literatura în domeniu include o serie de lucrări privind implicarea unor entități nonstatale, atrase în conflictul dintre FR și UA, cu precădere a entității denumite Ukraine IT Army, creată de autoritățile de la Kiev cu scopul de a reuni experți, indiferent de proveniența acestora, pentru a ajuta UA să combată atacurile cibernetice (Soesanto 2023, 93-106). Similar, Smith și Dean evaluează eficiența Ukraine IT Army și capacitatea de a gestiona aproximativ 200.000 de experți voluntari care au decis să se alăture entității (Smith și Dean 2023, 103-119). Există lucrări care evaluează implicarea unor entități externe pentru a sprijini UA, precum marile companii din domeniul tehnologic (de exemplu, Google, Microsoft, Meta, Apple și Amazon), și impactul generat de acest aspect (Matania și Sommer 2023). Alături de companiile private, au existat și state sau organizații internaționale (precum UE) care au trimis echipe ce pot sprijini UA pe componenta de asigurare a securității cibernetice (Sullivan 2023, 9-23).

Analiza atacurilor cibernetice asupra UA pe parcursul anului 2022

Pe parcursul anului 2022, au fost identificate un număr semnificativ de atacuri cibernetice derulate asupra infrastructurilor IT&C de pe teritoriul UA, cele mai relevante în acest sens fiind:

- În noaptea dintre 13 și 14 ianuarie 2022, website-urile mai multor organizații publice din UA au fost țintele unui atac cibernetic. Conform SSSCIP, atacul a inclus afișarea unor imagini provocatoare, în unele cazuri, criptarea sau ștergerea datelor (SSSCIP 2022a). Atacul a fost estimat ca fiind planificat în avans și a implicat diverse tipuri de malware, inclusiv distructiv (denumit WhisperKill), care avea drept scop indisponibilizarea infrastructurilor (CERT-UA 2022a). SSSCIP nu a inclus date cu privire la posibila asociere sau atribuire a campaniei de atacuri unei entități statale sau nonstatale. Conform Microsoft, țintele au fost atât organizații guvernamentale și nonguvernamentale, cât și companii private (Microsoft 2022).
- La data de 15 februarie 2022, un atac semnificativ de tip DDoS[3] a vizat compromiterea unor infrastructuri IT&C care aparțin unor organizații publice (printre care website-ul Ministerului Apărării și cel al Forțelor Armate) și private (precum Privatbank și Oschadbank, care au fost compromise) (SSSCIP 2022e). Conform autorității ucrainene, aceeași campanie de atacuri cibernetice a fost identificată și în seara zilei de 23 februarie 2022, cu o zi înainte de invazia FR în UA. De această dată, atacurile cibernetice s-au intensificat, fiind vizate website-urile Cabinetului de Miniștri, Verkhovna Rada (Parlamentul UA), Ministerului Afacerilor Externe și Serviciului de Securitate. În aceeași zi, SSSCIP raporta o intensificare a campaniilor de distribuție malware, a încercărilor de penetrare a infrastructurilor IT&C publice și private și a tentativelor de distrugere a datelor. De această dată, SSSCIP preciza că este clar faptul că aceste campanii au fost derulate de *„statul agresor”* (SSSCIP 2022r).

  Prezintă relevanță în context faptul că intensificarea atacurilor cibernetice s-a sincronizat cu debutul conflictului, ceea ce creează premisele unor acțiuni conjugate din partea FR asupra UA (Lewis 2022).

  La data de 6 martie 2022, SSSCIP publica o statistică, prin care anunța că numărul de atacuri cibernetice este în continuare unul record, ajungând la 2.800. De asemenea, a fost înregistrat un număr record, de 271 de atacuri de tip DDoS în 24 de ore. Aceste acțiuni au fost atribuite în totalitate Federației Ruse, autoritatea ucraineană susținând că sunt derulate în completarea atacurilor din aer, apă și de pe uscat (SSSCIP 2022q).

  Mai mult, la data de 25 martie SSSCIP a anunțat că, numai în săptămâna 15-22 martie, a înregistrat 60 de atacuri cibernetice, dintre care 11 asupra autorităților locale și centrale, 8 asupra sectorului de apărare, 6 asupra sectorului financiar, 6 asupra organizațiilor comerciale,

[3] Atacurile cibernetice de tip DDoS vizează întreruperea serviciilor, ca urmare a unor încercări repetate de epuizare a unei aplicații prin trafic de date excesiv (Microsoft, fără an).

4 asupra sectorului de telecomunicații, 2 asupra domeniului energetic, iar restul au vizat alte entități publice și private (SSSCIP 2022p).

➢ La data de 15 martie 2022, SSSCIP publica informații privind un nou malware care urmărește ștergerea datelor din sistemele compromise, denumit în industria de specialitate CaddyWiper. Prezintă relevanță că este primul caz în care SSSCIP citează două companii private (Eset și Microsoft) cu privire la identificarea acestui malware (SSSCIP 2022b). Campania a vizat entități din domeniul energetic și a avut drept obiectiv întreruperea alimentării cu energie electrică pe teritoriul UA, fiind atribuită actorului cibernetic de origine rusă APT SANDWORM (CERT-UA 2022b).

Prezintă interes și faptul că APT SANDWORM a fost atacatorul către care a fost atribuită campania cibernetică, din anul 2015, derulată asupra UA, care a avut drept țintă rețeaua energetică națională (Paverman 2019).

➢ La data de 6 aprilie 2022, SSSCIP a publicat date cu privire la un atac cibernetic care a avut drept țintă infrastructura UKRTELECOM, cea mai mare companie ucraineană de telefonie mobilă. Conform investigațiilor, atacul a avut un nivel ridicat de complexitate și a fost lansat de pe teritoriile ocupate la acel moment de către FR, iar scopul a fost acela de a prelua controlul infrastructurii de comunicații. În context, UKRTELECOM a fost nevoită să reducă la 13% capacitatea infrastructurii, pentru a permite echipelor de specialiști să prevină materializarea intențiilor atacatorilor. UKRTELECOM și SSSCIP au reușit refacerea infrastructurii și au menționat că nu dețin date suficiente încât să atribuite campania unui atacator specific (SSSCIP 2022c).

➢ La data de 11 aprilie 2022, a fost comunicat un anunț privind dificultățile de asigurare a comunicațiilor mobile pe teritoriul UA, SSSCIP derulând constant eforturi pentru menținerea activității furnizorilor de Internet și a celor de telecomunicații, precum Vodafone. Conform estimărilor, la acel moment doar 65% din infrastructura telecom a rămas operațională, afectând astfel posibilitatea ca cetățenii să comunice pe teritoriul UA (SSSCIP 2022i).

➢ La data de 12 aprilie 2022, SSSCIP a anunțat desfășurarea unor acțiuni de prevenire a unei noi campanii cibernetice derulate de APT SANDWORM, care a vizat întreruperea alimentării cu energie electrică pe teritoriul UA, urmărind compromiterea echipamentelor de rețea de la nivelul întreprinderilor private. Similar exemplului din data de 15 martie 2022, SSSCIP anunța faptul că a avut parte de sprijinul ESET și MICROSOFT în eforturile de prevenire a materializării atacului cibernetic. UA a declarat, de asemenea, faptul că menține cooperarea cu statele europene prin schimbul de informații cu privire la acest atac cibernetic. Totuși, SSSCIP menționează că scopul cooperării este acela de a identifica existența altor infrastructuri energetice de pe teritoriul UA compromise de APT SANDWORM (SSSCIP 2022h).

➢ O zi mai târziu, la data de 13 aprilie 2022, SSSCIP anunța că a primit informații de la partenerii internaționali privind compromiterea unei companii de distribuție a energiei electrice de către actorul rus APT SANDWORM, scopul fiind acela de a întrerupe alimentarea cu energie electrică a unei părți importante din teritoriul UA. La momentul intervenției,

atacul cibernetic era în desfășurare, reușind compromiterea unor resurse, însă fără a materializa intenția finală. Mai mult, SSSCIP a anunțat continuarea creșterii numărului atacurilor cibernetice, în special de tip DDoS, fiind identificate aproximativ de 25 de ori mai multe atacuri de acest tip, comparativ cu anul anterior (SSSCIP 2022l).

- Ulterior, la data de 16 aprilie 2022, SSSCIP anunța o nouă campanie de atacuri cibernetice de tip DDoS care a avut drept țintă website-urile unor autorități publice, reușind indisponibilizarea temporară a acestora. În urma intervenției echipelor tehnice, website-urile au fost repuse în funcțiune (SSSCIP 2022n).
- Pe parcursul lunii mai 2022, au fost continuate încercările de întrerupere a comunicațiilor, atacatorii reușind oprirea permanentă a acestora în zona Kherson, ocupată de FR. Locuitorii nu mai aveau acces la comunicații mobile sau Internet, iar SSSCIP anunța că nu poate face nimic în acest sens, zona aflându-se sub ocupație militară, iar echipamentele, controlate. Concomitent, autoritățile ucrainene anunțau că, în absența mijloacelor de comunicare, soldații FR patrulează și transmit prin sisteme audio știri propagandiste, pentru influențarea cetățenilor fără acces la comunicații în afara zonei. Mai mult, SSSCIP anunța că estimează că cetățenilor din zona Kherson le va fi oferit accesul la rețeaua telecom a FR, controlată de statul agresor (SSSCIP 2022m). La finalul anului, în noiembrie 2022, SSSCIP comunica faptul că a reușit restabilirea accesului la posturile de radio și televiziune ucrainene în Kherson, cu ajutorul companiei poloneze Emitel SA (SSSCIP 2022t).
- La data de 6 iunie 2022, SSSCIP informa că se află în derulare o campanie cibernetică, dublată de acțiuni propagandiste, prin care s-a reușit compromiterea celor mai importante rețele de televiziune ucrainene, în cadrul cărora s-au difuzat știri rusești. Știrile au fost difuzate în timpul în care televiziunile ucrainene transmiteau meciul de calificare al echipei naționale la campionatul mondial de fotbal. Cel mai probabil, atacatorii au reușit să obțină acces la un nod de comunicații TV, prin intermediul căruia au transmis traficul modificat (SSSCIP 2022j).

Până la finalul anului 2022, nu au fost publicate alte atacuri cibernetice de către SSSCIP, cu toate că au existat anumite campanii, raportate de industria privată, printre care întreruperile de energie electrică, din intervalul 10-12 octombrie 2022, conform raportării MANDIANT (Proska și alții 2023). De asemenea, SSSCIP nu a publicat un raport cu privire la campania asupra modemurilor satelitare VIASAT care funcționează în bandă KA și care au fost indisponibilizate pe teritoriul UA și al multor state europene (printre care Polonia, Marea Britanie, Franța), ca efect secundar (Boschetti, Gordon și Falco 2022). Cu toate acestea, multe state europene au atribuit această campanie cibernetică Federației Ruse, în anul 2022 (Steinbrecher 2022). Singura mențiune cu privire la această campanie, făcută de SSSCIP, a fost la data de 2 iulie 2022, când a precizat că UA folosește infrastructura satelitară STARLINK, pusă la dispoziție de către Elon Musk, pentru a asigura comunicațiile de rezervă, în cazul unui atac cibernetic asupra infrastructurii principale (SSSCIP 2022o).

Pe parcursul anului 2022, au mai existat raportări statistice privind intensitatea atacurilor cibernetice (de 3 ori mai mare decât în anul anterior (SSSCIP 2022u), domeniile vizate (cu precădere telecomunicații, medical și guvernamental (SSSCIP 2022g) și atacatori (în special grupări motivate ideologic și actori statali (SSSCIP 2022d). Totuși, un aspect de interes este cel din raportul din data de 1 mai 2022, când SSSCIP anunța că indiciile existente conduc către ipoteza conform căreia intensitatea atacurilor cibernetice ruse la adresa UA a atins un nivel maxim, serviciul ucrainean estimând că nu vor exista operațiuni cibernetice mai puternice (SSSCIP 2022k). Acest aspect poate indica o încercare de creștere a încrederii sociale și de menținere a atitudinii ofensive față de FR la un nivel ridicat, similar celui anterior conflictului militar (Paniotto 2020, 3-14). Pe de altă parte, este posibil ca UA să fi acționat în vederea promovării unei imagini puternice față de statul agresor, pentru a slăbi susținerea conflictului militar de către populația rusă din FR, aflată în proporție de 60% în anul 2022 (Kizilova 2022, 2-5). Demersul a fost susținut două luni mai târziu, când SSSCIP anunța faptul că intensitatea atacurilor cibernetice a continuat să se mențină la același nivel ridicat, însă calitatea acestora se afla pe un trend descendent (SSSCIP 2022f).

Un alt aspect care indică o abordare deosebită din partea SSSCIP este relevat într-un comunicat, din data de 1 mai 2022, în care UA transmitea că atacurile cibernetice rusești îndreptate împotriva infrastructurilor proprii sunt, de asemenea, un potențial atac asupra altor state partenere. Exemplificând, SSSCIP menționează că, în anul 2014, alegerile din UA au fost ținta unor atacuri cibernetice de origine rusă, iar doi ani mai târziu, același mod de operare a fost observat și în cadrul proceselor electorale ale SUA (SSSCIP 2022s). Astfel, având în vedere antecedentele pe componenta de securitate cibernetică, UA reiterează indirect necesitatea de a fi sprijinită pe parcursul conflictului, acesta nefiind de interes doar pentru cele două state participante (Ratten 2022, 265-271).

Analiza atacurilor cibernetice asupra UA pe parcursul anului 2023

În cursul anului 2023, SSSCIP a publicat un număr mai mic de comunicate cu privire la atacurile cibernetice comise împotriva rețelelor și sistemelor informatice proprii, cele mai relevante în acest sens fiind următoarele:

- La data de 1 ianuarie 2023, a fost publicat un comunicat care atribuia atacurile cibernetice, derulate prin intermediul malware-ului CaddyWiper, în luna ianuarie 2022, actorului cibernetic de origine rusă APT SANDWORM (SSSCIP 2023l), a cărui activitate este atribuită public serviciului militar de informații al FR (Akimenko și Giles 2020, 67-75).
- La data de 18 ianuarie 2023, SSSCIP a publicat o analiză privind o campanie cibernetică, ce a vizat compromiterea unor ținte din domeniul mediatic, cu precădere agenția de știri UKRINFORM. Comunicatul subliniază încercările FR de compromitere a factorilor de informare pentru populație, având drept

scop principal dezinformarea cetățenilor și, ulterior, influențarea acestora (SSSCIP 2023a).

➢ La data de 1 februarie 2023, au fost publicate o serie de investigații tehnice privind campaniile cibernetice, derulate de serviciul rus FSB asupra infrastructurilor informatice de pe teritoriul UA, fiind precizat faptul că activitatea este desfășurată prin atacuri cibernetice cu un nivel ridicat de complexitate și precizie, în contrast cu campaniile de atacuri de tip DDoS. Mai mult, SSSCIP precizează că acest tip de operațiuni ale FSB reprezintă cea mai mare amenințare cibernetică identificată pe parcursul conflictului militar (SSSCIP 2023k).

➢ O zi mai târziu, SSSCIP publica date cu privire la un atac cibernetic de tip watering hole[4], care a presupus crearea unui website, în cadrul căruia era folosită imaginea ministerului ucrainean de externe pentru a crea aparențele unui website legitim. Odată accesat, website-ul oferea vizitatorilor un program care urma să fie descărcat sub aparența unei aplicații ce putea identifica dacă sistemul utilizatorului este compromis. În realitate, aplicația avea conținut malware care ar fi infectat computerul vizitatorului website-ului, în cazul în care era instalată (SSSCIP 2023f). Campania este singura de acest tip, raportată de SSSCIP, și avea la bază exploatarea dorinței cetățenilor de a se informa cu privire la stadiul conflictului, pe baza unei surse guvernamentale de încredere.

➢ La data de 1 iulie 2023 a fost publicată o analiză cu privire la creșterea numărului atacurilor cibernetice care vizează, cu precădere, companii din domeniul IT&C de pe teritoriul UA. Scopul acestor atacuri a fost declarat ca fiind acela de a compromite aceste companii în vederea obținerii controlului asupra produselor software comercializate în UA și, ulterior, asupra utilizatorilor acestor soluții. De asemenea, SSSCIP menționează că industria privată evaluează că poate gestiona pe cont propriu acest tip de amenințări, însă există contraexemple recente care arată că mari companii din domeniu au fost compromise (SSSCIP 2023c).

➢ La 5 iulie 2023, SSSCIP a comunicat date cu privire la o campanie cibernetică ce a reușit compromiterea paginii de Facebook utilizată de Serviciul Național de Statistică al UA, atacatorii postând pe această pagină faptul că și infrastructura instituției a fost compromisă, fiind astfel indisponibilizat accesul la date statistice economice și sociale. În fapt, conform SSSCIP, atacatorii au reușit doar compromiterea paginii de Facebook, fără a avea acces la infrastructura Serviciului Național de Statistică, mesajul postat în numele instituției fiind fals (SSSCIP 2023e). Este posibil ca scopul acestor acțiuni să fi fost acela de destabilizare a încrederii populației în statisticile oficiale, publicate de UA. Astfel de acțiuni de propagandă au fost desfășurate constant de FR pe parcursul conflictului cu UA, având drept scop scăderea încrederii societății în autorități (Geissler și alții 2023).

[4] Watering hole – atac cibernetic care se bazează pe identificarea acelor website-uri utilizate, cu precădere, de grupul țintă și clonarea sau modificarea acestora astfel încât să compromită vizitatorii acelui domeniu (Krithika 2017).

➢ La data de 19 iulie 2023, SSSCIP a publicat o investigație tehnică cu privire la două aplicații malware cu complexitate tehnică ridicată, denumite CAPIBAR și KAZUAR, utilizate de APT TURLA, atribuit serviciului de informații al FR, FSB, pentru compromiterea unor ținte de pe teritoriul UA. SSSCIP notează faptul că a transmis toate rezultatele investigațiilor tehnice, inclusiv industriei private de specialitate (SSSCIP 2023j).

➢ La data de 13 decembrie 2023, SSSCIP anunța că, în urmă cu o zi, infrastructura IT&C a operatorului de telecomunicații Kyivstar a fost compromisă, astfel fiind indisponibilizată furnizarea serviciilor specifice către aproximativ 24 de milioane de clienți, câteva zile (Balmforth 2024). Pentru a reuși repunerea în funcțiune a operatorului, SSSCIP a solicitat ca serviciile roaming să fie oprite pe o perioadă limitată de timp, situație în care clienții nu au mai putut comunica în afara teritoriului ucrainean (SSSCIP 2023d). Prezintă relevanță faptul că SSSCIP nu a anunțat impactul atacului cibernetic pe website-ul oficial, însă declarațiile suplimentare, făcute de către directorul instituției pentru publicații europene, au relevat că infrastructura IT&C a Kyivstar a fost afectată în totalitate, malware-ul utilizat reușind să șteargă majoritatea datelor (Gatlan 2024), atacul fiind caracterizat drept cel mai mare din istorie asupra industriei telecom (Sapuppo 2023).

➢ Ultimul atac cibernetic, publicat de SSSCIP în perioada de referință, prezintă o campanie derulată de actorul cibernetic rus APT28, care a vizat atât ținte de pe teritoriul UA, cât și rețele și sisteme informatice din Polonia. SSSCIP transmite astfel din nou mesajul că atacurile cibernetice asupra UA nu sunt incidente izolate din punct de vedere geografic, ci pot afecta inclusiv state membre ale UE sau NATO (SSSCIP 2023i).

Prezintă interes faptul că, pe parcursul anului 2023, SSSCIP a avut o serie de raportări statistice cu privire la cele mai țintite domenii de către atacatorii cibernetici, astfel fiind menționate organizații comerciale, industria telecom, dezvoltatori software, aparatul guvernamental, sectorul de industrie și apărare, precum și autorități locale (SSSCIP 2023h). Mai mult, SSSCIP precizează faptul că, începând cu luna septembrie 2022, monitorizează cel puțin șapte actori cibernetici care vizează constant infrastructuri ale UA, toți fiind asociați guvernului FR (SSSCIP 2023g), precum și 23 de grupuri catalogate drept hacktiviste (SSSCIP 2023b).

De asemenea, este important de precizat că, până la finalul lunii ianuarie 2024, nu au fost publicate noi rapoarte cu privire la alte atacuri cibernetice derulate împotriva infrastructurilor IT&C de pe teritoriul UA.

Concluzii

Din punct de vedere metodologic, acest articol a urmărit, într-o primă etapă, selectarea și prezentarea celor 41 de rapoarte realizate de SSSCIP, în perioada ianuarie 2022 – ianuarie 2024, cu privire la atacurile cibernetice cu un nivel ridicat

de complexitate și care au reușit să producă un impact asupra infrastructurilor IT&C ucrainene, fiind astfel excluse acele campanii cibernetice tip phishing. Ulterior prezentării rapoartelor menționate, se remarcă o serie de aspecte de interes cu privire la modul de funcționare al instituției, la raportarea acesteia față de atacurile cibernetice, comise asupra infrastructurilor IT&C ucrainene, și față de modul de operare al actorilor cibernetici de origine rusă.

În primul rând, se remarcă faptul că cele mai vizate domenii în cadrul campaniilor cibernetice au fost cel al comunicațiilor și cel energetic. Acest aspect poate fi explicat prin faptul că domeniul energetic constituie o resursă foarte importantă atât pentru statul atacat, asigurând funcționarea de bază a acestuia (Kozak, Klaban și Šlajs 2023, 1-6), cât și pentru statul agresor, reprezentând un element care poate crea panică în rândul populației, odată ce a fost indisponibilizat (Lee 2022). În ceea ce privește zona de telecomunicații, rolurile principale ale acesteia sunt determinate de informarea populației cu privire la starea conflictului (în special prin posturile TV și radio) și de posibilitatea cetățenilor de a comunica între ei din motive de siguranță sau de a avea acces la persoane din afara statului (Bratich 2020, 311-332). Impactul se remarcă, cu precădere, în zona Kherson, unde trupele FR au acționat pentru a opri accesul la informații ucrainene, precum și posibilitatea de a comunica cu persoane din afara arealului. În ceea ce privește exponenții mediului hacktivist, aceștia au urmărit compromiterea website-urilor unor autorități publice atât pentru scăderea încrederii în instituțiile publice, cât și pentru a crea un sentiment de panică în rândul civililor, care, deși nu interacționau direct cu conflictul, puteau conștientiza efectele acestuia (Hupperich 2023). Un exemplu evidențiat în acest sens este compromiterea paginii de Facebook a Serviciului Național de Statistică al UA, acțiune care, deși nu a afectat datele instituției, a urmărit scăderea încrederii populației în informațiile publicate de aceasta.

În ceea ce privește capabilitățile actorilor cibernetici de origine rusă, se remarcă faptul că acestea au avut o varietate foarte mare, pornind de la atacuri distructive, precum cel derulat prin intermediul malware-ului CaddyWiper, până la campanii cibernetice de tip DDoS, care urmăreau indisponibilizarea temporară a unor resurse (Liedekerke și Frankenthal 2023). Conform rapoartelor SSSCIP, serviciile FR identificate cu precădere au fost FSB și GRU, evidențiindu-se actorul cibernetic APT SANDWORM, atribuit serviciului militar de informații (McFail, Hanna și Rebori-Carretero 2021, 2-3). De asemenea, poate fi punctat un anume nivel de sincronizare între forțele militare și capacitățile cibernetice, având în vedere raportarea SSSCIP care anunța o campanie cibernetică, derulată cu o zi înaintea invaziei UA, al cărei scop era probabil de susținere a forțelor armate ale FR în cadrul conflictului ce urma să aibă loc (Radu 2022, 533-544). De asemenea, prezintă interes creșterea semnificativă a numărului de atacuri cibernetice, ceea ce conduce la concluzia că segmentul cyber a avut un rol relevant din derularea conflictului din perioada ianuarie 2022 – ianuarie 2024.

Referitor la modul de funcționare al SSSCIP și la raportarea instituției față de campaniile cibernetice, se remarcă faptul că, inițial, atacurile cibernetice nu au fost

atribuite cu prea mare certitudine FR, aspect modificat pe parcursul timpului. Cu toate acestea, SSSCIP nu a publicat date tehnice suficiente încât să dovedească aceste acțiuni de atribuire publică, ceea ce conduce la concluzia că raportările au avut fundamente strategice politice, nu de natură tehnică. Astfel, retorica raportărilor a migrat către formulări care subliniau faptul că atacurile au fost derulate cu certitudine de către statul agresor. Mai mult, SSSCIP a evidențiat pe parcursul timpului din ce în ce mai multe raportări, în care preciza că nivelul de cooperare cu industria privată din domeniul IT&C este ridicat, nominalizând, cu precădere, companiile ESET și MICROSOFT, aspect ce poate urmări reliefarea existenței unei cooperări dezvoltate care sprijină UA în prevenirea și combaterea atacurilor cibernetice (Lilly și alții 2023, 71-83). Un alt aspect punctat de SSSCIP în repetate rânduri este faptul că impactul acțiunilor ofensive de natură cibernetică nu se resimte doar asupra UA, ci și asupra partenerilor, indiferent de localizarea acestora. Astfel, este posibil ca SSSCIP să fi urmărit creșterea solidarității față de UA în cadrul conflictului cu FR.

Un alt aspect important de remarcat este acela că, în cei doi ani de analiză, nu a fost prezentat niciun atac cibernetic materializat ca fiind asociat sau atribuit unor entități de origine diferită decât cea rusă. SSSCIP nu a raportat atacuri cibernetice de origine chineză, iraniană sau nord-coreeană, deși există actori cibernetici asociați acestor state, cu un nivel ridicat de activitate în mod obișnuit (Assoudeh 2020). Astfel, o ipoteză în acest sens ar putea fi aceea că SSSCIP a urmărit construirea unei retorici care să fie concentrată în totalitate asupra FR (nu asupra prezentării autentice a faptelor), sens în care a evitat publicarea unor rapoarte care să arate că ar exista și alte entități care urmăresc compromiterea unor rețele și sisteme din UA.

În final, este necesar de punctat că raportările SSSCIP s-au dovedit, în unele instanțe, ca fiind incomplete sau lacunare. Un exemplu relevant în acest sens este campania cibernetică asupra infrastructurii satelitare a VIASAT, neraportată de SSSCIP în totalitate, în special din punct de vedere tehnic. Un alt exemplu este cel referitor la raportul din data de 13 decembrie 2023, referitor la atacul cibernetic asupra operatorului Kyivstar, în care nu s-a precizat dimensiunea impactului atacului cibernetic derulat împotriva infrastructurii UA. Aceste aspecte conduc către două posibile concluzii: (1) decizia de a se raporta lacunar anumite incidente sau de a nu se raporta deloc a fost una de natură strategică, pentru a evita scăderea încrederii în rândul populației sau (2) rata ridicată a atacurilor cibernetice a generat greșeli de comunicare, SSSCIP nefiind capabil să mențină ritmul raportărilor racordat la numărul atacurilor cibernetice.

Referințe

Agrafiotis, Ioannis, Jason R.C. Nurse, Michael Goldsmith, Sadie Creese și David Upton. 2018. "A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate." *Journal of Cybersecurity* 4 (1). https://doi.org/10.1093/cybsec/tyy006.

Akimenko, Valeriy și Keir Giles. 2020. "Russia's Cyber and Information Warfare." *Asia Policy, National Bureau of Asian Research* 27 (2): 67-75. doi:10.1353/asp.2020.0014.

Assoudeh, Mitra. 2020. "Shaping Cybersecurity Strategy: China, Iran, and Russia in a Comparative Perspective." *Reno ProQuest Dissertations Publishing.* http://hdl.handle.net/11714/7624.

Balmforth, Tom. 2024. "Exclusive: Russian hackers were inside Ukraine telecoms giant for months". https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04/.

Boschetti, Nicolò, Nathaniel G. Gordon și Gregory Falco. 2022. "Space Cybersecurity Lessons Learned from the ViaSat Cyberattack." https://doi.org/10.2514/6.2022-4380.

Bratich, Jack. 2020. "Civil Society Must Be Defended: Misinformation, Moral Panics, and Wars of Restoration." *Communication, Culture and Critique* 13 (3): 311-332. https://doi.org/10.1093/ccc/tcz041.

CERT-EU. 2023. "Russia's war on Ukraine: one year of cyber operations". https://cert.europa.eu/static/threat-intelligence/TLP-CLEAR-CERT-EU-1YUA-CyberOps.pdf.

CERT-UA. 2022a. "Fragment of the study of cyberattacks 14.01.2022". https://cert.gov.ua/article/18101.

—. 2022b. "Sandworm Group Cyberattack (UAC-0082) on Ukrainian energy objects using INDUSTROYER2 and CADDYWIPER malware (CERT-UA#4435)". https://cert.gov.ua/article/39518.

Cyber Security Intelligence. 2022. "State Service of Special Communications & Information Protection of Ukraine (SSSCIP)". https://www.cybersecurityintelligence.com/state-service-of-special-communications-and-information-protection-of-ukraine-ssscip-7222.html.

Davydiuk, Andrii și Vitalii Zubok. 2023. "Analytical Review of the Resilience of Ukraine's Critical Energy Infrastructure to Cyber Threats in Times of War." *15th International Conference on Cyber Conflict: Meeting Reality (CyCon).* Tallinn, ESTONIA: IEEE. 121-139. doi:10.23919/CyCon58705.2023.10181813.

Furstenau, Leonardo Bertolin, Michele Kremer Sott, Andrio Jonas Ouriques Homrich și Liane Mahlmann Kipper. 2020. "20 Years of Scientific Evolution of Cyber Security: a Science Mapping." *International Conference on Industrial Engineering and Operations Management.* Dubai, UAE: IEOM Society International. https://www.researchgate.net/publication/340413661_20_Years_of_Scientific_Evolution_of_Cyber_Security_a_Science_Mapping.

Gatlan, Sergiu. 2024. *"Russian hackers wiped thousands of systems in KyivStar attack".* https://www.bleepingcomputer.com/news/security/russian-hackers-wiped-thousands-of-systems-in-kyivstar-attack/.

Geissler, Dominique, Dominik Bär, Nicolas Pröllochs și Stefan Feuerriegel. 2023. "Russian propaganda on social media during the 2022 invasion of Ukraine." *EPJ Data Science* 12 (1). doi:10.1140/epjds/s13688-023-00414-5.

Hernandez-Castro, Julio, Edward Cartwright și Anna Stepanova. 2017. "Economic Analysis of Ransomware." https://ssrn.com/abstract=2937641.

Hernandez-Castro, Julio și Edward Cartwright. 2020. "An economic analysis of ransomware and its welfare consequences." *The Royal Society Open Science.*

Hupperich, Thomas. 2023. "On DDoS Attacks as an Expression of Digital Protest in the Russo-Ukrainian War 2022." *2023 International Symposium on Networks, Computers and Communications.* Doha, Qatar: IEEE. doi:10.1109/ISNCC58260.2023.10323968.

Khonji, Mahmoud, Youssef Iraqi și Andrew Jones. 2013. "Phishing Detection: A Literature Survey." *IEEE Communications Surveys & Tutorials* 15 (4): 2091 - 2121. doi:10.1109/SURV.2013.032213.00009.

Kizilova, Kseniya. 2022. "Assessing Russian Public Opinion on the Ukraine War." *Social Science Open Access Repository* 2-5. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-86994-6.

Kloba, Lev și Taras Kloba. 2022. "Cyber threats of the banking sector in the conditions of the war in Ukraine." *Financial and Credit Activity - Problems of Theory and Practice* 5 (46): 19-28. doi:10.55643/fcaptp.5.46.2022.3883.

Kozak, Pavel, Ivo Klaban și Tomáš Šlajs. 2023. "Industroyer cyber-attacks on Ukraine's critical infrastructure." *2023 International Conference on Military Technologies (ICMT).* Brno, Czech Republic: IEEE. 1-6. doi:10.1109/ICMT58149.2023.10171308.

Krithika, N. 2017. "A study on wha (watering hole attack)–the most dangerous threat to the organisation." *International Journal of innovations in Scientific and Engineering Research (IJISER)* 4 (8): 196-198. https://web.archive.org/web/20180421102442id_/; http://www.ijiser.com/paper/2017/vol4issue8/Aug2017p101.1.pdf.

Lee, Chia-yi. 2022. "Why do terrorists target the energy industry? A review of kidnapping, violence and attacks against energy infrastructur." *Energy Research & Social Science* 87 (8): 102459. doi:10.1016/j.erss.2021.102459.

Lewis, James A. 2022. "Cyber War and Ukraine." https://www.csis.org/analysis/cyber-war-and-ukraine.

Liedekerke, Arthur de și Kira Frankenthal. 2023. "The Cyber Dimension in Russia's War of Aggression." doi:10.5771/9783748917205-239.

Lilly, Bilyana, Kenneth Geers, Greg Rattray și Robert Koch. 2023. "Business@War: The IT Companies Helping to Defend Ukraine." *15th International Conference on Cyber Conflict: Meeting Reality (CyCon)* (IEEE) 71-83. doi:10.23919/CyCon58705.2023.10181980.

Lonergan, Erica D, Margaret W Smith și Grace B. Mueller. 2023. "Evaluating Assumptions About the Role of Cyberspace in Warfighting: Evidence from Ukraine." *15th International Conference on Cyber Conflict (CyCon).* Tallinn, ESTONIA: IEEE. 85-102. https://doi.org/10.23919/CyCon58705.2023.10182101.

Matania, Eviata și Udi Sommer. 2023. "Tech titans, cyber commons and the war in Ukraine: An incipient shift in international relations." https://doi.org/10.1177/00471178231211500.

McFail, Michael, Jordan Hanna și Daniel Rebori-Carretero. 2021. "Detection Engineering in Industrial Control Systems. Ukraine 2016 Attack: Sandworm Team and Industroyer Case Study." *The MITRE Corporation* 2-3. https://www.mitre.org/sites/default/files/2022-04/pr-22-0094-detection-engineering-in-industrial-control-systems-ukraine-2016-attack-case-study.pdf.

Mcwhorter, Dan. 2014. "APT28 Malware: A Window into Russia's Cyber Espionage Operations?". https://www.mandiant.com/resources/blog/apt28-a-window-into-russias-cyber-espionage-operations.

Microsoft. fără an. „Definiția atacurilor DDoS". Accesat 14 ianuarie 2023. https://www.microsoft.com/ro-ro/security/business/security-101/what-is-a-ddos-attack.

—. 2022. "Destructive malware targeting Ukrainian organizations". https://www.microsoft.com/en-us/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/.

Mohurle, Savita și Manisha Patil. 2017. "A brief study of Wannacry Threat: Ransomware Attack 2017." *International Journal of Advanced Research in Computer Science* 8 (5). https://www.ijarcs.info/index.php/Ijarcs/article/view/4021.

Paniotto, Volodymyr. 2020. "The Attitude of Ukraine's Population to Russia and Russia's Population to Ukraine (2008–2020)." *NaUKMA Research Papers Sociology* 3: 3-14. doi:10.18523/2617-9067.2020.3.3-14.

Patil, Dharmaraj, Tareek Pattewar, Shailendra Pardeshi, Vipul Punjabi și Rajnikant Wagh. 2022. "Learning to Detect Phishing Web Pages Using Lexical and String Complexity Analysis." https://eudl.eu/doi/10.4108/eai.20-4-2022.173950.

Paverman, Joseph Herbert. 2019. "An Examination of Cyber-Attacks Carried Out by Russia to Perpetuate Expansion." *Utica College ProQuest Dissertations Publishing*. https://www.proquest.com/openview/a0cb326bdab5e2f4c65f0baca4d2ab47/1?pq-origsite=gscholar&cbl=18750&diss=y.

Proska, Ken, John Wolfram, Jared Wilson, Dan Black, Keith Lunden, Daniel Kapellmann Zafra, Nathan Brubaker, Tyler Mclellan și Chris Sistrunk. 2023. "Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology". https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology.

Radu, Claudiu-Cosmin. 2022. "Russia's approach to cyberspace." *International Scientific Conference Strategies XXI. Volume XVIII.* București: "Carol I" National Defence University Publishing House. 533-544. https://doi.org/10.53477/2971-8813-22-61.

Ratten, Vanessa. 2022. "The Ukraine/Russia conflict: Geopolitical and international business strategies." *Thunderbird - International Business Review* 65 (2): 265-271. https://doi.org/10.1002/tie.22319.

Sapuppo, Mercedes. 2023. "Ukrainian telecoms hack highlights cyber dangers of Russia's invasion". https://www.atlanticcouncil.org/blogs/ukrainealert/ukrainian-telecoms-hack-highlights-cyber-dangers-of-russias-invasion/.

Smith, Margaret W. și Thomas Dean. 2023. "The Irregulars: Third-Party Cyber Actors and Digital Resistance Movements in the Ukraine Conflict." *15th International Conference on Cyber Conflict: Meeting Reality (CyCon)* 103-119. doi:10.23919/CyCon58705.2023.10182061.

Soesanto, Stefan. 2023. "Ukraine's IT Army." *Global Politics and Strategy* 65 (2): 93-106. https://doi.org/10.1080/00396338.2023.2218701.

SSSCIP. 2022a. "A fragment of the January 14 cyber attack investigation has been published". https://www.cip.gov.ua/en/news/opublikovano-fragment-doslidzhennya-kiberatak-14-sichnya.

—. 2022b. ”A new program erasing data from computers has been detected”. https://www.cip.gov.ua/en/news/viyavleno-novu-programu-yaka-stiraye-dani-z-komp-yuteriv.

—. 2022c. ”Cyberattack against Ukrtelecom on March 28: the details”. https://www.cip.gov.ua/en/news/kiberataka-na-ukrtelekom-28-bereznya-detali.

—. 2022d. ”Cyberattacks against Ukraine are carried out by Russian military hackers”. https://www.cip.gov.ua/en/news/cyberattacks-against-ukraine-are-carried-out-by-russian-military-hackers.

—. 2022e. ”Cyberattacks on the sites of military structures and state banks”. https://www.cip.gov.ua/en/news/shodo-kiberataki-na-saiti-viiskovikh-struktur-ta-derzhavnikh-bankiv.

—. 2022f. ”Four Months of War: Cyberattack Statistic”. https://www.cip.gov.ua/en/news/chotiri-misyaci-viini-statistika-kiberatak.

—. 2022g. ”Hackers mainly attack state institutions, telecommunication operators, local authorities, logistics companies and medical resources of Ukraine”. https://www.cip.gov.ua/en/news/khakeri-atakuyut-perevazhno-derzhavni-ustanovi-operatoriv-zv-yazku-miscevi-organi-vladi-logistichni-kompaniyi-ta-mediaresursi-ukrayini.

—. 2022h. ”Heavy cyberattack on Ukraine’s energy sector prevented. https://www.cip.gov.ua/en/news/poperedzhena-masshtabna-kiberataka-na-energetichnii-sektor-ukrayini.

—. 2022i. ”Latest update on networks operation in Ukraine as of April 11, 15:00”. https://www.cip.gov.ua/en/news/operativna-informaciya-derzhspeczv-yazku-pro-robotu-mobilnogo-zv-yazku-internetu-ta-cifrovogo-telebachennya-v-ukrayini-stanom-na-15-00-11-kvitnya-2022-roku.

—. 2022j. ”Russian cyberattack on the OLL.TV service”. https://www.cip.gov.ua/en/news/kiberataka-rosiyi-na-servis-oll-tv.

—. 2022k. ”Russian cyberwarfare against Ukraine seem to have reached its peak”. https://www.cip.gov.ua/en/news/rosiiski-kibernastupalni-operaciyi-na-ukrayinu-imovirno-dosyagli-svogo-maksimalnogo-potencialu.

—. 2022l. ”Russian hackers attempted to cut electricity supply to many Ukrainians”. https://www.cip.gov.ua/en/news/rosiiski-khakeri-namagalisya-pozbaviti-dostupu-do-elektroenergiyi-znachnu-kilkist-ukrayinciv.

—. 2022m. ”Russian Invaders Disabled Communication Services in the South of Ukraine”. https://www.cip.gov.ua/en/news/rosiiski-okupanti-vidklyuchili-zv-yazok-na-pivdni-ukrayini.

—. 2022n. ”SSSCIP’s State Centre of Cybersecurity has neutralized an attack on public authorities’ websites”. https://www.cip.gov.ua/en/news/derzhavnii-centr-kiberzakhistu-derzhspeczv-yazku-neitralizuvav-ataku-na-saiti-derzhavnikh-organiv.

—. 2022o. ”Starlink in Ukraine: How Elon Musk’s Satellite Internet is Helping Now and What the Prospects Are”. https://www.cip.gov.ua/en/news/starlink-v-ukrayini-yak-suputnikovii-internet-vid-ilona-maska-dopomagaye-zaraz-ta-yaki-perspektivi.

—. 2022p. *”Statistics of Cyber Attacks on Ukrainian Critical Information Infrastructure: 15-22 March”*. https://www.cip.gov.ua/en/news/statistika-kiberatak-na-ukrayinsku-kritichnu-informaciinu-infrastrukturu-15-22-bereznya.

—. 2022q. ”The war continues not only on land, in the air and at sea. Cyberspace has also become an arena for hostilities”. https://www.cip.gov.ua/en/news/the-war-continues-not-only-on-land-in-the-air-and-at-sea-cyberspace-has-also-become-an-arena-for-hostilities.

—. 2022r. "Today's attacks are a continuation of the attacks that took place on February 15". https://www.cip.gov.ua/en/news/23-lyutogo-2022-roku-stavsya-chergovii-akt-kiberagresiyi-proti-ukrayini.

—. 2022s. "Ukraine is not the only target for russian hackers, but a major one". https://www.cip.gov.ua/en/news/ukrayina-ne-yedina-cil-rosiiskikh-khakeriv-prote-odna-z-golovnikh.

—. 2022t. "Ukrainian television and radio are back in Kherson". https://www.cip.gov.ua/en/news/do-khersona-povernulosya-ukrayinske-telebachennya-i-radio.

—. 2022u. "Within a month of war, there were already three times more hacker attacks than during the same period last year". https://www.cip.gov.ua/en/news/za-misyac-viini-vzhe-stalosya-maizhe-vtrichi-bilshe-khakerskikh-atak-riznogo-vidu-nizh-za-analogichnii-period-minulogo-roku.

—. 2023a. "A Cyberattack Failed to Disrupt Ukrinform News Agency". https://www.cip.gov.ua/en/news/kiberataka-ne-zmogla-zupiniti-robotu-informaciinogo-agentstva-ukrinform.

—. 2023b. "At least 23 russian cyber terrorist groups act against Ukraine". https://www.cip.gov.ua/en/news/proti-ukrayini-pracyuyut-shonaimenshe-23-rosiiski-kiberteroristichni-khakerski-grupi.

—. 2023c. "Attacks against IT companies and specialized software developers as a threat to critical infrastructure". https://www.cip.gov.ua/en/news/ataki-na-it-kompaniyi-ta-specializovanikh-rozrobnikiv-pz-yak-zagroza-kritichnii-infrastrukturi.

—. 2023d. "CERT-UA experts are investigating a cyberattack against Kyivstar telecom operator's network". https://www.cip.gov.ua/en/news/fakhivci-cert-ua-doslidzhuyut-kiberataku-na-merezhu-telekom-operatora-kiyivstar.

—. 2023e. "Cyberattack on the State Statistics of Ukraine: the enemy reports another non-existent «victory»". https://www.cip.gov.ua/en/news/kiberataka-na-derzhstat-ukrayini-vorog-ukotre-prozvituvav-pro-peremogu-yakoyi-ne-bulo.

—. 2023f. "Cybercriminals tried to steal data, disguising themselves as Ukrainian MFA". https://www.cip.gov.ua/en/news/kiberzlovmisniki-namagalisya-vikradati-dani-maskuyuchis-pid-ukrayinske-mzs.

—. 2023g. "How russian and pro-russian hackers attack Ukraine". https://www.cip.gov.ua/en/news/yaki-rosiiski-ta-prorosiiski-khakeri-atakuyut-ukrayinu.

—. 2023h. "Local public authorities are among the key targets for russian hackers". https://www.cip.gov.ua/en/news/miscevi-organi-vladi-odna-z-osnovnikh-mishenei-rosiiskikh-khakeriv.

—. 2023i. "Russian hackers attacked users in Ukraine and Poland once again: this time they used emails containing links to «documents»". https://www.cip.gov.ua/en/news/rosiiski-khakeri-vchergove-atakuvali-koristuvachiv-ukrayini-ta-polshi-cogo-razu-za-dopomogoyu-elektronnikh-listiv-z-posilannyami-na-dokumenti.

—. 2023j. "Russian hacking group Turla attacks defense forces using CAPIBAR and KAZUAR malware — CERT-UA investigation". https://www.cip.gov.ua/en/news/rosiiske-ugrupuvannya-turla-spryamovuye-ataki-proti-sil-oboroni-vikoristovuyuchi-shkidlivi-programi-capibar-ta-kazuar-doslidzhennya-cert-ua.

—. 2023k. ”Targeted cyberattacks remain among the major cyber threats posed by the FSB hackers — Report”. https://www.cip.gov.ua/en/news/targetovani-kiberataki-zalishayutsya-odniyeyu-z-osnovnikh-kiberzagroz-vid-khakeriv-iz-fsb-zvit.

—. 2023l. ”The attack on Ukrinform might have been carried out by the Sandworm hacking group, associated with russian GRU: preliminary results of CERT-UA investigation”. https://www.cip.gov.ua/en/news/ukrinform-mogli-atakuvati-khakeri-z-ugrupuvannya-sandworm-pov-yazanogo-z-rosiiskim-gru-poperedni-dani-doslidzhennya-cert-ua.

Steinbrecher, Dominique. 2022. ”Viasat KA-SAT attack (2022)”. https://cyberlaw.ccdcoe.org/wiki/Viasat_KA-SAT_attack_(2022).

Sullivan, Scott. 2023. ”Unpacking Cyber Neutrality.” *15th International Conference on Cyber Conflict (CyCon).* Talinn, ESTONIA: IEEE. 9-23. https://www.ccdcoe.org/uploads/doc/CyCon_2023_book_print.pdf.

Tarasenko, Oleh, Dmytro Mirkovets, Artem Shevchyshen, Oleksandr Nahorniuk-Danyliuk și Yurii Yermakov. 2022. ”Cyber security as the basis for the national security of Ukraine.” *Cuestiones Politicas* 40 (73): 583-599. https://doi.org/10.46398/cuestpol.4073.33.

Temple-Raston, Dina. 2023. ”In recent interview, ousted Ukrainian cyber official spoke about new Russian attacks, long-term plans”. https://therecord.media/victor-zhora-interview-click-here-ousted.

Visvizi, Anna și Miltiadis D. Lytras. 2020. ”Government at risk: between distributed risks and threats and effective policy-responses.” *Transforming Government: People, Process and Policy* 14 (3): 333-336. https://doi.org/10.1108/TG-06-2020-0137.

Willett, Marcus. 2022. ”The Cyber Dimension of the Russia–Ukraine War.” *Global Politics and Strategy* 64 (5): 7-26. https://doi.org/10.1080/00396338.2022.2126193.

Wilson, Richard L. și Alexia Fitz. 2023. ”Nuclear Weapons, Cyber Warfare, and Cyber Security: Ethical and Anticipated Ethical Issues.” *Proceedings of the 18th International Conference on Cyber Warfare and Security Vol. 18 No. 1.* Baltimore, MD: Towson University. 440-448. https://doi.org/10.34190/iccws.18.1.1050.

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

Integrarea capabilităților multidomeniu în operațiile unităților interarme din forțele terestre

The integration of multi-domain capabilities in land forces units combined arms operations

Mr.instr.sup.drd. Petru-Marian VEREȘ*
*Universitatea Națională de Apărare „Carol I", București, România

Abstract

Conflictele curente, în desfășurare pe tot globul pământesc, au evidențiat necesitatea unei noi forme de război care să reducă numărul de victime și gradul de distrugere și, care, în același timp, să atenueze efectele mijloacelor hibride, omniprezente în doctrina tuturor actorilor. Această nouă fizionomie a războiului are ca mijloc de obținere a succesului operația multidomeniu. Deși operații multidomeniu au fost executate și în trecut, conceptul care înglobează procesul acestor operații este nou și există încă modificări semnificative care trebuie să se aplice, astfel încât să se permită actorilor operaționalizarea acestuia. Acest articol are ca scop studierea particularităților integrării operațiilor multidomeniu în operațiile forțelor terestre, prin identificarea punctelor tari și limitărilor dezvoltării procesului acestora, a condițiilor și principiilor lor de integrare la nivelul forțelor terestre, reieșite din analiza comparativă a abordărilor SUA și Federației Ruse, precum și din lecțiile învățate din conflictele curente.

Current conflicts, ongoing across the globe, have highlighted the need for a new form of warfare that reduces the number of casualties and the degree of destruction and, at the same time, mitigates the effects of hybrid means, ubiquitous in the doctrine of all actors. This new approach to warfare utilizes multi-domain operations as a means of achieving success. Although multi-domain operations have been conducted in the past, the concept that encompasses the process of these operations is novel, and there are still significant adjustments that need to be made to make it operational for all actors. This article aims to study the integration of multi-domain operations into land operations by identifying the strengths and limitations of their development process, the conditions and principles of their integration at the land forces level, resulting from a comparative analysis of US and Russian Federation approaches, as well as from lessons learned from current conflicts.

Cuvinte-cheie:
lupta armată interarme; domeniu; efecte; angajare simultană și sincronizată a armelor; operații multidomeniu; capabilități.

Keywords:
combined arms combat; domain; effects; simultaneous and synchronized engagement of arms; multi-domain operations; capabilities.

Info articol
Primit: 26 ianuarie 2024; Evaluat: 18 februarie 2024; Acceptat: 6 martie 2024; Disponibil online: 5 aprilie 2024

Citare: Vereș, P.M. 2024. „Integrarea capabilităților multidomeniu în operațiile unităților interarme din forțele terestre". *Buletinul Universității Naționale de Apărare „Carol I"*, 13(1): 44-59. https://doi.org/10.53477/2065-8281-24-03

Evoluția artei operative, de-a lungul timpului, poate fi privită ca un efect al marilor campanii militare, definitorii pentru stadiul evoluției războiului și al diferitelor doctrine militare care au fost aplicate pe timpul operațiilor militare. În secolul trecut, doctrina militară a avut o evoluție masivă, trecând adesea de la un concept la altul, sau de la o abordare a tacticii la alta, pe parcursul aceleiași campanii. Comun tuturor conflictelor desfășurate în secolul 20 a fost faptul că forțele terestre erau instrumentul principal de câștigare a războiului și, în consecință, erau mereu sprijinite de celelalte categorii de forțe. Această obișnuință a națiunilor a fost perpetuată, cu mici excepții, până în prezent. Acest fapt reiese și din dezvoltarea redusă a capabilităților celorlalte domenii, aerian, naval, cosmic sau cibernetic (NATO Standard AJP-01 2022), capabilități complexe, greu de produs și costisitoare.

Doctrina forțelor terestre, aplicată în Primul Război Mondial, presupunea utilizarea tranșeelor, pentru protecția trupelor împotriva focului direct și indirect al armamentului de infanterie și artilerie. Această tactică a dus la numeroase perioade de impas, în care niciuna dintre tabere nu avea soluții de a-și înfrânge adversarul, iar manevrele majore erau adesea inutile și cu pierderi semnificative de vieți omenești. Abia în anul 1916, după integrarea tancului în operațiile forțelor terestre, o combinare eficientă a manevrei infanteriei, cu sprijinul focului de artilerie și loviturile frontale ale tancurilor, era posibilă, iar forțele Antantei de pe frontul de vest reușeau să rupă apărarea germanilor și să consolideze, prin mijloacele trupelor de geniu, obiectivele cucerite. Majoritatea istoricilor militari privesc Primul Război Mondial ca pe un moment de cotitură și de schimbare majoră, care a turnat fundația pentru lupta armată interarme contemporană (Simoens 2022).

Al Doilea Război Mondial, pe de altă parte, a forțat, practic, armatele participante să integreze toate armele disponibile, inclusiv la nivel de batalion, fiind prilejul prin care batalionul interarme apărea pe câmpul de luptă, configurat astfel, mai evident ca niciodată. În primii ani ai războiului, Germania a implementat doctrina ”blitzkrieg”, însemnând „război fulger”, care presupunea angajarea rapidă și coordonată a infanteriei, tancurilor și artileriei, cu sprijin aerian apropiat. Această configurare a unităților tactice a însemnat un salt major de la ideea de a masa tancuri sau infanterie în unități de nivel divizie la crearea unor unități interarme mecanizate, pornind de la nivelul batalionului. În același timp, nevoia de a contracara aceste unități germane a obligat taberele opuse să își construiască la fel unitățile și mai mult, de a crea forțe de dimensiuni mici, cu capablități antitanc, care îngreunau semnificativ pătrunderea unităților blindate și mecanizate prin dispozitivele de apărare.

Apariția și folosirea bombei atomice au provocat teoreticienii militari să ia în considerare posibilitatea ca războiul terestru convențional să fie depășit, iar o concentrare de forțe terestre pe spații mici să fie deosebit de riscantă. Mai mult, nevoia de a purta lupte de eliberare națională a dat naștere războiului de gherilă și operațiilor neconvenționale, schimbând fundamental doctrina primei jumătăți a secolului 20. Concepte, ca război de gherilă și contrainsurgență, vizibile mai ales în războiul din Vietnam, au determinat statele vestice să renunțe la dezvoltarea capabilităților convenționale de generație nouă, mecanizate și blindate, și să

reinvestească în unități ușoare de infanterie, cu mobilitate sporită și sprijin aerian constant (House 1984, 141).

Anul 1990 este marcat de un eveniment care a schimbat radical modul în care marile campanii militare se planifică, se pregătesc și se execută. Invazia irakiană în Kuweit și inabilitatea micului stat de a se apăra împotriva Irakului au determinat SUA și Arabia Saudită să intervină și militar. Operația "Desert Shield", din 1990-1991, a presupus dislocarea strategică a forțelor armate americane pe teritoriul Arabiei Saudite, iar implicarea aliaților din Europa sau din alte părți ale lumii în această campanie a produs cea mai mare acumulare de forțe armate din ultimii 20 de ani (Hooton și Cooper 2019, 65). A doua fază a acestei mari campanii a fost operația "Desert Storm", care presupunea atacarea și învingerea forțelor irakiene invadatoare, pentru a elibera statul Kuweit, prin mijloacele unei operații majore întrunite, aero-terestro-navală.

Intervenția coaliției, condusă de SUA în Irak, semnifica ultimul război al secolului 20, în care au fost implicate mase mari de capabilități convenționale, tancuri, artilerie, infanterie, geniu, logistică, asalt aerian și aviație (Hooton și Cooper 2019, 67), evidențiind din nou importanța configurării marilor unități tactice de forțe terestre, conform principiilor interarme, pentru a permite executarea unor manevre pe spații largi și pe distanțe mari, în scopul evitării punctelor tari ale inamicului și ocupării pozițiilor avantajoase.

În prezent, războiul convențional a devenit o componentă a războiului hibrid, în care operațiile militare se desfășoară în toate cele cinci domenii ale spațiului de luptă și nu au efecte cinetice, ca formă primară de obținere a succesului, ci combină efectele letale cu nonletale, tehnologia avansată, abordările orientate pe comportamentul publicului țintă și filosofiile de conducere sau de execuție, într-o armonie menită să orchestreze cât mai eficient capacitatea de luptă.

Evoluția puternică a capabilităților și doctrinei militare, accelerată mai ales după invazia Rusiei în Ucraina și anexarea Peninsulei Crimeea în 2014, a condus la dezvoltarea unor concepte și termeni, precum „război de generația a 4-a" sau chiar a 5-a, operații multidomeniu, război informațional, amenințare hibridă sau inteligența artificială, care plasează un concept tradițional și important precum războiul interarme într-o zonă umbrită, în care pericolul de a fi uitat de comunitatea științifică este tot mai mare, în ciuda importanței dovedite de-a lungul istoriei. Nu trebuie uitat faptul că, așa după cum spune și Murat Caliskan în articolul său "Hybrid warfare through the lens of strategic theory", din publicația *Defense and Security Analisys, „conceptele ne modelează înțelegerea militară și în consecință și forțele armate"* (Caliskan 2019), iar în acest fel, există posibilitatea de a elimina abordări coerente și eficiente pentru a încerca să le implementăm, cu un posibil succes limitat, pe cele mai moderne, dar care nu au încă o validare completă.

Cu toate acestea, războiul interarme nu a dispărut încă din doctrina națiunilor Alianței Nord-Atlantice (NATO), iar acest articol este menit să întărească

importanța unităților interarme ale forțelor terestre în operații, în contextul mediului de securitate actual. Conceptul de război interarme a fost subiectul multor articole științifice, însă cele mai multe dintre ele au fost orientate spre a prezenta particularități ale acestuia din timpul diferitelor campanii sau războaie ale istoriei, câteva dintre articole fiind concentrate pe a plasa conceptul în contextul unor medii de securitate, guvernate de abordări care, în prezent, fie sunt învechite sau depășite, fie nu mai au relevanță. Deosebit la acest articol este faptul că analizează importanța unităților interarme ale forțelor terestre în contextul operațiilor multidomeniu, o analiză de care teoreticienii militari au nevoie atât pentru a le oferi un sprijin în dezvoltarea cunoașterii privind locul și rolul forțelor terestre în operațiile multidomeniu, cât și în a le asigura un posibil instrument de utilizat în inițiativele orientate pe configurarea unităților tactice.

Articolul urmează trei direcții de cercetare principale, concretizate în capitole ale lucrării. În primul capitol, studiul abordează configurarea unităților tactice din forțele terestre după principiul interarme și și locul acestora în operațiile multidomeniu. Acest capitol scoate în evidență condiția critică necesară oricărei unități tactice, anume de a fi configurată interarme, pentru a avea posibilitatea integrării unor capabilități care să îi permită acționarea în toate domeniile spațiului de luptă și generarea efectelor în mediul operațional. Capitolul va discuta și de viziunea SUA și Federației Ruse în ceea ce privește configurarea unităților tactice interarme. În cel de-al doilea capitol, articolul prezintă posibilele limitări și provocări, reieșite din integrarea capabilităților multidomeniu în operațiile forțelor terestre, precum și posibilele metode de atenuare a acestora. În cele din urmă, lucrarea evaluează performanța grupurilor de luptă interarme de nivel batalion (BTG) ale Federației Ruse în conflictul din Ucraina și prezintă aspecte relevante, rezultate din integrarea acestora în operațiile multidomeniu desfășurate în acest război.

Rolul unităților interarme ale forțelor terestre în operațiile multidomeniu

Marile conflicte armate ale istoriei au reprezentat, pentru comunitatea științei militare, un izvor de informații privind actorii implicați, tacticile folosite în lupta armată, o bună oportunitate de a evalua performanțele unităților și capabilităților utilizate și, categoric, lecțiile învățate. Îm mod similar, și invazia Rusiei în Ucraina, care a început încă din anul 2014, constituie o sursă de informații importantă, din care teoreticienii au construit și conceptul de *operații multidomeniu*. Doctrina întrunită aliată AJP -1 definește operația multidomeniu ca fiind *„orchestrarea acțiunilor militare, de-a lungul tuturor domeniilor și mediilor, sincronizată cu activități nonmilitare, pentru a permite Alianței livrarea efectelor cu o viteză suficientă, ca ele să fie relevante"* (NATO Standard AJP-01 2022, 3). Pe de altă parte, doctrina militară a SUA, *FM 3-0 Operations*, definește operația multidomeniu ca fiind *„angajarea interarme a tuturor capabilităților forțelor terestre și întrunite, pentru a crea și exploata avantaje relative care cuceresc obiective, înfrâng forțele inamicului*

și consolidează câștigurile dobândite, în numele comandanților unităților întrunite" (Department of the Army 2022, 3-1). Diferența dintre cele două abordări principale ale conceptului este evidentă, însă aceasta este determinată și de necesitatea Alianței de a crea standarde aplicabile și implementabile la nivelul tuturor statelor membre, în contrast cu doctrina americană, care dezvoltă doctrina militară pentru a instrui propriile forțe.

Analizând cele două forme de definire a operațiilor multidomeniu, putem conveni asupra faptului că ele reprezintă acele acțiuni pe care forțele armate le întreprind prin mijloacele capabilităților din toate domeniile spațiului de luptă, care sunt menite să dobândească succesul în cel mai eficient mod. Deși diferențele de abordare nu schimbă radical natura operațiilor multidomeniu, trebuie să observăm că doctrina americană descrie acțiunile ca o angajare interarme a capabilităților din toate domeniile. Această abordare este un indicator al importanței configurării interarme a unităților, pentru a permite angajarea capabilităților din mai multe domenii și mai ales pentru a genera efecte în mai multe domenii.

Operațiile militare care produc efecte specifice celor multidomeniu necesită capabilități conforme, reziliente și înalt tehnologizate și unități tactice care să se caracterizeze prin flexibilitate și versatilitate, putere de luptă sporită, rază operațională extinsă și posibilitatea de a asigura executarea operației întrunite de-a lungul tuturor domeniilor. Aceste caracteristici ale unităților tactice din forțele terestre se reflectă din alăturarea sinergică a mai multor arme, servicii sau componente, din sincronizarea angajării acestora în lupta armată astfel încât contracararea unuia dintre aceste elemente să-l facă pe inamic vulnerabil la un altul. Ținând cont de aceste aspecte, putem deduce ușor faptul că o abordare interarme a operațiilor multidomeniu nu este doar o simplă metodă bună, ci una absolut necesară.

Caracterul interarme al unei unități este definit în doctrina americană ca *„aplicarea simultană și sincronizată a armelor, pentru a obține un efect mai mare decât cel obținut prin utilizarea fiecărui element separat sau secvențial*" (Department of the Army 2019, 3-9), iar acest lucru se reflectă și în configurarea unităților tactice, în special de nivel brigadă, divizie și corp de armată.

De-a lungul continuumului competiției (NATO Standard AJP-01 2022, 7) – cooperare, rivalitate, confruntare și conflict armat –, corpul de armată, ca mare unitate tactică, integrează capabilitățile survenite din toate domeniile la eșalonul tactic potrivit și angajează în luptă diviziile pentru a cuceri obiectivele componentei terestre a grupării de forțe întrunite. Diviziile, sprijinite de corpul de armată, înfrâng inamicul prin combinarea manevrei și focului brigăzilor luptătoare și a structurilor de arme subordonate, controlează terenul cucerit și consolidează succesul operației întrunite. Această integrare a capabilităților multidomeniu și angajarea acestora în conflictul armat, înțesat de incertitudine, comunicare mereu degradată și ferestre de oportunitate trecătoare, este posibilă numai prin dezvoltarea unei culturi, în care comandanții unităților tactice exercită inițiative

disciplinate și acceptă riscuri calculate, în interiorul filosofiei de conducere prin comanda misiunii – *mission command*.

Având în vedere aceste aspecte, putem defini rolul unităților tactice ale forțelor terestre în operațiile multidomeniu ca fiind de integrare și angajare în lupta armată a capabilităților multidomeniu, pentru a devansa inamicul din toate punctele de vedere și pentru a conserva puterea de luptă a unității.

În doctrina militară a SUA, corpul de armată și divizia asigură forței întrunite formațiuni interarme și comandamente flexibile și adaptabile la misiune, capabile să gestioneze crize și să execute operații terestre la scară largă, în timp ce armatele integrează și coordonează cababilități multiple, pentru a duce operații la scară largă, în cadrul operației întrunite. Corpurile de armată sau armatele pot avea roluri multiple, de conducere tactică (comandamente de componentă terestră) sau de conducere operativă (comandament de grupare de forțe întrunite). Aceste eșaloane tactice asigură comandanților combatanți forțe armate care posedă capabilități tehnice și tactice, necesare desfășurării operațiilor pe întreg spectrul operațiilor militare (Department of the Army 2021, 1-1).

Pe de altă parte, tactica rusească aduce în prim-plan armata interarme și armata blindată (de tancuri), ca eșalon principal între conducerea operativă sau strategică a forțelor armate și eșaloanele tactice. Aceste eșaloane tactice sunt organizate, în cea mai mare parte, pe brigăzi interarme, dar schimbările majore în dotarea forțelor armate, asociate cu tehnologizarea grăbită, provocată de războiul cu Ucraina, prevestesc o reorganizare a acestor armate pe divizii, și chiar pe corpuri de armată (Grau și Bartles 2016, 30). Aceste unități tactice au un puternic caracter interarme, însă au anumite limitări în ceea ce privește capabilitățile multidomeniu, acestea fiind reținute la eșaloanele operative și strategice, dar pot desfășura operații multidomeniu cibernetice și aeroterestre.

Unitățile interarme americane au o coerență logică în organizare. Comandamentul unui corp de armată american integrează, în primul rând, 3 până la 5 divizii interarme, brigăzi de arme și servicii, ISR (Intelligence, Surveillance, Reconnaissance), geniu, apărare CBRN (Chimic, Biologic, Radiologic, Nuclear), apărare antiaeriană, artilerie și rachete terestre, poliție militară, logistică și alte unități specializate, cu capabilitățile aferente. La rândul lor, diviziile americane au o structură similară corpului, integrând brigăzi luptătoare și batalioane de arme și servicii, însă diferă în capabilitate, în sensul efectelor pe care acestea le produc. Analizând ambele eșaloane tactice și efectele acestora, am ajuns la concluzia că efectele corpului de armată încep acolo unde se încheie cele ale diviziei, în spațiul de luptă multidomeniu, corpul având sarcina de a modela spațiul de luptă inaccesibil diviziilor pentru a permite acțiunea neobstrucționată a diviziilor, în mediul lor de operare. Mai exact, unitățile luptătoare robuste ale structurilor interarme tactice de nivel divizie sau corp beneficiază de sprijin luptă sau de servicii constant, sporindu-le executarea manevrei și extinderea razei operaționale.

În contrast, armata interarme rusească, organizată pe divizii, brigăzi sau regimente, în cazuri mai restrânse, așa cum arăta în bătălia Kievului, din 2022, presupunea generarea de *grupuri tactice de nivel batalion – battalion tactical group (BTG) –* , din organica brigăzilor, care erau sprijinite logistic de divizie și care erau conduse de armata interarme (Zabrodskyi și alții 2022, 45). Aceste formațiuni aveau compunerea de luptă a unui batalion întărit, iar caracterul interarme al acestuia era sporit de integrarea mai multor capabilități de sprijin luptă, artilerie și rachete în special, dar cu puterea de luptă a infanteriei redusă. În cadrul acestor BTG, rolul infanteriei consta în ocuparea și menținerea pozițiilor defensive, precum și în sprijinirea structurilor de tancuri.

Diferențele dintre cele două abordări, americană și rusă, sunt evidente. În conceptul american, accentul se pune pe sprijinirea unităților luptătoare pentru a asigura succesul manevrei acestora, consolidarea obiectivelor cucerite și executarea acțiunilor tactice fără întreruperi, pentru o lungă perioadă de timp. Metoda rusească, de angajare a structurilor tactice interarme, mizează mai mult pe o acțiune intensă a structurilor de sprijin luptă și pe efectele acestora, în special ale celor de foc direct și indirect cu proiectile de artilerie sau rachete, urmată de acțiunea forțelor luptătoare. Această metodă are vizibil o înclinare spre războiul de atriție, limitat în ceea ce privește manevra unităților luptătoare și bazat pe efectele altor mijloace, hibride îndeosebi, pentru înfrângerea inamicului.

Abordarea americană și, prin extindere, cea aliată se orientează pe integrarea capabilităților multidomeniu în operațiile interarme ale structurilor tactice, pentru a spori manevra acestora și pentru a modela spațiul de luptă astfel încât, prin manevră, să se exploateze punctele decisive și centrele de greutate ale inamicului în vederea reducerii pierderii de vieți omenești sau de capabilități în ambele tabere.

Foarte multe dintre aceste limitări ale conceptului interarme al Rusiei au condus la revenirea unor tactici învechite prin angajarea în luptă a acelor mici echipe de infanteriști „de sacrificiu", recrutați, de obicei, din provinciile Luhansk sau Donetsk, din rândul prizonierilor, deținuților sau din rândul militarilor mobilizați și slab pregătiți, care, după cum spun militarii ucraineni, atacă, sub influența narcoticelor sau coerciției comandanților, de regulă până sunt doborâți de focul apărării, sau sunt executați de proprii camarazi atunci când se retrag. Această tactică de atac în „valuri umane" are ca scop demascarea pozițiilor de apărare adverse, epuizarea resurselor și crearea unor condiții acceptabile pentru un nou atac (Watling și Raynolds 2023, 5).

Provocări reieșite din integrarea capabilităților multidomeniu în operațiile forțelor terestre și posibile metode de atenuare a acestora

Strategia militară a viitorului este gândită și creată urmând drumul de la cooperare la conflict armat, de-a lungul continuumului competiției. Alianța Nord-Atlantică,

prin conceptul strategic adoptat la Summitul de la Madrid, din 29 iunie 2022, orientează linia de efort principal dinspre prevenirea și managementul crizelor spre funcția acesteia, de descurajare și apărare (NATO 2022). Această reorientare este, în principal, provocată de evoluția amenințării la adresa Alianței, Federația Rusă, și de noua fizionomie a războiului, așa cum este identificată în conflictul ruso-ucrainean.

Noul război angajează capabilități multidomeniu în operațiile tactice, iar filosofia de luptă, precum cea rusă, dezvoltă necontenit capabilități A2/AD (Anti-Acces/Area Denial) și mijloace de angajare a focului direct și indirect cât mai distructive și performante. Contracararea amenințării Rusiei, în viziunea Alianței, presupune descurajarea agresiunii armate, iar dacă această strategie eșuează, înfrângerea inamicului prin depășirea acestuia în toate domeniile. Ca în majoritatea cazurilor, SUA au preluat, încă din 2018, inițiativa de a dezvolta un concept al forțelor terestre pentru operații multidomeniu, într-un context în care celelalte state membre ale Alianței nu aveau aceeași capacitate.

Conceptul american are ca idee centrală executarea operațiilor multidomeniu de către forțele terestre, ca element al forței întrunite, pentru a dobândi succesul în timpul competiției; la nevoie, forțele terestre pătrund și dezintegrează sistemele A2/AD ale inamicului și exploatează libertatea de manevră rezultată pentru a cuceri obiectivele strategice și a forța o întoarcere la competiție în termeni favorabili (TRADOC Pamphlet 525-3-1 2018, 7). SUA intenționează să ajungă la capabilitate operațională multidomeniu completă până în anul 2035.

SUA au alocat un buget în valoare de 773 de miliarde de dolari americani pentru apărare (US DoD 2022, 1-3), ocupând locul 1 la nivel mondial, din acest punct de vedere, în 2023. Având în vedere bugetul imens alocat de SUA și proiecția temporală estimată în acest moment, deducem clar faptul că principala limitare pentru a avea capabilitate multidomeniu completă este costul mare și timpul lung de operaționalizare. Dintre celelalte state membre ale NATO, Germania și Marea Britanie sunt următoarele clasate, ambele cu un buget de peste 65 de miliarde de dolari, alocat în 2021, conform unui comunicat de presă al Alianței (NATO 2023, 7), bugete semnificativ mai mici decât cel american. Acest fapt evidențiază și mai mult incapacitatea statelor membre ale NATO de a atinge un nivel acceptabil al capabilității multidomeniu. Nici Rusia nu pare a fi aproape de această capabilitate, cu o investiție, pentru apărare, care depășește ușor valoarea de 351 de miliarde de dolari în 2023, conform unui articol publicat de Reuters (Reuters 2023a), însă au fost vizibile îmbunătățiri în diferite segmente de apărare, în special pentru dezvoltarea sistemelor de rachete balistice de rază lungă. De asemenea, și China, un adversar confirmat care poate contesta SUA în putere militară, a avut cheltuieli de apărare în valoare de 224 de miliarde de dolari în 2023 (Reuters 2023b), însă, majoritatea cheltuielilor fiind orientată pe achiziția de echipamente mai moderne pentru forțe terestre și navale, nu neapărat pentru capabilități multidomeniu. Deocamdată, din datele prezente, doar SUA prezintă un concept solid de realizare a capabilității multidomeniu completă și alocă suficiente resurse în acest sens, însă dobândirea acestei capabilități va mai dura cel puțin 10 ani.

Din punct de vedere tactic integrarea capabilităților multidomeniu în operațiile forțelor terestre generează provocări unice. În timpul experimentării capabilităților multidomeniu, analiștii au constatat fluctuații în disponibilitatea capabilităților multidomeniu. Fiecare domeniu în parte are limite concrete, precum viteza sateliților pe orbite, rețele cibernetice închise, care necesită pătrunderi efective, sau timpii de realimentare cu combustibil, de repararare și reînarmare a aparatelor din mediul aerian, terestru sau maritim (Skates 2021, 70). Aceste constrângeri determină o disponibilitate temporară a tuturor capabilităților și pot crea dileme comandanților, în ceea ce privește alocarea lor.

Un principiu al operațiilor multidomeniu, introdus în doctrina americană și menționat în FM 3-0 Operations, este *„convergența”*, care, potrivit acestui manual, este rezultatul creat prin angajarea concentrată de capabilități din mai multe domenii și eșaloane împotriva unei combinații de puncte decisive în orice domeniu, pentru a crea efecte asupra unui sistem, decident, unei formațiuni, sau într-o zonă geografică specificată (Department of the Army 2022, 3-3). După cum menționam anterior, capabilitățile multidomeniu sunt reținute, în viziunea americană, la nivelul corpului de armată și sunt angajate pentru a modela lupta diviziei. Din acest punct de vedere, putem constata faptul că divizia, ca eșalon fundamental pentru operațiile interarme, are limitări în angajarea multidomeniu, având efecte semnificative în mediul terestru și aerian și efecte reduse în celelalte trei domenii. Acest lucru implică eforturi majore de coordonare și de sincronizare între acțiunile diviziei și cele ale corpului de armată pentru realizarea convergenței. Mai mult, capabilitățile cosmice și cibernetice înalt tehnologizate sunt scumpe și, adesea, insuficiente, fiind reținute de eșaloanele operative și strategice, limitând disponibilitatea acestora și la nivelul corpului de armată, ceea ce nu poate decât îngreuna respectarea acestui principiu.

Însă, dacă ne imaginăm efectele unei convergențe de succes, într-o operație multidomeniu, probabil, inamicul va suferi neutralizări multiple ale punctelor tari, care nu permit executarea unei operații coerent și cu șanse de succes, încă din primele faze ale operației. Pentru o convergență de succes, planificarea și pregătirea acesteia sunt cruciale. Deducem din condițiile reușitei unei convergențe faptul că sincronizarea acțiunilor reprezintă cea mai dificilă provocare. Conform procesului militar de luare a deciziei (MDMP), identificarea punctelor critice ale inamicului depinde de calitatea produselor de evaluare a acestuia. Aceste produse sunt construite prin procese integratoare, conexe la MDMP, precum pregătirea informativă a mediului operațional – *Intelligence Preparation of the Opererational Environment (IPOE)* – și procesul de achiziție a țintelor – *Joint Targetting (JT).*

Prin IPOE, se identifică elementele inamicului, referitoare la capabilitățile acestuia, la centrul lui de greutate, la doctrina aplicată în luptă, cu integrarea lecțiilor învățate din istoria de luptă, precum și cursurile probabile de acțiune ale inamicului (NATO Standard AJP 3-9 2016, 2-17). De asemenea, prin JT, se identifică și se prioritizează acele ținte de mare valoare (*High Value Targets – HVT*), ținte cu câștig ridicat (*High Payoff Targets – HPT*), ținte critice (*Time-Sensitive Targets – TST*) sau alte ținte

ale inamicului, pentru a stabili angajarea adecvată a acestora în vederea obținerii efectelor conform intenției comandantului și obiectivelor operației (NATO Standard AJP 3-9 2021, 1-1). Suprapunerea produselor rezultate din cele trei procese, MDMP, IPOE și JT, revelează punctele critice ale inamicului.

Mai departe, comandantul marii unități tactice va direcționa statul major în ceea ce privește modalitatea de angajare a acelor puncte critice. Acesta va urmări sincronizarea angajării capabilităților din toate domeniile, pentru a da lovituri simultane inamicului și pentru a produce efecte decisive pentru întreaga operație, încă de la inițierea acesteia. De regulă, statul major va pune la dispoziția comandantului instrumentele care să ajute la sincronizarea acțiunilor, prin care acesta să fie în măsură să direcționeze acțiunile unității interarme pe care o conduce.

Provocările integrării capabilităților multidomeniu în unitățile interarme ale forțelor terestre reies și din necesitatea configurării unor subunități care pot integra și angaja aceste capabilități. Unitățile tactice interarme, în mod tradițional, sunt configurate pentru a duce războiul interarme. Configurarea unei unități tactice de angajare multidomeniu urmărește dezvoltarea operațiilor multidomeniu, iar în prezent, nu există unități tactice care să ducă independent acest tip de operații. Angajarea multidomeniu de astăzi presupune un efort întrunit, iar capabilitățile sunt angajate și coordonate la nivel operativ.

Totuși, într-un articol, publicat de Asociația Forțelor Terestre ale SUA, Charles McEnany ne oferă o variantă de configurare a unei structuri multidomeniu (Figura 1), cu un orizont de operaționalizare nu mai târziu de 2035. Configurația acestei structuri urmărește 4 funcțiuni: efecte, focuri, protecție și susținere (McEnany 2022).

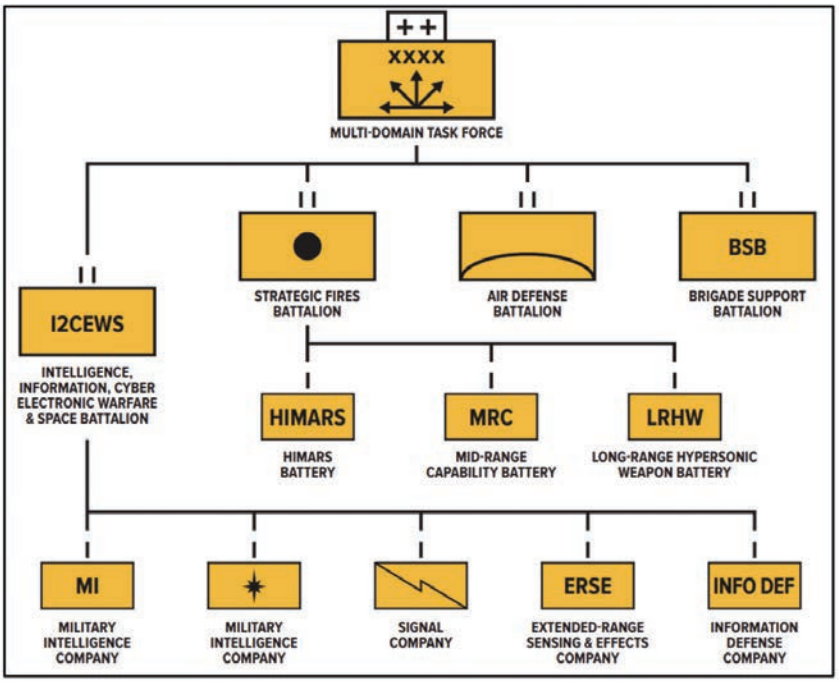

Figura 1 Compunerea structurii multidomeniu (McEnany 2022)

Această structură are o compunere similară unităților interarme, însă capabilitățile microstructurilor diferă semnificativ. Dacă unitățile interarme erau configurate astfel încât să neutralizeze într-un mod eficient puterea de luptă a inamicului tactic pentru succesul operației, structura multidomeniu are ca scop angajarea capabilităților A2/AD, pentru asigurarea libertății de acțiune a forței întrunite, prin angajarea sincronizată a efectelor cinetice și noncinetice (Chief of Staff Paper #1 2021). Durata lungă de operaționalizare a acestui tip de structură, chiar și pentru o națiune cu un avans considerabil în ceea ce privește operațiile multidomeniu, SUA, relevă dificultatea cu care structura de forțe poate angaja efecte multidomeniu. Mai mult, un posibil conflict care să presupună necesitatea unei astfel de structuri poate accelera procesul de configurare și operaționalizare, iar acest fapt poate avea efecte negative asupra capabilității acesteia.

Performanța forțelor terestre rusești în operațiile multidomeniu din conflictul ruso-ucrainean

După invazia Rusiei în Ucraina și anexarea Crimeei, forțele armate ruse au parcurs un proces de reconfigurare, trecând la o înfățișare nouă. Înainte de această reformă a forțelor terestre rusești, armata interarme a Rusiei era organizată pe divizii interarme, care, la rândul lor, erau organizate pe regimente. În mare parte, caracterul interarme ale acestor structuri nu era scos în evidență cum este în ziua de azi, iar forțele de sprijin luptă sau sprijin cu servicii erau reținute sub alte comenzi, având acțiunile coordonate la acel nivel, rămânând ca diviziile și regimentele să nu fie altceva decât o masare de tancuri, de infanterie mecanizată și de infanterie motorizată, cu puțin sprijin de armă.

Așa după cum evidențiază Charles Bartles și Lester Grau, în cartea *The Russian Way of War – Force Structure, Tactics, and Modernization of the Russian Ground Forces*, noua fizionomie a forțelor terestre rusești, aplicată și în conflictul din Ucraina, are ca eșalon tactic și operativ armata interarme, organizată pe brigăzi. Schimbarea majoră pe care reforma o aduce presupune generarea acelor BTG-uri, din cadrul brigăzilor, pentru a proiecta puterea de luptă a unei brigăzi (Grau și Bartles 2016, 37). Deși această schimbare era în curs de implementare, în faza inițială a războiului din Ucraina din 2022, rușii au atacat cu mari unități tactice, care erau configurate după ambele variante: armate configurate și pe divizii cu regimente, dar și pe brigăzi. Totodată, la baza construirii acestor mari unități tactice, este BTG-ul, fiind alegerea Rusiei în bătălia Kievului și în operațiile militare din Donbass, pentru angajarea forțelor Ucrainei la nivel tactic.

BTG utilizat în Ucraina era compus din personalul bine pregătit și din capabilitățile cu cel mai bun grad de operativitate din cadrul unei brigăzi, pentru a crea un batalion „întărit". Problema de personal cu care se confrunta batalionul consta în faptul că militarii, din toate categoriile de personal, nu se cunoșteau, nu s-au instruit în comun și nici nu au luptat vreodată împreună. Mai mult, unitățile tactice din forțele terestre

se confruntau cu o lipsă acută de ofițeri de stat major, iar subofițerii nu erau integrați corespunzător în cadrul BTG. Pentru a atenua neajunsurile provocate de lipsa de personal, rușii au recurs la detașarea multora dintre aceștia de la brigăzi sau divizii aflate mai sus pe scara ierarhică, pentru a crea state majore operaționalizate la nivelul BTG-urilor (Nistorescu 2022, 140). Aceste limitări vor crea, în cele mai multe cazuri, probleme de moral, de coeziune și chiar cu un impact semnificativ asupra acțiunilor tactice executate prin reducerea razei operaționale a marilor unități de nivel brigadă sau divizie. Nu putem vorbi de un război eficient fără trupe bine instruite, prolifice în câmpul tactic, generate prin dezvoltarea unei instituții militare profesioniste (Stanciu 2018, 195).

Deși batalioanele erau bine echipate cu sisteme de artilerie și rachete, adesea dincolo de capacitatea comandantului de batalion de a le gestiona, aceste grupuri de luptă nu aveau sisteme de supraveghere, achiziție ținte sau război electronic. Acest fapt are un impact major asupra capacității lor de a contracara acțiunile inamicului în spectrul electromagnetic, militarii BTG-ului recurgând inclusiv la utilizarea rețelei de telefonie mobilă a cetățenilor ucraineni. Bineînțeles, această eroare a permis forțelor ucrainene să obțină informații vitale privind planurile și intențiile rușilor. Mai mult, aceste informații revelau și statusul curent al trupelor rusești, starea moralului și puterea de luptă rămasă. De asemenea, lipsa sistemelor de apărare cibernetică a condus și la întreruperea funcționării sistemelor ISTAR, determinând incapacitatea comandanților ruși de a ajunge la o înțelegere comună a situației, de a avea o imagine terestră clară sau estimări corecte vizavi de operațiile în desfășurare.

Totuși, deși BTG rusesc nu dispunea de sprijin de geniu dezvoltat, se putea observa faptul că aveau mobilitate sporită în câmpul tactic, în special pentru trecerea peste văi sau râuri, datorită sprijinului constant cu poduri de asalt sau cu poduri fixe, primit de la eșalonul armatei interarme (Watling și Raynolds 2023, 10).

Probabil, cel mai important aspect care a afectat performanța forțelor terestre rusești a fost transformarea comandamentului armatei interarme în comandament de forțe întrunite, care să coordoneze capabilitățile din mai multe domenii. În linii mari, teatrul de operații ucrainean avea forțe rusești terestre, aeriene și navale, cu capabilități din mediul cosmic și cibernetic multiple, coordonate de comandanți ai forțelor terestre. În acest fel, deducem faptul că forțele terestre rusești se constituie în categorie de forțe sprijinită, celelalte categorii având doar rol de sprijin, limitând beneficiile aduse de operația întrunită.

Astfel, operațiile aeriene, fiind coordonate de comandamentul terestru, aveau raza operațională, în termeni de timp, spațiu sau scop, redusă la a cuceri obiectivele stabilite de comandantul terestru. De asemenea, țintele angajate prin acțiunile forțelor aeriene serveau nevoilor forțelor terestre de a ocupa elemente de infrastructură critică (Zabrodskyi și alții 2022, 45). De asemenea, forțele aeriene, pe măsură ce conflictul evolua, erau în mare parte folosite pentru asigurarea sprijinului aerian apropiat forțelor terestre. Asigurând sprijinul apropiat pentru militarii din

poziții de apărare sau asalt, anula, practic, modelarea adâncimii inamicului, pentru a permite libertatea de acțiune a forțelor terestre. Drept urmare, având forțe aeriene concentrate în mare parte pe direcțiile de înaintare ale forțelor terestre, adâncimea, ca atribut de bază al operației, așa cum este scris în *FM 3-0 Operations/2022,* nu era extinsă și era grav afectată și în celelalte domenii. Componenta terestră are un rol important în extinderea adâncimii, facilitând accesul celorlalte capabilități din toate domeniile, în special a celor spațiale și cibernetice, care îmbunătățesc protecția formațiilor tactice și neutralizează sistemele de apărare antiaeriană ale inamicului (Department of the Army 2022, 3-7).

În general, forțele terestre ruse care au acționat în războiul din Ucraina au avut rezultate slabe, fapt dovedit și prin incapacitatea realizării obiectivului principal: cucerirea Kievului și înfrângerea forțelor armate ucrainene. Randamentul slab al rușilor reiese, în principal, din lipsa maximizării efectelor operației întrunite prin limitarea utilizării capabilităților multidomeniu în sprijinirea forțelor terestre. De asemenea, această metodă de a duce războiul a redus considerabil raza operațională a marilor unități tactice din forțele terestre prin concentrarea efortului pe generarea acestor BTG, cu personal și capabilități din cadrul eșaloanelor tactice superioare, reducând posibilitățile acestora de a executa operații majore la scara largă și bazându-se pe sprijinul de arme și logistic al eșalonului armatei interarme.

Probabil, așa după cum arată și studiul amplu și relevant, făcut de Jack Watling și Nick Reynolds, cea mai importantă problemă care a afectat operațiile militare ale Rusiei din Ucraina a fost moralul scăzut al trupelor, lipsa de instruire și profesionalism și lipsa unei filosofii de conducere și execuție, bazată pe coeziune, încredere și competență.

Concluzii

Anul 2024 a început având conflicte majore în desfășurare pe glob, caracterizate, în primul rând, printr-un mare număr de victime omenești, cele mai multe din rândul civililor. Războiul ruso-ucrainean, operațiile militare desfășurate de Israel pentru neutralizarea grupării Hamas din Fâșia Gaza sau războiul civil din Yemen sunt exemple de conflicte în care condiția de a nu avea un număr mare de pierderi omenești și o distrugere masivă a infrastructurii este impusă de capacitatea forțelor armate de a planifica și executa operații multidomeniu. Din imaginile postate de mass-media sau rețelele de socializare, ne dăm seama de faptul că nu se poate discuta despre operații multidomeniu în aceste conflicte, peisajul statelor în care se desfășoară conflictele scoțând în evidență localități întregi transformate în moloz, crize umanitare greu de imaginat și lipsa unor soluții de încheiere a crizelor.

Din demersul de cercetare efectuat, se deduce faptul că operațiile multidomeniu sunt orientate pe reducerea duratei conflictelor, a victimelor, a distrugerilor de

infrastructură și pe economisirea puterii de luptă a actorilor implicați. Acest ideal al operațiilor multidomeniu nu poate fi realizat fără investiții majore, fără resurse considerabile, orientate spre cercetare și dezvoltare, pentru construirea acelor capabilități care să permită comandantului militar să aibă în permanență o imagine reală și clară, cuprinzătoare și constant actualizată a mediului operațional, precum și capacitatea de a angaja centrele de greutate și punctele critice ale inamicului, indiferent de poziționarea acestora în spațiul de luptă.

Constatăm astfel că națiunile lumii sunt, în prezent, departe de a avea forțe și capabilități multidomeniu operaționalizate. SUA au un avans destul de mare în ceea ce privește operaționalizarea unui concept de operații multidomeniu, dar asta nu înseamnă că state, precum China sau Rusia, nu vor contesta poziția americanilor, în viitor, în orice domeniu al spațiului de luptă, prin dezvoltarea de concepte și de programe proprii. Totuși, faptul că SUA se îndreaptă spre acest obiectiv, estimând o operaționalizare a conceptului până în 2035, are beneficii majore pentru NATO. Statele membre ale Alianței ar trebui să își asume un rol de participant în dezvoltarea unui concept de operații multidomeniu, beneficiind de experiența și progresul SUA în acest sens. În orice caz, membrii Alianței ar trebui, cel puțin, să participe la dezvoltarea conceptului american, pentru a întări capacitatea părții europene de apărare și descurajare a amenințării, și să contribuie la implementarea acestuia într-un mod colectiv în Europa.

În altă ordine de idei, deducem, din studierea performanței Forțelor Armate Rusești în Ucraina, faptul că forțele terestre, angajate într-un mediu operațional multidomeniu, trebuie reconfigurate astfel încât să renunțe la caracterul de componentă sprijinită și să înceapă să producă efecte sincronizate cu celelalte patru componente, în cadrul operației întrunite. Rolul forțelor terestre interarme în operațiile multidomeniu trebuie să includă sprijinirea celorlalte componente care produc efecte în celelalte domenii, pentru că astfel se extinde raza operațională a grupării de forțe întrunite, în scop, spațiu și timp, element crucial pentru succesul marilor campanii.

Referințe

Caliskan, Murat. 2019. "Hybrid Warfare through the Lens of Strategic Theory." *Defense and Security Analysis* 35 (1): 40-58. doi:10.1080/14751798.2019.1565364.

Chief of Staff Paper #1. 2021. "Army Multi-Domain Transformation." https://api.army.mil/e2/c/downloads/2021/03/23/eeac3d01/20210319-csa-paper-1-signed-print-version.pdf.

Department of the Army. 2019. "Army Doctrine Publication 3-0 Operations". https://irp.fas.org/doddir/army/adp3_0.pdf.

—. 2021. "Field Manual 3-94 Army, Corps and Division Operations". https://irp.fas.org/doddir/army/fm3_94.pdf.

—. 2022. "Field Manual 3-0 Operations." https://irp.fas.org/doddir/army/fm3-0.pdf.

Grau, Lester W. și Charles K. Bartles. 2016. "The Russian Way of War - Force Structure, Tactics, and Modernization of the Russian Ground Forces". https://www.armyupress.army.mil/Portals/7/Hot%20Spots/Documents/Russia/2017-07-The-Russian-Way-of-War-Grau-Bartles.pdf.

Hooton, Ernest A. și Tom Cooper. 2019. *Desert Storm. Volume I: The Iraqi Invasion of Kuwait and Operation Desert Sheild 1990-1991.* Helion & Company Limited.

House, Jonathan M. 1984. "Toward Combined Arms Warfare: A Survey of 20th-Century Tactics, Doctrine, and Organization". https://www.armyupress.army.mil/Portals/7/combat-studies-institute/csi-books/house.pdf.

McEnany, Charles. 2022. "Multi-Domain Task Forces A Glimpse at the Army of 2035." https://www.ausa.org/publications/multi-domain-task-forces-glimpse-army-2035.

NATO. 2022. "Conceptul Strategic al NATO 2022." Adoptat de șefii de stat și de guvern în cadrul Summitului NATO de la Madrid din 29 iunie 2022. https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept-ro.pdf.

—. 2023. "Defence Expenditure of NATO Countries (2014-2023)." https://www.nato.int/nato_static_fl2014/assets/pdf/2023/7/pdf/230707-def-exp-2023-en.pdf.

NATO Standard AJP 3-9. 2016. *Allied Joint Doctrine for Intelligence Procedures.* Edition B, Version 1, NATO Standardization Office.

—. 2021. *Allied Joint Doctrine for Joint Targetting.* Edition B, version 1, NATO Standardization Office.

NATO Standard AJP-01. 2022. "*Allied Joint Doctrine*". https://assets.publishing.service.gov.uk/media/659ea238e96df5000df843f3/AJP_01_EdF_with_UK_elements.pdf.

Nistorescu, Claudiu Valer. 2022. "The Battle of Kyiv – Considerations on the conduct of military operations at the tactical level". *Romanian Military Thinking Conference.* Bucharest: The Defence Staff.

Reuters. 2023a. *Russian budget expenditure in 2023 to total $351 bln - finance minister.* https://www.reuters.com/markets/europe/russian-budget-expenditure-2023-total-351-bln-finance-minister-2023-12-27/.

—. 2023b. *China plans 7.2% defence spending rise this year, faster than GDP target.* https://www.reuters.com/world/china/china-says-armed-forces-should-boost-combat-preparedness-2023-03-05/.

Simoens, Tom. 2022. "Combined Arms Warfare As The Key To Success On The Contemporary Battlefield?" *The Defense Horizon Journal.* https://tdhj.org/blog/post/combined-arms-warfare-success-battlefield/.

Skates, Jesse L. 2021. "Multi-Domain Operations at Division and Below." *Military Review - The Proffesional Journal of the U.S. Army*. https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/January-February-2021/Skates-Multi-Domain-Ops/.

Stanciu, Cristian-Octavian. 2018. "War – A Complex Social Phenomenon." *International Scientific Conference Strategies XXI, Technologies – Military Applications, Simulations And Resources* . Bucharest: "Carol I" National Defense University.

TRADOC Pamphlet 525-3-1. 2018. “The U.S. Army in Multi-Domain Operations 2028.” https://adminpubs.tradoc.army.mil/pamphlets/TP525-3-1.pdf.

US DoD [United States Department of Defense]. 2022. ”Defense Budget Owerview”. https://comptroller.defense.gov/Portals/45/Documents/defbudget/FY2023/FY2023_Budget_Request_Overview_Book.pdf.

Watling, Jack și Nick Raynolds. 2023. ”Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine”. https://static.rusi.org/403-SR-Russian-Tactics-web-final.pdf.

Zabrodskyi, Mykhaylo, Jack Watling, Oleksandr V. Danylyuk și Nick Reynolds. 2022. ”Preliminary Lessons in Conventional Warfighting from Russia’s Invasion of Ukraine: February–July 2022”. https://static.rusi.org/359-SR-Ukraine-Preliminary-Lessons-Feb-July-2022-web-final.pdf.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

Dinamica dezinformării. Impactul camerelor de ecou în modelarea opiniei publice online din România

Disinformation Dynamics. Unveiling the Impact of Echo Chambers in Shaping Online Public Opinion

Drd. Ștefania-Elena STOICA*
*Universitatea Națională de Apărare „Carol I", București, România

Abstract

Proliferarea dezinformării și apariția camerelor de ecou în mediul online reprezintă provocări semnificative pentru democrațiile moderne, având un impact direct asupra opiniei publice și asupra comportamentelor sociale. Studiul prezent se concentrează pe analiza unui grup Facebook, centrat în jurul unei figuri politice proeminente din România, cu 93.800 de membri și cu o medie de zece postări zilnice. Folosind tehnici avansate de "machine-learnig" (învățare automată), precum și de "hate speech-detection" (detectarea discursului negativ) prin intermediul IA (inteligență artificială), cercetarea evidențiază crearea sistematică a camerelor de ecou ca mediu propice fenomenului de amplificare a dezinformării. Rezultatele demonstrează impactul major pe care camerele de ecou online îl au asupra opiniei publice și subliniază nevoia de a menține integritatea informațiilor în mediile digitale. Studiul prezintă importanță atât pentru oamenii de știință, cât și pentru factorii de decizie politică și practicienii din mass-media sau social media, indicând o nevoie critică de a aborda provocările curente, reprezentate de fenomenul de dezinformare și de efectele camerelor de ecou din mediul online.

The proliferation of misinformation and the emergence of echo chambers in the online environment pose significant challenges to modern democracies, directly impacting public opinion and social behaviors. This study focuses on the analysis of a Facebook group centered around a prominent Romanian political figure, boasting 93,800 members and averaging ten daily posts. Using advanced machine learning and AI-based hate speech detection, the study uncovers systematic echo chamber construction and the amplification of misinformation. The findings emphasize the influence of online echo chambers on public opinion and underscore the need to maintain information integrity in the media landscape and communication. This research has important implications for scholars, policymakers, and media practitioners, indicating the critical need to address the challenges posed by misinformation and echo chambers in the online environment.

Cuvinte-cheie:
dezinformare; cameră de ecou; prejudecăți cognitive; bulă de filtrare; polarizare; manipularea știrilor false; rețele sociale.

Keywords:
disinformation; echo chamber; cognitive biases; filter bubble; polarizing; fake-news manipulation; social networks.

Info articol
Primit: 31 ianuarie 2024; Evaluat: 18 februarie 2024; Acceptat: 18 martie 2024; Disponibil online: 5 aprilie 2024
Citare: Stoica, Ș.E. 2024. „Dinamica dezinformării. Impactul camerelor de ecou în modelarea opiniei publice online din România." *Buletinul Universității Naționale de Apărare „Carol I"*, 13(1): 60-77. https://doi.org/10.53477/2065-8281-24-04

În era informației digitale, camerele de ecou se formează cu precădere în cadrul rețelelor sociale online și reprezintă un mediu propice polarizării grupurilor sociale prin capacitatea oferită de acestea pentru o interacțiune mult mai selectivă a utilizatorilor cu diferite persoane sau surse de informare care promovează un anumit tip de conținut. Acest fenomen se subscrie modului în care credințele sunt exacerbate sau întărite prin comunicare și repetare într-un sistem închis (Ciampaglia, Menczer și TheConversationUs 2018). Înrădăcinarea dezinformării este de cele mai multe ori facilitată de exploatarea prejudecăților cognitive, creându-se astfel o buclă care se autoperpetuează, aducând cu sine o îngreunare a gândirii critice și discursurilor informale ale indivizilor (Donis 2021).
Deși conceptul camerei de ecou nu este unul nou, iar acesta nu apare doar în mediul online, termenul a fost, inițial, folosit de Eli Parizer, pentru a descrie un proces de filtrare a datelor de către site-uri web prin „crearea unui univers unic informațional" personalizat pentru fiecare utilizator (Pariser 2011, 10). Unul dintre cele mai mari pericole pe care le prezintă acest proces de filtrare este auto-intoxicarea sau îndoctrinarea oamenilor cu propriile idei, prin expunerea acestora în mod repetat doar la materiale și informații familiare, concomitent cu excluderea acelor date care contrazic credințele sau părerile acestora (Pariser 2011, 13).

Dezinformarea apare în mod recurent în așa-zisele camere de ecou, întrucât aceste medii izolate oferă un teren fertil pentru diseminarea deliberată a informațiilor false sau înșelătoare ("*fake-news*") către un public țintă, caracterizat printr-o capacitate scăzută de a pune la îndoială sau de a examina critic o informație, aspect datorat prejudecăților cognitive (Ceron și de-Lima-Santos 2023, 61-90). Potrivit unui studiu, realizat de Asociația Americană de Psihologie, campaniile de dezinformare manipulează prejudecățile cognitive pentru a modela percepțiile sociale prin prezentarea de informații care se aliniază cu credințele umane, confirmând astfel concepțiile și judecățile eronate ale acestora. Când anumite persoane sunt expuse, inițial, la informații false, acestea devin un punct de referință de la care indivizilor le este dificil să se abată. În plus, în camera de ecou gândirea de grup exacerbează lipsa controlului critic, deoarece opinia unanimă a grupului suprimă disidența și încurajează acceptarea dezinformării ca adevăr (Nisbet și Kamenchuk 2019, 65-82). Un alt studiu, efectuat la Harvard Kennedy School, privind dezinformarea a constatat că acțiunile specifice acesteia pot exploata prejudecățile cognitive, cum ar fi biasul confirmării, părtinirea disponibilității și efectul adevărului iluzoriu în manipularea opiniei publice (Murphy și alții 2023). Cu alte cuvinte, într-o cameră de ecou online în care aceleași idei se repetă frecvent, dezinformarea poate prinde rădăcini și se poate amplifica, profitând de anumite credințe eronate ale indivizilor și validând ideile acestora mai puțin veridice.

Cercetare

Această cercetare își propune *să investigheze măsura în care algoritmii din social media pot facilita formarea camerelor de ecou*, precum și *modalitatea în care unii actori*

de pe scena politică exploatează aceste platforme în scopul răspândirii dezinformării, respectiv obținerii unor câștiguri financiare sau de capital politic. Acești actori folosesc tehnici sofisticate pentru a putea manipula prejudecățile cognitive ale grupurilor sociale, creând un ciclu în care indivizii devin complici la propagarea dezinformării, prin nevoile acestora de afirmare și de apartenență la un grup. În timp, camerele de ecou devin autosusținute, aspect evidențiat de faptul că membrii grupului se angajează din ce în ce mai mult în comportamente selective de căutare a informațiilor, consolidându-și credințele preexistente. Prin identificarea elementelor care ajută la formarea și exploatarea camerelor de ecou, acest studiu oferă noi perspective asupra modului în care platformele de comunicare socială pot fi eficient orientate către acțiuni de reducere a dezinformării online (Barberá 2020, 34-35).

Analiza literaturii de specialitate

Acest studiu se bazează pe cercetările anterioare ale fenomenului camerelor de ecou, respectiv dezinformarea și prejudecățile cognitive, în scopul de a examina modul în care opinia publică online este manipulată, inclusiv prin intermediul algoritmilor personalizați ai platformelor sociale. Prin analizarea teoriei bulelor de filtrare dezvoltate de Eli Parizer, în 2011, a legii polarizării grupurilor propuse de Cass Sunstein, în 1999, și prin încorporarea unor perspective din lucrarea „Propaganda în rețea", elaborată de Yochai Benkler și alți autori, în 2018, acest studiu aduce în discuție noi abordări ale acestor manifestări.

Algoritmii personalizați din platformele sociale contribuie la consolidarea camerelor de ecou prin generarea unor cicluri de feedback care mențin și întăresc convingerile deja existente ale utilizatorilor. Acest fenomen este accentuat și mai mult de modul în care algoritmii platformelor online sunt configurați pentru a menține utilizatorii angrenați. Ally Daskalopoulos et al. (2021) au remarcat, în Raportul Camerei Regionale Detroit, faptul că o mare parte dintre consumatorii de știri online interacționează adesea cu știri false și răspândesc la rândul lor informații neverificate, contribuind astfel la fenomenul de polarizare politică și dezinformare. În acest sens, existența camerelor de ecou în mediul platformelor digitale poate avea consecințe semnificative asupra discursului public și polarizării societății. Acestea restricționează accesul la informații alternative sau noi, la păreri contradictorii sau dezincriminate, aducând atingere proceselor democratice (Garrett 2009, 265-285; Woolley și Howard 2016; Lewandowsky, Ecker și Cook 2017, 353-369).
Contrar sugestiilor lui Axel Bruns (2019), care susțin faptul că utilizatorii pot interacționa în mediul online cu o gamă mai variată de conținut decât este sugerat în teoriile „bulelor de filtrare", majoritatea cercetărilor subliniază importanța expunerii selective și a prejudecății de confirmare (biasuri cognitive) în fenomenul de divizare a societății în grupuri opuse sau distincte (Cinelli și alții 2021).

Acest studiu aduce în prim-plan procesul prin care dezinformarea se înrădăcinează în conștiința umană. Astfel, conform cercetărilor lui Diaz Ruiz și Nilsson (2023),

dezinformarea se răspândește mai ales prin aprofundarea nemulțumirilor, bazate pe conceptele de identitate și credințe sau valori. Cercetarea acestora se concentrează pe o singură cameră de ecou, formată în cadrul platformei online YouTube, prin intermediul căreia este promovată ideea eronată că pământul este plat. Aceștia reușesc să arate modul în care retorica dintr-un mediu online joacă un rol crucial în răspândirea dezinformării. Tehnicile și acțiunile de manipulare care exploatează credințele și valorile legate de identitatea culturală și religioasă nu sunt singurele mijloace de a atrage indivizii în camere de ecou. Un alt studiu asupra societății americane a constatat că emoțiile generate de titlurile știrilor false joacă un rol semnificativ în răspândirea și viralizarea acestor știri. În general, participanții la studiu au fost mai dispuși să acorde credibilitate titlurilor de știri care corespundeau convingerilor lor. În același timp, au fost mai puțin dispuși să accepte știrile care le-au stârnit emoții negative puternice și care nu se potriveau cu valorile lor politice. O concluzie poate fi aceea că dezinformarea este concepută pentru a afecta latura emoțională a publicului, nu numai cea cognitivă, folosindu-se de canalele de comunicare predominante în era digitală de astăzi – mediul online.

Conform cercetării efectuate de Dag Wollebæk și de colaboratorii săi în 2019, s-a constatat că dezinformarea exercită o influență semnificativă asupra emoțiilor. Acest studiu a relevat că frica și furia sunt cele mai puternice emoții, asociate campaniilor de dezinformare în mediul online, mai ales în context politic. Studiul a analizat societatea din Norvegia, în anul 2017, și a descoperit că persoanele care experimentează emoții specifice fricii sunt mai deschise la dezbateri, atât în favoarea, cât și împotriva convingerilor proprii. Aceasta conduce la o intensificare a căutării de informații, în special din perspective opuse, îmbunătățind astfel calitatea și cantitatea informațiilor colectate. Frica și anxietatea determină, de asemenea, persoanele să pună sub semnul întrebării fapte și evenimente specifice. Pe de altă parte, furia face ca oamenii să se bazeze pe indicii euristice și rutine existente, diminuând astfel interesul pentru căutarea de noi informații. Aceasta conduce la un comportament de căutare a acțiunilor cu un grad crescut de risc și poate intensifica raționamentul părtinitor în sfera politică, conducând la formarea camerelor de ecou.

Studiul abordează domenii insuficient investigate în contextul social din România, referitoare la formarea camerelor de ecou și la proliferarea dezinformării. Acest fapt subliniază necesitatea unei cercetări extinse asupra modului în care subiectele din anumite rețele sociale care înregistrează un câștig mare de popularitate într-un interval de timp scurt afectează implicarea utilizatorilor și pot conduce la modificarea convingerilor sau valorilor acestora. Se remarcă oportunitatea de a investiga cum utilizatorii pot fi supuși unor schimbări cognitive, mai ales în contextul dezinformării, respectiv modul în care aceștia stabilesc un echilibru între răspunsurile emoționale și cele raționale și între informațiile veridice și cele înșelătoare. Profunzimea cercetărilor referitoare la aceste dinamici în literatura de specialitate argumentează în favoarea unei explorări suplimentare.

Mai mult, fenomenul cunoscut sub denumirea de postare repetitivă și efectul „maimuță zburătoare", care nu a fost încă suficient explorat, merită o atenție sporită. Acest termen, utilizat în sens metaforic, ilustrează modul în care membrii unui grup din camerele de ecou contribuie la răspândirea și întărirea dezinformării. Astfel, narațiunile false pot deveni virale și pot persista, indiferent de lipsa lor de acuratețe. Este esențială înțelegerea mult mai profundă a impactului acestor fenomene digitale asupra realităților din viața reală, cu accent deosebit asupra repercusiunilor negative în societatea românească.

Culegerea datelor

Studiul de față vizează analiza unui grup de Facebook din România, evidențiind fenomenul de extremism și divizare, observat a fi în creștere atât în țările Uniunii Europene, cât și la nivel global. Platformele online, mai ales rețelele sociale, au devenit medii fertile răspândirii extremismului politic și polarizării. Acest fenomen este amplificat de algoritmi care personalizează conținutul, conform preferințelor utilizatorilor, favorizând astfel formarea camerelor de ecou. În aceste spații, indivizii sunt izolați în bule informaționale, expuși doar la informații care consolidează convingerile lor inițiale. Conform organizațiilor precum OpenDemocracy, în țări precum România s-a constatat o creștere alarmantă a extremismului și polarizării politice, fenomen care devine din ce în ce mai vizibil în camerele de ecou online. Această creștere a polarizării subliniază o diviziune ideologică accentuată, reflectată prin decalajul digital.

Un exemplu relevant al tendințelor extremiste în România este reprezentat de o persoană care a devenit notorie pentru retorica și comportamentul său extremist, mai ales în timpul pandemiei. Această persoană a exprimat opoziție față de restricțiile impuse de autorități pentru stoparea răspândirii virusului COVID-19 și a adoptat o poziție vocală antivaccinare. Cu o prezență puternică pe platforme de socializare precum Facebook, unde participă activ în diverse grupuri sau pagini, acest caz evidențiază manifestarea extremismului online și impactul său semnificativ asupra societății românești.

Studiul inițial a explorat grupuri de Facebook care promovau perspectivele asociate cu această persoană, ulterior postările fiind extrase prin observare directă. Procesul de selecție a vizat identificarea celor mai semnificative și proeminente grupuri, concentrându-se, în final, pe un singur grup cu 93.800 de membri și o medie de zece postări pe zi (cel mai relevant și actual în termeni de postări, asociate cu această persoană). Colectarea manuală a datelor a avut loc pe parcursul unui an, din ianuarie până în decembrie 2023, permițând o analiză detaliată a discursului grupului și oferind o înțelegere profundă a situației actuale, în special în contextul alegerilor anticipate din România din 2024.

Metode de analiză

Studiul aplică o combinație de metode computaționale avansate, precum Alocarea Dirichletului Latent (LDA), Procesarea Limbajului Natural (NLP), Recunoașterea Entității Numite (NER) și învățarea automată, alături de tehnici analitice manuale, pentru a furniza o analiză exhaustivă a dinamicii dintr-o cameră de ecou (Akhtar și alții 2023, 633-657). Prin adoptarea unei abordări multifațetate, cercetarea se apleacă asupra complexității utilizării limbajului, difuzării dezinformării și a modelelor de angajare în rețelele sociale. În cadrul studiului, am aplicat un proces de modelare tematică, unde LDA sau algoritmi similari sunt folosiți pentru a identifica și a clasifica principalele teme și subiecte din postările de pe rețelele sociale, oferind o bază pentru înțelegerea narațiunilor predominante.

De asemenea, studiul integrează o componentă de extracție a caracteristicilor, care implică identificarea și analiza mențiunilor specifice despre persoane, locuri și instituții, folosind, în principal, NER, un instrument crucial din cadrul NLP, pentru a clasifica și a organiza elementele esențiale din textele analizate.

Mai mult, studiul acordă o atenție crescută și analizei limbajului emoțional și manipulativ. Acesta presupune examinarea textului pentru a identifica acele componente ale limbajului care au fost concepute să evoce răspunsuri emoționale sau să manipuleze anumite percepții, proces îmbunătățit prin algoritmi de analiză a sentimentelor și prin instrumente de tip NLP (He, Hu și Pei 2023). În plus, studiul analizează frecvența postărilor, gradul de implicare (”*engagement*”) și momentul publicării acestora. Acest lucru implică utilizarea unor tehnici de analiză statistică, precum și vizualizarea datelor pentru a înțelege frecvențele sau modelele de activitate, respectiv angajamentul utilizatorilor în cadrul camerei de ecou.

În continuare, am dezvoltat o matrice pentru analiza textelor de dezinformare, inspirându-mă din analize detaliate ale literaturii de specialitate, din studii dedicate dezinformării și din experiența proprie cu materiale din campanii de dezinformare. Această matrice oferă un cadru structurat pentru evaluarea sistematică a unui număr mare de texte sau mesaje, subliniind, totodată, că, deși eficientă, metodologia poate fi încă perfecționată, reprezentând un domeniu activ de cercetare. Metodologia structurată urmărește reducerea interpretărilor subiective prin aplicarea unor criterii obiective, și facilitează compararea rezultatelor, consolidând principiile cercetării științifice. Din perspectiva naturii complexe și polivalente a dezinformării, matricea permite o analiză multidimensională, oferind cercetătorilor instrumentele necesare explorării în detaliu a unor aspecte, precum utilizarea limbajului, fiabilitatea surselor și coerența informațiilor. Această abordare cuprinzătoare asigură o înțelegere profundă a complexității fenomenului de dezinformare, evidențiind importanța unui cadru structurat în analiza acestui tip de conținut.

Criterii privind dezinformarea	Criterii explicative
Limbaj emoţional şi senzaţionalist	Autorul foloseşte un limbaj încărcat emoţional sau senzaţional pentru a provoca răspunsuri emoţionale
Denaturarea faptelor sau a contextului	Prezentarea unor informaţii inexacte sau scoase din context
Apel la frică şi urgenţă	Utilizarea temerilor şi crearea unui sentiment de urgenţă
Lipsa dovezilor credibile	Absenţa sprijinului din surse credibile
Credibilitatea îndoielnică a sursei	Bazarea pe surse cu credibilitate îndoielnică
Inconsecvenţe factuale	Prezenţa contradicţiilor în conţinut sau cu fapte
Contradicţia înţelegerii stabilite	Abaterea semnificativă de la cunoştinţele acceptate pe scară largă, fără dovezi substanţiale
Retorica polarizantă „noi vs. ei”	Folosirea limbajului divizator pentru a crea un sentiment de grup şi de grup opus
Generalizarea excesivă şi stereotipizarea	Folosirea generalizărilor şi stereotipurilor
Informaţii selective sau omise	Omiterea informaţiilor critice sau prezentarea selectivă a faptelor
Manipularea citatelor sau surselor	Modificarea citatelor sau surselor pentru a induce în eroare
Lipsa de transparenţă în aprovizionare	Nedezvăluirea surselor şi ascunderea originii informaţiilor
Logică sau argumentare inconsecventă	Folosirea argumentelor bazate pe raţionamente eronate sau pe logică inconsecventă
Utilizarea elementelor vizuale neverificate sau false	Bazarea pe elemente vizuale neverificate sau dovedit false
Titluri hiperbolice sau provocatoare	Folosirea titlurilor exagerate sau provocatoare
Opinie prezentată ca fapt	Prezentarea opiniilor ca şi cum ar fi informaţii
Anacronism	Referirea la evenimente sau contexte inexacte pentru a induce în eroare
Erori logice	Utilizarea raţionamentelor care conţin erori logice

Figura 1 Matricea dezinformării

Constatări

În etapa următoare, am efectuat o analiză detaliată a datelor extrase. Această colecţie extinsă de date a inclus informaţii, precum: data postării, conţinutul mesajelor, profilurile utilizatorilor, conexiunile în reţeaua socială, feedback-ul primit, gradul de interacţiune şi alţi identificatori unici. Această analiză a permis si evidenţierea diferitelor naraţiuni, discursuri de ură, utilizarea limbajului emoţional, exprimarea sentimentelor negative şi folosirea tehnicilor de amplificare în cadrul postărilor din grupul de Facebook. Cu toate acestea, trebuie să menţionez faptul că, pentru a înţelege pe deplin baza naraţiunilor subsumate unor potenţiale mesaje de dezinformare, a fost realizată şi o analiză calitativă a conţinutului mesajelor prin examinarea temelor principale ale unui text, precum şi a ideologiilor şi elementelor retorice utilizate în postări. În urma acestor analize, s-au reliefat următoarele tipare specifice de manipulare, amplificare şi polarizare în cadrul camerelor de ecou şi dezinformare:

a) Crearea unui sentiment de comunitate şi apartenenţă

Am observat că folosirea limbajului incluziv a avut un impact semnificativ în promovarea unui sentiment de comunitate şi apartenenţă în cadrul grupului. Cuvinte precum „noi”, „împreună” împreună cu hashtaguri, precum #solidaritate, #Împreună, #Comunitate, subliniază o identitate comună între membrii grupului. De asemenea, hashtaguri precum #TradiţiaNeDefineşte, #SchimbareaDeCareAvemNevoie, #ErouAlNostru, #unire, #RespectPentruCulturaNoastră întăresc acest sentiment,

oamenii identificându-se cu grupul și prin prisma valorilor comune. Limbajul utilizat nu doar consolidează sentimentul de a face parte dintr-un grup distinct și unitar, atrăgându-i pe cei care caută un sentiment de apartenență, ci și joacă un rol semnificativ în conturarea identității sociale.

Această abordare are și un impact semnificativ asupra modelării identității sociale. Utilizarea narațiunilor de tip „noi/ei" afectează aspecte psihologice cheie, cum ar fi identitatea socială, favoritismul în grup și derogarea față de ceilalți.

În anumite contexte, răspândirea informațiilor false într-o cameră de ecou poate avea consecințe grave, precum exacerbarea polarizării în cadrul grupului și consolidarea percepțiilor negative față de grupurile externe. Potrivit lui Sunstein, platformele de socializare pot acționa adesea ca niște camere de ecou, promovând un sentiment de identitate de grup și încurajând utilizatorii să caute informații care se aliniază credințelor lor, ignorând alternativele (Sunstein 1999).

b) Mesajele repetitive

În contextul dezinformării și creșterii rapide a camerelor de ecou, grupul pe care l-am analizat oferă un exemplu semnificativ. Acesta a fost înființat la data de 25 octombrie 2021 și a înregistrat o creștere accelerată de noi membri (aproximativ 100.000 de membri în doar 2 ani). Numai în ultima săptămână a perioadei de studiu, grupul a adăugat 174 de noi membri, cu o creștere medie zilnică de aproximativ 130 de membri. Această rată de creștere în continuă ascensiune indică influența și extinderea grupului.

De asemenea, se remarcă faptul că, doar într-un singur an (2023), postările din grup au generat peste 700.000 de reacții (aprecieri), aspect ce reflectă un nivel semnificativ de implicare din partea membrilor săi. Acest model de creștere rapidă și de implicare crescută este caracteristic camerelor de ecou, unde mesajele repetitive și conținutul direcționat pot atrage și menține rapid audiența, amplificând astfel răspândirea și impactul dezinformării.

Pe lângă activitățile online, implicarea formatorului de opinie în evenimente publice, precum și sensibilizarea comunității prin participarea activă la acțiuni în lumea reală, sunt aspecte care au contribuit la creșterea grupului în mediul online. Această interacțiune între activitățile offline și implicarea online a dus la extinderea acoperirii sociale a grupului și la consolidarea influenței sale în România atât în mediul digital, cât și în cel real.

c) Consolidarea unei identități comune

Camerele de ecou folosesc adesea un limbaj care întărește percepția unei identități de grup unificate, mutând accentul de la indivizi la colectivitate. Această identitate comună este construită în jurul unor convingeri, opinii sau ideologii, servind ca o forță de unificare puternică în cadrul grupului. De exemplu, formatorul de opinie vorbește într-o postare despre grupul pe care îl reprezintă și despre susținătorii din mediul online astfel: *„spiritul nostru #patriotic rămânem hotărâți în #război cu încercările de import ale #obiceiurilor străine care nu au legătură cu identitatea noastră #națională. #Halloween, o tradiție originară din Irlanda, încearcă să pătrundă în cultura noastră. Această sărbătoare păgână a fost adoptată în multe țări ca o formă de*

divertisment, dar noi suntem hotărâți să respingem influențele străine care amenință să ne #distrugă tradițiile autentice (...)". În continuare, reafirmarea identității naționale este evidentă, deoarece situația este prezentată ca un „război" împotriva obiceiurilor străine, subliniind importanța menținerii unei identități românești distincte. Cu toate că nu este menționat explicit în această parte, mesajul general al postării pledează pentru celebrarea tradițiilor românești și respingerea celor străine, întărind ideea că obiceiurile naționale sunt parte integrantă a identității grupului. Postarea poziționează emițătorul ca apărător al identității naționale împotriva obiceiurilor străine, creând o poveste de protecție și rezistență care întărește coeziunea și unitatea grupului. Folosirea termenilor precum „#război" și accentuarea „spiritului nostru patriotic" servesc ca un apel la acțiune, pentru susținători, să se mobilizeze în jurul cauzei menținerii identității naționale, consolidând și mai mult identitatea comună a grupului.

d) Reducerea receptivității vizavi de punctele de vedere opuse

Într-o altă postare, persoana publică face afirmații referitoare la o altă personalitate, potrivit cărora aceasta „îi îndeamnă pe tineri să nu mai plece peste hotare: «Vă încurajez să vă proiectați un viitor în România»", comentariile membrilor grupului indicând în mare parte o puternică dezaprobare și cinism față de încurajarea tinerilor de către alt formator de opinie față de cel simpatizat de a rămâne în România. Mulți comentatori văd acest lucru ca pe un gest nesincer sau manipulator. Această uniformitate a sentimentului și lipsa contraargumentelor vizibile sau a perspectivelor diverse sugerează un efect de cameră de ecou, în care predomină un singur punct de vedere, iar opiniile divergente sunt fie absente, fie respinse. Unele dintre mesaje includ:

- *Ristea D.*: „Da, stați în țară dragi tineri, că au nevoie de carne de tun."* Acest comentariu exprimă cinism față de tinerii care rămân în România, sugerând că este nevoie de ei doar ca resurse consumabile, implicând o lipsă de preocupare reală pentru bunăstarea lor.
- *Monica P.*: „Pleacă, trădătorule! Vrei carne de tun?!"* Reiterând un sentiment similar, prin acest comentariu, autorul etichetează personalitatea publică neîndrăgită drept „trădător" și îl acuză că dorește ca tinerii să fie „carne de tun", indicând o profundă neîncredere și o percepție negativă.
- *Rodica I.*: „Să îi trimiți în război nemernicule... al globaliștilor."* Acest comentariu intensifică și mai mult sentimentul negativ, acuzând o altă personalitate publică de faptul că trimite tinerii la război și se aliniază cu globaliștii, reflectând o neîncredere și ostilitate adânc înrădăcinate.

Când identitatea de grup se împletește cu credințe sau ideologii specifice, orice provocare la adresa acestora se simte ca un atac personal asupra grupului și, prin extensie, asupra individului.

e) Folosirea frecventă a limbajului negativ

Utilizând instrumentul de analiză a matricei de dezinformare (exemplificat în Figura 2), am constatat că o proporție semnificativă a limbajului folosit în camera de ecou, reprezentând 47,25% din mesaje, are un caracter negativ, instigator la ură sau manipulator. Acest nivel ridicat de negativitate este deosebit de important,

în contextul camerelor de ecou, din mai multe motive. În primul rând, aceasta consolidează convingerile comune ale membrilor grupului, promovând un puternic sentiment de unitate împotriva grupurilor percepute ca fiind diferite sau împotriva ideilor contrare. Acest lucru se realizează adesea prin conturarea unei dinamici clare de tipul „noi versus ei". În al doilea rând, limbajul negativ stârnește reacții emoționale mai intense, în comparație cu limbajul neutru sau pozitiv, ceea ce conduce la creșterea angajamentului în cadrul camerei de ecou. Această reacție emoțională sporită poate întări și mai mult convingerile membrilor. În cele din urmă, negativitatea prezentă în camerele de ecou contribuie la polarizarea și radicalizarea opiniilor, deoarece crește rezistența membrilor la informații externe sau la puncte de vedere alternative. Prezența semnificativă a cuvintelor negative, așa după cum rezultă din analiza realizată, subliniază rolul limbajului emoțional și divizibil în modelarea dinamicii din camerele de ecou.

f) Comunicarea spontană și emoția puternică

În analiza modelelor de comunicare ale camerei de ecou, am constatat folosirea semnificativă a limbajului manipulator, identificând 2.076 de cuvinte sau expresii (uneori repetate) în diferite postări. Acest limbaj manipulator include termeni și sintagme, precum „*șocant*", „*brutal*", „*limitat*", „*cenzură*", „*șocat*", „*devastatoare*", „*incendiară*", „*limitări impuse*", „*un eveniment pe care nu-l puteți rata*", „*mințit*", „*manipulare totală*", „*armă*", „*profiluri false*", „*știri false*", „*insulte*", „*niciodată nu mai îndrăznești*", „*haos*", „*tragedie*", „*tristă*", „*devastatoare*", „*suferă*", „*demisia*", „*esențială*", „*vânzătorii*", „*gâtul nostru*", „*acuză*" și „*ăștia*" ș.a.m.d. Aceste cuvinte și expresii manipulative, care conțin declanșatori emoționali, sunt frecvent utilizate în cadrul grupului pentru a influența opiniile și emoțiile publicului. O analiză mai detaliată a 825 de postări arată că, în medie, fiecare postare sau mesaj conține aproximativ 5,78 cuvinte manipulative, demonstrând dependența grupului de limbajul persuasiv pentru a modela opinii și emoții. Cuvintele manipulatoare identificate, așa după cum se observă în fraze, precum „Demiterea lui Arafat, arestarea și condamnarea lui pe viață pt genocid", „*Pentru a nu spune adevărul, mi-au interzis să vorbesc*" și „Manipularea DNA, filmări plătite la comandă și scoase din context", sunt concepute pentru a evoca reacții emoționale puternice și pentru a forma opinii. Acest lucru demonstrează uzitarea limbajului încărcat emoțional pentru a influența și a manipula cititorii sau publicul. În plus, comunicarea în cadrul acestor camere de ecou se caracterizează prin spontaneitate. Acest lucru este exemplificat prin folosirea frecventă a cuvintelor licențioase și a semnelor de exclamație, a cuvintelor capitalizate, care acționează ca „markeri" ai emoțiilor puternice și ai stărilor de excitare sporite. Într-un astfel de mediu polarizat, aceste expresii ale emoțiilor indică adesea fie un acord puternic, fie un dezacord vehement față de credințele și prejudecățile comune predominante în cadrul grupului.

În plus, prezența cuvintelor vulgare sau licențioase în discursul grupului indică un stil de comunicare mai puțin formal, dar mai pasional și, uneori, agresiv (Wollebæk și alții 2019). În mediile hiperpartizane, o astfel de utilizare a cuvintelor servește adesea unor scopuri duble: exprimarea emoțiilor intense, cum ar fi furia sau disprețul, în special față de opiniile sau grupurile opuse, și consolidarea unității

în interiorul grupului împotriva adversarilor. Această caracteristică lingvistică contribuie la atmosfera încărcată și adesea controversată a camerei de ecou. În mod similar, folosirea semnelor de exclamație amplifică intensitatea emoțională a unui mesaj. În plus, semnele de exclamație pot spori rezonanța emoțională a mesajelor, făcându-le să pară importante și să devină memorabile.

g) O dinamică crescută a subiectelor abordate în cadrul aceleiași camere de ecou (Figura 2)

Această dinamică în abordarea cât mai diversificată a unor subiecte servește mai multor scopuri: în primul rând, atrage subiecți din medii diverse și cu interese diferite, și în al doilea rând, joacă un rol crucial în modificarea percepțiilor. Camera de ecou analizată manipulează eficient percepțiile membrilor săi prin trecerea rapidă de la un subiect la altul, schimbând astfel stările lor emoționale și cognitive. Această tactică este insidioasă, deoarece nu permite creierului suficient timp pentru a se adapta de la procesarea conținutului emoțional la gândirea rațională.

Astfel, discuțiile analizate acoperă o gamă largă de subiecte care răspund diverselor interese și credințe ale publicului. Categorii precum „Probleme sociale", „Cultură și identitate românească", „Media și comunicare", „Politică", „Naționalism", „Religie și stil de viață" servesc drept instrumente practice pentru a menține membrii implicați și activi în cadrul camerei de ecou. Cu toate acestea, este important să observăm tehnica de manipulare, în care un fapt neutru este validat, înainte de a trece subtil la dezinformare și discurs de ură. Această schimbare continuă face dificilă capacitatea membrilor de a discerne schimbarea veridicității conținutului, rezultând astfel un răspuns emoțional din partea acestora, cu privire la date manipulate sau false.

Categorii	Categorizarea hashtagurilor – modelare NLP
Probleme sociale	#CopiiiSuntViitorul, #oameni, #părinți, #Comunitate, #grădiniță, #școală, #sociale, #Împreună, #solidaritate, #binele, #respect, #drepturile, #justiție, #doaradevărul, #drepturi, #amintire, #înțelegere, #recunoștință, #adevăr, #toleranță, #hotărâți, #speciale, #TraficulDeDroguri, #ConfidențialitateFinanciară, #LibertateEconomică, #SchimbareaDeCareAvemNevoie, #pace, #incompetență, #nurăzboi.
Cultura și identitatea românească	#decembrie, #TradițiaNeDefinește, #Datini, #istoric, #OrașulCuInimăVeche, #tebea.
Media și comunicare	#DezvăluiriCuImpact, #tiktok, #televiziuni, #socialmedia, #știri, #facebook, #televiziune, #tipografie, #dezvăluiri, #ziare, #informație, #actual, #live, #instagram, #vocea, #dezbatere, #Laudatium.
Politică	#SchimbareaDeCareAvemNevoie, #pace, #incompetență, #nurăzboi, #șieusuntvoluntar, #sosromânia, #DemisieArafat, #raedarafata, #ResponsabilitateSauDemisie, #uk, #canada, #germania.
Naționalism	#Conștiență, #bucovina, #RomâniaReală, #patriotism, #țară, #națiune, #patriot, #bunderomânia, #ErouAlNostru, #român, #române, #demnitate, #unirea, #istorie, #distrugă, #românia, #unire, #independent.
Religie	#mihail, #sfânt, #ÎngeriiPăzitori, #cer.
Stil de viață	#iubire, #poet, #carte, #simpozion, #viață, #cântece, #dramaturg, #viitorul, #MoștenireLiterară, #RespectPentruCulturaNoastră.

Figura 2 Schimbarea rapidă a subiectelor printre mai multe mesaje de ură și conspirație

Studii, cum ar fi cel realizat de Institutul Reuters pentru Studiul Jurnalismului, au arătat că oscilația constantă între diferite subiecte, stări emoționale și raționale subminează capacitatea indivizilor de a evalua critic informațiile prezentate, ducând la o acceptare treptată a dezinformării ca adevăr (Brennen 2019). Acest fenomen evidențiază strategiile sofisticate ale camerelor de ecou, de a manipula opiniile și credințele. Un alt studiu, realizat de Harvard Kennedy School, a constatat că majoritatea utilizatorilor obișnuiți de internet la nivel global își fac griji cu privire la dezinformare, grupurile tinere și cu venituri mici exprimând cele mai înalte niveluri de îngrijorare (Knuutila, Neudert și Howard 2022).

h) Utilizarea unui spectru larg de teme negative pentru a influența membrii (Figura 3)
Variația amplă de categorii negative utilizate în postările camerei de ecou reflectă o strategie sofisticată de a implica membrii la diferite niveluri emoționale și intelectuale. Această strategie consolidează coeziunea internă a camerei de ecou și are impact asupra dinamicii societății, în ansamblu, contribuind la polarizare, dezinformare și la subminarea discursului public.
Prevalența unor categorii care includ conotații negative, calomnie, discriminare, bigotism și opresiune indică o abordare deliberată de a provoca reacții emoționale puternice, adesea negative, pentru a întări identitatea și credințele grupului. Totodată, prezența unor categorii, precum „Soluții și inovații", „Sprijin și solidaritate" și „Speranță și aspirație", arată faptul că există o abordare dual de combinare a narațiunilor negative și pozitive, în scopul menținerii angajamentului publicului țintă și susținerii narativei strategice a grupului.

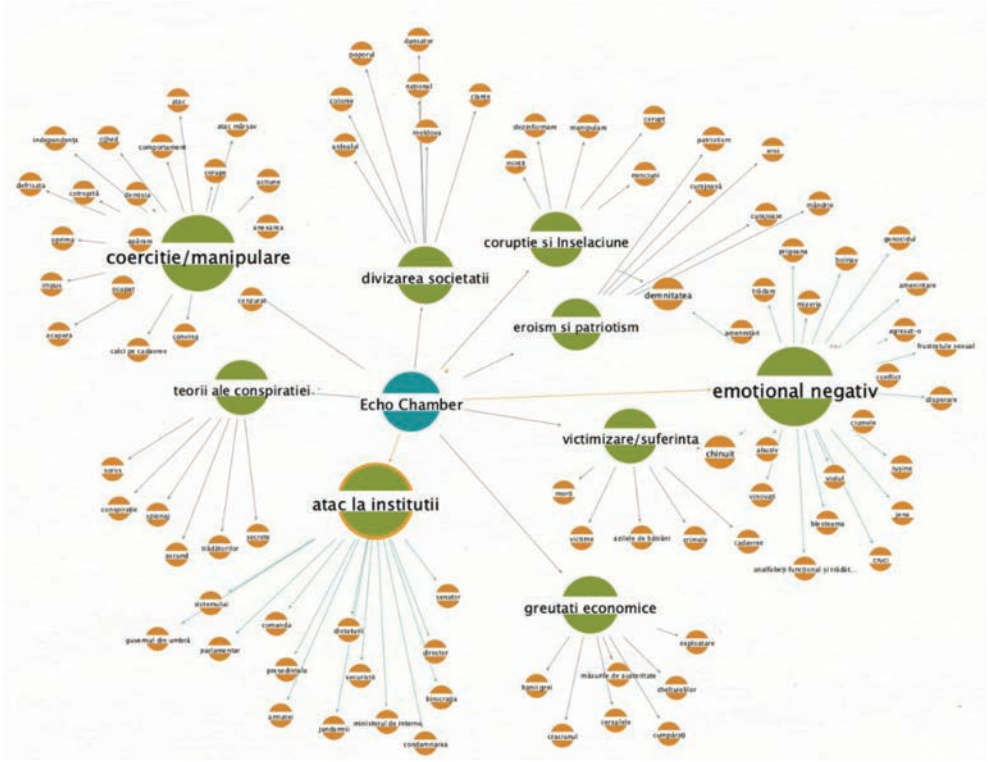

Figura 3 Modelarea și gruparea subiectelor pe cuvinte-cheie cu conținut instigator la ură, emoțional sau negativ, găsite în camera de ecou

De asemenea, cuvintele-cheie și mesajele regăsite în cadrul camerei de ecou (Figura 3) sugerează o abordare complexă și multifațetată, caracteristică dezinformării și manipulării opiniei publice. Fiecare set de cuvinte-cheie este folosit cu scopul de a influența percepțiile publicului, de a adânci diviziunile sociale, de a submina încrederea în instituții și de a provoca răspunsuri emoționale în rândul cititorilor:

- **Coerciție/Manipulare**: cuvinte precum „conving", „calci pe cadavre", „a acapara", „ocupa", „impus", „oprima", „defrișată", „cotropită", „demisia", „independența", „COVID", „comportament", „corupe", „atac", „atac mârșav", „acțiune", „anexare", „cenzurat" sugerează o narativă menită să prezinte acțiuni forțate sau înșelătoare, atribuindu-le anumitor grupuri sau indivizi pentru a-i discredita sau a justifica comportamente agresive sau lipsite de etică.
- **Divizarea societății**: „Ardealul", „colonie", „poporul", „trădător", „Moldova" sunt cuvinte folosite pentru a exacerba tensiunile regionale, etnice sau naționale, reliefând efortul de a fragmenta unitatea societății prin evidențierea sau fabricarea diviziunilor și încurajarea resentimentelor între diferite comunități.
- **Corupție și înșelăciune**: cele mai uzitate cuvinte au fost „minți", „dezinformare", „manipulare", „corupție minciuni", elemente tipice în narative menite să submineze încrederea în persoane publice, în organizații sau instituții ale statului, pe care le acuză de comportamente necinstite sau frauduloase, adesea fără dovezi.
- **Teorii ale conspirației**: mențiunea „conspirație", „secrete", „trădătorilor", „ascund", „spionaj", „Soros" indică promovarea unor teorii nefondate, care susțin că forțe obscure orchestrează evenimente din culise pe scena politică românească. Aceste narative se bazează adesea pe prejudecăți, paranoia sau conexiuni speculative pentru a explica situații complexe prin lentile simplificate, superficiale.
- **Atacuri asupra instituțiilor**: cuvinte care vizează „sistemul", „guvernul din umbră", „parlament", „comandă", „președintele", „armata", „dictatura", „jandarmii", „securiștii", „ministrul de interne", „condamnare", „birocrație", „director", „senator" demonstrează un efort de a eroda încrederea în instituțiile guvernamentale și societale, prezentându-le ca fiind corupte, opresive sau ilegitime.
- **Greutăți economice**: termeni precum „banii grei", „Crăciunul", „cerealele", „măsurile de austeritate", „cumpărat", „cheltuielile", „exploatare" reflectă preocupări legate de condițiile și politicile economice, posibil răstălmăcind faptele sau contextul real pentru a incita la furie sau disperare vizavi de situația economică, atribuind vina unor entități sau politici specifice, fără o perspectivă echilibrată.
- **Victimizare/suferință**: Spre exemplu, cuvintele „morți", „victime", „azile de bătrâni", „crime", „cadavre" se concentrează pe evidențierea unor cazuri reale sau imaginare de suferință pentru a stârni empatie, furie sau frică din partea oamenilor, adesea pentru a influența opinia sau pentru a justifica puncte de vedere radicale sau acțiuni.
- **Apeluri emoționale negative**: termeni precum „chinuit", „abuziv", „vinovați", „analfabeți funcționali și trădători", „blestem", „viol", „cruci", „rușine", „ciumele", „disperare", „conflict", „frustrat sexual", „agresor", „amenințare", „genocid",

„bolnav", „mizerie", „prigoană", „trădare" sunt concepuți pentru a evoca emoții negative puternice, având ca scop manipularea sentimentelor publicului pentru a provoca indignare, frică sau ură, ocolind analiza rațională care poate fi aplicată pe un anumit subiect.

Scopul utilizării unor astfel de cuvinte în tematicile abordate în camerele de ecou este adesea de a polariza societatea, de a distrage atenția de la problemele esențiale sau de a consolida puterea prin crearea unui mediu în care discursul rațional este umbrit de frică, suspiciune și furie.

Interpretarea rezultatelor

Examinarea acestei camere de ecou (grup Facebook) furnizează informații valoroase, în contextul prejudecăților cognitive și dezinformării, extinzând astfel înțelegerea fenomenului. Observațiile studiului au fost făcute în urma analizei categoriilor sociale și a grupării subiectelor în cadrul grupului de Facebook. Diversitatea orientărilor tematice și a tacticilor manipulative predominante în camera de ecou este în concordanță cu diversele prejudecăți cognitive, cum ar fi prejudecata de confirmare, în care indivizii favorizează informațiile care confirmă convingerile lor preexistente.

Limbajul emoțional și manipulativ utilizat agravează și mai mult acest fenomen, deoarece acesta este conceput pentru a provoca reacții puternice și pentru a descuraja gândirea critică, făcând membrii mai receptivi în acceptarea informațiilor false ca adevărate.

Utilizarea temelor bazate pe identitate, cum ar fi naționalismul și patriotismul, împreună cu portretizările negative ale grupurilor exterioare, contribuie la polarizarea grupului. Această polarizare este întărită de gândirea de grup, un fenomen în care dorința de armonie sau conformitate în cadrul grupului duce la luarea unor decizii iraționale sau disfuncționale. Într-un astfel de mediu, punerea la îndoială sau contestarea convingerilor grupului devine tot mai dificilă, ceea ce duce la un set de opinii omogene și extreme.

Implicații

Rezultatele studiului au implicații semnificative asupra înțelegerii naturii camerelor de ecou într-un context mai larg și asupra elaborării strategiilor de combatere a dezinformării. Mecanismele identificate, cum ar fi utilizarea limbajului încărcat emoțional și manipulator, dezvoltarea unui puternic sentiment de comunitate și prezența unei comunicări spontane, intens emoționale nu sunt specifice doar grupurilor pe care le-am studiat. Dinamica pe care am observat-o reflectă un model global mai extins, în care camerele de ecou, caracterizate de tehnici manipulative, apar în diverse contexte, subliniind necesitatea unei abordări globale a acestor provocări. Astfel de medii sunt deosebit de favorabile extremismului, oferind o

platformă în care ideile extremiste sunt exacerbate și normalizate, ceea ce poate duce la radicalizarea indivizilor sau a maselor, în special în cadrul populațiilor vulnerabile. În plus, influența camerelor de ecou se poate extinde inclusiv la procesele democratice și la întreaga stabilitate a societății, polarizând opinia publică, erodând adevărurile comune și subminând discursul democratic. Acest lucru poate duce la destabilizarea lumii moderne, cauzată de acțiuni bazate pe percepții distorsionate și dezinformare. Abordarea acestor provocări necesită înțelegerea mecanismelor camerelor de ecou pentru a dezvolta strategii eficiente de combatere a dezinformării. Aceasta implică, dar nu numai, creșterea gradului de conștientizare, promovarea educației în domeniul mass-mediei, încurajarea expunerii la diverse puncte de vedere și abordarea aspectelor structurale ale platformelor de comunicare socială care contribuie la formarea acestor camere.
Efectele camerelor de ecou asupra coeziunii sociale și integrității democratice necesită o reevaluare a rolului social media în discursul public, respectiv implementarea unor reglementări mai bune pentru a reduce dezinformarea și sprijinirea inițiativelor care încurajează gândirea critică și verificarea faptelor.

Limitări

În mod evident, studiul de față prezintă și limitări care merită a fi luate în considerare, deoarece acestea pot influența generalizarea și aplicabilitatea rezultatelor obținute. În primul rând, studiul se concentrează exclusiv pe un procent redus din rândul posibilelor camere de ecou, fiind axat în mod specific pe anumite segmente sociale din România, mai exact pe un singur grup reprezentativ pentru sfera politică actuală. Având în vedere contextul cultural și istoric unic al României, strategiile adoptate de administratorii sau de figurile reprezentative ale acestor camere de ecou și natura discursului din interiorul lor pot să nu fie reprezentative în totalitate pentru fenomene similare din alte țări sau culturi (Arguedas și alții 2022).

În plus, prejudecățile cognitive, care joacă un rol semnificativ în formarea și menținerea camerelor de ecou, pot varia de la o populație la alta. Aceste prejudecăți sunt influențate de o serie de factori, inclusiv de contextul cultural, social și de perioadele istorice, ceea ce înseamnă că modelele cognitive observate în studiu nu pot fi aplicate universal. Deși cercetarea furnizează informații de interes privind funcționarea camerelor de ecou și impactul acestora, studiul de față, aplicat la o scară mai mare, va trebui să fie mult mai cuprinzător. Mai mulți factori externi pot influența dinamica camerelor de ecou, precum restricțiile politice, condițiile economice sau evenimentele externe, cum ar fi războaiele din țările vecine, elemente care nu au fost incluse în analiză. Acești factori pot avea un impact semnificativ asupra opiniei publice și răspândirii dezinformării.

Pe scurt, în timp ce studiul aduce contribuții esențiale la înțelegerea camerelor de ecou într-un context social și cultural specific din România, aceste limitări ar trebui luate în considerare atunci când se dorește replicarea lui. Cercetările viitoare pot

aborda aceste limitări prin includerea unui spectru mai larg de camere de ecou și prin analizarea factorilor de influență.

Concluzii

Rezultatele acestui studiu privind camera de ecou din cadrul platformei Facebook analizată oferă perspective importante asupra naturii unor astfel de medii și sugerează existenta unor elemente definitorii fenomenului de dezinformare. Această cercetare indică faptul că mecanismele identificate, inclusiv limbajul încărcat emoțional, cultivarea unui simț comunitar puternic și comunicarea haotică, spontană reflectă probabil o tendință globală mai largă în camerele de ecou.

Această cameră de ecou oferă teren fertil extremismului, amplificând ideile rigide și conducând la radicalizarea indivizilor sau a grupurilor, în special în cadrul populațiilor vulnerabile. În plus, ele pot avea un impact semnificativ asupra proceselor democratice și stabilității societății prin polarizarea opiniei publice și erodarea adevărurilor comune, ceea ce poate duce la destabilizarea lumii reale, alimentată de dezinformare. Abordarea acestor probleme necesită înțelegerea modului în care funcționează camerele de ecou și o strategie cuprinzătoare, care implică alfabetizarea media, expunerea la diverse puncte de vedere ale publicului și schimbări structurale în rețelele sociale. Factorii politici și autoritățile de reglementare joacă, de asemenea, un rol crucial și ar trebui să fie informați cu privire la aceste implicații pentru a dezvolta politici și reglementări eficiente.

Referințe

Akhtar, P., A.M. Ghouri, H.U.R. Khan, M.A.U. Haq, U. Awan, N. Zahoor, Z. Khan și A. Ashraf. 2023. "Detecting fake news and disinformation using artificial intelligence and machine learning to avoid supply chain disruptions." *Annals of Operations Research* 327: 633-657. https://doi.org/10.1007/s10479-022-05015-5.

Arguedas, A.R., C.T. Robertson, R. Fletcher și R.K. Nielsen. 2022. "Echo chambers, filter bubbles, and polarisation: a literature review." *Reuters Institute.* doi:10.60625/risj-etxj-7k60.

Barberá, P. 2020. „Social Media, Echo Chambers and Political Polarization." În *Social media and democracy. The State of the Field, Prospects for Reform*, editor Nathaniel Persily și Joshua A. Tucker, 34-55. https://www.cambridge.org/core/books/social-media-and-democracy/social-media-echo-chambers-and-political-polarization/333A5B4DE1B67EFF7876261118CCFE19.

Benkler, Y., R. Farris și H. Roberts. 2018. *Network Propaganda.* Oxford University Press. https://doi.org/10.1093/oso/9780190923624.001.0001.

Braddock, K. 2022. "Vaccinating against hate: Using attitudinal inoculation to confer resistance to persuasion by extremist propaganda." *Terrorism and Political Violence* 34 (2): 240-262. https://doi.org/10.1080/09546553.2019.1693370.

Brennen, J.S. 2019. "Misinformation: The evidence on its scope, how we encounter it, and our perceptions of it." *Reuters Institute for the Study of Journalism.* https://reutersinstitute.politics.ox.ac.uk/news/misinformation-evidence-its-scope-how-we-encounter-it-and-our-perceptions-it.

Bruns, A. 2019. "Filter bubble." *Internet Policy Review* 8 (4). https://doi.org/10.14763/2019.4.1426.

Ceron, Wilson și Mathias-Felipe de-Lima-Santos. 2023. "Disinformation Echo Chambers on Facebook." In *Fighting Fake Facts*, 61-90. MDPI Books. https://doi.org/10.3390/books978-3-0365-1347-8-4.

Ciampaglia, G.L., F. Menczer și TheConversationUs. 2018. "Biases Make People Vulnerable to Misinformation Spread by Social Media." *Scientific American.* https://www.scientificamerican.com/article/biases-make-people-vulnerable-to-misinformation-spread-by-social-media/.

Cinelli, Matteo, Gianmarco De Francisci Morales, Alessandro Galeazzi și Michele Starnini. 2021. "The echo chamber effect on social media." *Proceedings of the National Academy of Sciences* 118 (9): e2023301118. https://doi.org/10.1073/pnas.2023301118.

Daskalopoulos, A., N. Hernandez, F. Jason, H. Jenvey, D. Gustafson, R. Mosley, C. Rodriguez, N. Schoonover și S. Townsend. 2021. "Thinking outside the bubble: Addressing polarization and disinformation on social media." *CSJS Journalism Bootcamp.* https://journalism.csis.org/thinking-outside-the-bubble-addressing-polarization-and-disinformation-on-social-media/.

Donis, L. 2021. „How to filter bubbles and echo chambers reinforce negative beliefs and spread misinformation through social media." *Debating Communities and Networks XII.* https://networkconference.netstudies.org/2021/2021/04/25/how-filter-bubbles-and-echo-chambers-reinforce-negative-beliefs-and-spread-misinformation-through-social-media/.

Garrett, R.K. 2009. "Echo chambers online?: Politically motivated selective exposure among Internet news users." *Journal of Computer-Mediated Communication* 14 (2): 265-285. https://doi.org/10.1111/j.1083-6101.2009.01440.x.

He, L., S. Hu și A. Pei. 2023. "Debunking Disinformation: Revolutionizing Truth with NLP in Fake News Detection." https://arxiv.org/abs/2308.16328.

Horner, G.C., D. Galletta, J. Crawford și A. Shirsat. 2021. "Emotions: The Unexplored Fuel of Fake News on Social Media." *Journal of Management Information Systems* 38 (4): 1039-1066. doi:10.1080/07421222.2021.1990610.

Knuutila, A., L.M. Neudert și P.N. Howard. 2022. "Who is afraid of fake news? Modeling risk perceptions of misinformation in 142 countries." *Misinformation Review, Harvard Kennedy School.* https://misinforeview.hks.harvard.edu/article/who-is-afraid-of-fake-news-modeling-risk-perceptions-of-misinformation-in-142-countries/.

Lewandowsky, S., U.K.H. Ecker și J. Cook. 2017. "Beyond Misinformation: Understanding and Coping with the "Post-Truth" Era." *Journal of Applied Research in Memory and Cognition* 6 (4): 353-369. https://doi.org/10.1016/j.jarmac.2017.07.008.

Murphy, G., C. De Saint Laurent, M. Reynolds, O. Aftab, K. Hegarty, Y. Sun și C.M. Greene. 2023. "What do we study when we study misinformation? A scoping review of experimental research (2016-2022)." *Harvard Kennedy School Misinformation Review.* https://misinforeview.hks.harvard.edu/article/what-do-we-study-when-we-study-misinformation-a-scoping-review-of-experimental-research-2016-2022/.

Nikolov, D., D.F.M. Oliveira, A A. Flammini și F. Menczer. 2015. "Measuring online social bubbles." *PeerJ Computer Science.* https://doi.org/10.7717/peerj-cs.38.

Nisbet, E.C. și O. Kamenchuk. 2019. "The Psychology of State-Sponsored Disinformation Campaigns and Implications for Public Diplomacy." *The Hague Journal of Diplomacy* 14 (2): 65-82. https://doi.org/10.1163/1871191X-11411019.

O'Shaughnessy, N. 2020. „From disinformation to fake news: forwards into the past." În *The SAGE Handbook of Propaganda*, pp. 55-70. SAGE Publications Ltd. https://doi.org/10.4135/9781526477170.

Pariser, E. 2011. *The Filter Bubble: What the Internet Is Hiding from You.* https://dl.acm.org/doi/10.5555/2029079.

Ruiz, C. Diaz și T. Nilsson. 2023. "Disinformation and Echo Chambers: How Disinformation Circulates on Social Media Through Identity-Driven Controversies."" *Journal of Public Policy & Marketing* 42 (1): 18-35. https://doi.org/10.1177/074391562.

Sunstein, C.R. 1999. "The Law of Group Polarization." (John M. Olin Program in L. & Econ. Working Paper No. 91). https://dash.harvard.edu/bitstream/handle/1/13030952/The%20Law%20of%20Group%20Polarization.pdf.

Travierso, M. 2021. "Measuring magnetism: how social media creates echo chambers." *Nature Italy.* https://www.nature.com/articles/d43978-021-00019-4.

Vosoughi, S. și S. Arala. 2018. "The spread of true and false news online." *Science* 359 (6380): 1146-1151. https://doi.org/10.1126/science.aap9559.

Walter, S., M. Brüggemann și S. Engesser. 2018. "Echo Chambers of Denial: Explaining User Comments on Climate Change." *Environmental Communication* 12 (2): 204-217. https://doi.org/10.1080/17524032.2017.1394893.

Wollebæk, D., R. Karlsen, K. Steen-Johnsen și B. Enjolras. 2019. "Anger, Fear, and Echo Chambers: The Emotional Basis for Online Behavior." *Social Media + Society* 5 (2). https://doi.org/10.1177/2056305119829859.

Woolley, S.C. și P. Howard. 2016. "Automation, algorithms, and politics/ Political communication, computational propaganda, and autonomous agents – Introduction." *International Journal of Communication* (10). https://ijoc.org/index.php/ijoc/article/view/6298/1809.

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

Implicații ale terorismului jihadist în spațiul cibernetic

Implications of the jihadist terrorism in cyberspace

Drd. Bianca BRANDEA*
*Universitatea din București, Facultatea de Limbi și Literaturi Străine
Școala Doctorală „Limbi și identități culturale", România

Abstract

Atacul terorist din 11 septembrie 2001 a marcat schimbarea percepției Occidentului asupra Orientului Mijlociu și viceversa. Urmat de prezența militară a SUA în Orientul Mijlociu, acest eveniment a contribuit la dezvoltarea mijloacelor de acțiune teroristă din întreaga lume și la popularizarea jihadului. Atitudinea ostilă a Occidentului astfel succedată a întreținut starea de tensiune dintre cele două spații. De-a lungul timpului, grupărilor jihadiste și teroriste li s-au alăturat membri originari din Occident, care au fost convinși de importanța „misiunilor" pe care și le-au asumat ulterior. În prezenta lucrare, ne vom concentra asupra transpunerii și continuării ostilităților în spațiul geografic și cibernetic, ținând cont inclusiv de conflictul israeliano-palestinian actual.

The terrorist attack on the 11th of September, 2001, marked the change in the West's perception of the Middle East and vice versa. Followed by the US military presence in the Middle East, this event contributed to the development of the means of terrorist actions around the world and the popularization of jihad. The hostile attitude of the West thus succeeded in maintaining the state of tension between the two spaces. Over time, jihadist and terrorist groups have been joined by members originating from the West who were convinced by the importance of the "missions" they later undertook. In the present paper, we will focus on the transposition and continuation of hostilities in both geographic and cyber spaces, with reference even to the current Israeli-Palestinian conflict.

Cuvinte-cheie:
terorism; jihad; securitate; conflict; hacktivism; propagandă; apărare; terorism cibernetic.

Keywords:
terrorism; jihad; security; conflict; hacktivism; propaganda; defense; cyberterrorism.

Info articol
Primit: 12 februarie 2024; Evaluat: 28 februarie 2024; Acceptat: 13 martie 2024; Disponibil online: 5 aprilie 2024
Citare: Brandea, B. 2024. „Implicații ale terorismului jihadist în spațiul cibernetic".
Buletinul Universității Naționale de Apărare „Carol I", 13(1): 78-86. https://doi.org/10.53477/2065-8281-24-05

Începutul secolului XXI a adus schimbări majore în percepția Occidentului asupra Orientului Mijlociu, fapt ce a contribuit la delimitarea, respectiv segregarea celor două spații. Progresul tehnologic occidental perpetuu se desfășoară în același timp cu evoluția mentalităților și măsurilor orientale de ostilitate față de supremația Occidentului. În prezenta lucrare, vom analiza situații în care interferența celor două spații a fost necesară pentru îndeplinirea unor acțiuni ofensive și combative, de la mediul fizic până la mediul virtual.

Conflictele armate internaționale din ultimul deceniu – cu precădere cele desfășurate în Europa de Est și Orientul Mijlociu[1] – au consolidat rivalitatea dintre SUA și Rusia și au repornit negocierile pozițiilor aliaților fiecăreia. Conflictul Israelului împotriva Palestinei este cel mai important pe care îl vom avea în vedere în cele ce urmează, fapt pentru care vom observa câteva dintre cele mai importante implicații ale acestuia de-a lungul istoriei.

[1] Zona la care ne vom referi în prezenta lucrare este denumită de istorici drept Orientul Apropiat, fiind inclusă în aria amplă a Orientului Mijlociu.

Cu prilejul tensiunilor militare internaționale, în general, fenomenul radicalizării devine din ce în ce mai frecvent în rândul civililor interesați să susțină în mod activ cauza în care cred. Accesul neîngrădit la internet facilitează circulația materialelor menite să atragă noi adepți care fie împărtășesc deja convingerile promovate, fie devin interesați sau atrași de ele. În cazul radicalizării atacatorilor din spațiul cibernetic, propaganda la care sunt expuși are scopul de a forma „trupe" invizibile pentru a contribui la ostilitățile dintr-un „front", la rândul său, invizibil. Este de menționat faptul că astfel de „trupe" nu sunt create doar prin intermediul propagandei accesibile pe internet, ci includ membri care au concepții extremiste provenite din alte surse, în special de natură politică.

Mediul cibernetic este expus în mod constant amenințărilor atât psihologice, cât și cu repercusiuni în mediul fizic. Așadar, în contextul conflictelor armate actuale din proximitatea României, UE și NATO, gradul ridicat de alertă în spațiul cibernetic este necesar pentru a încerca preîntâmpinarea și contracararea amenințărilor, atacurilor de diverse tipuri, propagandei și dezinformării, ținând cont de faptul că astfel de evenimente au avut deja loc, sub pretextul contestării poziției României.

Jihad cibernetic sau terorism cibernetic?

Propaganda jihadistă răspândită în mediul online de către organizații teroriste precum Al-Qaida sau ISIS reprezintă un mod de intimidare a occidentalilor, dar și de recrutare a musulmanilor din ambele spații, respectiv încurajarea nonmusulmanilor de a se converti la islam pentru a se alătura jihadului. Este important de precizat faptul că, într-un asemenea context, islamul este folosit drept instrument de manipulare și radicalizare, încurajându-se valori care

nu se regăsesc în islamul autentic sau care chiar i se opun, promovându-se astfel o imagine incompletă și incorectă a religiei (Toma 2013, 72).

În cazul anumitor jihadiști, radicalizarea a însemnat adoptarea unui nou mod de viață, în care sunt urmărite scopuri precum înființarea unui nou califat, uciderea celor care nu urmează regulile și valorile pe care ei le consideră ca fiind ale islamului, distrugerea sau remodelarea Occidentului și în special a marilor puteri etc. (Leiken 2012, 142-144). Cu toate că grupările jihadiste sunt divizate în funcție de scopuri și ideologii, susținerea cauzei palestiniene reprezintă un ideal comun. De exemplu, abordarea online a grupării Al-Qaida nu este concentrată doar asupra ofensării Israelului, ci presupune și incriminarea statelor arabe care susțin perspectivele Occidentului în conflictul din Palestina. În plus, din analizele efectuate de Europol asupra propagandei online a grupării Al-Qaida în anul 2021, reieșea că aceasta susține că jihadul implică angajarea fiecărui musulman în susținerea cauzei palestiniene, încurajând, totodată, atacurile împotriva Israelului, „cruciaților" și țărilor arabe „zioniste" (Europol 2022, 39). Întreținând astfel de convingeri, informațiile publicate de ISIS sunt menite să convingă audiența că jihadiștii sunt, de fapt, musulmanii reali (Frampton, Fisher și Prucha 2017, 24).

În alt studiu, publicat de Europol, în anul 2017, jihadul cibernetic este descris drept „exploatarea globalizată a internetului de către Statul Islamic, care se identifică drept Califatul Cibernetic, prin intermediul discursului specific având scopul de a atrage hackeri din întreaga lume pentru a se implica în războiul din media împotriva «cruciaților» și a se alătura Califatului Cibernetic Unit" (Antinori 2017, 6).
Acestea sunt doar câteva dintre conceptele care stau la baza amenințărilor în plan real, însă în cele ce urmează, ne vom concentra asupra situației din „frontul" cibernetic și asupra motivațiilor comune, identificate în ambele planuri.

Este notabil faptul că jihadul și terorismul sunt două concepte distincte. Potrivit *Dicționarului de securitate internațională*, jihadul, deși tradus adesea ca „război sfânt", este descris ca punct central al islamului, semnificând luptă, strădanie sau efort. Jihadul poate avea caracter ofensiv cu scopul de răspândire a islamului, sau defensiv, în situațiile în care islamul este atacat (Robinson 2010, 119). În ceea ce privește terorismul, acestuia nu i s-a atribuit o definiție precisă, fiind descris ca un fenomen care „constă în utilizarea ilegală a forței de către actorii nonstatali cu scopul de a crea teroare în rândul populațiilor civile și de a forța guvernele la concesii politice. Folosirea violenței ilegale este ceea ce deosebește terorismul de activitatea politică normală, de violența legală/judiciară și de războiul convențional" (Robinson 2010, 227).

Cât despre diferențierea dintre jihad cibernetic și terorism cibernetic, este de precizat faptul că informațiile difuzate în numele unei organizații teroriste sau al unui jihadist care acționează singur se încadrează în jihadul cibernetic. În schimb, terorismul cibernetic are ca scop desfășurarea atacurilor cu scopul de a contribui la conflicte economice, politice și psihologice (Babanoury 2014), și, în sens strict, la folosirea spațiului cibernetic drept instrument pentru a vătăma fizic indivizi și obiecte (Torres 2016, 109).

Așadar, plasând cele două concepte în domeniul securității cibernetice, observăm că propaganda jihadistă utilizează pretextul religios pentru a atrage adepți, islamul fiind, de fapt, aparența acțiunilor politice intenționate, în timp ce terorismul reprezintă starea tensionată și atacurile motivate de pretexte similare.

Terorismul în pas cu progresul cibernetic

În studiul său asupra fenomenului radicalizării celei de-a doua generații de imigranți asiatici și africani în Europa, Robert S. Leiken menționează atracția tinerilor extremiști față de identitatea aleasă, în detrimentul celei moștenite. O astfel de identitate este conturată ca urmare a eșecului integrării atât în rândul nativilor europeni, cât și a neidentificării cu familia extinsă și comunitatea originară a părinților imigranți. În consecință, discursul justificativ, oferit de grupările teroriste, împreună cu sentimentul de apartenență la o comunitate unită reprezintă contextul ideal de canalizare a furiei simțite de-a lungul vieții (Leiken 2012, 410).

Diverși specialiști argumentează că terorismul, asociat extremismului islamist, nu este suficient de dezvoltat din punct de vedere tehnologic pentru a reprezenta o amenințare majoră. Hunker (2010) remarcă faptul că atacurile cibernetice perturbatoare, provocate de teroriști, sunt probabile și posibile, având mai degrabă rolul de a provoca enervarea maselor, cibernetica în sine nefiind o armă a terorii (Hunker 2010, 12). Torres (2016) susține că jihadiștii nu au pregătirea tehnică necesară unui război cibernetic, tendința acestora fiind mai degrabă către propagandă și *hacktivism* (Torres 2016, 108-9).

Interesul față de progresul tehnologic continuu și expunerea la rețelele de socializare, unde pot circula materiale propagandiste și știri de interes, alături de principiul expus de Leiken (2012), pot constitui un factor de risc la adresa securității generale și cibernetice, inclusiv a României. Potrivit Strategiei Naționale de Apărare a Țării pentru perioada 2020-2024, în rândul riscurilor enumerate se încadrează și „intensificarea propagandei islamist-jihadiste globale care alimentează riscurile radicalizării pe teritoriul național, inclusiv în rândul cetățenilor români, conferind perspective dificil de anticipat și contracarat" (Administrația Prezidențială, 27).

În general, atenția organizațiilor teroriste islamiste este îndreptată, cu precădere, spre statele care sprijină SUA în acțiunile desfășurate în Orientul Mijlociu. Din acest punct de vedere, România ar putea constitui o țintă „legitimă", fapt motivat și de implicarea permanentă a României în consiliile și comitetele internaționale de securitate (Andreescu și Radu 2015, 273). „Expusă indirect, prin asociere cu NATO, UE, SUA și statele europene implicate articulat în combaterea flagelului, țara noastră rămâne o țintă de oportunitate" (Administrația Prezidențială, 25).
România a fost deja ținta atacurilor de tip DDoS, revendicate de gruparea prorusă de hackeri Killnet și prilejuite de sprijinul militar și social, acordat Ucrainei, ca urmare

a războiului început de Rusia (Oancea 2022). Pentru asemenea atacuri efectuate de hacktiviști, sunt în continuare eligibile statele care susțin Ucraina, cel puțin până la finalul conflictului militar (SRI 2022).

Hackingul și *hacktivismul*: armele voluntarilor în timpul conflictelor armate

Între *hacktivism* și terorism cibernetic, există atât asemănări, cât, în special, deosebiri. *Hacktivismul* presupune un nivel scăzut de perturbare a funcționalității țintelor, obiectivele principale fiind umilirea acestora și câștigarea vizibilității. În ceea ce privește terorismul cibernetic, autorii urmăresc să rămână nedepistați, iar scopurile principale sunt de a submina securitatea instituțională și încrederea publică prin atacarea infrastructurilor critice și a serviciilor de urgență. Caracteristicile comune ale celor două concepte sunt răspândirea propagandei, intențiile de recrutare și strângerea de fonduri, respectiv instrumente și tehnici similare de atac. În cazurile în care *hacktiviștii* și teroriștii cibernetici au viziuni opuse, nu este exclus ca, între cele două tipuri de grupări, să existe atacuri cibernetice (Baldi, Gelbstein și Kurbalija 2003, 18-19).

Implicarea grupării Killnet în conflictul dintre Palestina și Israel nu reprezintă cu certitudine intenția de a susține Palestina sau gruparea Hamas, fiind mai degrabă o oportunitate de a lansa atacuri cibernetice împotriva Israelului. Acțiunile acesteia beneficiază de interesul altor grupări cu interese similare din lume, așa după cum reiese din cooperarea cu Anonymous Sudan în campania împotriva „regimului Israel" (Hollingworth 2023). Deși nu există dovezi concrete ale apartenenței membrilor grupărilor sus-numite la organizații teroriste sau jihadiste, putem identifica două elemente importante care fac parte din tiparul amenințărilor teroriste.

Primul element este redat de alegerea țintelor de nivel înalt. Comiterea cu succes a unor atacuri asupra unui guvern simbolizează interacțiunea dintre atacator și victimă. În acest mod, atacatorul are certitudinea transmiterii mesajelor ostile și a recunoașterii potențialului distructiv. Obținerea controlului asupra unui spațiu cibernetic guvernamental înseamnă, drept urmare, abilitatea de a deține controlul asupra securității întregului stat vizat.

Al doilea element este constituit din implicarea voluntară a străinilor în susținerea cauzelor și/sau realizarea atacurilor. Analog aderării nonarabilor și nonmusulmanilor la grupări jihadiste, observăm motivația grupărilor proruse și sudaneze de a contribui la vătămarea spațiului cibernetic guvernamental israelian.

Pe de altă parte, radicalizarea reprezintă un principiu cheie în comportamentul și mentalitatea jihadiștilor și teroriștilor. În ceea ce privește *hacktiviștii*, radicalizarea nu este neapărat un element definitoriu, ținând cont de faptul că majoritatea atacurilor importante sunt înfăptuite în perioade de tensiuni politice. În schimb, caracterul

extremist este mai degrabă comun atât *hacktiviștilor*, cât și jihadiștilor și hackerilor. În plus, imaginile civililor palestinieni răniți în timpul conflictului – în special ale copiilor – au contribuit, de-a lungul timpului, la creșterea numărului de jihadiști și la amplificarea dorinței acestora de a acționa împotriva Israelului, în mod special, dar și a statelor occidentale care îl susțin. În lucrarea *Ways of cyberterrorism* este menționat exemplul lui Nizar Trabelsi, un jihadist acuzat de amplasarea unei bombe într-o bază militară din Belgia, care a mărturisit că imaginile unei fete omorâte în Fâșia Gaza l-au încurajat să devină membru Al-Qaida în anul 2001 (Topor 2019, 87).

Pentru o mai bună claritate asupra tensiunilor internaționale actuale, este relevant să amintim câteva aspecte importante din istoria ultimelor decenii. În studiul său, publicat în anul 1990, privind tensiunile politice arabo-israeliene și Războiul Rece, Jerome Slater prezintă conflictul ca fiind prins în rivalitatea dintre SUA și Uniunea Sovietică, unde URSS și-ar fi urmat ideologia expansionistă asupra Orientului Mijlociu, eliminând influențele SUA și NATO din zonă și, în special, independența energetică a Occidentului, Japoniei și SUA (Slater 1990, 557-559). În plus, Slater amintește de susținerea activă, din partea URSS, pentru înființarea statului Israel, incluzând recunoașterea diplomatică declarată Israelului, în anul 1948, în cadrul Consiliului ONU; unii istorici motivează poziția URSS din respectiva perioadă prin intenția acesteia de a diminua influența britanică în Orientul Mijlociu (Slater 1990, 562).

La nivel formal, evoluția conflictului depinde în mare măsură de atitudinea „marilor puteri” și a „superputerii”, respectiv de definirea celei din urmă. Conform studiului Alexandrei Sarcinschi, statutul de „superputere” ar putea fi atribuit Statelor Unite ale Americii, însă în ultimele decenii, este luat în considerare declinul puterii SUA, urmat de posibila atribuire a acestui rang unui alt stat. Cât despre „marile puteri” actuale, recunoscute internațional ca având acest statut sunt SUA, Marea Britanie, China, Franța, Rusia, Japonia și Germania (Sarcinschi 2010, 20-21). În contextul în care Israelul joacă rolul principal în conflictul declanșat în anul 1948 și intensificat în 2023, sunt relevante teoriile conform cărora Israelul intenționează să devină o superputere în Orientul Mijlociu (Khashan 2020), la nivel mondial (Kor 2021), în domeniul tehnologiei (Forbes 2015), respectiv al inteligenței artificiale în domeniul războiului (Williams 2023).

Pe „frontul” cibernetic, se conturează astfel două aspecte definitorii pentru perspectivele extremiștilor, alăturați fiecăreia dintre părțile oponente: partea aliată Israelului urmărește obținerea supremației cibernetice și, în special, informaționale, în timp ce partea aliată Palestinei se opune acestor acte, acționând mai degrabă în replică la ofensivele continue ale Israelului. În general, atacurile cibernetice de natură teroristă sunt catalogate drept atacuri perturbatoare, comise de actori statali și nonstatali, iar războiul cibernetic este considerat o formă specială de atac perturbator. Într-un război cibernetic, este inclusă atacarea perturbatoare a spațiului unui stat de către alt stat, fapt ce se poate încadra în rândul acțiunilor de utilizare a forței (Hunker 2010, 2-4).

Într-un articol referitor la perspectiva cibernetică a conflictului din Fâșia Gaza, publicat de compania singaporeză Cyfirma, securitatea cibernetică este deosebit de importantă nu numai pentru statele implicate, dar și pentru aliații lor. Această concluzie se bazează, cu precădere, pe desfășurarea atacurilor cibernetice de către grupuri de *hacktiviști* și pe amenințările din partea altor tipuri de actori din diverse regiuni care au țintit site-uri guvernamentale, sectoarele educațional și media, panouri publicitare, centrale electrice, sisteme de alertă și chiar informații militare sensibile. De asemenea, articolul menționează posibilitatea Iranului și a aliaților săi de a conduce acțiuni „preventive" în viitorul apropiat, ca urmare a atacurilor Israelului împotriva Palestinei (Cyfirma 2023).

Într-un alt articol al Cyfirma privind atacurile hackerilor și *hacktiviștilor* în contexte conflictuale ale relațiilor internaționale, este recomandată intervenția diplomatică a guvernelor cu scopul de a diminua tensiunile geopolitice. Într-o astfel de abordare, este prevăzută prevenirea activităților *hacktiviste* prin eliminarea motivațiilor pe care se bazează (Cyfirma 2024).

Concluzii

Conflictele internaționale în care sunt implicate Occidentul și Orientul Mijlociu atrag inclusiv interesul civililor din ambele zone, care, în acest scop, își pot desfășura acțiunile ofensive în mediul cibernetic. Conflictul dintre Palestina și Israel constituie un prilej pentru intensificarea propagandei de factură jihadistă și teroristă, căreia i se alătură adepți atât din spațiul occidental, cât și oriental.

Argumentele folosite pentru a justifica ura și eventuala poziție ofensivă împotriva Occidentului sunt, în prezent, sporite, ca urmare a susținerii oferite de Occident Israelului, fapt ce poate implica creșterea numărului amenințărilor de natură teroristă în mediul cibernetic și în afara lui. Dezacordul față de pozițiile adoptate de guvernele occidentale este exprimat inclusiv în rândul anumitor civili originari din Occident, care, motivați de empatie și cu convingerea că pot contribui la schimbarea peisajului politic internațional, aderă la o formă interpretată a religiei care oferă aparența concordanței cu ideologiile după care aceștia se ghidează. Astfel, o parte importantă a amenințărilor din contextele conflictuale sunt concretizate prin exploatarea factorului psihologic atât al atacatorilor, care au ocazia de a-și satisface nevoia de validare, cât și al țintelor în rândul cărora este instalată starea de teroare.

România este o posibilă țintă, din cauza apartenenței la UE și în tratate, precum NATO, însă tocmai această apartenență este crucială pentru menținerea și sporirea nivelului de securitate, precum și a cooperării în vederea îndeplinirii acestor scopuri. În concluzie, complementar implicării militare și logistice în zonele de conflict, reziliența și dimensiunea defensivă a mediului cibernetic al României rămân extrem de importante, indiferent de evoluția evenimentelor.

Referințe

Administrația Prezidențială. 2020. „Strategia Națională de Apărare a Țării pentru perioada 2020-2024.” https://www.presidency.ro/files/userfiles/Documente/Strategia_Nationala_de_Aparare_a_Tarii_2020_2024.pdf.

Andreescu, Anghel și Nicolae Radu. 2015. *Jihadul islamic. De la „înfrângerea terorii” și „războiul sfânt” la „speranța libertății”.* București: Editura RAO.

Antinori, Arije. 2017. *The “Jihadi Wolf” threat the evolution of terror narratives between the (cyber-)social ecosystem and self-radicalization “ego-system”.* Haga: Europol Public Information.

Babanoury, Julien. 2014. ”Cyber Jihad: The Internet’s contribution to Jihad”. https://incyber.org/en/cyber-jihad-the-internets-contribution-to-jihad-par-julien-babanoury-ceis/.

Baldi, Stefano, Gelbstein, Eduardo și Kurbalija, Jovan. 2003. *Hacktivism, cyber-terrorism and cyberwar. The activities of the uncivil society in cyberspace.* Msida: DiploFoundation.

Cyfirma. 2023. ”Israel Gaza conflict: the cyber perspective”. https://www.cyfirma.com/outofband/israel-gaza-conflict-the-cyber-perspective/.

—. 2024. ”Caught in the Crossfire : How International Relationships Generate Cyber Threats”. https://www.cyfirma.com/outofband/caught-in-the-crossfire-how-international-relationships-generate-cyber-threats/.

Cyware. 2019. ”Flame 2.0 spyware found using strong encryption algorithm to avoid detection”. https://cyware.com/news/flame-20-spyware-found-using-strong-encryption-algorithm-to-avoid-detection-36939d76.

Europol. 2022. *Online Jihadist Propaganda 2021 in review.* Luxemburg: Publications Office of the European Union.

Forbes, Steve. 2015. ”How The Small State Of Israel Is Becoming A High-Tech Superpower”. https://www.forbes.com/sites/steveforbes/2015/07/22/how-the-small-state-of-israel-is-becoming-a-high-tech-superpower/.

Frampton, Martyn, Ali Fisher și Nico Prucha. 2017. *The New Netwar: Countering Extremism Online.* Londra: Policy Exchange.

Hollingworth, David. 2023. ”Killnet and Anonymous Sudan join forces to target Israel in widespread hacking campaign”. https://www.cyberdaily.au/security/9652-killnet-and-anonymous-sudan-join-forces-to-target-israel-in-widespread-hacking-campaign.

Hunker, Jeffrey. 2010. *Cyber war and cyber power: Issues for NATO doctrine.* Roma: NATO Defense College.

Khashan, Hilal. 2020. ”Israel Becomes the Middle East’s Superpower”. https://geopoliticalfutures.com/israel-becomes-the-middle-easts-superpower/.

Kor, Moira. 2021. ”I’m going to turn Israel into a world superpower”. https://www.jns.org/im-going-to-turn-israel-into-a-world-superpower/.

Leiken, Robert S. 2012. *Islamiștii europeni. Revolta tinerei generații.* Traducere de Sorin Șerb. București: Corint Books.

Oancea, Dorin. 2022. „Grupul de hackeri pro-rus Killnet a revendicat atacul cibernetic ce a afectat mai multe site-uri ale instituţiilor din România". https://www.mediafax.ro/externe/grupul-de-hackeri-pro-rus-killnet-a-revendicat-atacul-cibernetic-ce-a-afectat-mai-multe-site-uri-ale-institutiilor-din-romania-20782645.

Robinson, Paul. 2010. *Dicționar de securitate internațională.* Traducere de Monica Neamț. Cluj-Napoca: CA Publishing.

Sarcinschi, Alexandra. 2010. *Rolul actorilor statali în configurarea mediului internațional de securitate.* București: Editura Universității Naționale de Apărare „Carol I".

Slater, Jerome. 1990. "The Superpowers and an Arab-Israeli Political Settlement: The Cold War Years." *Political Science Quarterly* 105 (4): pp. 557-577.

SRI. 2022. "Buletin Cyberint." II Semester. https://sri.ro/assets/files/publicatii/buletin-cyber-sem-2-2022-RO.pdf.

Toma, Gabriel. 2013. *Terorismul internațional. Reacții ale actorilor regionali și globali.* Iași: Institutul European.

Topor, Sorin. 2019. "Ways of cyberterrorism." *Bulletin of "Carol" National Defence University* 8 (3): 82-90.

Torres, Manuel. 2016. *The limits of cyberterrorism*. Editor H. Giusto. *Daesh and the terrorist threat: from the Middle East to Europe* (Foundation for European Progressive Studies -Fondazione Italianieuropei) 108-114.

Williams, Dan. 2023. "Israel aims to be «AI superpower», advance autonomous warfare". https://www.reuters.com/world/middle-east/israel-aims-be-ai-superpower-advance-autonomous-warfare-2023-05-22/.

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

Strategii narative în acțiune – text, formă și context

Narrative strategies in action – text, form, and context

Căpitan drd. Anca CIORNEI*
*Universitatea Națională de Apărare „Carol I", București, România

Abstract

Schimbările majore din mediul global de securitate, care au avut loc la sfârșitul mileniului trecut, continuă să marcheze profund inclusiv primul sfert al secolului al XXI-lea, caracterizat prin modificări substanțiale ale instrumentelor clasice utilizate în desfășurarea unui conflict. De asemenea, transformarea mediului informațional a condus la apariția, la dezvoltarea, la adaptarea și la contextualizarea utilizării narațiunilor strategice, cu scopul de a influența percepțiile oamenilor asupra acțiunilor puterilor statale și de a produce efecte, în sensul dorit de către acestea. Scopul prezentului articol este de a supune atenției narațiunile strategice, ca parte a confruntărilor hibride contemporane, urmărind a aduce o mai bună înțelegere a acestui subiect, cu observarea modului în care acestea sunt folosite și cu ce efecte, în funcție de forma sub care apar. Mai mult, lucrarea propune o delimitare conceptuală multinivel, abordând narațiunile strategice din perspectiva textului, contextului și formei, așa cum sunt evidențiate în cele mai recente lucrări din domeniul de specialitate. Totodată, vom supune atenției și folosirea lor în context aliat, cu referire la documentele de lucru pe care NATO le utilizează în comunicarea strategică, cu scopul de a influența grupurile țintă și audiențele atât interne, cât și externe.

The major changes in the global security environment that took place at the end of the last millennium continue to deeply mark the first quarter of the 21st century, characterized by substantial changes in the classical instruments used in conducting a conflict. Also, the transformation of the informational environment has led to the emergence, development, adaptation, and contextualization of the use of strategic narratives with the aim of influencing people's perceptions of the actions of power states and producing effects in the sense desired by them. The purpose of this article is to subject strategic narratives to attention, as part of contemporary hybrid confrontations, aiming to bring a better understanding of this subject, observing how they are used and with what effects, depending on the form in which they appear. Moreover, the article proposes a multilevel conceptual delimitation, approaching strategic narratives from the perspectives of text, context, and form, as highlighted in the most recent research in the specialized field. We will also consider their use in an allied context, with reference to working documents that NATO uses in strategic communication to influence target groups and audiences, both internal and external.

Cuvinte-cheie:
strategii narative; comunicare strategică; război cognitiv.

Keywords:
narrative strategies; strategic communication; cognitive warfare.

Info articol
Primit: 30 ianuarie 2024; Evaluat: 21 februarie 2024; Acceptat: 15 martie 2024; Disponibil online: 5 aprilie 2024
Citare: Ciornei, A. 2024. „Strategii narative în acțiune – text, formă și context". *Buletinul Universității Naționale de Apărare „Carol I"*, 13(1): 87-99. https://doi.org/10.53477/2065-8281-24-06

Începutul celui de-al XXI-lea secol a adus în lumina reflectoarelor schimbări puţin aşteptate, cu efecte diverse, începând de la nivel individual şi continuând până la nivel societal, în care sunt implicate atât marile puteri statale, cât şi numeroase organizaţii, având interese în direcţii precum industria, economia ori alte domenii importante, cu impact asupra populaţiei. Mai mult, dacă în perioada Războiului Rece puteam vorbi despre o anumită simetrie în relaţiile dintre cele două mari blocuri politico-militare, URSS şi SUA, în prezent asistăm la emergenţa unor forme multiple de asimetrie în conflictele contemporane, ca rezultat al diferenţierii dintre războiul convenţional şi noile tipuri de conflicte.

Se poate spune că prezentul este caracterizat de riscuri, oportunităţi, incertitudini şi ameninţări, iar toate aceste elemente pot căpăta diverse forme, în funcţie de modificările rapide din plan social, ştiinţific, tehnologic, geopolitic sau chiar climatic, într-o perioadă în care globalizarea produce efecte continue care se propagă în direcţii neaşteptate.

Dacă în trecut puteam încadra o acţiune militară ca fiind una terestră, aeriană sau maritimă, spaţială ori cyber, fiecare reprezentând înglobarea celor cinci spaţii, în ultima perioadă se poate vorbi despre o dimensiune cognitivă a războiului, prin intermediul căreia percepţiile oamenilor pot fi influenţate, folosind diverse metode şi mijloace de manipulare, cu scopul de a obţine rezultatele dorite, spre exemplu schimbarea viziunii asupra anumitor valori.

Totodată, pe fondul unui interes ridicat asupra cercetării noilor tipuri de conflict, într-un raport, publicat pe site-ul Comandamentului Aliat pentru Transformare (ACT) al NATO, războiul cognitiv este definit ca fiind *„totalitatea activităților desfășurate în strânsă legătură cu alte instrumente de putere, cu scopul de a afecta atitudinile și comportamentele prin influențarea, protejarea și/sau perturbarea cunoștințelor individuale și de grup pentru a obține un avantaj”* (NATO-ACT 2023).

În aceeași direcție, într-un raport, publicat pe platforma *Innovation Hub*, Bernand Claverie şi François du Cluzel au înaintat următoarea idee: *„Războiul cognitiv este cu noi. Principala provocare este dată de faptul că este invizibil; tot ce se vede este impactul lui, însă până atunci (...) de multe ori este prea târziu”* (Claverie și Du Cluzel 2022). Cu alte cuvinte, în conflictele în care bătăliile se duc în mințile oamenilor, efectele acțiunilor actorilor sunt vizibile imediat ce intențiile și-au atins deja scopul.

O abordare care vine în completarea celor de mai sus îi aparține actualului președinte al Academiei Române, Ioan Aurel Pop, care, încă din 2017, afirma că *„informaţia şi comunicarea au o importanţă enormă pentru cercetarea istorică. Se spunea, până nu demult, că cine stăpâneşte informaţia stăpâneşte lumea. Astăzi, se mai adaugă ceva – cine stăpâneşte comunicarea poate stăpâni lumea sau poate stăpâni comunităţi tot mai largi. O mare parte dintre deformările care activează în lumea de astăzi au avut bazele teoretice în istorie. Pentru a putea compara şi pentru a răspunde acestor provocări, este nevoie să ne cultivăm cel mai performant computer, creierul uman*” (Pop 2017).

Dacă este să dezbatem pe marginea acestei noi dimensiuni, cea informațională, în care ponderea în foarte mare măsură este deținută de latura cognitivă, atunci este imperios să supunem atenției și instrumentele folosite în acest scop, pentru a putea duce războiul pe un asemenea teritoriu. Fără îndoială, *narațiunile strategice* dețin un rol decisiv în generarea și coordonarea unor astfel de confruntări hibride.

Din perspectivă metodologică, pentru atingerea obiectivelor pe care ni le propunem în acest articol, vom aborda analiza documentelor și a lucrărilor de specialitate încercând să aprofundăm conceptul de narațiuni strategice și cel al strategiilor narative, precum și efectele pe care acestea le au asupra audiențelor vizate în momentul în care sunt puse în aplicare.

În ceea ce privește structura articolului, acesta cuprinde abordările teoretice ale narațiunilor strategice, dezvoltă strategiile narative prin prisma formei, structurii și nivelurilor de acțiune și, totodată, prezintă utilizarea lor în context aliat. Toate aceste elemente urmăresc să evidențieze importanța narațiunilor strategice și a strategiilor narative într-o perioadă caracterizată de schimbări majore în actualul mediu de securitate.

Totodată, prin abordarea acestor concepte, lucrarea contribuie la o mai bună înțelegere a dimensiunii cognitive a conflictelor actuale și identifică elemente care pot fi regăsite în actul dezinformării și manipulării audiențelor, aspecte din ce în ce mai prezente în confruntările hibride.

Narațiunile strategice – abordări teoretice

Termenul de *narațiune*, la modul general, pornește de la neologismul din limba franceză – *narration*, provenit din limba latină – *narration,* cu sensul de *povestire*. Acest termen este, de fapt, modul de expunere prin care se relatează fapte și întâmplări, într-o succesiune temporală. Mai mult, este parte a unui discurs și presupune existența următoarelor elemente: narator, acțiune și personaje, cu accent pe succesiunea și dinamismul întâmplărilor. Cu alte cuvinte, așa după cum afirmau Miskimmon, O'Loughlin și Roselle în anul 2014, *„narativele sunt formate și proiectate într-un mediu de comunicare*" (Miskimmon, O'loughlin și Roselle 2014b, 89).

Ținând cont de faptul că orice narațiune urmează o linie gramaticală, atunci trebuie să aducem în discuție și termenul de *naratologie*, propus, în anul 1969, de către teoreticianul francez Tzvetan Todorov, care vorbește în lucrările sale despre *naratologia tematică*, în care se dezbat conținuturile narative și povestirile redate de către personaj sau narator, și cea *formală,* în care se analizează modul de reprezentare narativă a discursului, relația dintre narator și personaje, precum și poziționarea lor față de actul narativ (Todorov 1971, 125-151). Tot el a stabilit, în lucrarea *Categoriile narațiunii literare* și cele două componente ale narațiunii, privită ca poveste – logica acțiunilor și raporturile dintre personaje (Todorov 1966, 125-151). Din perspectiva

lui, narrarea este încredințată direct personajelor sau naratorului, ambele fiind greu de identificat în stare pură. O astfel de abordare vine în sprijinul celor care vor să decodifice povestirile și care analizează modul în care mesajele sunt prezentate de către cei implicați în narare, folosind actul narativ pentru a nuanța sau a direcționa mesajul în sensul dorit.

În aceeași linie, în lucrarea sa, din 1999, intitulată *Semiotică, societate, cultură*, Daniela Rovența-Frumușani vorbește despre crearea de narațiuni și structuri narative ca fiind *„strategia care ne permite să facem lumea inteligibilă, fiind un model esențial de organizare a datelor*" (Rovența-Frumușani 1999, 105). Cu alte cuvinte, prin crearea unor narative logice și bine structurate, se pot obține efecte care pot conduce către descifrarea intențiilor inițiale și interpretarea lor, până la înțelegerea sensului informațiilor transmise. Mai mult, ea face o trecere în revistă și analizează structurile narative, plecând de la lucrarea lui Aristotel, intitulată *Poetica,* în care se vorbește despre personaje și acțiuni, urmărind modelul lui Propp, în care acțiunile narative devin fundamentale, făcându-se referire la introducere, realizare și concluzie. O astfel de abordare este utilă în a conștientiza că narațiunile sunt create în mod conștient, aplicate cu un anume scop și adaptate contextului, astfel încât rezultatele obținute să poată fi interpretate cât mai clar.

Abordate cronologic, numeroși cercetători, teoreticieni și experți în domeniul comunicării au studiat narațiunile utilizate de către marii actori în plan social pentru a putea identifica rolul acestora, formele pe care le pot căpăta și efectele pe care le au în momentul în care sunt folosite. Spre exemplu, Oliver Schmitt a evidențiat cum sunt percepute strategiile narative, utilizate în discursurile politice, și care este legătura dintre ele și oamenii politici, ținând cont și de tipologia miturilor politice (Schmitt 2018, 487-511). În acest sens, el a evidențiat cât de important este ca, în discursurile lor, intelectualii să își adapteze mesajele astfel încât ele să fie pe înțelesul publicului.

Narațiunile strategice, pe de altă parte, fac trimitere către conceptul de putere, către balanța de putere dintre state, către relațiile internaționale și studiile de securitate, așa după cum reiese și din una dintre lucrările lui Barry Buzan, care induce și idea conform căreia discursurile politice trebuie adaptate și explicate, în vederea, realizării securității, prin introducerea termenului de *securitizare* (Buzan 2008). Prin strategiile narative, statele reușesc să se poziționeze unele față de altele, ori chiar față de anumite valori care sunt sau nu împărtășite de către masele de indivizi.

Fără îndoială, nu am putea să aducem în discuție termenul de strategie, pus în context militar, diplomatic sau geopolitic, fără să facem trimitere la *Arta Războiului* a lui Sun Tzu, care reliefează importanța planificării și adaptabilității, precum și înțelegerea profundă a mediului în care sunt purtate acțiunile militare, în vederea obținerii victoriei și avantajului în luptă nu doar prin forță, ci, mai ales, prin inteligență, prin înțelegerea caracteristicilor adversarilor și prin anticiparea mișcărilor acestora (Tzu 1994).

În egală măsură, McCarty prezintă strategiile într-o manieră mai complexă, încadrându-le în cinci categorii distincte (McCarthy 2000, 31-42):

- *Strategia ca plan* presupune o prestabilire a unei acțiuni, trasând linii directoare spre a ajunge la obiectivele propuse, premergătoare situației, cu implicații amplificate în cunoștință de cauză și cu scop bine definit;
- *Strategia ca tactică* este aplicată, în principal, pentru a contracara intențiile adversarilor;
- *Strategia ca model* încearcă să stabilească un model de comportament, deoarece strategia rezultă din acțiunile pe care oamenii le întreprind;
- *Strategia ca poziție* identifică locul actorului în plan atât intern, cât și extern, devenind o forță de mediere;
- *Strategia ca perspectivă* reprezintă o modalitate proprie de percepere a mediului extern.

Privite din cele cinci unghiuri, se poate trage concluzia că strategiile sunt esențiale atunci când obiectivele urmează a fi proiectate, iar narațiunile utilizate, având în spatele lor o strategie foarte bine definită, sunt instrumente definitorii în preluarea avantajului strategic, pe timpul oricărui tip de conflict.

Revenind la sintagma de *narațiuni strategice,* aceasta este din ce în ce mai folosită în confruntările contemporane. Încercând să corelăm această sintagmă cu clasificarea strategiilor, prezentată anterior, se poate trage concluzia că narațiunile de tip strategic includ un anumit plan atunci când sunt concepute, au obiective clar definite în vederea aplicării lor eficiente, urmăresc un model, în funcție de feedbackurile rezultate în urma utilizării lor, sunt formulate în funcție de grupurile țintă pe care le vizează și anticipează reacțiile celor implicați.

Potrivit lui O'Loughlin, narațiunile sunt create și proiectate în mediul internațional, urmărind trei idei esențiale (Miskimmon, O'loughlin și Roselle 2014b):

- apar în interacțiunile interumane, definesc lumea și afectează comportamentele umane;
- au ca element central actorii politici care folosesc narațiunile în mod strategic;
- mediul de comunicare afectează în mod fundamental maniera în care narațiunile sunt comunicate și influențează publicul vizat.

Conform aceluiași autor, strategiile narative sunt din ce în ce mai folosite în domenii precum științele politice sau relațiile internaționale, iar ele reprezintă un instrument util și eficient pentru obținerea rezultatelor dorite de către stat și conducătorii acestuia, în scopul influențării comportamentelor și atitudinilor indivizilor sau ale întregilor mase de cetățeni.

Sintetizând, putem spune că *„o narațiune devine strategică atunci când prescrie un tip de ordine care servește unor interese particulare. Trebuie spus că orice narațiune strategică este formată din două ingrediente majore: putere și comunicare. Joncțiunea*

dintre cele două construiește adevăruri, adică impune evenimentelor interne și internaționale sensurile dorite de establishment, ceea ce, înseamnă că narațiunile strategice generează percepții, emoții, conduite, adică realitate socială (Dumitrescu 2020, 27). Cu alte cuvinte, dacă aducem în discuție faptul că, prin aplicarea narațiunilor strategice, se urmărește poziționarea publicului față de o anume realitate pe care o prezentăm, ne putem referi, de asemenea, și la propagandă sau persuasiune asupra publicului țintă, un proces de comunicare în care *„actorii cu cele mai bune argumente sunt învingători, pentru că ei sunt cei ce reușesc să convingă"* (Popescu 2022, 122).

Narațiunea strategică poate fi privită ca o povestire, formulată și transmisă în mod intenționat, cu apel la valorile durabile, împărtășite de membrii unei organizații, la originile acestora ca și colectiv, precum și ceea la ce doresc să realizeze în viitor și, foarte important, care sunt pașii ce trebuie parcurși astfel încât intențiile să devină fapte și certitudini.

Diacronic, narațiunile strategice au apărut și sunt din ce în ce mai utilizate, ca urmare a evoluției mediului informațional și ca nevoie de adaptare la schimbările apărute în actualul context internațional. Ele pot fi privite ca instrumente întrebuințate în lupta care se duce cu mințile oamenilor, cu încercarea de a influența și de a obține rezultate în direcțiile dorite. Schimbarea comportamentelor maselor, în funcție de propriile interese, și influențarea lor, în sensul respectării anumitor valori, sunt doar câteva dintre obiectivele care se au în vedere atunci când se apelează la strategiile narative. Cu cât aceste narațiuni sunt mai bine structurate și încadrate în anumite tipare, cu atât ele pot crea efecte care pot conduce la înclinarea balanței către o anumită latură a confruntării hibride ce are loc în perioada actuală.

Prin urmare, conceptul de *narațiuni strategice* se va diferenția de conceptul de *strategii narative,* întrucât primul face referire la actul de comunicare și la elementele implicate în tot acest proces, în timp ce al doilea urmărește comportamentul comunicativ, tehnicile folosite de către cei ce inițiază procesul, având ca scop îndeplinirea unor obiective, anterior stabilite.

Narațiuni strategice – formă, structură și niveluri de acțiune

Deși nu se poate discuta încă despre o delimitare clară a lor sau despre o structură standard, care poate fi urmărită în cuprinsul lor, narațiunile strategice au trezit interesul mai multor teoreticieni și cercetători, care au încercat să identifice structura, forma și elementele cheie ce pot fi regăsite atunci când se utilizează astfel de construcții narative.

Miskimmon, O'Loughlin și Roselle, plecând de la constatarea că *„narațiunile strategice sunt instrumente prin intermediul cărora actorii politici încearcă să construiască o interpretare comună a trecutului, prezentului și viitorului politicii*

mondiale, cu intenția de a influența comportamentul actorilor interni și internaționali" (Miskimmon, O'loughlin și Roselle 2014b, 445), au identificat un set de caracteristici ale acestor narațiuni de tip strategic, prezentând o nouă manieră de abordare a lor care cuprinde *cinci componente* cheie (Miskimmon, O'Loughlin și Roselle 2017):

a) sunt orientate spre viitor. Deși o narațiune strategică se poate se referi la trecut și/sau prezent, aplicativitatea sa este conectată la conturarea politicii în viitor;

b) sunt strâns corelate cu identitatea. Articulează o poziție distinctă (națională/regională) pe o problemă specifică, pe un domeniu de politică sau, în general, cu privire la locul statului în politica mondială sau în sistemul internațional;

c) conținutul nu este unul fix, ci este un produs social dinamic și mereu negociat, bazat pe interacțiunile statelor atât cu societățile lor, cât și cu alți actori externi, relevanți în sfera de influență;

d) pot deriva din experiențele din istorie, făcând apel la acțiuni precedente, la experiențe anterioare și la reputația istorică, dobândită de-a lungul timpului;

e) audiența lor este atât internă, cât și externă. Pot fi utilizate pentru fidelizarea publicului intern, pe de o parte, iar pe de altă parte, pentru folosirea acestuia în delimitarea și comunicarea percepției colective în sfera internațională.

Analizând toate aceste elemente, se poate ajunge la concluzia că narativele strategice nu au un anumit tipar, ci pot suferi modificări, în funcție de intențiile inițiale, de valorile împărtășite de către cei care emit astfel de narațiuni, de valorile pe care le respectă audiența și de paternul publicului vizat, fie el intern sau extern.

Într-o altă analiză a acelorași autori, se prezintă narațiunile strategice în trei pași, urmărindu-se formarea, proiecția și recepționarea lor (Miskimmon, O'Loughlin și Roselle 2018). Sunt construite, de cele mai multe ori, de către partidele de guvernare și de ministerul de externe, ulterior sunt făcute publice prin intermediul discursurilor liderilor politici, ca într-un final, să fie recepționate de audiența vizată. În tot acest circuit, cei care formulează narațiunile răspund la interpretările audienței, precum și la comportamentul acestora față de mesajele care le sunt transmise și ajustează conținutul pentru a obține efectele maxime dorite, asigurându-se că narațiunile nu sunt doar inteligibile, ci și convingătoare. Toate aceste demersuri sunt făcute conștient în vederea contracarării noilor tipuri de riscuri și amenințări hibride care apar la adresa securității, pe de o parte, iar pe de altă parte, pentru urmărirea și promovarea propriilor scopuri legate de balanța de putere, de sfere de influență, de dezinformare ori de slăbirea coeziunii la nivel societal.

Ținând cont de aspectele enumerate anterior, nu putem continua analizarea narativelor sau a povestirilor fără a adera și la ideea Hannei Merejota, conform căreia povestirea este aspectul narațiunii care ne modelează înțelegerea cognitivă a lumii, orientările noastre afective și simțurile (Meretoja 2018). Așadar, de aici putem să extragem ideea că narațiunile sunt utilizate luând în considerare nu numai partea rațională a publicului țintă, ci și emoțiile acestuia, și elementele care pot fi modelate, făcându-se apel la latura afectivă și la cea senzorială, aspecte cu o complexitate de decodificare și interpretare mult mai mare și de mai lungă durată. Prin urmare,

folosirea narațiunilor și obținerea efectelor pot suferi modificări, în funcție de reacțiile provocate, ceea ce presupune o adaptare continuă a mesajelor transmise.

De asemenea, când aducem în discuție *forma* lor, narațiunile pot fi transmise pe diverse canale sau pot fi regăsite sub diverse forme. În acest sens, se pot distinge narațiuni sub forma textelor, narațiuni sonore, imagistice (foto, hărți), multimedia, iar acestea pot fi distribuite fie prin intermediul mass-mediei tradiționale, fie cu ajutorul social media, din ce în ce mai prezentă în viața fiecărui individ, având ca scop câștigarea minților oamenilor și percepțiilor acestora față de intențiile actorilor politici (Bjola, Cassidy și Manor 2019, 83-101).

Toate acestea pot fi diseminate pentru a fi activate pe trei *niveluri de acțiune* în care narațiunile pot fi încadrate: internațional, național și la nivel de problemă. La nivel internațional, narațiunile sunt folosite pentru a descrie cum este lumea structurată, care sunt interesele internaționale și, de ce nu, care este ordinea mondială. În plan național, acestea evidențiază statutul actorului statal, care sunt obiectivele și valorile lui și cum urmărește să fie perceput de către alți jucători statali. La nivel de problemă, narațiunile creează cadrul utilizării anumitor politici guvernamentale și, totodată, explică de ce anumite politici sunt necesare și cum vor fi ele implementate eficient. Cele trei niveluri sunt, de cele mai multe ori, interdependente. Ele interferează astfel încât scopul inițial stabilit să fie atins în marja de timp estimată (Miskimmon, O'Loughlin și Roselle 2014a, 70-84).

În plus față de toate aspectele evidențiate anterior, trebuie enunțat și faptul că narațiunile strategice sunt folosite în contextul actual nu numai pentru a ne poziționa față de anumite aspecte și valori, ci și pentru a atrage un capital de imagine și simpatie din partea audienței pe care o educăm prin intermediul fiecărui act narativ pe care îl cultivăm conștient (Saliu 2023, 209-224). Tocmai de accea RL Boyd a supus atenției, într-una dintre lucrările sale, și conceptul de *arc narativ*. În viziunea lui, există asemănări și deosebiri între structurile narative, în funcție de procedeele de construcție ale acestora, de variabilele implicate și de fazele prin care trec până la momentul în care ajung să afecteze comportamentele umane vizate (Boyd, Blackburn și Pennebaker 2020).

Strategiile narative utilizate în context aliat

Încercând să identifice *contextul* în care a apărut nevoia de analiză a narațiunilor strategice, Oliver Schmitt consideră că aceasta are la bază interesul de a examina importanța persuasiunii în conflictele contemporane, modul în care campaniile militare actuale sunt prezentate publicului internațional sau național și modul în care o comunitate politică dezbate problemele strategice. Așadar, acest interes apare ca urmare a nevoii de aliniere la noile metode de acțiune utilizate în gestionarea conflictelor, astfel încât toți cei implicați să acționeze, pe cât posibil, în cunoștință de cauză în vederea obținerii rezultatelor estimate în planificarea inițială (Schmitt 2018, 487-511).

Pentru a fi înțeles pe deplin și pentru a identifica factorii implicați și acțiunile acestora, orice conflict trebuie analizat din perspective politice, diplomatice, relații internaționale, economice sau militare. Urmărind oricare dintre aceste ramuri, putem observa cum fiecare dintre actorii implicați utilizează în confruntare o serie de narațiuni strategice pentru a se poziționa în funcție de obiectivele avute și pentru a crea situații de avantaj strategic în confruntările hibride, în urma influențării societății în direcțiile vizate.

În ultimele trei decenii, NATO a fost implicată în diverse operații și misiuni, iar pentru aceasta, a trebuit să comunice mereu de ce și cum face acest lucru, în primul rând, pentru a-și atinge obiectivele strategice propuse, dar și pentru a contrabalansa narațiunile adversarilor (Nissen 2014). Pentru aceasta, Alianța a trebuit să își ajusteze continuu propriile strategii narative atât pentru a crea o înțelegere comună a aliaților asupra acțiunilor ei, cât și pentru a-și susține legitimitatea și caracterul defensiv în fața contestatarilor, în același timp încercând să elimine teama de a-și comunica aceste acțiuni și de a se axa, mai degrabă, pe ceea ce comunică acțiunile în sine (Mullen 2009).

Spre exemplu, pentru a crește încrederea publicului tânăr în capacitatea structurilor Alianței, de a proteja populația și teritoriul aliat, precum și pentru a explica implicarea în exerciții multinaționale sau în misiuni internaționale, în anul 2017, NATO a demarat, a susținut și a dezvoltat una dintre cele mai mari campanii de comunicare strategică, intitulată #WeAreNATO, prin intermediul căreia a facilitat accesul tinerilor la informații despre NATO prin diverse manifestări. Pentru aceasta, narațiunile strategice utilizate au căpătat diverse forme (imagini, texte, video) și au fost folosite în mai multe contexte și pe mai multe canale (conferințe de presă, evenimente publice, interviuri) de către lideri ai NATO, care au explicat misiunea principală a Alianței (NATO-ACT 2017).

Mai mult, prin intermediul Conceptului Strategic, apărut, în anul 2022, la Madrid, Alianța își propune să facă publice interesele comune ale ei, reiterând, o dată în plus, caracterul defensiv și intențiile ferme de descurajare a escaladării oricărui tip de conflict. În cuprinsul documentului, apar, sub formă de text, narativele urmărite de NATO și responsabilitățile pe care le atribuie statelor aliate (NATO 2022). Punerea în aplicare a acestui document, la fel ca toate acțiunile din ultima perioadă, desfășurate de către aliați, face apel și la comunicarea strategică, folosită în vederea atingerii obiectivelor comune propuse, ținând cont de concepte care se referă la diplomația publică, afaceri publice sau afaceri publice militare (Johnsson 2011).

Analizând toate aceste aspecte, putem trage concluzia că, prin intermediul narațiunilor de tip strategic, NATO nu doar comunică sau informează, ci și urmărește să educe audiența, cu scopul de a produce emoții care se pot transpune în susținere din partea maselor și în împărtășirea valorilor comune.
Ca termen, la nivelul NATO, narațiunea a fost reglementată printr-un document în 2014. Acesta supunea atenției termenul de narațiune și modul de dezvoltare

a acesteia, pas cu pas, cu scopul de a fi folosită ca instrument, în contextul unei viitoare strategii informaționale militare. În cuprinsul lui, apărea, pentru prima dată, conceptul de *arc narativ*, în care traiectoria arcului (acțiune-efect) este constituită din participanți sau actori care întreprind acțiuni care pot căpăta forme, precum produse text, video, audio, discursuri, toate acestea conducând către rezultatele favorabile urmărite sau către inițierea unei anumite dorințe. Când o narațiune ajunge la final, provocând satisfacție sau nemulțumire, atunci ea este considerată rezolvată. De asemenea, în același document, se supune atenției și sintagma de peisaj narativ care cuprinde mai multe variabile (mituri, povestiri, istorii, povești religioase sau de ficțiune) ce interacționează, fiind parte integrată a mediului informațional, care conduc către crearea contextului favorabil transmiterii construcțiilor narative de tip strategic (MNIOE 2014).
Dacă luăm în considerare utilizarea narațiunilor în mediul informațional, trebuie să ținem cont de faptul că acestea pot fi folosite pentru propagandă, în toate formele ei, în scopul influențării opiniilor, emoțiilor, atitudinilor și comportamentelor indivizilor (Reddi, Kuo și Kreiss 2023, 2201-2218). Cu alte cuvinte, informarea intenționată, cu scopul de a obține efecte, utilizează mai multe canale de propagare a informațiilor, pentru a influența, uneori negativ, percepțiile indivizilor și pentru a afecta credibilitatea.

În prezent, informația este un instrument cheie în relațiile dintre state. Atunci când sunt folosite ca armă în războiul informațional, narațiunile strategice se bazează pe amestecul dintre adevăr și fals și pe prezentarea eronată a faptelor, pentru a induce publicului interpretări distorsionate și părtinitoare, aceste reacții fiind efecte ale propagandei, influențării și dezinformării (Barclay 2018).

În NATO Strategic Communication Handbook sunt prezentate strategiile narative și modul în care acestea trebuie abordate pentru o mai bună înțelegere a mediului informațional. Conform acestui document, narațiunile reprezintă comunicarea coerentă a diverșilor actori implicați în operații, cu scopul de a genera percepții cu privire la anumite valori comune. Pentru ca acest lucru să aibă loc, strategiile narative, temele, mesajele folosite în discurs, precum și utilizarea vulnerabilităților anumitor segmente de audiență reprezintă doar câteva dintre elementele definitorii ale acestui proces. Identificarea poveștilor în diferite narațiuni permite o înțelegere cuprinzătoare a peisajului narativ și a mediului informațional, tocmai de aceea în tot acest demers sunt implicate și alte domenii, precum operațiile informaționale (InfoOps), relațiile publice militare, operațiile psihologice (PSYOPS), cooperarea civil-militară (CIMIC), modulul de informații (J2), consilierea politică (POLAD) și culturală (CULAD). Aceste domenii pot sprijini demersul de comunicare și de înțelegere și pot contribui la atingerea unui rezultat integrat. Acest aspect se poate realiza prin intermediul unei comunicări strategice organizaționale foarte bine sincronizate, care ține cont de aspectele specifice fiecărui domeniu anterior amintit (NATO 2017).
Potrivit NATO, comunicarea strategică reprezintă utilizarea coordonată și adecvată a activităților de comunicare și a capabilităților, în sprijinul politicilor, operațiilor și activităților Alianței, cu scopul de a promova obiectivele NATO (NATO, fără an).

În contextul comunicării strategice, narațiunile strategice fac parte din războiul informațional pentru a provoca tulburări informaționale pe frontul intern al adversarului. Când acest lucru are loc, ele pot crea realități alternative despre fapte și evenimente, sau chiar pot modifica percepția colectivă, în sensul schimbării sprijinului pentru conducere. Ca rezultat, narațiunile strategice, dezinformarea și războiul informațional pot deveni și instrumente ale comunicării de criză, în timpul situațiilor de conflict, și pot acționa în direcția manipulării mediului informațional.

Concluzii

Într-o perioadă caracterizată, în primul rând, de incertitudine și de schimbări continue, precum și de bătălia pentru putere și informații, rolul strategiilor narative devine definitoriu. Este din ce în ce mai dificil să putem separa strategiile narative de interese, riscuri sau amenințări. În toată această confruntare, în care mesajele transmise sau primite trebuie decodate și interpretate, este necesară identificarea metodelor și mijloacelor pentru a contracara efectele nedorite, generate de toate aceste noi provocări.

Narațiunile strategice ajută atât la formularea strategiei, cât și la comunicarea acțiunilor. Informarea strategiei și a acțiunilor asociate acesteia, de exemplu operațiile militare, asigură coerența cu intențiile avute inițial. Altfel spus, asigură corelarea dintre cuvinte și fapte, chiar dacă narațiunea strategică este, în mod normal, construită ca parte integrantă a procesului de formulare a strategiei. Astfel, caracteristica de bază a narațiunilor strategice este aceea că oferă un cadru, prin care se pot structura activități de informare care explică trecutul, prezentul și viitorul conflictelor, cu scopul de a obține rezultatele dorite.
Frecvența cu care sunt diseminate informațiile în ultima perioadă creează o societate din ce în ce mai interconectată, ceea ce face ca importanța strategiilor narative să fie tot mai mare, rolul lor de influențare fiind definitoriu.

Strategiile narative pot fi studiate din perspectiva mai multor dimensiuni. Abordarea lor prin prisma discursului politic și, de asemenea, prin analizarea în funcție de audiențele pe care le vizează și de valorile pe care le supun atenției, sunt doar câteva aspecte ce vor fi detaliate într-un articol viitor. Această abordare reprezintă o parte a cercetării doctorale a autoarei. Plecând de la aceste aspecte, ne propunem ca, pe viitor, să avem în vedere corelarea modului în care narațiunile strategice impactează dimensiunea cognitivă a conflictelor și să identificăm modelele acestora utilizate de către marii actori statali, urmărind aspectele definitorii care pot schimba rezultatele estimate în cadrul unui proces de influențare.

Opinăm că, în momentul de față, nu au fost identificate utilizări conturate și clar definite ale narațiunilor strategice și, de asemenea, nu putem delimita exact strategiile sau tehnicile narative care conduc la obținerea superiorității în confruntările actuale, motiv pentru care cercetările viitoare se vor axa pe o analiză aprofundată a modelelor folosite de către marii actori politici, care au ca scop direcționarea audiențelor în sensurile dorite.

Referințe

Barclay, Donald A. 2018. *Fake news, propaganda, and plain old lies: how to find trustworthy information in the digital age. Rowman & Littlefield* 227.

Bjola, Corneliu, Jennifer Cassidy și Ilan Manor. 2019. "Public Diplomacy in the Digital Age." *The Hague Journal of Diplomacy* 14 (1-2): 83-101.

Boyd, Ryan, Kate Blackburn și James Pennebaker. 2020. "The narrative arc: Revealing core narrative structures through text analysis." *Science advances* 6.2 (eaba2196).

Buzan, Barry. 2008. *People, states & fear: an agenda for international security studies in the post-cold war era.* ECPR Press.

Claverie, Bernard și François Du Cluzel. 2022. "Cognitive Warfare Concept." https://innovationhub-act.org/wp-content/uploads/2023/12/CW-article-Claverie-du-Cluzel-final_0.pdf.

Dumitrescu, Lucian. 2020. *Narațiuni strategice: securizare și legitimitate în relațiile internaționale.* București: Editura Institutului de științe politice și relații internaționale „Ion I.C. Brătianu".

Johnsson, Magnus. 2011. "NATO and the Challenge of Strategic Communication." *NATO Defense College.* http://diva-portal.org/smash/gen/dim2:454747/FULLTEXT02.pdf.

McCarthy, Daniel J. 2000. "View from the top: Henry Mintzberg on strategy and management." *The Academy of Management Perspective* 14 (3): 31-42. http://www.jstor.org/stable/4165656.

Meretoja, Hanna. 2018. *The Ethics of Storytelling: Narrative Hermeneutics, History, and the Possible.* Oxford: Oxford University Press.

Miskimmon, Alister, Ben O'Loughlin și Laura Roselle. 2014a. „Strategic narrative: A new means to understand soft power." *Media, War & Conflict* (University of Oxford) 7 (1): 70-84.

—. 2014b. *Strategic narratives: Communication power and the new world order.* Routledge.

—. 2017. *Forging the World: Strategic Narratives and International Relations.* Royal Holloway.

—. 2018. "Strategic Narrative: 21st Century Diplomatic Statecraft/Narrativa estratégica : el arte de la diplomacia en el siglo XXI." *Revista Mexicana de Política Exterior* 113.

MNIOE, [Multinational Information Operations Experiment]. 2014. "White Paper - Narrative Development in Coalition Operations." v 1.0, Mayen.

Mullen, Michael. 2009. "Joint Force Quarterly." *Defense Technical Information Centre*. https://apps.dtic.mil/sti/pdfs/ADA535610.pdf.

NATO. fără an. "About Strategic Communication". Accesat ianuarie 2024. https://stratcomcoe.org/about_us/about-strategic-communications/1.

—. 2017. *NATO Strategic communication Handbook.* Vol. V 1.0.

—. 2022. "NATO 2022 Strategic Concept". https://www.nato.int/strategic-concept/.

—. 2023. ”Allied Command Transformation”. https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind/.

NATO Strategic Communication Centre of Excellence. fără an. *About Strategic Communication.* Accesat decembrie 2023. https://stratcomcoe.org/about_us/about-strategic-communications/1.

NATO-ACT. 2017. ”We Are NATO - Defence and Security Campain Toolkit”. https://www.act.nato.int/wp-content/uploads/2023/06/nato-dsct.pdf.

—. 2023. ”Cognitive Warfare: Strengthening and Defending the Mind”. https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind/.

Nissen, Tomas Elkajer. 2014. “Strategizing NATO’s Narratives.” *Strategy in NATO. Palgrave Studies in Governance, Security and Development* (McMilan).

Pop, Ioan Aurel. 2017. „Războiul informațional, sub lupă”. https://www.promptmedia.ro/2017/04/razboiul-informational-sub-lupa-conferinta-la-academia-romana/.

Popescu, Maria Magdalena. 2022. *Comunicarea strategică a informațiilor.* București: Top Form.

Reddi, Madhavi, Rachel Kuo și Daniel Kreiss. 2023. “Identity propaganda: Racial narratives and disinformation.” *New Media & Society* 25 (8): 2201-2218.

Rovența-Frumușani, Daniela. 1999. *Semiotică, societate, cultură.* Iași: Institutul European.

Saliu, Hasan. 2023. “Narratives of Public Diplomacy.” *Truth Era: The decline of Soft Power. Communication & Society* 36 (2): 209-224.

Schmitt, Oliver. 2018. “When are strategic narratives effective? The shaping of political discourse through the interaction between political myths and strategic narratives.” *Contemporary Security Policy* 39 (4): 487-511. https://doi.org/10.1080/13523260.2018.1448925.

Todorov, Tzvetan. 1966. “Les catégories du récit littéraire.” *Communications - Recherches sémiologiques: l’analyse structurale du récit.* (Edwardsville) (8): 125-151. https://doi.org/10.3406/comm.1966.1120.

—. 1971. *The 2 Principles of Narrative.* The Johns Hopkins University Press.

Tzu, Sun. 1994. *The art of war.* Hachette UK.

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

Abordări integratoare și relaționale ale rezilienței în concepția și acțiunea Alianței Nord-Atlantice

Integrative and relational approaches to resilience in the NATO concept and action

Colonel (r.) prof.univ.dr. Gheorghe MINCULETE*
Lector univ.dr. Veronica PĂSTAE**
*Academia Forțelor Terestre „Nicolae Bălcescu", Sibiu, România
**Universitatea Națională de Apărare „Carol I", București, România

Abstract

Conceptul de reziliență, adecvat operațiilor specifice, a fost folosit în cadrul NATO încă din anul 2010. Particularitatea termenului rezidă în fazele caracteristice de implementare în mediul operațional aliat, ceea ce generează o conduită adecvată de identificare, analiză și eludare a riscurilor, de rezistență la factorii perturbatori și de impact, recuperare, refacere și restabilire a potențialui inițial de forță și acțiune. Forțele combatante ale Alianței vor avea posibilitatea menținerii integrității și funcționalității adecvate, chiar și în condiții restrictive și cu dificultate crescută, prin implementarea, la nivelurile organizațional și acțional, a celor două componente ale rezilienței stratificate (operațională sau militară și civilă). În acest mod, va fi realizat un nivel ridicat de protecție, stabilitate și viabilitate a dispozitivelor de luptă ale forțelor tactice și/sau joint în fața unui ansamblu de amenințări și acțiuni complexe ale forțelor unui stat neprietenos (inamic). Prin cele relevate, cercetarea prezentă include o abordare teoretică, cu posibilități de concretizare în sfera rezilienței aplicate în domeniile civil și militar ale NATO, fiindcă include detalii importante cu caracter programatic, raportate la consecințele confruntării armate ruso-ucrainene, derulate începând cu 24 februarie 2022. De aici, au rezultat o serie de elemente relevante pentru consolidarea puterii acționale a forțelor joint și tactice, destinate a fi angajate în operații cu caracter național și multinațional în cadrul Alianței Nord-Atlantice, împotriva oricăror forțe agresive adverse.

The concept of resilience, suitable for specific operations, has been used within NATO since 2010. The particularity of the term resides in the characteristic phases of implementation in the allied operational environment, which generates appropriate conduct of identifying, analyzing, and avoiding risks, resistance to disruptive and impactful factors, recovery, restoration, and reconstruction of the initial force and action potential. The Alliance's combatant forces will maintain integrity and adequate functionality, even under restrictive, difficult conditions, by implementing, at organizational and operational levels, the two components of layered resilience (operational or military and civil). In this way, a high level of protection, stability, and viability of combat structures of tactical and/or joint forces will be achieved, to face the threats and complex actions of unfriendly (enemy) forces. Through the findings, the present research includes a theoretical approach, with possibilities of concretization in applied resilience in NATO civilian and military fields, because it includes important programmatic details, related to the consequences of the Russian-Ukrainian armed confrontation, which started on February 24, 2022. From here, relevant elements resulted in the consolidation of action power of joint and tactical forces, meant to be engaged in national and multinational operations within the North Atlantic Alliance, against any hostile aggressive forces.

Cuvinte-cheie:
instabilitate; competiție; reziliență; reziliență stratificată; reziliență civilă; reziliență operațională (militară); protecție; stabilitate; funcționabilitate.

Keywords:
instability; competition; resilience; layered resilience; civil resilience; operational (military) resilience; protection; stability; functionality.

Info articol
Primit: 21 ianuarie 2024; Evaluat: 14 februarie 2024; Acceptat: 11 martie 2024; Disponibil online: 5 aprilie 2024

Citare: Minculete, G. și V. Păstae. 2024. „Abordări integratoare și relaționale ale rezilienței în concepția și acțiunea Alianței Nord-Atlantice". *Buletinul Universității Naționale de Apărare „Carol I"*, 13(1): 100-116. https://doi.org/10.53477/2065-8281-24-07

Instabilitatea generalizată, competiția strategică și șocurile recurente conturează peisajul de securitate extins. Amenințările pot proveni de la actori atât statali, cât și nestatali, sub diverse forme, precum atacuri teroriste, atacuri cibernetice sau război hibrid, care estompează liniile dintre conflictele convenționale și cele neconvenționale. Importanța angajamentului și a cooperării civilo-militare este evidentă, în fața amenințărilor generate de schimbările climatice, de dezastrele naturale, precum inundațiile, incendiile și cutremurele, de pandemii și de războiul de agresiune al Rusiei împotriva Ucrainei. Pe măsură ce noile tehnologii devin omniprezente, societățile statelor NATO devin mai interconectate și interdependente în domeniile economic, financiar, informațional și cibernetic. Această interdependență a adus beneficii semnificative, dar a creat, de asemenea, vulnerabilități și dependențe. În contextul actual al securității, o reziliență eficientă și susținută necesită o abordare cuprinzătoare. Aceasta implică utilizarea întregii game de capacități militare și civile, precum și o colaborare activă între guvern, sectorul privat și societatea civilă (NATO 2023c).

În perioada imediat următoare anexării Crimeei, planificatorii și comandanții Alianței au pus în aplicare o serie de măsuri cruciale pentru implementarea Conceptului NATO actualizat, inclusiv, pentru elaborarea Strategiei Militare a Organizației în anul 2019. Ca urmare, miniștrii apărării aliați au aprobat, în anul 2020, *conceptul privind descurajarea și apărarea* zonei euroatlantice. În aceste condiții, a devenit deosebit de important termenul de reziliență – menționat, inițial, în Conceptul strategic NATO din anul 2010 (NATO 2010). În 2019, liderii NATO au agreat, în cadrul Declarației de la Londra, să intensifice eforturile pentru consolidarea rezilienței. Apoi, la Forumul Global de Securitate GLOBSEC de la Bratislava, din 2020, secretarul general Jens Stoltenberg a accentuat direcțiile viitoare ale rezilienței în cadrul Alianței: „De fapt, reziliența este în ADN-ul NATO. (...) Articolul 3 din Tratatul de la Washington impune aliaților datoria de a deveni mai rezilienți. Când a fost redactat tratatul, preocuparea era un atac armat din partea Uniunii Sovietice. Astăzi, ne confruntăm cu o gamă mult mai largă de provocări. De aceea creșterea rezistenței este o sarcină cheie pentru viitor" (van Mill 2023, 84).

În anul 2021 NATO a evidențiat necesitatea implementării *rezilienței naționale și colective* ca *„o bază esențială credibilă pentru descurajare și apărare*" (NATO 2021), având în vedere noile provocări și amenințări militare globale. Conceptul strategic al Alianței din anul 2022, aprobat în cadrul Summitului NATO de la Madrid (LSE IDEAS 2023), confirmă importanța concretizării *rezilienței naționale și colective* în toate acțiunile esențiale aliate, prima reprezentând-o *descurajarea și apărarea*, ca obiectiv major, reconfirmat la Summitul NATO de la Vilnius, din 2023 (NATO 2023d).

Reziliența la nivel național și colectiv în cadrul NATO se referă la capacitatea de pregătire, rezistență, răspuns și recuperare rapidă în urma șocurilor și perturbărilor strategice, acoperind întregul spectru al amenințărilor. În esență, reprezintă abilitatea individuală a aliaților, a colectivității Alianței și a NATO, ca organizație, de a face față perturbărilor și șocurilor și de a-și continua activitățile. Redistribuirea geostrategică

și militară a potențialului de forță implică transformarea continuă a instrumentului militar de putere al NATO, precum și alinierea capacităților militare și nonmilitare în toate statele membre. În acest sens, reziliența Alianței se bazează pe o combinație între pregătirea civilă și capacitatea militară. În acest context, pregătirea civilă contribuie direct la pregătirea defensivă a NATO – sisteme militare bine întreținute, capabile să se vindece rapid, adaptabile, durabile și sisteme militare în desfășurare, susținute și activate de capacitățile civile sunt necesare pentru a asigura securitatea și stabilitatea în întreaga Alianță (NATO-ACT 2023c).

În cadrul SUA, Departamentul Apărării (Department of Defense – DOD) a dezvoltat o interpretare extinsă a conceptului de reziliență, aplicând-o în contextul apărării naționale. Această perspectivă se reflectă în elaborarea diverselor politici, doctrine, orientări și pe site-urile oficiale ale DOD și serviciilor militare. De exemplu, în Directiva 4715.21 privind „Adaptarea la Schimbările Climatice și Reziliență" ("Climate Change Adaptation and Resilience"), DOD a definit reziliența ca „abilitatea de a anticipa, pregăti și adapta la condițiile în schimbare și de a rezista, răspunde și reveni rapid după perturbări". Această definiție este asociată tuturor domeniilor gestionate de DOD, cum ar fi instalațiile, personalul, operațiile, transportul, lanțurile de aprovizionare-livrare, cercetarea, dezvoltarea, testarea și evaluarea. Un alt exemplu ilustrează modul în care armata SUA definește reziliența în cadrul „Programului de Îngrijire a Recuperării Armatei" ("Army Recovery Care Program") – un program dedicat soldaților răniți, bolnavi și accidentați. Aici, reziliența este descrisă ca „abilitatea mentală, fizică, emoțională și comportamentală de a înfrunta și gestiona adversitatea, de a se adapta la schimbare, de a se recupera, de a învăța și de a evolua din provocări" (Herrera 2021, 2). Acest concept acoperă multiple aspecte ale vieții militarilor și evidențiază importanța dezvoltării abilităților necesare pentru a face față și a depăși provocările întâlnite în serviciul lor (Wheeler 2021, 2).

Actualmente, Comandamentul Aliat pentru Transformare (Allied Command Transformation – ACT) conduce procesul de adaptare acțională a Alianței prin implementarea conceptului fundamental de luptă al NATO (NATO-ACT 2023a). Acest demers include necesitatea dezvoltării operaționale a puterii Alianței, în baza conceptului *rezilienței stratificate* (Layered Resilience) elaborat de către ACT, în conformitate cu cerințele transformării militare, adaptării și menținerii securității într-un mediu internațional complex, caracterizat de creșterea continuă riscurilor și amenințărilor militare (NATO-ACT 2023c).

În vederea realizării în mod echilibrat a acestei lucrări cu caracter de noutate, am procedat, din punct de vedere științific, la identificarea surselor, la obținerea, analiza, evaluarea, interpretarea informațiilor și datelor necesare realizării conținutului secvențelor. A rezultat, astfel, un studiu cât se poate de actual, util celor interesați în înțelegerea rolului și importanței rezilienței în concepția și acțiunea NATO, în scopul realizării altor lucrări științifice de interes.

Construcția holistică a studiului este centrată, la modul concret, pe reziliența stratificată, ale cărei componente sunt concretizate, sub aspect științific, astfel: reziliența civilă în secvența doi; reziliența operațională (militară) în secvențele trei și patru.

Aspecte generale privind reziliența națională și colectivă în cadrul NATO

Fiecare țară membră a NATO trebuie să dispună de reziliența necesară întâmpinării, cu pierderi mult diminuate, a eventualelor șocuri majore, generate de dezastre naturale, de eșecurile infrastructurilor critice sau de atacurile hibride ori armate. Dacă avem în vedere natura conceptului, *reziliența* reprezintă potențialul individual și colectiv de pregătire, de rezistență, de răspuns și de recuperare rapidă în urma impactului factorilor perturbatori, pentru asigurarea continuității activităților specifice funcționării fiecărui stat al Alianței. În acest sens, în baza Articolului 3 din Tratatul Atlanticului de Nord, asigurarea rezilienței naționale și colective sunt esențiale în procesele de proiectare și de realizare a descurajării și apărării credibile, vitale pentru concretizarea eforturilor NATO de protejare a societăților, populațiilor și valorilor comune. Societățile moderne sunt extrem de complexe, cu sectoare integrate și interdependente și cu servicii vitale. Acest lucru le face vulnerabile la perturbări majore, în cazul unui atac terorist sau hibrid asupra infrastructurii critice (NATO 2023c). În Figura 1 evidențiez infrastructuri critice, prezente (în totalitate sau parțial) în statele membre ale NATO.

Figura 1 Potențialul critic civil al fiecărui al stat al NATO (Roepke și Thankey 2019)

Legendă:

- Energy = Energie
- Health = Sănătate
- Transport = Transport;
- Financial = Financiar/ Finanțe;
- ICT= TIC; Tehnologia informației (și a comunicațiilor);
- Water = Apă;
- Food = Hrană;
- Public&Legal Order and Safety = Ordinea și siguranța publică;
- Chemical and Nuclear Industry = Industria chimică și nucleară;
- Space and Research = Cercetare spațială/ Spațiu și cercetare.

În cea mai mare parte a perioadei Războiului Rece, planificarea civilă de urgență, cunoscută pe atunci sub numele de pregătire civilă, a fost eficient organizată și susținută cu resurse de către Aliați, reflectându-se cu precădere în structura și

comanda NATO. În anii '90 însă, o mare parte din planificarea detaliată, din structurile și capacitățile pregătirii civile au suferit reduceri semnificative atât la nivel național, cât și la nivelul NATO. Evenimente precum anexarea ilegală a Crimeei de către Rusia în 2014 și ascensiunea ISIS/Daesh au marcat o schimbare în mediul strategic. Acestea au determinat Alianța să-și consolideze postura de descurajare și apărare. Între timp, amenințările teroriste și hibride, în special atacurile cibernetice recente, continuă să vizeze populația civilă și infrastructurile critice, preponderent deținute de sectorul privat. Aceste evoluții au avut un impact major, evidențiind necesitatea sporirii rezilienței prin pregătirea civilă. Astăzi, Aliații adoptă o abordare pas cu pas în acest sens, într-un efort care completează modernizarea militară a NATO și postura sa generală de descurajare și apărare (Roepke și Thankey 2019).

La Summitul de la Varșovia, din 2016, liderii aliați au convenit să intensifice reziliența NATO în scopul abordării întregului spectru de riscuri și amenințări, pentru a dezvolta capacitățile individuale civile ale țărilor membre, alături de capabilitățile colective, destinate rezistenței oricărei forme de atac armat. Aceștia au stabilit *șapte cerințe de bază* pentru evaluarea nivelului de pregătire al țărilor aliate privind reziliența civilă națională (figurile 2 și 3): asigurarea continuității funcționale a guvernului și a serviciilor guvernamentale critice (implică capacitatea de a lua decizii și de a comunica cu cetățenii în timpul unei crize); realizarea aprovizionării continue cu energie și elaborarea planurilor de rezervă pentru a gestiona întreruperile (accentul se pune pe capacitatea de a furniza energie în mod constant și de a gestiona întreruperile prin planuri bine definite); gestionarea eficientă a deplasărilor necontrolate ale oamenilor, concomitent cu dislocările de capabilități militare aliate (cu accent pe abilitatea de a gestiona și controla deplasările de persoane, inclusiv din zonele militare); asigurarea unor provizii de hrană și apă suficiente și reziliente (protejate în special de întreruperi sau sabotaje); proiectarea și asigurarea capacității de a face față victimelor în masă și crizelor de sănătate perturbatoare (accentul va fi pus pe realizarea sistemelor de sănătate civile care pot gestiona situații de criză, cu stocuri adecvate de provizii medicale); funcționarea telecomunicațiilor și rețelelor cibernetice în condiții de criză, inclusiv prin utilizarea tehnologiei 5G, cu opțiuni robuste pentru restabilirea acestor sisteme; asigurarea deplasării rapide a forțelor NATO pe teritoriul alianței, având în vedere ca serviciile civile să poată conta pe rețelele de transport, chiar și în timpul unei crize (van Mill 2023, 85). Aceste cerințe reflectă angajamentul aliaților în consolidarea rezilienței naționale și colective, contribuind astfel la securitatea și stabilitatea Alianței NATO prin asigurarea continuității guvernării, serviciilor esențiale pentru populație și sprijinului civil pentru armată.

În scopul reducerii potențialelor vulnerabilități și riscuri de atac în timp de pace, criză și conflict, statele NATO vor avea în vedere o asociere deplină a eforturilor militare de apărare a teritoriilor și populațiilor cu pregătirea civilă solidă în domeniile continuității guvernării, serviciilor esențiale pentru populație și realizării sprijinului civil în operațiile militare de nivel joint cu statut național și multinațional. În acest sens, având în vedere distrugerile majore, făcute de armata rusă în Ucraina, și sabotajul împotriva conductelor Nord Stream la nivelul NATO și Uniunii Europene, la data

de 16 martie 2023 s-a constituit un grup operativ în scopul conștientizării situației, împărtășirii celor mai bune practici și dezvoltării principiilor necesare îmbunătățirii rezilienței în interiorul ambelor organizații. Cu ocazia anunțării inițiativei comune de lucru, în ianuarie 2023 secretarul general al NATO – Jens Stoltenberg – a afirmat, în prezența președintelui Comisiei Europene – Ursula von der Leyen: „Vrem să analizăm împreună cum să facem infrastructura noastră critică, tehnologia și lanțurile de aprovizionare-livrare mai reziliente la viitoare amenințări și să luăm măsuri pentru a atenua potențialele vulnerabilități. Acesta va fi un pas important pentru devenirea societăților noastre mai puternice și mai sigure" ("We want to look together at how to make our critical infrastructure, technology and supply chains more resilient to potential threats, and to take action to mitigate potential vulnerabilities. This will be an important step in making our societies stronger and safer"). Tot atunci, liderii NATO și UE au procedat la semnarea unei noi declarații comune, în scopul construirii parteneriatului dintre aceste organizații la un nivel evoluat, inclusiv în privința utilizării tehnologiilor emergente, perturbatoare și a spațiului, luând în considerare și influențele schimbărilor climatice asupra dimensiunii securității.

Potrivit celor relevate, este evident că forțele operaționale multinaționale joint ale NATO, mai ales cele dislocate în perioade de crize și conflict, vor depinde stringent de serviciile aferente sectoarelor civile și comerciale în procesele realizării transporturilor, comunicațiilor, furnizării energiei și chiar proviziilor esențiale, îndeosebi hrană și apă, muniții și combustibili, în scopul îndeplinirii misiunilor primite. Așadar, rezultă, de aici, importanța pregătirii civile solide, pentru a permite societăților din țările aliate de a rezista la atacurile și/sau perturbările majore apărute în orice moment, în vederea continuării sprijinirii forțelor combatante ale Alianței, pentru realizarea obiectivelor operaționale și atingerea stării finale (NATO 2023c).

Particularități ale rezilienței operaționale în cadrul Alianței

Scopul concretizării rezilienței operaționale (Resilient MIoP) în cadrul NATO îl reprezintă susținerea descurajării și apărării Alianței împotriva oricărui adversar prin constituirea și folosirea capacităților de anticipare, de pregătire și de adaptare la amenințări și pericole, precum și prin implementarea opțiunilor de rezistență, de răspuns și de recuperare rapidă în fața șocurilor strategice (van Mill 2023, 85).

Modernizarea continuă a NATO a determinat utilizarea *conceptului de reziliență stratificată* (The Layered Resilience Concept), care include două componente ce se augmentează reciproc, adică *reziliența operațională (militară)* și *reziliența civilă*, considerate pioni esențiali ai susținerii instrumentului militar de putere al Alianței (Figura 2). Reziliența stratificată relevă capacitatea NATO de a răspunde și de a se adapta rapid la diverse niveluri de riscuri și amenințări, de la cele convenționale până la cele cibernetice și/sau hibride. Focalizarea principală a conceptului este pe reziliența operațională (militară), în scopul sporirii aplicabilității și realizării interdependențelor acesteia cu reziliența civilă (prezentată în secvența 2). În acest

Figura 2 Imagini ale rezilienței stratificate (operațională și civilă) în cadrul NATO (van Mill 2023, 84)

Legendă:

The Layered Resilience Concept considers military and civil resilience necessary to support the military instrument of power = Conceptul de reziliență stratificată consideră reziliența operațională și civilă ca necesară în sprijinirea instrumentului militar de putere.

mod, vor fi consolidate capabilitățile NATO de rezistență, de recuperare și de adaptare la șocurile strategice (van Mill 2023, 85-86).

În urma invaziei Ucrainei de către armata rusă la 24 februarie 2022, experții NATO au apreciat că este absolut necesară dezvoltarea unui proces de planificare a rezilienței, similar cu procesul de planificare a apărării NATO (NATO Defence Planning Process – NDPP) în scopul armonizării și integrării planurilor, strategiilor și capacităților naționale de reziliență. Acest demers a fost considerat esențial pentru a coordona un răspuns colectiv puternic din partea NATO, concomitent cu constituirea unui grup operativ de reziliență la nivel înalt, cu misiunea de a identifica și de a propune: lecțiile multidimensionale privind reziliența, în baza experienței Ucrainei în fața amenințărilor convenționale, hibride și societale; cerințele atât naționale, cât și colective de reziliență, pentru a ajuta la realizarea unei unități mai eficiente de efort; recomandările privind politicile și investițiile viitoare, pentru atingerea obiectivului de consolidare a rezilienței europene (Dowd și Cook 2022, 1-4).

Ulterior, complexitatea și amplitudinea, specifice conceptului de reziliență stratificată (elaborat), a implicat, la nivelul Alianței, constituirea unui cadru tematic adecvat pentru *șapte zone* proprii *rezilienței operaționale* (Figura 3). În mod individual, zonele (enumerate în continuare) au necesitat înființarea unor grupuri tematice de lucru – conduse de națiunile aliate desemnate –, astfel: Sistemul de Comandă și Control-C2, Franța (Command and Control-C2 System, France); Capacitatea de Luptă, Polonia (Warfighting Capability, Poland); Înțelegerea Situațională, Grecia (Situational Understanding, Greece); Logistică/Mobilitatea Forțelor, Germania (Logistics/Deployability of Forces, Germany); Planificarea Răspunsului, România (Response Planning, Romania); Infrastructura Militară, Regatul Unit (Military Infrastructure, United Kingdom); Perseverența, Ungaria (Perseverance, Hungary).

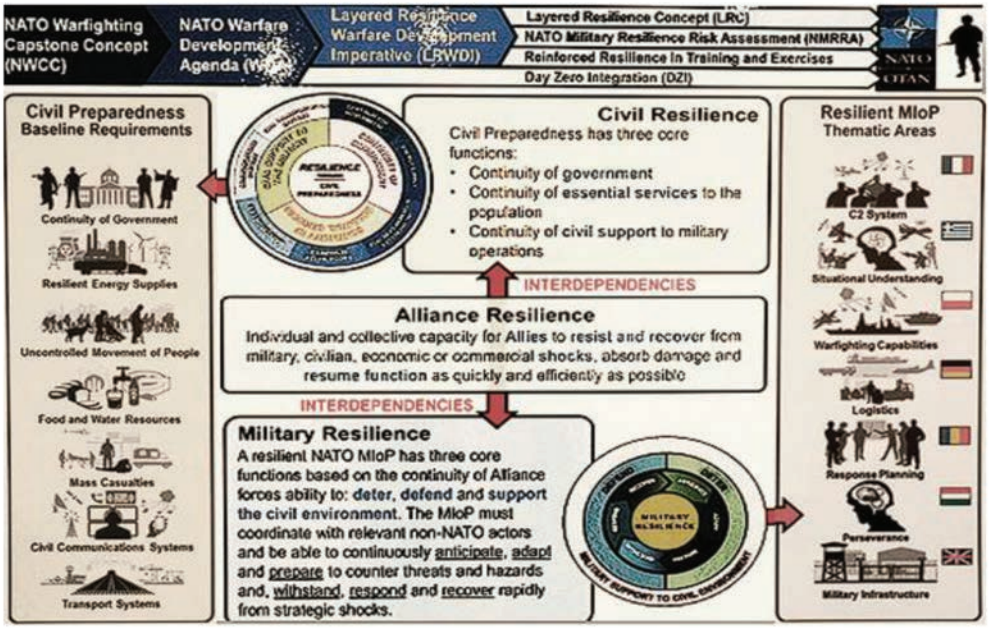

Figura 3 Zonele rezilienței stratificate, cu accent pe reziliența operațională (Dowd și Cook 2022, 86)

Legendă:

Sus (Page Header)

- NATO Warfighting Capstone Concept (NWCC) = Conceptul de consolidare a descurajării și apărării NATO;
- NATO Warfare Development Agenda = Agenda NATO de dezvoltare a războiului;
- Layered Resilience Warfare Development Imperative (LRWDI) = Imperativul de dezvoltare a războiului de reziliență stratificată (LRWDI);
- Layered Resilience Concept (LRC) = Conceptul de reziliență stratificată (LRC) ;
- NATO Military Resilience Risk Assessment (NMRRA) = Evaluarea riscurilor NATO privind reziliența militară (NMRRA);
- Reinforced Resilience in Training and Exercises = Reziliență sporită în antrenamente și exerciții;
- Day Zero Integration (DZI) = Integrarea din Ziua Zero (DZI).

Centru (Center)

- Civil Resilience = Reziliența civilă;
- Civil Preparedness has three core functions: Pregătirea civilă are trei funcții de bază:
- Continuity of government = Continuitatea guvernării;
- Continuity of essential services to the population = Continuitatea serviciilor esențiale către populație
- Continuity of civil support to military operations = Continuitatea sprijinului civil al operațiilor militare.
- Interdependencies = Interdependențe
- Alliance Resilience – Individual and collective capacity for Allies to resist and recover from military, civilian, economic and commercial shocks, absorb damage and resume function as quickly and efficiently as possible = Reziliența Alianței – Capacitatea individuală și colectivă a Aliaților de a rezista și de a se recupera în urma șocurilor militare, civile, economice și comerciale, de a absorbi daunele și de a relua funcționarea cât mai rapid și eficient posibil.
- Military Resilience – A resilient NATO MIoP (NATO military instrument of power) has three core functions based on the continuity of Alliance forces ability to: deter, defend and support the civil environment. The MIoP must coordinate with relevant non-NATO actors and be able to continuously anticipate, adapt and prepare to counter threats and hazards and, withstand, respond and recover rapidly from strategic shocks = Reziliența militară – Potențialul militar de putere (MIoP) rezilient al NATO are trei funcții, bazate pe continuitatea capacității forțelor Alianței de a: descuraja, apăra și sprijini mediul civil. MIoP trebuie să se coordoneze cu actorii relevanți din afara NATO (non-NATO) și să fie capabil să anticipeze, să se adapteze și să se pregătească în mod continuu pentru a contracara amenințările și pericolele și să reziste, să răspundă și să se recupereze rapid în urma șocurilor strategice.

Coloană stânga:

Civil Preparedness Baseline Requirements = Cerințe de bază privind pregătirea civilă:

- Continuity of Government = Continuitatea guvernării;
- Resilient Energy Supplies = Surse de energie reziliente;
- Uncontrolled Movement of People = Deplasarea necontrolată a persoanelor;
- Food and Water Resources = Resurse alimentare și de apă;
- Mass Casualties = Victime în masă;
- Civil Communication Systems = Sisteme de comunicații civile ;
- Transport Systems = Sisteme de transport.

Coloană dreapta:

Resilient MIoP Thematic Areas = Domenii (tematice) MIoP reziliente;

- C2 System (Command and Control-C2 System, France) = Sistemul de Comandă și Control-C2, Franța;
- Situational Understanding (Greece) = Înțelegerea Situațională (Grecia);
- Warfighting Capabilities (Poland) = Capabilități de luptă;
- Logistics (Germany) = Logistică (Germania);
- Response Planning (Romania) = Planificarea răspunsului (România);
- Perseverance (Hungary) = Perseverență (Ungaria);
- Military Infrastructure (United Kingdom) = Infrastructura militară (Regatul Unit).

Pentru îndeplinirea obiectivelor specifice, grupurile de lucru tematice vor fi susținute de părțile interesante și de experții necesari fiecărui domeniu. Prin metodele și procedeele utilizate, aferente domeniilor enumerate, vor fi realizate mai multe tipuri de analize, în scopul obținerii tuturor informațiilor utile deteminărilor specifice de potențiale riscuri, vulnerabilități și deficiențe critice, care vor fi luate în considerare în procesele dezvoltării în viitor a potențialului militar de putere (Dowd și Cook 2022, 85-86).

Fiindcă România este implicată într-una dintre cele șapte zone amintite, experții Centrului Euroatlantic pentru Reziliență (Euro-Atlantic Resilience Centre, E-ARC) au participat, în septembrie 2023, la lucrările seminarului organizat în Polonia, pentru dezvoltarea conceptului rezilienței stratificate a NATO. În acest scop, specialiștii E-ARC au coordonat, cu implicarea unor experți ai MApN, procesul elaborării conținutului doctrinei Alianței privind *„planificarea răspunsului”*, luând în considerare mai multe obiective NATO privind reziliența, cu accent pe: „continuitatea lanțului de comandă; proceduri militare structurate; mobilizarea rapidă a forțelor de rezervă; un echilibru armonios între capabilități și capacități” (E-ARC 2023).

Operațiile viitorului implică o confruntare continuă a forțelor tactice și/sau joint proprii cu forțele adverse, ceea ce necesită luarea în considerare, proiectarea și manifestarea rezilienței operaționale (componentă a rezilienței stratificate) la

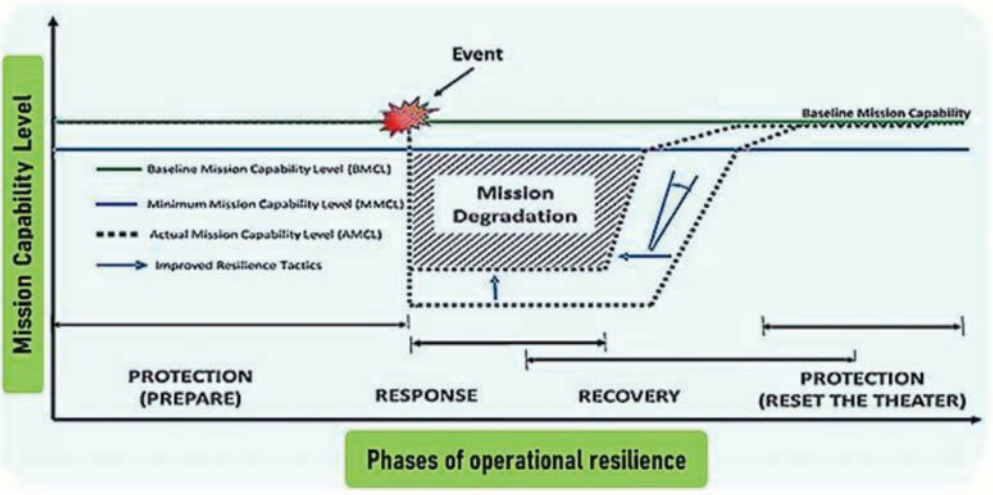

Figura 4 O imagine privind configurarea rezilienței operaționale la nivelul unei forțe de nivel tactic și/sau joint multinaționale (Herrera 2021, 3)

Legendă:

- ✓ Mission capability Level = Nivelul capabilității pentru misiune;
- ✓Phases of operational resilience = Fazele rezilienței operaționale;
- ✓Mission degradation = Degradarea misiunii;
  - Baseline Mission Capability Level (BMCL) = Nivelul capabilității misiunii de referință (BMCL);
  - Minimum Mission Capability Level (MMCL) = Nivel minim al capabilității de misiune (MMCL);
  - Actual Mission Capability Level (AMCL) = Nivel actual al capabilității de misiune (AMCL);
  - Improved Resilience Tactics = Tactici de îmbunătățire a rezilienței;
- ✓Protection (Prepare) = Protecție (Pregătire);
- ✓Response = Răspuns;
- ✓Recovery = Recuperare;
- ✓Protection (Reset the Theater) = Protecție (Resetarea teatrului).

nivelurile tactic și/sau joint, potrivit etapelor derulării acesteia (parțial sau în totalitate). Așadar, reziliența operațională evidențiază un proces de protecție pregătitoare, evitare, eludare, lovire-impact, răspuns, refacere și protejare în continuare a capabilităților forței combatante (cu statut național și multinațional) în fazele acționale integrate misiunilor care trebuie îndeplinite de către aceasta în teatrul de operații joint multinaționale. În consecință, reziliența operațională implică – pe faze –, conform Figurii 4, prevederea și aplicarea unui management adecvat riscului operațional la nivelul acțional amintit. Rezultă așadar că acțiunile intensive ale inamicului cu diferite tipuri de forțe și mijloace pot determina reducerea ritmului operațiilor, mai ales din cauza epuizării resurselor, pierderilor de personal și echipamente, nivelului redus și incert al stocurilor, epuizării fizice și psihice a luptătorilor și pierderii motivației lor acționale (Herrera 2021, 2-5).

În contextul evidențiat, liderii structurilor operaționale și de sprijin logistic, de la nivelurile tactic și/sau joint, sunt responsabili de colaborarea atât pe orizontală, cât și pe verticală în interiorul organizațiilor militare din care fac parte, inclusiv în cadrul unei grupări de forțe întrunite (joint). Prin urmare, sinergia acțională, creată și dezvoltată de către fiecare lider combatant, împreună cu potențialul logistic disponibil, reprezintă pilonii esențiali ai creșterii, menținerii sau refacerii rezilienței operaționale (Figura 5) a fiecărei structuri acționale de nivel tactic și/sau joint (Minculete 2023, 230-232).

Continuând cu reziliența operațională a unei forțe joint sub comandă NATO, rezultă că potențialul de augmentare a acesteia determină menținerea infrastructurilor teritoriale și/sau critice implicate și asigurarea continuă a resurselor (din surse militare și civile) necesare planificării și desfășurării operațiilor pe durata unei campanii, în fața atacurilor complexe ale inamicului, menite să ducă la eșecul acțiunilor acestora. Rezultă, deci, că forțele operaționale joint și rețeaua logistică de sprijin integrată trebuie să aibă capacitatea de a opera fără întreruperi semnificative și de a se adapta la încercările intensive ale forțelor adverse de a le denatura și diminua intențiile și resursele prin acțiuni de forță multiple (Hagen și alții 2016, 6-11).

Dacă evitarea factorilor perturbatori (de risc) nu mai poate avea loc, chiar dacă au fost luate măsuri vizibile de intervenție, în baza cerințelor implicate de efortul acțional, vor apărea discrepanțe insurmontabile între acțiunile dinamice ale forțelor combatante și sprijinul logistic imediat, necesar acestora (Ryczynski și Tubis 2021, 16-22). Așadar, sub aspectul manifestării rezilienței logistice operaționale, se va produce într-un interval scurt de timp o criză specifică prin deficit parțial sau total de resurse și servicii logistice (specifice domeniilor: aprovizionare; transport; mentenență; servicii de campanie) și de sprijin medical, cunoscută în sfera economică sub denumirea de *punct culminant al logisticii* (”logistics culmination”), iar la nivel operațional militar – din punctul meu de vedere – *punct critic logistic* (”logistics critical point”) sau *deficit critic logistic* (”logistics critical deficit”) (Minculete 2023, 143-145). Manifestarea dereglării sprijinului logistic operațional este evidențiată în Figura 6.

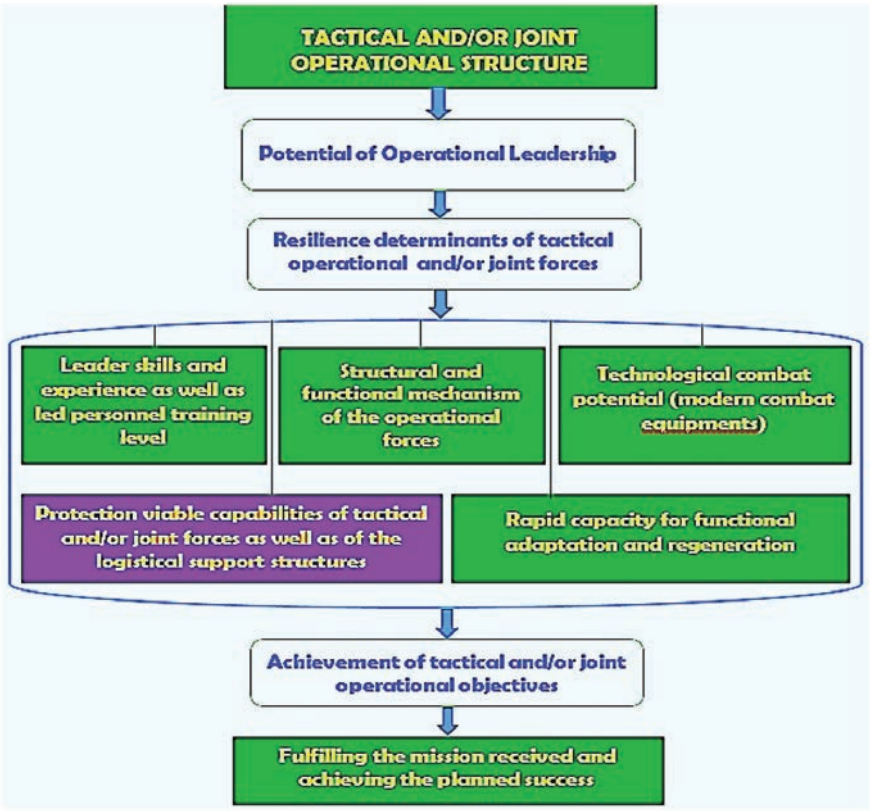

Figura 5 Determinări obiective ale rezilienței operaționale la nivelurile tactic și/sau joint (Minculete 2023, 231)

Legendă:

✓ Tactical and/or Joint Operational Structure = Structura operațională tactică și/sau joint;
✓ Potential of Operational Leadership = Potențialul de conducere operațională;
✓ Resilience determinants of tactical operational and/or joint forces = Determinanți ai rezilienței forțelor operaționale tactice și/sau joint;
✓ Leader skills and experience as well as led personnel training level = Abilități și experiență de lider, precum și nivelul de pregătire a personalului condus;
✓ Structural and functional mechanism of the operational forces = Mecanismul structural și funcțional al forțelor operaționale;
✓ Technological combat potential (modern combat equipments) = Potențialul de luptă (echipamente moderne de luptă);
✓ Protection viable capabilities of tactical and/or joint forces as well as logistical support structures = Capabilități viabile de protecție a forțelor tactice și/sau joint, precum și a structurilor de sprijin logistic;
✓ Rapid capacity for functional adaptation and regeneration = Capacitate rapidă de adaptare funcțională și regenerare;
✓ Achievement of tactical and/or joint operational objectives = Realizarea obiectivelor operaționale tactice și/sau joint;
✓ Fulfilling the mission received and achieving the planned success = Îndeplinirea misiunii primite și obținerea succesului planificat.

Invadarea nejustificată și ilegală a Ucrainei de către Rusia, care a generat cel mai amplu conflict din Europa de la al Doilea Război Mondial, se caracterizează acum printr-un conflict armat de uzură și o angajare logistică intensă. Această confruntare complexă a evidențiat imperativul de a aborda aspecte adesea neglijate, dar cruciale în asigurarea capacităților operaționale esențiale, necesare dislocării, execuției și menținerii cu succes a operațiilor planificate, pentru îndeplinirea întocmai a misiunilor primite și atingerea stării finale (Dowd, Jankowski și Cook 2023, 8-9). În aceste condiții, se impune perfecționarea rapidă a capacității de pregătire și a abilității forțelor operaționale NATO, care trebuie susținute de o logistică operațională modernă, eficace și eficientă, pentru asigurarea unui răspuns adecvat, de contracarare a amenințărilor actuale și viitoare (NATO-ACT 2023b).

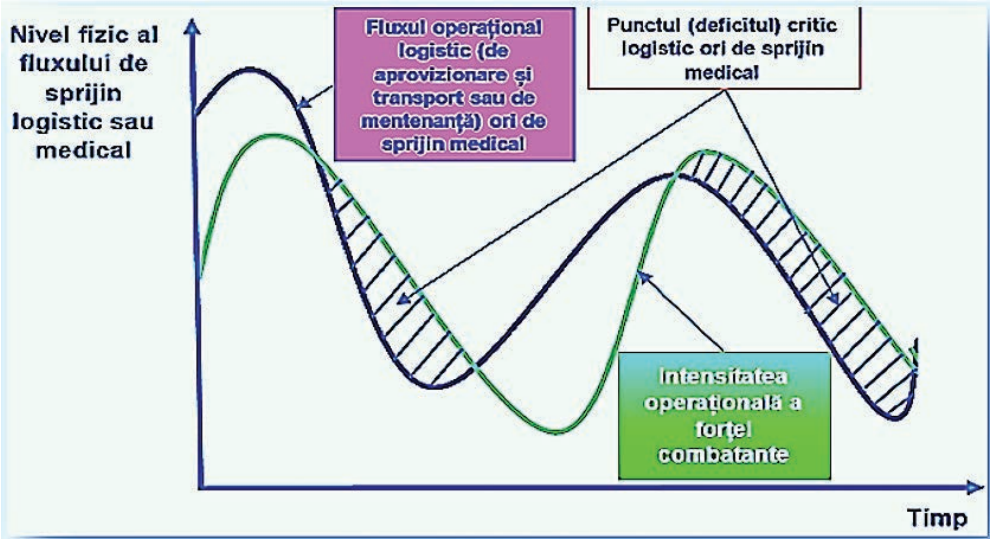

Figura 6 O imagine asupra punctului (deficitului) critic logistic al unei forțe tactice și/sau joint multinaționale (Minculete 2023, 144)

Din cele prezentate, pentru construirea unei reziliențe operaționale ridicate, care să aibă efectele holistice așteptate la nivel organizațional și interorganizațional, rezultă necesitatea planificării și desfășurării intensive de către forțele operaționale naționale și multinaționale NATO a antrenamentelor și exercițiilor, a modelării și simulării, precum și a jocurilor de război, pentru testarea liderilor, luptătorilor și pentru validarea proceselor. Potrivit experților Alianței, în cadrul scenariilor de instruire, care implică ambele tipuri de reziliență – civilă și operațională (militară) –, vor trebui incluse: agenții civile, organizații internaționale și organizații neguvernamentale, actori comerciali și forțe de apărare civilă; mediile și amenințările complexe actuale și viitoare. Totodată, haosul și eșecurile, apărute pe timpul desfășurării antrenamentelor și exercițiilor de către structurile și sistemele operaționale NATO, vor trebui acceptate, în scopul îmbunătățirii execuției care va fi evaluată, în funcție de specific, în baza indicatorilor calitativi și cuantificabili de reziliență (NATO-ACT 2022, 5).

Descurajarea și apărarea, factori esențiali în realizarea rezilienței operaționale

Rolul *descurajării* în domeniul militar a constat întotdeauna în nivelul potențialului operațional al unui stat, comparabil cu al adversarilor săi. Prin descurajare, pot fi atenuate sau diminuate amenințările adverse și, implicit, evitate consecințele unei crize extinse care s-ar putea manifesta. Abordările doctrinare moderne evidențiază descurajarea, în primul rând, ca proces psihologic, punând accent pe înțelegerea abilă a mentalității elitelor forțelor adverse, care definesc și propagă amenințarea prin utilizarea puterii militare a forțelor din subordine, precum și pe capacitatea de influențare a conduitei imediate a acestora. Așadar, acțiunile de coordonare și de transmitere sincronizată a mesajelor pe diverse canale de comunicare au rolul de schimbare a comportamentelor liderului sau liderilor statali adverși, în urma perceperii costurilor și consecințelor multiple ale eventualelor acțiuni militare

nesăbuite, la ordinul acestora. De aici, rezultă configurarea doctrinară a rezilienței operaționale care se axează, în afară de latura comportamentală, și pe teoria jocurilor care a fost și este aplicată prin descurajarea cu potențiale militare convenționale și/sau nucleare (Wheeler 2021).

Atunci când descurajarea urmează să atingă punctul critic de eșec, forțele operaționale NATO (cu statut național și multinațional) vor trebui să pună în aplicare *planurile de apărare* permanentă și pe cele de contingență (construite în avans, în baza unor scenarii operaționale posibile), pentru a face față amenințărilor iminente, cel puțin pe termen scurt, și pregătirea condițiilor necesare câștigării inițiativei, dacă aceasta a fost diminuată sau pierdută (Wheeler 2021).

Potrivit celor relevate, un exemplu istoric sugestiv pentru apărarea și descurajarea forțelor adverse îl reprezintă *războiul statului finlandez, din toamna și iarna anilor 1939-1940, împotriva forțelor invadatoare sovietice,* al cărui potențial a fost dat de forța celor peste 600.000 de militari. Apărarea Finlandei era constituită numai din: 300.000 de militari (inclusiv rezervele și recruții); un număr mic de tancuri; câteva avioane de luptă; un număr infim de muniții pentru o forță de artilerie insignifiantă. Totuși, compensarea a reprezentat-o societatea civilă finlandeză, pregătită să se confrunte cu un inamic mult superior. Dar, după cum este cunoscut în istorie, mari bătălii au fost câștigate de multe ori de forțe flexibile și mult mai reduse decât cele inamice, și aici, în armata finlandeză destul de inferioară celei adverse, aproape toți soldații au fost, pe lângă vânători abili, și schiori experimentați, capabili de luptă și de supraviețuire în condițiile extreme ale iernii Cercului polar. În armata invadatoare sovietică, majoritatea recruților, care trebuiau să reziste sălbăticiei înghețate, nu dispuneau de echipamentul adecvat mediului respectiv de luptă, lipsindu-le articole importante, precum pantofii de zăpadă și schiurile. Mai mult, forțele de apărare finlandeze le-au atras pe cele invadatoare, treptat, în interiorul teritoriului național, acoperit de un strat înalt de zăpadă. Concomitent, apărătorii s-au organizat în grupuri mici și independente de hărțuire, cu mobilitate sporită, capabile de atacuri rapide și eficiente, ceea ce le-a permis să nimicească unitățile sovietice inferior echipate și pregătite. Acestea au fost împiedicate să se desfășoare, au fost forțate să se deplaseze în coloane masive pe drumuri greu accesibile, în timp ce luptătorii finlandezi, deosebit de motivați pentru eliberarea țării lor, beneficiau de libertatea totală de mișcare și de atac. Ulterior, după o perioadă de 105 zile de confruntări intense, conflictul armat, început la 30 noiembrie 1939, s-a încheiat printr-un acord de pace, convenit între cele două părți. A rezultat totuși o pierdere de 11% din teritoriul Finlandei, compensată însă de păstrarea suveranității statale. Cealaltă parte, URSS, a pierdut pe teritoriul statului ocupat mai mult de 200.000 de oameni, comparativ cu doar 25.000 de victime finlandeze, ceea ce a reprezentat o imagine deosebit de negativă a reputației internaționale a sovieticilor (NATO 2023b).

Astăzi, puterea militară de apărare a NATO, instalată în partea de est a teritoriului său, reprezintă un element important de descurajare. Această componentă a fost realizată în ultimii ani, când statele aliate, situate în teritoriile nordice și sudice ale

flancului estic al NATO, au constituit, în baza celor convenite la nivelul Alianței, opt grupuri de luptă (battle groups, BG), cu structuri multinaționale (fiecare cu câte o națiune cadru). Așadar, încă din 2017 a fost înființat câte un BG în Estonia, Letonia, Lituania, iar din 2022 în Ungaria, Slovacia, România și Bulgaria. Mai mult, tot pentru descurajare și apărare, pe acest flanc estic – de la Marea Baltică, în nord, până la Marea Neagră, în sud – aliații au mai dislocat un număr semnificativ de nave, avioane și alte trupe (NATO 2023b).
Din data de 24 ianuarie 2024, a început desfășurarea (în nord-estul SUA) a unuia dintre cele mai ample exerciții militare ale NATO (considerate după Războiul Rece), denumit "Steadfast Defender 2024", planificat a fi realizat în decursul mai multor luni (Felstead 2024). Capabilitățile operaționale mobilizate pentru realizarea exercițiului sunt „în jur de 90.000 de militari (din 31 de state aliate NATO și Suedia); 50 de nave de război (de la portavioane la distrugătoare); peste 80 de avioane de luptă (F-35, FA-18, Harriers, F-15), elicoptere și nenumărate vehicule aeriene fără pilot; peste 1.100 vehicule de luptă (din care peste 150 de tancuri; 500 de vehicule de luptă de infanterie și 400 de vehicule blindate de transport de trupe)" (NATO 2024; Reuters 2024).

Scopul acestui exercițiu complex este: testarea și perfecționarea planurilor de apărare ale Alianței, astfel încât să fie consolidată apărarea europeană împotriva acțiunilor posibile ale „unui adversar apropiat" (Felstead 2024); desfășurarea și susținerea operațiilor complexe „în mai multe domenii, de-a lungul mai multor luni, pe o suprafață geografică de mii de kilometri, din Nordul Înalt până în Europa Centrală și de Est în orice condiții" (Garamone 2024); demonstrarea capacității Alianței de consolidare a zonei euroatlantice „prin mișcarea transatlantică a forțelor din America de Nord", (ceea ce implică verificarea capacității Alianței de pregătire și transport strategic rapid al forțelor nord-americane în scopul „întării apărării Europei"). Manevrele militare specifice exercițiului vor fi realizate în cadrul „unui scenariu de conflict simulat ce ar apărea cu un adversar de aproape același calibru" (Garamone 2024).

După finalizarea Noii Strategii Militare a NATO în anul 2019 și a conceptului asociat pentru *descurajarea și apărarea euroatlantică* în anul următor, a fost aprobat *Planul Strategic* (Strategic Plan) pentru întreaga arie de responsabilitate a Comandantului Suprem Aliat pentru Europa (SACEUR). Acesta reprezintă *un plan militar unic* pentru utilizarea forțelor Alianței atât în interiorul, cât și în afara zonei NATO, având în vedere ambele amenințări majore: Rusia și grupurile teroriste. Detaliile fundamentale privind modul de abordare a amenințărilor specifice au fost apoi completate cu planuri regionale și subordonate detaliate. Așadar, în cadrul Summitului de la Vilnius au fost aprobate *planurile regionale (regional plans)* – deținute de către cele trei comandamente de forțe joint (Joint Force Commands) –, precum și cele *șapte planuri strategice (the seven strategic plans) aflate la dispoziția comandanților de domenii funcționale*. Comandamentele NATO amintite acoperă în totalitate zona de responsabilitate a SACEUR (Area of Responsibility – AOR), adică zonele (cu comandamentele joint): nordică și atlantică (la Norfolk – Virginia); centrală – cu statele baltice până la Alpi (la Brunssum – Olanda); sud-estică (inclusiv Marea Mediterană și Marea Neagră (la Napoli – Italia) (LSE IDEAS 2023).

Concluzii

Amenințările A2/AD (Anti-Access/Area Denial) evoluate în mediile strategic emergente din Europa, Orientul Mijlociu și Asia-Pacific au determinat SUA și NATO ca forțele joint aliate să devină suficient de rezistente la orice atac advers prin generarea puterii de luptă necesare și reziliente, în scopul atingerii obiectivelor operaționale la nivelurile tactic, joint și strategic. Opțiunile adecvate proiectării și realizării unei rezilienţe operaționale corespunzătoare de către o forță joint multinațională a Alianței necesită o analiză pertinentă a interacțiunilor la nivel de teatru dintre atacurile potențiale ale adversarului și acțiunile proprii de contracarare oportună, eficace și eficientă a acestora.

Sub aspect societal, reziliența reprezintă, în cadrul Alianței, abilitatea unei societăți de a rezista și de a se recupera după șocuri, precum dezastre naturale, eșecuri ale infrastructurii critice sau atacuri hibride ori armate. De aici, rezultă, mai întâi, două aspecte cheie ale rezilienței, respectiv capacitatea de absorbire și revenire dintr-o stare de criză. Apoi, actorii reziliențI trebuie să fie capabili să răspundă la o gamă de șocuri potențiale, fie anticipate, fie neașteptate, și să aibă capacitatea de a supraviețui.

Din punct de vedere operațional, reziliența reprezintă capabilitatea de absorbire a șocurilor la nivelurile strategic, operativ și tactic prin reducerea riscurilor, ceea ce necesită un management adecvat. Pentru orice organizație militară din cadrul NATO, este importantă implementarea rezilienței operaționale prin adoptarea unui cadru funcțional adecvat care să cuprindă etapele critice ale anticipării, detectării, descurajării, rezistenței, răspunsului și recuperării. Fiecare dintre aceste elemente trebuie susținut de proceduri bine fundamentate, pentru a fi consolidată, astfel, capacitatea oricărei structuri operaționale cu statut național și/sau multinațional de a face față provocărilor și/sau amenințărilor.

La nivelul Alianței, reziliența nu reprezintă doar un termen modern, ci un obiectiv esențial, a cărui implementare generează flexibilitate, adaptabilitate și rezistență. Aceasta necesită proceduri de încorporare a rezilienței stratificate, prin componentele operațională (militară) și civilă, în cadrul acțiunilor complexe de dislocare și de angajare a forțelor statelor membre ale NATO în operații joint cu statut național și multinațional pentru apărarea teritoriului Alianței.

În final, rolul rezilienței în cadrul NATO este dat de importanța ei majoră pentru atingerea obiectivelor de securitate și eficiență a organizației în vederea contracarării în orice moment a oricăror amenințări, transformate tot mai mult sub aspectele complexității și diversificării. În aceste condiții, Alianța va deveni tot mai pregătită, adaptată continuu, întărită colaborativ și capabilă să gestioneze eficient riscurile, astfel încât să poată asigura condițiile de stabilitate și securitate în cadrul unui mediu dinamic internațional de securitate, devenit tot mai imprevizibil.

Referințe

Dowd, Anna, Dominik P. Jankowski, și Cynthia Cook. 2023. ”European Warfighting Resilience and NATO Race of Logistics: Ensuring That Europe Has the Fuel It Needs to Fight the Next War.” https://www.csis.org/analysis/european-warfighting-resilience-and-nato-race-logistics-ensuring-europe-has-fuel-it-needs.

Dowd, Anna, și Cynthia Cook. 2022. ”Bolstering Collective Resilience in Europe.” https://www.csis.org/analysis/bolstering-collective-resilience-europe.

E-ARC [Centrul Euroatlantic pentru Reziliență]. 2023. „E-ARC participă la seminarul NATO din Polonia privind reziliența stratificată”. https://e-arc.ro/tag/layered-resilience/.

Felstead, Peter. 2024. ”Steadfast Defender 24’, NATO’s largest exercise since the Cold War, kicks off.” https://euro-sd.com/2024/01/major-news/36158/steadfast-defender-kicks-off/.

Garamone, Jim. 2024. “NATO Begins Largest Exercise Since Cold War.” https://www.defense.gov/News/News-Stories/Article/Article/3656703/nato-begins-largest-exercise-since-cold-war/.

Hagen, Jeff, Forrest E. Morgan, Jacob L. Heim, și Matthew Carroll. 2016. *The Foundations of Operational Resilience-Assessing the Ability to Operate in an Anti-Access/Area Denial (A2/AD) Environment.* Santa Monica, California: RAND Corporation.

Herrera, G. James. 2021. “Military Installation Resilience: What Does It Mean?” https://apps.dtic.mil/sti/pdfs/AD1147490.pdf.

LSE IDEAS. 2023. “NATO’s 2022 Strategic Concept: One Year On.” https://www.lse.ac.uk/ideas/Assets/Documents/updates/2023-SU-NATO-OneYearOn.pdf.

Minculete, Gheorghe. 2023. *Determinări relaționale privind modernizarea logisticii operaționale.* Sibiu: Editura Techno Media.

NATO. 2010. “Active Engagement, Modern Defence – Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation adopted by Heads of State and Government in Lisbon.” https://www.nato.int/cps/en/natohq/official_texts_68580.htm.

—. 2021. ”Strengthened Resilience Commitment. paragraph 4.” https://www.nato.int/cps/en/natohq/official_texts_185340.htm.

—. 2023a. “NATO and European Union launch task force on resilience of critical infrastructure.” https://www.nato.int/cps/en/natohq/news_212874.htm.

—. 2023b. ”NATO’s military presence in the east of the Alliance.” https://www.nato.int/cps/en/natohq/topics_136388.htm.

—. 2023c. ”Resilience, civil preparedness and Article 3.” https://www.nato.int/cps/en/natohq/topics_132722.htm.

—. 2023d. “Vilnius Summit Communiqué.” https://www.nato.int/cps/en/natolive/official_texts_217320.htm?selectedLocale=en.

—. 2024. ”NATO Exercise Steadfast Defender 2024.” https://ac.nato.int/archive/2024/nato-exercise-steadfast-defender-2024.

NATO-ACT. 2022. "NATO Resilience Symposium." https://www.act.nato.int/wp-content/uploads/2023/05/20221018_resilience_symposium_report-1.pdf.

—. 2023a. "Adaptable Strategy: NATO Warfighting Capstone Concept's 20-Year Vision for NATO and Allied Forces." https://www.act.nato.int/article/nwccs-20year-vision-for-nato/.

—. 2023b. "Allied Command Transformation Enhances NATO's Logistics and Sustainment Supply Chains." https://www.act.nato.int/article/act-enhances-natos-logistics-sustainment-supply-chains/.

—. 2023c. "Resilience and Civil Preparedness in NATO." https://www.act.nato.int/article/resilience-and-civil-preparedness-in-nato/.

—. 2024. "NATO's Steadfast Defender 2024: Unprecedented Military Exercise Signals Alliance Unity and Preparedness." https://www.act.nato.int/article/steadfast-defender-2024-signals-alliance-unity-and-preparedness/.

Reuters. 2024. "NATO to hold biggest drills since Cold War with 90,000 troops." https://www.reuters.com/world/europe/nato-kick-off-biggest-drills-decades-with-some-90000-troops-2024-01-18/.

Roepke, Wolf-Diether și Hasit Thankey. 2019. "Resilience: the first line of defence." *NATO REVIEW.* https://www.nato.int/docu/review/articles/2019/02/27/resilience-the-first-line-of-defence/index.html.

Ryczynski, J. și A.A. Tubis. 2021. "Tactical Risk Assessment Method for Resilient Fuel Supply Chains for a Military Peacekeeping Operation." *Energies* 14(15) (15): 4679. https://doi.org/10.3390/en14154679.

van Mill, Jeroen (Lieutenant Colonel). 2023. "The Future of NATO's Resilience. Concepts and Wargaming." *The Three Swords* (39). https://www.jwc.nato.int/application/files/9616/9804/8578/RESILIENCE.pdf.

Wheeler, Gerhard. 2021. "Operational Resilience: Applying The Lessons of War." https://nationalpreparednesscommission.uk/wp-content/uploads/2021/05/Operational-Resilience-Applying-the-Lessons-of-War.pdf.

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

Teoria complexului regional de securitate – studiu de caz, statele riverane Mării Negre

The theory of the regional security complex — Case study, the riparian states of the Black Sea

Mrd. Adrian GHENADE*
Drd. Elena ONU**
*Academia Națională de Informații Mihai Viteazul, București, România
**Școala Națională de Științe Politice și Administrative, București, România

Abstract

Cunoscută în Antichitate sub denumirea de Pontus Euxinus, Marea Neagră a reprezentat, din cele mai vechi timpuri, puntea de legătură dintre civilizația europeană și civilizația orientală. Posesoarea unui mozaic multivariat de culturi, zona Mării Negre a facilitat, de-a lungul secolelor, atât dezvoltarea relațiilor comerciale și politice, cât și declanșarea și întreținerea de conflicte, fiind precum Sabia lui Damocles. Situată la intersecția a trei zone de securitate (euroatlantică, rusă și orientală), Marea Neagră constituie, în prezent, un spațiu vulnerabil în materie de securitate. Moștenitoarea unei culturi bizantine, majoritatea statelor riverane prezintă o politică internă și externă alambicată, fiind prinse între idealismul lumii occidentale și realismul spațiului estic european. Totodată, revizionismul Federației Ruse și cel al Turciei în materie de politică externă va însemna și o schimbare a dinamicii relațiilor dintre statele riverane Mării Negre, care s-ar putea solda fie cu revenirea acesteia la statutul de lac rusesc, fie cu o împărțire a sferelor de influență între Federația Rusă și Turcia. În acest sens, pentru a analiza viitoarea dinamică a securității statelor riverane, am utilizat teoria complexului regional de securitate, pe care o considerăm foarte potrivită în studiul nostru pentru regiunea Mării Negre.

Known in Antiquity as the Pontus Euxinus, the Black Sea has been the bridge between European and Eastern civilizations since ancient times. Possessing a multi-varied mosaic of cultures, the Black Sea area has facilitated over the centuries, both the development of commercial and political relations and the maintenance and production of conflicts, being like the Sword of Damocles. Located at the intersection of three security zones (Euro-Atlantic, Russian, and Eastern), the Black Sea is currently a vulnerable space in terms of security. Heir to Byzantine culture, most of the riparian states have a complicated internal and external policy, being caught between the idealism of the Western world and the realism of the Eastern European space. At the same time, the revisionism of the Russian Federation and Turkey in terms of foreign policy will also mean a change in the dynamics of the relations between the states bordering the Black Sea, which could result either in its return to the status of a Russian lake or in a division of the spheres of influence between the Russian Federation and Turkey. In this sense, in order to analyze the future security dynamics of the riparian states, we used the theory of the regional security complex, which we consider very appropriate in our study of the Black Sea region.

Cuvinte-cheie:
Marea Neagră; teoria complexului de securitate; poststructuralism; Școala de la Copenhaga; NATO; securitate.

Keywords:
Black Sea; security complex theory; poststructuralism; Copenhagen School; NATO; security.

Info articol
Primit: 9 februarie 2024; Evaluat: 29 februarie 2024; Acceptat: 18 martie 2024; Disponibil online: 5 aprilie 2024

Citare: Ghenade, A și E. Onu. 2024. „Teoria complexului regional de securitate – studiu de caz, statele riverane Mării Negre”. *Buletinul Universității Naționale de Apărare „Carol I”*, 13(1): 117-130. https://doi.org/10.53477/2065-8281-24-08

Naşterea abordării complexului regional de securitate

Contextul perioadei anilor 80'- 90'este marcat de o schimbare de paradigmă în privința abordării și înțelegirii studiului relațiilor internaționale și relațiilor de securitate.
Noul curent de gândire nu este într-o antiteză totală cu curentul tradiționalist, venind mai mult ca o completare a acestuia. Astfel, dacă curentul de gândire tradiționalist asocia problemele militare (hard power) ca reprezentând singura amenințare reală pentru supraviețuirea statelor, curentul de gândire nontradiționalist va considera că problemele de securitate sunt de natură militară, economică, socială, societală și ecologică. În acest sens, nontradiționaliștii oferă un nivel de analiză inclusiv la nivelul societății, și chiar al indivizilor, și nu doar la nivelul statelor. Abordarea este în deplină concordanță cu noua realitate caracteristică sfârșitului Războiului Rece, fiind marcată de curentul neoliberalist și idealist, în care accentul va fi pus mai mult pe individ decât pe stat. De asemenea, nontradiționaliștii vor analiza securitatea pe nivel, acesta fiind național, regional, internațional/global/sistemic.

Unul dintre principalii gânditori ai noului curent nontradiționalist și, totodată, pionierul noului curent este Barry Buzan, profesor britanic de științe politice la LSE. În lucrarea *People, States and Fear: National Security Problem in International Relations,* din 1983, critică concepția tradițională în materie de securitate, ajungând să formuleze principalele elemente ale viitoarei abordări a Școlii de la Copenhaga, inclusiv ideea că statul și societatea sunt cele două obiecte referente ale securității. În cadrul acestei lucrări, Barry Buzan va enunța și un nou concept derivat de securitate, *complexul de securitate,* care va constitui o nouă înțelegere a relațiilor dintre state, în materie de securitate, la nivel regional.

Complexul de securitate reprezintă existența unui grup de țări cu caracteristici durabile, semnificative și intrinseci ale problemelor de securitate. În acest set de state, percepțiile majore de securitate sunt atât de interrelaționate, încât problemele lor de securitate naţională nu pot fi analizate și soluționate raţional, fără raportare la celelalte state. Dinamica formării și structura acestuia sunt determinate de statele din cadrul lui, mai exact de perspectivele statelor față de securitate și de interacțiunile dintre state. Complexul de securitate aparține curentului postmodernist, curent care pune accent, în primul rând, pe componenta socială în analiza securității, abordarea fiind una de natură multisectorială (Buzan 1983, 105-110).

Sistemul internațional este format din mai multe complexe de securitate, foarte multe dintre ele suprapunându-se sau intersectându-se între ele. Acestea pot să fie de mai multe tipuri: geografice, politice, strategice, istorice, economice și culturale, unele complexe de securitate putând să aibă mai multe caracteristici sau chiar pe toate.
În baza curentului postmodernist, analiza securității prin raportare la complexul de securitate se face la nivel regional, chiar dacă, din complex, fac, uneori, parte și state din afara regiunii.

Logica regiunilor de securitate se bazează pe faptul că securitatea internațională este o chestiune de relaționare. Securitatea internațională se referă la modul în care colectivitățile umane relaționează unele cu altele când vine vorba de amenințări și vulnerabilități, chiar dacă, uneori, se referă la modul în care aceste colectivități relaționează cu amenințările din partea mediului natural. Accentul asupra naturii relaționale a securității este în conformitate cu scrierile privind studiile de securitate, care au subliniat dinamicile relaționale, precum dilemele de securitate, echilibrul puterii, cursele înarmării și regimurile de securitate.

Pentru ca un grup de state să poată fi considerat complex de securitate, acesta trebuie să aibă un tipar teritorial distinctiv al interdependenței care să deosebească membrii unui complex de securitate de alte state vecine. Complexele regionale de securitate nu pot exista în două condiții: în unele zone, statele locale au atât de puține capacități încât puterea lor se proiectează puțin sau chiar deloc în afara propriilor granițe. Aceste state au perspective de securitate direcționate spre interior și între ele nu există o interacțiune de securitate suficient de mare pentru a genera un complex local. Prezența directă a puterilor externe este atât de mare încât suprimă dinamica de securitate dintre statele locale. Această stare se mai numește și acoperire (de exemplu, colonialismul, dinamica securității europene din timpul Războiului Rece, rivalitate SUA-URSS).
Pentru ca un grup de state să poată constitui un complex de securitate, este necesar ca acesta să îndeplinească următoarea structură, toate condițiile trebuind să fie întrunite cumulativ: 1) aranjarea unităților în același spațiu geografic și existența unor diferențe între ele; 2) existența unor tipare de amiciție sau inamiciție; 3) distribuirea puterii între principalele unități (Buzan 1983, 110-115).

La nivel conceptual, există două tipuri de complexe regionale: cele omogene (clasice, enunțate, pentru prima dată, în lucrarea *People, States and Fear: National Security Problem in International Relations,* din 1983, de Barry Buzan) și cele eterogene (care păstrează caracteristicile complexelor clasice, dar care sunt completate de spectrul economic, financiar, social, cultural, societal, fiind enunțate în lucrarea *Regions and Powers: The Structure of international Security*, din 2003, de Barry Buzan, în colaborare cu Ole Waever).

Teoria clasică a complexului de securitate

Rațiunea din spatele ei este că, pentru majoritatea actorilor de la nivelul unităților, securitatea politico-militară se încadrează în mănunchiuri de mărime medie, iar teoria cea mai relevantă este cea care se referă la nivelul regional. De asemenea, teoria clasică a complexelor de securitate afirmă existența subsistemelor regionale ca obiecte ale analizei de securitate și oferă un cadru analitic de lucru cu aceste sisteme. Teoria s-a concentrate, în primul rând, pe stat ca unitate cheie și pe sectoarele politic și militar. Toate statele din sistem sunt interconectate într-o țesătură de interdependență de securitate. Tiparul de interdependență într-un sistem

internațional divers din punct de vedere geografic, dar și anarhic, este bazat pe clustere regionale, pe care le numim complexe de securitate. Interdependența de securitate este evident mai intensă între statele din interiorul unor astfel de complexe decât între statele din afara lor. Complexele de securitate se referă la intensitatea relativă a relațiilor de securitate interstatale, care formează tipare regionale distincte, configurate atât de distribuția puterii, cât și de relațiile istorice de amiciție sau inamiciție.
Deoarece acestea sunt formate din grupări locale de state, complexele clasice de securitate nu au numai un rol central în relațiile dintre membrii lor; ele condiționează central, dacă este cazul, modul în care puterile externe penetrează regiunea.

Dinamica externă a complexelor de securitate poate fi localizată de-a lungul unui spectru, în funcție de ceea ce definește interdependența de securitate: amiciția sau inamiciția. La polul opus, se află formarea conflictelor, în care interdependența se naște din frică, din rivalitate și din percepția reciprocă de amenințare. La mijloc, se situează regimurile de securitate, în care statele se tratează reciproc ca potențiali dușmani, în care s-au încheiat acorduri de asigurare, cu scopul de a reduce dilema de securitate dintre ele. La polul pozitiv al spectrului, se află o comunitate pluralistă de securitate, în care statele nu mai așteaptă și nu se mai pregătesc de utilizarea forței în relațiile dintre ele. Integrarea regională va elimina un complex de securitate cu aceleași limite, transformându-l dintr-un subsistem anarhic de state într-un singur actor mai mare în cadrul sistemului. Integrarea regională a membrilor unui complex va transforma structura de putere a respectivului complex. Complexul de securitate este un produs al sistemului anarhic (Buzan 1983, 93-95).
Datorită faptului că dinamica de putere este foarte solidă, iar relațiile de amiciție/inamiciție se schimbă constant, există patru opțiuni structurale de evaluare a impactului asupra unui complex regional de securitate: menținerea statu-quoului, transformarea internațională, transformarea externă și acoperirea.
Teoria complexului regional de securitate poate fi utilizată pentru a genera scenarii definitive și pentru a structura studiul și predicțiile legate de posibilitățile de schimbare și stabilitate (Buzan 1983, 113-115).

După Războiul Rece, relațiile internaționale au dobândit un caracter mai regionalizat. Regiunile sunt un tip special de subsisteme. Hans Mourizen susține că statele sunt mai mult fixe decât mobile. La nivel de securitate, regiunile au următoarele caracteristici: sunt compuse din două sau mai multe state, acestea constituind un grup coerent din punct de vedere geografic, relațiile dintre state fiind marcate de interdependența din domeniul securității, care poate fi pozitivă sau negativă.

Marea Neagră – Teatru de operațiuni și al întâlnirii Rusia-NATO

Securitatea regională a Mării Negre și balanța geostrategică constituie factorii și premisele pentru conturarea unui posibil scenariu care ar implica existența unui nou Război Rece. Multitudinea de grupuri etnico-religioase, corelate cu existența

mai multor sfere de securitate, face extrem de dificilă delimitarea unor granițe fixe și stabile pentru regiunea Mării Negre. Astfel, folosind o terminologie specifică post-Război Rece, ne putem referi la regiunea Marea Neagră – Marea Caspică, respectiv la regiunea Marea Mediterană – Marea Neagră (Fiedler şi Stelmach 2018, 14). Această delimitare o considerăm esențială, în special datorită faptului că Regiunea Mării Negre constituie inclusiv o arie de securitate pentru NATO. Acest lucru este relefiat prin existența Sistemului de Apărare Antirachetă (denumire dată în mandatul Bush jr.), apărută, initial, sub denumirea de Inițiativa de Apărare Strategică (1983) (Negruț şi Neacșu 2022, 114).
Potrivit raportului privind revizuirea sistemului de apărare împotriva rachetelor balistice (Balistic Missile Defense Review Raport) al Departamentului american al Apărării (1 februarie 2010), se aveau în vedere patru faze pentru realizarea acestuia, dintre care, ulterior, au rămas doar trei.

Faza 1 constă în protejarea unor porțiuni ale Europei de Sud-Est, prin desfășurarea unui sistem radar înaintat.
Această fază a demarat, la 7 martie 2011, prin trimiterea, pe Marea Mediterană, a navei americane USS Monterey, echipată cu sistemul Aegis, respectiv prin operaționalizarea unui radar în sud-estul Turciei, la Kurecik.

Faza 2 (orizont de timp 2015) presupunea extinderea protecției aliaților NATO prin operaționalizarea unei noi generații de interceptori SM3-IB (care să poată fi lansați de la sol), amplasați într-o bază terestră, respectiv la Deveselu (jud.Olt).

Faza 3 (orizont de timp 2018) este reprezentată de extinderea acoperirii sistemului la toate statele membre ale NATO din Europa, prin introducerea în exploatare a unei noi versiuni a interceptorului SM3, care urmează a fi amplasat într-o bază terestră, în nordul Europei (Redzikowo, Polonia).

Faza 4 (orizont de timp 2020) a fost anulată în martie 2013. Inițial, aceasta presupunea extinderea protecției la eventuale atacuri cu rachete intercontinentale, inclusiv prin dezvoltarea în continuare a rachetelor SM3 și a sistemelor radar, cu amplasarea în Polonia a unei clase de interceptare. Anularea fazei a intervenit în contextul amenințărilor cu eventuale atacuri cu rachete balistice, la adresa SUA, din partea Coreei de Nord.

Dincolo de relația foarte bună pe care o au SUA, România a fost aleasă ca bază terestră din motive geostrategice: o țară de mărime medie, aflată la frontiera estică a structurilor euroatlantice, într-o zonă geografică din ce în ce mai vulnerabilă la amenințări cu rachete cu rază scurtă de acțiune. Din punct de vedere geostrategic și având în considerare componenta sudică a EPAA, România se află în cea mai bună poziție pentru a găzdui interceptori tereștri (Negruț și Neacșu 2022, 113-117).

De asemenea, NATO a identificat trei regiuni de o importanță deosebită pentru securitatea Alianței: Marea Baltică, Marea Neagră și Marea Egee (NATO 2023).

Potrivit noii perspective, zona sud-caucaziană a devenit linia roșie dintre NATO și Federația Rusă.
De cealaltă parte, Rusia identifică acțiunile NATO ca având un caracter ofensiv, contravenind în acest sens cu propria sa securitate. Potrivit revistei poloneze *New Eastern Europe*, împreună cu noua infanterie navală și cu Unitățile Forțelor Speciale, care sunt deja utilizate în operațiunile de tipul război hibrid, Rusia își va folosi propriile sale forțe care o vor ajuta în implementarea propriei sale agende politice în zonă (Petriashvili 2019). Acest lucru a fost concretizat și prin investițiile militare, făcute de Rusia, aceasta cheltuind, în perioada 2016-2020, potrivit Ministerului rus al Apărării, suma de 2,4 miliarde de dolari pentru arealul Mării Negre.

De asemenea, insecuritatea constituită de domeniul militar va fi completată de insecuritatea din partea amenințărilor hibride, acestea survenind pe axa economică Marea Neagră – Marea Caspică – Asia Centrală. Aceste amenințări hibride, reprezentate de terorism, trafic de arme, migrație ilegală au fost accentuate și de decizia Rusiei de a se retrage, în anul 2015, din cadrul Tratatului privind Forțele Convenționale din Europa (CFE Treaty), retragerea diplomatică fiind completată de agresiunea militară asupra Ucrainei, din 2022, fapt ce a transformat regiunea Mării Negre într-o zonă cu o puternică instabilitate politică, economică, socială și militară. Utilizând terminologia lui Nye, putem afirma că, în prezent, Marea Neagră constituie un teatru de operațiuni (Ney 1967).
În acest sens, considerăm că actuala confruntare Rusia – NATO din zona geografică a Mării Negre constituie un Război Rece la nivel global, actorii implicați în mod direct în cadrul acestuia, împreună cu aliații lor având capacitatea de a-l extinde și în alte arii geografice.

Teoria complexului de securitate – studiu de caz Marea Neagră după anexarea Peninsulei Crimeea de către Federația Rusă

La nivelul securității, regiunea Mării Negre este o zonă nesigură, aici suprapunându-se trei zone de securitate: europeană, euroasiatică și islamică, acest lucru determinând existența atât a unor relații de inamiciție, cât și a unor alianțe, bazate pe prietenie între statele riverane (Cojocaru 2014, 23).
Fiind un spațiu comercial încă din vremea Antichității, regiunea Mării Negre a constituit, în primul rând, un spațiu de tranzit pentru diferite popoare, fapt ce va marca pe deplin istoria acestei regiuni prin mozaicul multicultural și etnic creat. Privită în ansamblu, deși diversitatea unei regiuni înseamnă de cele mai multe ori o creștere a creativității și toleranței între populațiile din jur, pare că, în cazul regiunii Mării Negre, se aplică principiul sabiei lui Damocles, această regiune fiind, în aproape toată istoria ei, marcată de conflictele dintre statele riverane. De la războaiele ruso-otomane și până la actuala invazie a Ucrainei de către Rusia, zona Mării Negre a constituit, aproape tot timpul, o zonă instabilă politic și militar, fiind preferat războiul, în locul comerțului. Astfel, se poate explica faptul că, deși deține aproximativ între 70 și 200 de miliarde de barili de petrol (o cantitate mai mare decât

rezervele din Marea Nordului și din Alaska la un loc, ceea ce transformă regiunea în a doua zonă din lume din punctul de vedere al potențialului energetic, pentru Occident), regiunea Mării Negre, din cauza securității instabile, nu se bucură pe deplin de potențialul său economic (Cojocaru 2014, 25).

Astfel se naște întrebarea „*Ce determină această instabilitate a regiunii?*".
Un răspuns la această întrebare îl constituie faptul că statele riverane Mării Negre (Rusia, Turcia, Ucraina, România, Bulgaria și Georgia) se află într-un complex regional de securitate. După cum am spus mai sus, existența oricărui complex regional de securitate este determinată de îndeplinirea cumulativă a trei condiții, pe care statele riverane Mării Negre le îndeplinesc.

Aranjarea unităților în același spațiu geografic și existența unor diferențe între ele: statele din regiunea Mării Negre se află în aceeași arie geografică, fiind situate în regiunea estică a Europei, având ieșire directă la Marea Neagră. De asemenea, deși se află în aceeași proximitate geografică, la nivelul statelor, diferențele dintre ele sunt substanțiale în ceea ce privește cultura, etnia, limba și, în unele cazuri, chiar religia. Din cauza acestor diferențe substanțiale regăsite la nivelul statelor, fiecare țară riverană Mării Negre are un specific al său care o face total diferită de celelalte țări din jur, fiind greu de realizat o uniformizare în materie de specific zonal.

Existența unor tipare de amiciție sau inamiciție: regiunea Mării Negre a fost/este spațiul de ciocnire dintre ruși și turci. Încă de pe vremea lui Petru cel Mare, rușii au dorit transformarea Mării Negre într-un lac rusesc, singurul obstacol în realizarea acestui obiectiv fiind Imperiul Otoman. Astfel, de la 1683 și până în prezent, Rusia și Turcia și-au disputat constant influența asupra Mării Negre, o zonă geostrategică extrem de importantă pentru realizarea politicii externe expansioniste a ambelor puteri. De asemenea, un alt conflict a fost cel dintre România și Bulgaria. Ca urmare a Congresului de la Berlin din 1878, România obținea ieșirea la Marea Neagră, în urma cedării Dobrogei de către Bulgaria. Astfel, noua graniță dintre cele două tinere state va reprezenta un motiv de conflict îndelungat, ambele entități, până în anul 1945, aflându-se în tabere separate atât în cele două războaie balcanice, cât și în ambele războaie mondiale.

Totodată, chiar și atunci când în regiunea Mării Negre a existat un tipar de amiciție între state, în care cinci dintre cele șase state riverane erau parte a unei alianțe comune, Pactul de la Varșovia (URSS – Rusia, Ucraina și Georgia actuală –, România și Bulgaria), au existat neînțelegeri de natură teritorială, România cedând Ucrainei, în anul 1948, Insula Șerpilor, fapt ce a creat tensiuni în rândul aliaților. Deși, în anul 2009, Tribunalul de la Haga recunoștea României 79,34% din teritoriul insulei (restul revenind Ucrainei), ambele state au în continuare pretenții mult mai mari față de acest teritoriu, diferendele continuând inclusiv în prezent.

De asemenea, un alt tipar de inamiciție este cel dintre Rusia și Georgia. La începutul anului 2000, Rusia a adoptat un nou concept la nivelul politicii externe și al cadrului

geostrategic, declarându-se a fi o mare putere (Smith 2020, 7). De asemenea, prin adoptarea acestui concept, Rusia își va manifesta și primele semne de revizionism, sugerând că intervenția în conflictele înghețate postsovietice (atât în cele din zona Mării Negre, cât și în cele din zonele limitrofe) este justificată, în concordanță cu statutul său. Acest lucru a dus la primele tendințe de revizionism din partea Rusiei. În anul 2004, Georgia, prin poziția sa geografică la Marea Neagră, reprezenta o nouă poartă de acces a petrolului din Marea Neagră, permițând instalarea de conducte care puteau ocoli Federația Rusă. La rațiunile economice, putem adăuga și dorința Georgiei de a fi parte a Uniunii Europene și NATO, organizații care i-ar fi permis o detașare substanțială de statutul său de fostă republică socialist sovietică. Prin urmare, în anul 2008, Rusia va interveni direct în războiul din Georgia, Abhazia și Osetia de Sud, declarându-și independența, act care, în prezent, este recunoscut la nivel internațional doar de Federația Rusă (Cojocaru 2014, 110-112), Nicaragua și Siria (Curtifan 2018).
Deși toate conflictele din trecut au avut o influență substanțială asupra regiunii Mării Negre, conflictul dintre Rusia și Ucraina a avut cu adevărat cel mai mare impact asupra regiunii. Vom aborda acest conflict ulterior, întrucât în cadrul acestui eseu, îi voi acorda o secțiune specială.

Distribuirea puterii între principalele unități: Fiecare țară riverană Mării Negre are un cuvânt de spus în privința politicilor de securitate din zonă. Totuși, în legătură cu distribuirea puterii, în prezent, Marea Neagră cunoaște doi actori principali – Rusia și Turcia, cărora li s-a alăturat, mai nou, și Ucraina. În acest sens, putem opina faptul că Rusia deține, în momentul de față, detașat avantajul componentei *hard power*, prin capabilitățile militare de care dispune în zonă, fapt dovedit și de politica agresivă pe care constant o practică. Turcia, datorită controlului asupra celor două strâmtori (Bosfor și Dardanele), esențiale pentru legătura cu Marea Mediterană, deține, astfel implicit, și principala zona economică și comercială a Mării Negre, fapt ce îi conferă un avantaj mult mai complex în fața Rusiei, fiind mai puternică în privința componentei smart, Turcia având posibilitatea de a îmbina componenta economică cu cea militară. De cealaltă parte, Ucraina, până la conflictul din Crimeea, deținea avantajul soft al regiunii Mării Negre, cele mai multe companii petroliere cu capital străin aflându-se în zona comercială a Ucrainei, fiind, totodată, și cea mai atractivă zonă de investiții externe. Un exemplu relevant în acest sens este reprezentat de compania Skifska, deținută de corporația britanico-olandeză Royal Dutch Shell, care, în 2012, a obținut dreptul de forare petrolieră, începând cu anul 2015 (din păcate, inițiativa va fi abandonată, ca urmare a războiului din Crimeea). De asemenea, până la anexarea Crimeii de către Federația Rusă, Ucraina deținea avantajul de a avea cel mai mare port la Marea Neagră, Sevastopol fiind atât cel mai mare port, cât și cel mai bine poziționat din punct de vedere strategic, fiind o punte de legătură cu Marea Mediterană, cu Marea Azov, cu zona Maghrebului și chiar cu Orientul Mijlociu (Cojocaru 2014, 74-75).

Astfel, putem remarca faptul că, la nivelul regiunii Mării Negre, împărțirea puterii era relativ echilibrată, neexistând un actor care să îi domine pe toți ceilalți. De

asemenea, observăm că toate condițiile necesare existenței unui complex regional de securitate în zona Mării Negre erau îndeplinite simultan, fapt ce demonstrează existența unui astfel de complex.

Mai mult, folosind metoda contraexemplului, remarcăm că inclusiv cele două limitări care nu ar fi permis formarea unui complex de securitate (incapacitatea statelor de a-și proiecta puterea în afara propriilor granițe, respectiv existența unei puteri externe atât de mari încât să suprime dinamica securității dintre statele locale) nu sunt posibile pentru regiunea Mării Negre. În primul rând, regiunea dispune de actori capabili să își proiecteze puterea în afara granițelor. Luând din nou cazul Federației Ruse, putem observa că, prin conceptul de Mare Putere, utilizat în politica sa externă, aceasta este capabilă să își proiecteze capacitățile militare în afara propriilor sale granițe, în acest sens întreținând o serie de conflicte înghețate în fostele sale state satelit, dar și în afara continentului european (războiul din Siria, anul 2015). De asemenea, în anul 2015, Rusia va adopta o nouă doctrină navală, care va oferi Mării Negre o însemnată tactică atât la nivel defensiv, cât și la nivel ofensiv, respectiv economic. La nivel defensiv, Doctrina Navală privea Marea Neagră drept un mijloc esențial de blocare a extinderii NATO și a desfășurării capacităților militare în apropierea granițelor Rusiei (Davis 2015, 10-11). Prin anexarea Crimeii (denumită și un portavion al Mării Negre), la nivel ofensiv, Rusia a reușit să obțină controlul și influența căilor de comunicație de pe întreg acvariul Mării Negre, de la est la vest. Poziția extrem de bună a Crimeii la nivel geopolitic si geostrategic a permis trimiterea de trupe rusești în cadrul conflagrației din Siria, demonstrând capacitatea Rusiei de a crea presiuni pe flancul sudic al NATO, Africa de Nord, Orientul Mijlociu, dar și o cale de acces secundară către Oceanul Planetar. Un alt stat riveran care dispune de capacitatea de a-și proiecta puterea în afara granițelor este Turcia, care constituie a doua armată NATO, ca mărime (Dinu 2020, 7-9).

De asemenea, pentru regiunea Mării Negre, nu există o putere externă atât de mare încât să poată suprima dinamica securității dintre statele locale. Deși am fi tentați să afirmăm faptul că NATO (și, implicit, Statele Unite) reprezintă un factor care poate limita definitiv dinamica securității din rândul statelor riverane, acest lucru nu s-a întâmplat în totalitate.

Deși trei dintre cele șase state riverane sunt membre ale NATO, iar două state au vederi prooccidentale (Ucraina și Georgia), NATO și, implicit, SUA dispun de capacități militare limitate pentru desfășurarea unei acțiuni în această regiune. Cu toate că, la data de 16 martie 2023, președintele Comisiei Permanente Selectate pentru Informații a Camerei Reprezentanților, Mike Turner, împreună cu congresmanul Bill Keating, membru de rang înalt al Subcomisiei pentru Afaceri Externe a Camerei Reprezentanților pentru Europa, au introdus, spre aprobare, Legea pentru Securitatea Mării Negre, care are drept scop oprirea extinderii conflictelor la nivelul Mării Negre, fiind percepute drept o chestiune de securitate pentru Statele Unite, acest lucru cunoaște limitări substanțiale de natură juridică (The Senate of the United States 2023).

Potrivit Convenției de la Montreux din 1936, navele de război ale statelor care nu au ieșire directă la Marea Neagră, nu trebuie să aibă un tonaj care să depășească 15.000 de tone, acestora nefiindu-le permis să rămână mai mult de 21 de zile în apele mării. În aceste condiții, cu Rusia și Turcia drept actori dominanți, este aproape imposibil, pentru o putere externă, să modifice radical dinamica dintre statele riverane mai bine decât un stat riveran (Britannica 1936).
Astfel, indiferent de tipul de alianță politico-militară în care se regăsesc statele din jurul Mării Negre, principala putere deținută în regiune va fi proiectată doar de către statele riverane.

Complexul de securitate din Marea Neagră, ca urmare a conflictului din Marea Neagră

Așa după cum am demonstrat cu argumentele anterioare, regiunea Mării Negre constituie și facilitează existența unui complex de securitate. În prezent, Rusia reprezintă principalul actor din zonă care menține constant relații de inamiciție cu restul statelor riverane, cel mai proaspăt conflict fiind cel avut cu Ucraina.
Rusia și Ucraina împărtășesc o istorie milenară, relația dintre cele două state fiind marcată de conflicte și alianțe constante. La nivel de elemente comune pentru cele două popoare, putem observa că acestea prezintă o geneză comună la nivel geografic (Kievul fiind orașul de „naștere" al ambelor regate), au fost, vreme de aproape 70 de ani, parte a aceleiași unități politice (URSS) și au avut creștinismul de rit ortodox drept element identitar comun. Însă, în ciuda asemănărilor, de-a lungul istoriei, cele două țări par să fi împărtășit mai multe divergențe decât amiciții. În acest sens, putem aminti faptul că Ucraina a fost parte a Marelui Ducat al Lituaniei (Uniunea Polonă Lituaniană), un regat care a avut, de-a lungul timpului, conflicte directe atât cu Rusia Țaristă, cât și cu Rusia Imperială. Faptul că Ucraina a fost parte din Uniunea Polono-Lituaniană se va regăsi inclusiv în caracterul naționalist al ucrainenilor, ei considerându-se un popor diferit de ruși. La nivel cultural, se remarcă, de asemenea, diferențe substanțiale între cele două popoare, tradițiile și valorile fiind destul de diferite.
Astfel, putem observa că ambele popoare au o identitate națională suficient de diferită, permițându-le astfel, teoretic, să evolueze pe direcții separate din punct de vedere politic, economic și social.

Ca urmare a destrămării URSS în 1991, Rusia și Ucraina vor redeveni două entități separate la nivel politic, economic și social care vor căuta să își formeze o politică proprie atât la nivel intern, cât și extern.
La nivel de securitate, în ultima decadă a secolului XX, regiunea Mării Negre a fost extrem de stabilă, cu excepția Tansnistriei, niciun conflict neavând loc, relațiile dintre state fiind doar de natură economică.

Primul semn relevant pentru o dorință de schimbare a Ucrainei și o desprindere de sub influența statelor din CSI a venit în 2004, în timpul Revoluției Portocalii, când mii de ucraineni au mărșăluit pentru o mai bună integrare în Europa. Alt moment

în care s-a observat o distanțare tot mai mare a Ucrainei față de Federația Rusă a fost Summitul NATO de la București, din 2008, când Ucraina a transmis comunității internaționale dorința clară de a se alătura NATO. Toate aceste acțiuni vor culmina în 2014 cu primul conflict armat, după aproape un secol, între cele două țări, odată cu anexarea de către Rusia a Peninsulei Crimeea. La nivelul complexului de securitate, anexarea Crimeii de către Rusia a marcat o renunțare la statu-quoul din cadrul regiunii vechi de aproximativ 70 de ani. De asemenea, prin anexarea Crimeii, Rusia și-a mărit considerabil avantajul tactic și geostrategic în regiune, întrucât astfel a reușit să obțină controlul și influența asupra căilor de comunicație de pe întreg acvariul Mării Negre, de la est la vest. Poziția extrem de bună a Crimeii la nivel geopolitic si geostrategic a permis trimiterea de trupe rusești în cadrul conflagrației din Siria, demonstrând capacitatea Rusiei de a crea presiuni pe flancul sudic al NATO, Africa de Nord, Orientul Mijlociu, dar și o cale de acces secundară către Oceanul Planetar.

Astfel, prin anexarea Crimeii, Rusia a reușit să transforme, la nivel extern, complexul de securitate al Mării Negre, prin modificarea structurii sale (Dinu 2020, 10-11). Mergând până în prezent, putem observa că războiul din Ucraina a modificat din nou dinamica actualului complex regional de securitate al Mării Negre.

Deși în regiune sunt adversari tradiționali, Rusia și Turcia par că, în prezent, sunt dornice mai mult să evite un conflict una cu cealaltă decât să înceapă unul. De asemenea, agresiunea din Ucraina determină o apropiere a României și Bulgariei una față de cealaltă, regiunea lor de securitate fiind, de altfel, și spectrul de securitate al NATO și al Uniunii Europene. Însă, după cum am spus mai sus, capabilitățile militare ale NATO pentru spațiul Mării Negre sunt limitate prin prevederile Convenției de la Montreux, fapt ce produce o vulnerabilitate în materie de securitate, în eventualitatea degenerării ulterioare a conflictului.

De asemenea, o altă zonă sensibilă în cadrul actualului context o constituie Georgia, care, după ce a avut de suferit, ca urmare a separatismului din anul 2008, în prezent, are multiple vulnerabilități, în condițiile unei posibile escaladări a conflictului, fiind o potențială victimă directă a unui eventual revizionism rusesc (Osetia de Sud și Abhazia). În acest sens, o grijă față de securitatea națională a Georgiei a fost deja manifestată de NATO, România, alături de Marea Britanie, deținând mandatul de ambasadă Punct de Contact NATO în Georgia, pentru o perioadă de doi ani. Faptul că o țară riverană Mării Negre are un asemenea mandat în actualul conflict într-o altă țară manifestă îngrijorare față de o generare ulterioară a acestui conflict.

La nivelul actualului război din Ucraina, Kievul a încercat să își consolideze principalele artere strategice de la Marea Neagră. În acest sens, a urmărit să apere portul Odesa, printr-un amplu proces de derusificare. Totodată, încă de la începutul conflictului, Ucraina a scufundat nava Moscova – una dintre principalele nave de război ale Rusiei –, reușind să câștige, de asemenea, un avantaj tactic însemnat în cadrul acestui conflict.

După cum am spus și la început, teoria complexului de securitate poate fi utilizată inclusiv pentru generarea de scenarii pentru anumite conflicte. În acest sens, consider că, în cazul principalilor doi beligeranți, Rusia și Ucraina, rolul Mării Negre capătă o dublă semnificație, întrucât pentru Rusia, înseamnă hegemonie, în vreme ce pentru Ucraina, înseamnă supraviețuire. Mulți experți consideră că oricine controlează sau domină Marea Neagră poate proiecta cu ușurință putere asupra continentului european, în principal în Balcani și în Europa Centrală, dar și în estul Mediteranei, în Caucazul de Sud și în nordul Orientului Mijlociu.
Astfel, o eventuală victorie a Rusiei în conflict îi va oferi posibilitatea de a avea șanse tot mai mari de a transforma Marea Neagră într-un „lac rusesc", fapt ce i-ar permite să revină inclusiv la ambiția de pe vremea lui Petru cel Mare, de a avea acces la Marea Mediterană, având posibilitatea reală de a modifica Regimul Strâmtorilor, impunându-și astfel dominația totală asupra Mării Negre.

Pe de altă parte, o potențială victorie a Ucrainei ar marca, probabil, o revenire la statu-quoul specific regiunii, prin restabilirea aceloraşi sfere de influență anteconflict. De asemenea, o potențială aderare a Ucrainei la NATO ar marca o creștere a influenței Alianței Nord-Atlantice în regiune, fapt ce ar permite, probabil, și o modificare a prevederilor Convenției de la Montreux.

Așa după cum am spus și la începutul lucrării, în regiunea Mării Negre se întrepătrund trei arii de securitate: europeană, euroasiatică și islamică. La momentul actual, Turcia este singura țară care este străbătută de toate aceste demarcații, fiind actorul *smart power* din această regiune. Realegerea lui Recep Erdogan ca președinte va însemna o reluare a politicilor sale neootomaniste, fapt evidențiat și de dorința acestuia de a face din Turcia un jucător important în Orientul Mijlociu și, implicit, în lumea islamică.
Un rol important în acest scenariu îl va juca și actuala „redobândire" a Nagorno-Karabakh de către Azerbaidjan, un partener tradițional al Turciei. Astfel, complexul regional de securitate ar fi extins, inclusiv către zona Orientului Apropriat, fapt ce ar determina lărgirea sa și includerea de noi actori.

Mai mult, slăbirea de către Rusia a sprijinului acordat Armeniei va face ca Erevanul să caute în altă parte alianțe de securitate, inclusiv în SUA, Franța, India și Georgia, dar și reanalizarea continuării participării la Organizația Tratatului de Securitate Colectivă (OTSC), aflată sub influența Moscovei.
Deși Rusia are două baze militare în Armenia care sunt desemnate să se ocupe de sectorul extern sudic sau din Caucaz și de împrejurimile acestuia, iar prim-ministrul armean, Nikol Pashinyan, a permis Rusiei să-și extindă influența militară în regiunea sa, în ciuda rolului Moscovei în Nagorno-Karabah, o eventuală reorientare a Armeniei către SUA ar duce la aderarea acestei țări la subcomplexul de securitate Georgia-Ucraina.
Acest fapt ar crește vulnerabilitatea în materie de securitate a tuturor statelor riverane, mărind, totodată, dinamica relațiilor dintre acestea. Consider că acest scenariu ar fi posibil, în eventualitatea slăbirii enorme a Rusiei și Ucrainei, din cauza

acestui conflict, urmată de o posibilă implozie a Rusiei și de împărțirea sa în mai multe state, respectiv zone de influență, precum și de Ucrainăcare, postrăzboi, nu ar beneficia de o reconstrucție și nu ar fi primită în Uniunea Europeană sau în NATO.

Concluzii

Putem afirma că teoria complexului regional de securitate este un instrument util pentru realitățile geopolitice și geostrategice ale secolului XXI, aceasta ajutându-ne să observăm modul în care se formează și se desfășoară conflictele din diferite regiuni geografice ale lumii, fiind una dintre teoriile care ne oferă și oportunitatea de a putea genera anumite scenarii privind evoluția ulterioară a acestora.

De asemenea, deși a fost elaborată în secolul anterior și îmbunătățită în anul 2003, aceasta este în continuare una de actualitate prin prisma faptului că pune accentul inclusiv pe componenta socială, dar și pe sectoarele financiar, economic și societal, fiind o teorie extrem de complexă. În baza analizei realizate mai sus, putem remarca faptul că teoria respectă noua realitate a sistemului internațional post Război Rece prin prisma faptului că regiunile constituie, în prezent, principala dinamică în materie de amiciție/conflict, dovadă fiind majoritatea conflictelor derulate. Astfel, în baza ei, putem identifica acele zone de pe glob care prezintă caracteristicile necesare constituirii unui complex regional de securitate, astfel putând crea anumite blocuri comerciale și economice care să ajute la dezvoltarea anumitor regiuni și, implicit, la consolidarea securității, sau putem identifica acele regiuni care prezintă riscul generării unui potențial conflict regional care să prezinte anumite consecințe, concretizate în pierderi de vieți omenești și materiale, cu scopul de a-l diminua sau poate chiar de a-l evita.

Referințe

Britannica. 1936. "Montreux Convention." https://www.britannica.com/event/Montreux-Convention.

Buzan, Barry. 1983. *People, States and Fear: National Security Problem in International Relations.* Marea Britanie: Wheatsheaf books Ltd.

Cojocaru, Marius George. 2014. *NATO și Marea Neagră.* Târgoviște: Cetatea de Scaun.

Curtifan, Tudor. 2018. „Abhazia și Osetia de Sud, recunoscute de Siria. Georgia, replică imediată." https://www.defenseromania.ro/abhazia-i-osetia-de-sud-recunoscute-de-siria-georgia-replica-imediata_591759.html#google_vignette.

Davis, Anna. 2015. "The 2015 Maritime Doctrine of the Russian Federation." *U.S. Naval War College Digital Commons*, 10-11.

Dinu, Leonardo. 2020. "The Crimean Aircraft Carrier. Russian federation militarization of the black sea." https://www.newstrategycenter.ro/wp-content/uploads/2019/11/FLANKS-Policy-Brief-The-Crimean-Aircraft-Carrier.-Russian-Federation-Militarization-of-the-Black-Sea.pdf.

Fiedler, Radoslaw și Andrezej Stelmach. 2018. *Beyond Europe: Politics and Change in Global and Regional Affairs.* Berlin: Logos Verlag Berlin.

NATO. 2023. "Deterrence and defence". https://www.nato.int/cps/en/natohq/topics_133127.htm.

Negruț, Silviu și Marius-Cristian Neacșu. 2022. *Geostrategia.* București: METEOR PRESS.

Ney, Virgil. 1967. "Evolution of a theater of operations headquarters, 1941-1967." https://apps.dtic.mil/sti/pdfs/AD0675414.pdf.

Petriashvili, Sophia. 2019. "The shift of dominance in the Black Sea." *New Eastern Europe.*

Smith, M.A. Dr. 2020. *Russian Foreign Policy 2000: The Near Abroad.* Camberley, Anglia: The Conflict Studies Research Centre.

The Senate of the United States. 2023. "S.804 - Black Sea Security Act of 2023." https://www.congress.gov/bill/118th-congress/senate-bill/804/text.

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

Durata de folosință a construcțiilor militare din patrimoniul Ministerului Apărării Naționale: între eficiență și adaptabilitate

The service life of military constructions from the heritage of the Romanian Ministry of National Defense: between efficiency and adaptability

Căpitan arhitect drd. Adina SEGAL*
*Direcția domenii și infrastructuri, Ministerul Apărării Naționale;
Universitatea de arhitectură și urbanism Ion Mincu, București

Abstract

Infrastructura militară din România a suferit transformări semnificative de-a lungul timpului. Perioadele de expansiune și de modernizare au alternat cu momentele de restrângere și, uneori, cu trecerea unor cazărmi în administrare civilă. Aceste schimbări reflectă nu doar evoluțiile tehnologice, ci și adaptarea la cerințele dinamice ale apărării naționale.
Regulamentele de infrastructuri din 2008 leagă durata de folosință a facilităților militare direct de activitatea militară, subliniind nevoia de infrastructură flexibilă și adaptabilă. În acest context, articolul analizează cadrul legislativ privind amortizarea investițiilor, uzura construcțiilor și autorizarea lucrărilor, evidențiind importanța corelării reglementărilor militare cu cele civile.
În concluzii, se analizează discrepanțele dintre legislația națională și regulamentele militare, sugerând revizuiri și completări ale regulamentelor existente, în special în ceea ce privește facilitățile temporare și semipermanente, pentru a răspunde mai eficient nevoilor actuale și viitoare ale apărării naționale.

Romania's military infrastructure has undergone significant transformations over time. Periods of expansion and modernization have alternated with phases of reduction and, sometimes, the transfer of barracks into civilian administration. These changes reflect not just technological advancements but also the adaptation to the dynamic requirements of national defense.
The 2008 infrastructure regulations link the employment duration of military facilities directly to military activity, highlighting the need for a flexible and adaptable infrastructure. In this context, the article examines the legislative framework regarding the amortization of investments, the wear and tear of constructions, and the authorization of works, emphasizing the importance of aligning military regulations with civil ones.
In conclusion, the article analyzes the discrepancies between national legislation and military regulations, suggesting revisions and additions to the existing regulations, particularly regarding temporary and semi-permanent facilities, to meet the current and future needs of national defense more effectively.

Cuvinte-cheie:
infrastructură pentru apărare; construcții speciale; cazărmi;
legislație pentru construcții; reglementări militare.

Keywords:
Defense Infrastructure; Military Constructions; Barracks; Construction Legislation; Military Regulations.

Info articol
Primit: 12 februarie 2024; Evaluat: 29 februarie 2024; Acceptat: 18 martie 2024; Disponibil online: 5 aprilie 2024
Citare: Segal, A. 2024. „Durata de folosință a construcțiilor militare din patrimoniul Ministerului Apărării Naționale: între eficiență și adaptabilitate". *Buletinul Universității Naționale de Apărare „Carol I"*, 13(1): 131-143. https://doi.org/10.53477/2065-8281-24-09

Infrastructura militară din România a traversat o serie de transformări semnificative de-a lungul timpului, evoluând odată cu apariția și dezvoltarea armatei permanente. Această evoluție reflectă nu doar schimbările tehnologice și arhitecturale, ci și adaptarea la cerințele tactice și operaționale în continuă schimbare. În acest context, un aspect esențial îl constituie durata de utilizare a construcțiilor militare. Acest articol explorează modul în care durata de viață a construcțiilor militare, influențată de standardele tehnice și cerințele operaționale, modelează strategiile de asigurare a infrastructurii armatei, subliniind importanța echilibrului dintre eficiența investițiilor și capacitatea de adaptare a structurilor militare la nevoile în evoluție ale apărării naționale.

1. Evoluția infrastructurii militare

Evoluția infrastructurii militare din România a fost un proces de adaptare continuă la nevoile strategice ale armatei, alternând între perioade de expansiune și modernizare și cele de restrângere și conversie a facilităților pentru utilizare civilă.
Evoluția infrastructurii militare românești a început cu adaptarea unor structuri existente, precum hanurile, pentru a răspunde nevoilor operaționale imediate ale armatei. Limitările acestor facilități improvizate au condus rapid la necesitatea dezvoltării unor construcții militare specializate. Primele cazărmi realizate sub influența experților din armata țaristă în sistem multifuncțional, au fost esențiale pentru etapa inițială de dezvoltare a infrastructurii militare. Dezvoltarea fost accelerată după Unirea Principatelor Române, când creșterea numărului de unități militare a marcat un punct de cotitură în dezvoltarea infrastructurii militare. Această perioadă a fost caracterizată de trecerea la un sistem pavilionar în proiectarea cazărmilor și introducerea *Regulamentului Casarmelor*, reprezentând un pas important în standardizarea și modernizarea construcțiilor militare (Herjeu 1902, 193-308).

Această tendință de extindere și modernizare a continuat în perioadele celor două războaie mondiale. În timpul Primului Război Mondial, majoritatea cazărmilor au fost ocupate de forțele inamice, ceea ce a necesitat reabilitarea și extinderea lor după război. În perioada Celui de-Al Doilea Război Mondial, investițiile în construcții permanente s-au dublat, reflectând nevoia continuă de expansiune și modernizare a infrastructurii militare (Târzioru 1995, 212).
La sfârșitul anului 1952, în contextul deteriorării relațiilor internaționale, armata română a început construirea de noi cazărmi și lucrări de fortificații. Însă în 1958, retragerea trupelor sovietice a eliberat o mare parte din infrastructura militară, care apoi a trecut în administrarea civilă.

Modernizarea infrastructurii existente a fost un proces continuu, însă o nouă etapă a urmat în 1968, când, în urma ocupării Cehoslovaciei de către trupele Pactului de la Varșovia, România a intensificat investițiile pentru modernizarea și extinderea cazărmilor, pentru a întări capacitatea de luptă a armatei. În schimb, după 1989,

transformările politice și economice au condus la o restructurare majoră a armatei, cu efecte semnificative asupra infrastructurii: între 1995 și 2006, numeroase cazărmi au fost transferate către administrația civilă, ca urmare a renunțării la serviciul militar obligatoriu (Petrișor 2011, 93).
În concluzie, istoria infrastructurii militare românești ilustrează o adaptare constantă la cerințele armatei și un echilibru între necesitățile de modernizare și cele de eficiență. Această dinamică subliniază importanța unei abordări strategice în definirea duratei de viață și de folosință a construcțiilor militare pentru a asigura gestionarea eficientă a infrastructurii militare.

2. Durata de folosință a construcțiilor militare

Privind durata de funcționare a construcțiilor militare, regulamentele militare, aliniate la normativele civile încă din anii '60, au stabilit standarde care reflectă atât destinația clădirilor, cât și materialele folosite. Revizuirile regulamentelor de infrastructuri din 2008 au introdus o perspectivă nouă, legând durata de folosință direct de activitatea militară și subliniind necesitatea unei infrastructuri flexibile și adaptabile.
Regulamentul proprietății imobiliare în Ministerul Apărării Naționale[1] oferă o bază pentru înțelegerea și abordarea ***duratei de folosință*** a construcțiilor, în contextul militar clasificând facilitățile militare în patru categorii: inițiale, temporare, semipermanente și permanente. Facilitățile inițiale, exemplificate prin corturile folosite de armata română, sunt structuri temporare și relocabile, destinate utilizării pe termen scurt, de obicei nu mai mult de 6 luni, în scenarii, precum exerciții militare sau situații de urgență. Acestea oferă condiții austere, fiind rapid și ușor de montat și demontat. În contrast, facilitățile temporare, care includ corturi îmbunătățite și construcții din containere modulare, sunt proiectate pentru utilizare pe o durată mai lungă, de până la 5 ani, oferind condiții de viață îmbunătățite, cu acces la utilități, precum electricitatea și apa. Facilitățile semipermanente, realizate din materiale mai durabile, ca oțelul sau pereți compoziți prefabricați, sunt concepute pentru a fi utilizate între 5 și 25 de ani, reprezentând o soluție optimă pe termen mediu. Acestea sunt mai rapid de executat decât construcțiile permanente și, conform Regulamentului, trebuie să poată fi adaptate pentru a răspunde în timp cerințelor schimbătoare. Pe de altă parte, facilitățile permanente reprezintă soluția cea mai durabilă, fiind construcții fixe și definitive, proiectate pentru funcțiuni speciale sau reprezentative și adecvate pentru folosirea pe termen lung.

Această clasificare, introdusă prima oară în *Regulamentul proprietății imobiliare* din 2008, introduce în regulamentele militare durata de funcționare a construcțiilor temporare, precum și un concept nou pentru legislația construcțiilor din România, construcțiile semipermanente.

[1] Adoptat prin Ordinul nr. M.91, din 12 septembrie 2008, pentru aprobarea *Regulamentului proprietății imobiliare în Ministerul Apărării Naționale* și actualizat prin Dispoziția șefului Direcției domenii și infrastructuri nr. DDI-13, din 17 iunie 2022, pentru aprobarea *Regulamentului proprietății imobiliare în Ministerul Apărării Naționale*.

Preluarea unor noțiuni din reglementările Departamentului pentru Apărare al Statelor Unite (DoD)[2] reprezintă un pas spre modernizarea construcțiilor militare, însă, întrucât aceste prevederi nu au fost în totalitate corelate cu legislația națională din domeniul construcțiilor, aplicarea acestei noi structuri conceptuale privind durata construcțiilor în context militar rămâne la stadiul de intenție.

Clădirile militare sunt supuse atât reglementărilor specifice domeniului militar, cât și legislației naționale pentru construcții. În domeniul construcțiilor, durata este stabilită de 3 parametri: durata de existență, stabilită prin autorizație, durata de existență, proiectată în funcție de uzură și durata de funcționare în vederea amortizării investiției. Prin urmare, pentru corelarea reglementărilor militare cu cele civile, este necesară clarificarea cadrului legal și definirea unor termeni precum durata de funcționare, durata de existență sau durata de viață.

2.1. Amortizarea investiției imobiliare

Economia planificată din perioada comunistă presupunea existența unor norme privind durata de viață a fiecărui tip de clădire în vederea calculării amortizării investițiilor și planificării lucrărilor de reparații. Aceste reglementări care se aplicau și construcțiilor militare clasificau construcțiile, în funcție de destinație și de natura materialelor din care erau realizate, și precizau frecvența și costul lucrărilor de întreținere și de reparații capitale. Începând cu 1975, *Normele tehnice de cazare* includ nomenclatorul clădirilor și construcțiilor speciale, în care erau precizate durata de serviciu normată a fiecărui tip de clădire, în funcție de destinație și de natura materialelor din care era realizată, inclusiv normele de întreținere și de reparații capitale (Colban 1998, 30). ***Durata de serviciu normată*** începea de la data punerii în funcțiune a clădirii și reprezenta durata de amortizare la care se raporta planificarea reparațiilor capitale ca frecvență și valoare. Acest normativ a funcționat până la înlocuirea lui în 2008 cu regulamente care tratau separat lucrările de întreținere și de reparații curente[3] față de normele de domenii și infrastructuri[4].

În noile regulamente, clasificarea și duratele normate de funcționare a construcțiilor aparținând Ministerului Apărării Naționale sunt stabilite ca durata maximă, precizată în *Catalogul privind clasificarea și duratele normale de funcționare a mijloacelor fixe*, aprobat prin Hotărârea Guvernului nr. 2139, din 30 noiembrie 2004.
Clasificarea aprobată în 2004 actualizează prevederile *Hotărârii nr. 964/1998 pentru aprobarea clasificației și a* ***duratelor normale de funcționare*** *a mijloacelor fixe,* care reprezenta o schimbare de paradigmă care a aliniat România la tendințele internaționale, simplificând clasificarea activelor corporale amortizabile prin reducerea numărului de grupe și clase.

[2] UFC 1-201-01, Non-permanent DOD facilities in support of military operations prevede: Nivel de construcție temporar: Acest nivel implică clădiri și facilități proiectate și construite pentru o durată de viață de până la 5 ani; Nivel de construcție semipermanent: Clădirile și facilitățile de acest nivel sunt proiectate pentru o durată de viață de sub 10 ani, dar cu întreținere și reparații adecvate, acestea pot fi extinse până la 25 de ani.

[3] Normele tehnice pentru lucrări de întreținere și reparații curente la clădirile și construcțiile speciale din patrimoniul imobiliar al Ministerului Apărării Naționale, aprobate prin Ordinul nr. M44, din 9 mai 2008, și actualizate prin Dispoziția șefului Direcției domenii și infrastructuri nr. DDI-4, din 14 aprilie 2020, pentru aprobarea Normelor tehnice pentru lucrări de întreținere și reparații curente la clădirile și construcțiile speciale din patrimoniul imobiliar al Ministerului Apărării Naționale.

[4] Normele tehnice de domenii și infrastructuri, aprobate prin Ordinul nr. M. 45, din 9 mai 2008, și actualizate prin Dispoziția șefului Direcției domenii și infrastructuri nr. DDI-12, din 13 aprilie 2022, pentru aprobarea Normelor tehnice de domenii și infrastructuri.

Începând din 1998, materialul din care este realizat un activ nu mai este considerat un criteriu esențial. În schimb, se adoptă o abordare modernă, bazată pe performanță, care presupune ca fiecare activ să îndeplinească o funcție specifică pentru o perioadă prestabilită de funcționare, indiferent de materialul folosit la fabricarea sa. De exemplu, o construcție cu destinație administrativă, indiferent de materialele din care este făcută, trebuie să funcționeze între 40 și 60 de ani pentru a amortiza investiția.

Conform *Hotărârii Guvernului nr. 2139, din 30 noiembrie 2004, pentru aprobarea Catalogului privind clasificarea și duratele normale de funcționare a mijloacelor fixe*, pentru construcțiile care fac parte din sistemul național de apărare, ordine publică și siguranță națională, se vor stabili norme specifice pentru clasificarea și determinarea duratelor normale de funcționare. Aceste norme se vor elabora de autoritățile împuternicite din cadrul sistemului de apărare și se vor aviza de Ministerul Finanțelor Publice, asigurându-se astfel o abordare adaptată specific acestui sector.

Relevanța acestei durate se reflectă în activitatea de administrare a cazărmilor, întrucât, conform *Regulamentului proprietății imobiliare în Ministerul Apărării*, demolarea construcțiilor se execută numai după aprobarea scoaterii din funcțiune, iar scoaterea din funcțiune a construcțiilor înainte de expirarea ***duratei normale de utilizare***[5] se cercetează administrativ[6]. În situații excepționale, activele fixe pot fi scoase din funcțiune înainte de a atinge durata normală de utilizare, în baza unei expertize tehnice, dacă prezintă uzură fizică avansată și continuarea utilizării lor devine periculoasă sau ineficientă economic[7].

În concluzie sistemul general de clasificare a duratelor de funcționare ale activelor fixe nu detaliază cerințele particulare ale infrastructurii militare. Pentru a răspunde adecvat nevoilor distincte ale infrastructurii sistemului de apărare național, pentru asigurarea flexibilității și adaptabilității necesare, ar fi oportună dezvoltarea unor standarde specifice care să definească duratele normale de funcționare pentru facilitățile temporare și semipermanente.

În contextul regulamentelor Ministerului Apărării Naționale, durata normală de funcționare a construcțiilor este stipulată atât în *Normele tehnice de domenii și infrastructuri,* cât și în *Normele tehnice pentru lucrări de întreținere și reparații curente la clădirile și construcțiile speciale din patrimoniul Ministerului Apărării*. Pentru eliminarea redundanțelor, *Normele tehnice pentru lucrări de întreținere și reparații curente* ar putea include duratele normale de funcționare pentru facilitățile temporare și semipermanente, în timp ce *Normele tehnice de domenii și infrastructuri* doar ar putea face referire la documentul cuprinzător, optimizând astfel coerența și eficiența cadrului legislativ în domeniul infrastructurii militare.

[5] Durata normală de utilizare este sinonimă cu durata normala de funcționare, în Normele tehnice pentru lucrări de întreținere și reparații curente fiind folosită sintagma „durata normală de utilizare/ funcționare".
[6] Articolul 56.
[7] Instrucțiunile privind scoaterea din funcțiune și casarea activelor fixe, precum și declasarea și casarea bunurilor materiale, altele decât activele fixe, în Ministerul Apărării Naționale, aprobate prin Ordinul nr. M.92, din 16 septembrie 2013.

2.2. Uzura în timp a construcțiilor

Hotărârea nr. 1276, din 22 decembrie 2021, privind modificarea anexei la Hotărârea Guvernului nr. 2.139/2004 pentru aprobarea Catalogului privind clasificarea și duratele normale de funcționare a mijloacelor fixe precizează că, pentru stabilirea clasificării și duratelor normale de funcționare a mijloacelor fixe specifice sistemului național de apărare, se va ține cont de parametrii tehnico-economici, stabiliți de proiectanți și de producători prin cărțile sau documentațiile tehnice ale mijloacelor fixe respective, precum și de efectele uzurii morale. Privită prin prisma uzurii în timp, durata normală de viață a clădirilor sau a elementelor de construcții și instalații aferente este definită în contextul mai multor reglementări civile și militare.

Durata normală de utilizare este mai redusă decât durata de viață fizică a construcției. Normativul *GE 032-97 privind executarea lucrărilor de întreținere și reparații la clădiri și construcții speciale* definește ***durata de existență a construcției***, preluată și în *Normele tehnice pentru lucrări de întreținere și reparații curente la clădirile și construcțiile speciale*, ca fiind *„perioada de timp după care construcția sau elementul de construcție încetează definitiv să își îndeplinească funcțiunea pentru care a fost creat”*. Normativul prezintă în Anexa 1 duratele de viață ale clădirilor și construcțiilor speciale în condiții de mediu normal, precum și duratele de existență pentru elementele de construcții și instalații care compun clădirile, la Anexa 2. Duratele de viață subliniază un punct final în ciclul de viață al structurii sau al unor elemente componente, moment în care nu mai sunt utilizate eficient pentru scopul stabilit inițial. Durata de existență a construcției este asigurată prin lucrări de întreținere și reparații și chiar extinsă prin lucrări de reabilitare și modernizare. Astfel, pe durata ciclului de viață al clădirii, se definește o durată de viață proiectată, precum și o durată de funcționare normală.

Durata de viață proiectată este durata estimată de către proiectant[8] pentru care o structură sau o parte din aceasta este folosită în scopul prevăzut, fără a fi necesare reparații majore, în condițiile asigurării lucrărilor de întreținere[9]. ***Durată de funcționare normală***[10] este determinată ținând cont de durata tehnico-economică, stabilită de proiectant și de producător prin documentațiile tehnice, precum și de efectele uzurii morale. Această durată coincide cu durata de amortizare[11].

În concluzie, durata de viață a unei construcții se extinde peste durata de amortizare, adică durata de funcționare normală, dar pe durata ciclului de viață al clădirii, se vor realiza lucrări de reparații și de reabilitare cu o frecvență dată de durata de viață proiectată care se raportează la uzura materialelor componente.

Analizând caracteristicile facilităților militare temporare și semipermanente prin prisma acestei concluzii, se impune necesitatea adaptării soluțiilor

[8] SR EN 15978:2012 Dezvoltare durabilă a lucrărilor de construcție. Evaluarea performanței de mediu a clădirilor. Metodă de calcul.

[9] Cod de proiectare. Bazele proiectării construcțiilor CR 0-2012, 1.3.1 Termeni pentru proiectare.

[10] Normele tehnice pentru lucrări de întreținere și reparații curente la clădirile și construcțiile speciale din patrimoniul imobiliar al Ministerului Apărării, aprobate prin Ordinul nr. M44, din 9 mai 2008, Anexa 1 Glosar, pct. 6.

[11] GE 032-97 Normativ privind executarea lucrărilor de întreținere și reparații la clădiri și construcții speciale.

tehnice la durata de funcționare, respectiv alegerea unor materiale al căror cost, raportat la uzura în timp, justifică utilizarea lor pe o durată de funcționare limitată de 5-10 ani, respectiv de 10 până la 25 ani.

2.3. Autorizarea lucrărilor de construire

Un alt aspect al clasificării propuse în funcție de durata de folosință este utilizarea construcțiilor provizorii pentru asigurarea facilităților inițiale și a celor temporare, în timp ce, pentru facilitățile semipermanente și cele permanente, se realizează construcții definitive.

Indiferent de materialele din care sunt realizate, construcțiile provizorii au o **durată de existență *limitată***, stabilită în autorizația de construire. După expirarea termenului prevăzut în autorizație, acestea se demontează pentru a aduce terenul la starea inițială, conform obligațiilor impuse prin autorizație.

Construcțiile temporare se caracterizează prin flexibilitatea lor mai mare, în comparație cu cele permanente, fiindcă nu sunt supuse standardelor tehnice la fel de riguroase. Această particularitate permite o adaptabilitate mai mare în ceea ce privește selecția materialelor și dotărilor, cum ar fi izolația termică sau conectarea la utilități, în funcție de cerințele specifice și de costuri. Având un scop temporar sau servind nevoilor fluctuante, aceste construcții oferă o soluție rapidă și eficientă pentru infrastructură, fără a necesita investiții pe termen lung în materiale sau tehnologii costisitoare. În plus, conform legislației privind autorizarea lucrărilor de construcții, construcțiile provizorii sunt supuse acelorași condiții de autorizare ca și cele definitive, dar cu o procedură simplificată, bazată pe o documentație tehnică cu conținut redus, prezentat în Anexa 2 din *Normele Metodologice de aplicare a Legii nr. 50/1991 privind autorizarea executării lucrărilor de construcții*.

Însă nici legislația națională și nici regulamentele militare nu tratează facilitățile militare temporare în mod specific, ceea ce lasă loc de ambiguități în ceea ce privește standardele minime care trebuie asigurate și documentația necesară autorizării lucrărilor de construcții. Un document care ar putea servi drept model este normativul armatei americane pentru facilitățile temporare și semipermanente, UFC 1-201-01, care precizează, pe lângă tipologiile de facilități nepermanente, și situațiile în care acestea se folosesc, și ce standarde trebuie asigurate, și ce documentație trebuie prezentată pentru autorizarea acestora.

2.4. Schimbarea destinației clădirii

Construcțiile sunt constant afectate de modificările apărute în timp în organizarea activității unităților militare. Schimbarea destinației unei clădiri poate implica modificări semnificative ale condițiilor de utilizare și, în funcție de gradul de adaptare necesar și de resursele disponibile pentru realizarea acestor modificări, poate influența în mod direct durata de utilizare a construcției (Parker 2016, 134). În unele cazuri, schimbarea destinației unei construcții poate prelungi durata de utilizare prin transformarea acesteia într-o facilitate care să răspundă mai bine nevoilor operaționale și strategice ale armatei. Totuși, în alte situații, schimbarea destinației

unei construcții poate determina scoaterea din funcțiune și demolarea acesteia, dacă lucrările necesare pentru adaptarea la noile cerințe nu sunt fezabile economic.

Cele patru categorii de facilități, prezentate în *Regulamentul proprietății imobiliare în Ministerul Apărării Naționale*, inițiale, temporare, semipermanente și permanente, sunt clasificate pe baza complexității constructive (uzura și durata proiectată) și a duratei de folosință (durata de existență autorizată, durata de amortizare, durata de funcționare). În plus, subliniind caracterul flexibil și adaptabil al infrastructurii militare, prin *Regulament* se precizează că arhitectura facilităților semipermanente asigură *„posibilitatea recompartimentării/redistribuirii/remodelării spațiilor din aceste construcții sau reconstruirea lor parțială, cu cheltuieli minimale, pentru adaptarea cu ușurință în viitor la cerințe noi”*.

Printr-o abordare proactivă încă din procesul de planificare, se poate asigura o soluție flexibilă, orientată către maximizarea eficienței și durabilității infrastructurii militare, în concordanță cu evoluția cerințelor operaționale. Strategiile adoptate pentru adaptarea construcțiilor la destinații diferite constau în utilizarea arhitecturii modulare sau a clădirilor cu plan liber (Schmidt 2016, 84). Construcțiile modulare sunt caracterizate prin flexibilitate și adaptabilitate la nevoile schimbătoare, putând fi reconfigurate sau extinse, în funcție de cerințele operaționale. Realizate din containere, acestea sunt soluții mobile care pot fi ușor transportate, amplasate, demontate și reutilizate în alt context. Aceasta este soluția tehnică cea mai des folosită pentru asigurarea facilităților temporare. O altă strategie pentru maximizarea eficienței și durabilității infrastructurii este utilizarea pavilioanelor cu plan liber. Aceste clădiri pot fi adaptate pentru diverse funcțiuni, de la birouri și săli de conferințe, la ateliere de mentenanță sau spații pentru întreținere fizică, permițând reconfigurarea spațiului interior, în funcție de necesități.

Capacitatea acestor construcții de a se adapta în timp prin schimbarea destinației ridică probleme de încadrare într-una dintre categoriile existente în vederea stabilirii duratei de amortizare, *Catalogul privind clasificarea și duratele normale de funcționare a mijloacelor fixe* ținând cont de destinația clădirilor. Durata de viață a acestor construcții este influențată de durata proiectată, de uzura materialelor, care ține cont de durata de folosință, stabilită din perspectivă militară, respectiv 5-10 ani pentru cele temporare și 10-25 ani pentru cele semipermanente. În concluzie, pentru a stabili durata de amortizare a acestor construcții, sunt necesare norme specifice Ministerului Apărării Naționale.

3. Construcții militare adaptabile

Infrastructura militară românească a cunoscut o evoluție semnificativă în ultimii 20 de ani, adaptându-se cerințelor și provocărilor mediului de securitate actual. O schimbare notabilă este adoptarea unor tipologii noi de construcții caracterizate

prin adaptabilitate. Printre acestea, se numără construcțiile modulare din containere și construcțiile cu elemente structurale din table cutate. Aceste soluții constructive reprezintă un răspuns rapid care permite armatei să își ajusteze infrastructura, în funcție de dinamica specifică domeniului militar.

Figura 1 Poligon urban la Cincu (SMFT 2022)

Figura 2 Module tip container (Cabine și Containere, fără an)

Construcțiile mobile din module tip container reprezintă structuri prefabricate de dimensiunea unui container de transport, adaptate ca spații funcționale în diverse scopuri, cum ar fi birouri, depozite sau unități medicale. Aceste construcții sunt caracterizate de capacitatea lor de a fi ușor transportate, montate și demontate, oferind flexibilitate și adaptabilitate în diverse contexte și necesități. Flexibilitatea construcțiilor modulare din containere constă în capacitatea acestora de a se adapta rapid și eficient la diverse funcțiuni și cerințe prin reconfigurarea și extinderea modulară a structurilor, într-un mod rentabil și ecologic, asigurând capacitatea de a răspunde rapid cerințelor operaționale fluctuante.

Conform *Regulamentului proprietății imobiliare,* utilizarea construcțiilor relocabile nu presupune etapele de aprobare necesare unei investiții imobiliare, aprobarea simplificată reprezentând un avantaj suplimentar, întrucât procesul de realizare a construcției este accelerat.

Folosirea acestor construcții prezintă și o serie de dezavantaje care includ confortul limitat, izolarea termică și fonică slabă sau limitările spațiale. În majoritatea cazurilor, fără eforturi tehnice deosebite, aceste construcții nu îndeplinesc criteriul de eficiență energetică, impus construcțiilor permanente sau facilităților semipermanente, astfel încât utilizarea lor se limitează, în general, la durata precizată în regulament, de respectiv 5-10 ani, care de altfel este corelată cu soluția tehnică pentru acest tip de structuri, durata proiectată fiind în jur de 10 ani.

Întrucât utilizarea acestor module tip container acoperă o paletă mare de funcțiuni, în vederea stabilirii duratei de amortizare, propunem definirea unei clase noi de construcții, dedicată acestor tipuri de structuri, a cărei durată de folosință să se raporteze la durata proiectată și la uzura materialelor, respectiv *construcții militare operaționale* cu durata de utilizare de 10 ani.

Figura 3 Elemente structurale din tablă curbată
(Agenția media a armatei 2019)

Figura 4 Pavilioane din tablă curbată
(Agenția media a armatei 2022)

Clădirile cu elemente structurale din tablă sunt construite modular, permițând, prin proiect, extinderea și reconfigurarea lor, conform cerințelor. Producția lor implică fabricarea elementelor structurale din tablă, care sunt apoi asamblate pe șantier pentru a forma structura finală a clădirii. Aceste construcții sunt izolate la interior, asigurând, alături de instalațiile interioare (electrice, termice, sanitare), eficiența și confortul termic specifice construcțiilor permanente.
Realizate prin structurile proprii ale armatei, implementarea acestor construcții se realizează pe baza unor proiecte tehnice de execuție, întocmite de specialiști în domeniu și verificate de verificatori de proiecte, atestați conform reglementărilor în vigoare.

În cazărmile armatei române, construcțiile cu elemente structurale din table cutate sunt folosite pentru adăpostirea și întreținerea aeronavelor, pentru depozitare sau ca dispensare, terenuri de sport, pentru asigurarea nevoilor de hrană, odihnă sau igienă ale personalului militar. În plus, adaptabilitatea și flexibilitatea în utilizare, datorate planului liber, asigură posibilitatea de reconfigurare și reutilizare în diferite scopuri și pentru funcțiuni succesive.

În consecință, durata de viață a construcțiilor nu este definită de destinația inițială, ci mai degrabă de durata proiectată, determinată de uzura materialelor și de gradul de întreținere. Pentru clarificarea acestei probleme, propunem definirea unei clase noi de construcții, dedicată acestor tipuri de structuri, a cărei durată de folosință să se raporteze la durata proiectată și la uzura materialelor, respectiv construcții militare adaptabile, cu durata de utilizare de 25 de ani.

Concluzii

Construcțiile modulare tip container și cele realizate cu elemente structurale din tablă oferă un grad înalt de adaptabilitate și flexibilitate în utilizare, permițând reconfigurarea și utilizarea pentru diverse scopuri și funcțiuni, cum ar fi spații de birouri, de depozitare sau ateliere de mentenanță. Cu toate acestea, capacitatea lor de a se adapta multiplelor destinații lasă loc de interpretare în stabilirea duratei de

amortizare, deoarece acestea nu se încadrează în categoriile existente în Catalogul privind clasificarea și duratele normale de funcționare a mijloacelor fixe, sau nu este corelată cu duratele de funcționare, precizate în regulamentele militare.

Introducerea unor tipologii moderne de construcții a adus oportunități de modernizare a infrastructurii existente, dar și provocări în ceea ce privește coordonarea legislației naționale în construcții cu noile regulamente militare de infrastructură. În ceea ce privește durata de utilizare a construcțiilor în contextul regulamentelor MApN, se constată că sistemul general de clasificare a duratelor de funcționare ale activelor fixe nu răspunde în totalitate cerințelor specifice infrastructurii militare. Astfel, este necesară elaborarea de standarde specifice care să definească duratele de funcționare adecvate pentru facilitățile temporare și semipermanente, ținând cont de nevoile specifice ale apărării naționale și de necesitatea flexibilității și adaptabilității infrastructurii. Pentru aceste facilități, din perspectiva uzurii în timp a construcțiilor, este oportună standardizarea unor soluții tehnice deja testate, care își justifică costul, raportat la durata de funcționare, de 5-10 ani, pentru, cele temporare, și de 10-25 ani, pentru cele semipermanente. În final, legislația națională și regulamentele militare nu tratează în mod specific autorizarea lucrărilor de construcții militare temporare, lăsând loc de ambiguități în privința standardelor și documentației necesare. Normativul armatei americane, UFC 1-201-01, oferă un model util pentru abordarea acestor aspecte, stabilind standardele și documentația necesară facilităților nepermanente.

În concluzie, abordarea diferențelor dintre legislația națională și regulamentele militare este necesară pentru a asigura eficiența infrastructurii militare românești, în contextul său actual și viitor. Pentru elaborarea unor norme care să completeze regulamentele existente și care să ofere o bază clară în stabilirea duratei de utilizare, în contextul militar al construcțiilor modulare tip container și al celor realizate cu elemente structurale din tablă, precum și al altor tipologii constructive pentru asigurarea facilităților semitemporare, este oportună realizarea unui regulament care să precizeze:

- tipologiile constructive și soluțiile tehnice de realizare;
- standardul tehnic minimal referitor la gradul de izolare, la protecția la incendiu, la siguranța în exploatare;
- documentația tehnică necesară autorizării lucrărilor de amplasare și responsabilitățile în elaborarea acesteia (în special clarificarea conținutului documentației tehnice care însoțește completul de module tip container);
- tipul de activ fix (echipament militar sau construcție) și durata de folosință în vederea amortizării.

De asemenea, pentru a asigura un răspuns eficient ca durată în timp și costuri, acest regulament ar trebui însoțit de un catalog cu proiecte tip, care să cuprindă soluții testate și optimizate de asigurare a diverselor facilități din cazărmile armatei prin utilizarea construcțiilor modulare, prefabricate sau construcții cu plan generic, cum sunt clădirile cu elemente structurale din tablă cu plan liber.

Referințe

Agenția media a armatei. 2019. „Ziduri reci, cu suflet la temelie.” http://presamil.ro/ziduri-reci-cu-suflet-la-temelie/.

—. 2022. „Cine mai are grijă de patrimoniul armatei?” http://presamil.ro/cine-mai-grija-de-patrimoniul-armatei/.

Cabine & Containere. fără an. „Cabina sector militar.” Accesat 20 februarie 2024. https://www.cabine-containere.ro/cabina-sector-militar/.

Colban, Gh. C. 1998. *Elemente de legislație în construcții și asigurare tehnico-materială de cazare.* București: Editura Academiei Tehnice Militare.

Departamentul Apărării al Statelor Unite ale Americii. 2022. „Facilități nepermanente ale DOD în sprijinul operațiilor militare.” UFC 1-201-01. https://www.wbdg.org/FFC/DOD/UFC/ufc_1_201_01_2022_c4.pdf.

Direcția domenii și infrastructuri. 2020. „Dispoziția șefului Direcției domenii și infrastructuri nr. DDI-4, din 14 aprilie 2020 pentru aprobarea Normelor tehnice pentru lucrări de întreținere și reparații curente la clădirile și construcțiile speciale din patrimoniul imobiliar al Ministerului.” Accesat prin aplicația Lexmil din rețeaua INTRAMAN la 17 martie 2023.

—. 2022a. „Dispoziția nr. DDI-13, din 17 iunie 2022 pentru aprobarea Regulamentului proprietății imobiliare în Ministerul Apărării Naționale.” Accesat prin aplicația Lexmil din rețeaua INTRAMAN la 17 martie 2023.

—. 2022b. „Dispoziția șefului Direcției domenii și infrastructuri nr. DDI-12, din 13 aprilie 2022 pentru aprobarea Normelor tehnice de domenii și infrastructuri.” Accesat prin aplicația Lexmil din rețeaua INTRAMAN la 17 martie 2023.

Guvernul României. 1994. „Ordin nr. 746, din 9 iunie 1994 pentru aprobarea Normelor metodologice de aplicare a Legii nr. 15/1994 privind amortizarea capitalului imobilizat în active corporale și necorporale.” *Monitorul Oficial*, nr. 180. 15 iulie 1994. https://legislatie.just.ro/Public/DetaliiDocumentAfis/5317.

—. 1998. „Hotărârea nr. 964, din 23 decembrie 1998 pentru aprobarea clasificației și a duratelor normale de funcționare a mijloacelor fixe.” *Monitorul Oficial*, nr. 520. 30 decembrie 1998. https://legislatie.just.ro/Public/DetaliiDocumentAfis/16651.

—. 2004. „Hotărârea nr. 2139, din 30 noiembrie 2004 pentru aprobarea Catalogului privind clasificarea și duratele normale de funcționare a mijloacelor fixe.” *Monitorul Oficial,* nr. 46. 13 ianuarie 2005. https://legislatie.just.ro/Public/DetaliiDocumentAfis/58613.

Herjeu, C. 1902. *Istoria Armei Geniului.* București: I.V. Socecu.

Ministerul Apărării Naționale. 2008a. „Ordinul nr. M. 45, din 9 mai 2008 pentru aprobarea Normelor tehnice de domenii și infrastructuri.” *Monitorul Oficial*, nr. 405. 29 mai 2008. https://legislatie.just.ro/Public/DetaliiDocumentAfis/93541.

—. 2008b. „Ordinul nr. M.44, din 9 mai 2008 privind aprobarea Normelor tehnice pentru lucrări de întreținere și reparații curente la clădirile și construcțiile speciale din patrimoniul imobiliar al Ministerului Apărării.” *Monitorul Oficial*, nr. 402. 28 mai 2008. https://legislatie.just.ro/public/DetaliiDocument/93499.

—. 2008c. „Ordinul nr. M.91, din 12 septembrie 2008 privind aprobarea Regulamentului proprietății imobiliare în Ministerul Apărării." *Monitorul Oficial*, nr. 668. 26 septembrie 2008. https://legislatie.just.ro/Public/DetaliiDocument/97630.

—. 2013. „Ordinul nr. M.92, din 16 septembrie 2013 privind aprobarea Instrucțiunilor pentru scoaterea din funcțiune și casarea activelor fixe, precum și declasarea și casarea bunurilor materiale, altele decât activele fixe, în cadrul Ministerului Apărării Naționale." https://legislatie.just.ro/Public/DetaliiDocument/151635.

—. 2018. „Ordinul nr. M.40, din 8 martie 2018 privind aprobarea Procedurii comune de autorizare a executării lucrărilor de construcții cu caracter special." *Monitorul Oficial,* nr. 738. 27 august 2018.

Ministerul Dezvoltării, Lucrărilor Publice și Administrației. 2012. „Cod de proiectare. Bazele proiectării construcțiilor CR 0-2012". https://www.mdlpa.ro/userfiles/reglementari/Domeniul_I/I_19_1_CR_0_2012.pdf.

—. fără an. „Normativ privind executarea lucrărilor de întreținere și reparații la clădiri și construcții speciale GE 032-97." Accesat 15 ianuarie 2004. https://www.mdlpa.ro/pages/reglementare22.

Parker, Daniel M. 2016. *Obsolescence: An Architectural History.* Chicago: Everand.

Parlamentul României. 1991. „Legea nr. 50, din 29 iulie 1991 (**republicată**) privind autorizarea executării lucrărilor de construcții." *Monitorul Oficial*, nr. 933. 13 octombrie 2004. https://legislatie.just.ro/Public/DetaliiDocument/55794.

—. 2015. „Legea nr. 227, din 8 septembrie 2015 privind Codul fiscal." Monitorul Oficial, nr. 688. 10 septembrie 2015. https://static.anaf.ro/static/10/Anaf/legislatie/L_227_2015.pdf.

Petrișor, A.I. 2011. *FATE - Conversia fostelor baze militare în centre antreprenoriale. O perspectivă românească.* București: Editura Ars Docendi.

Schmidt, R. și S. Austin. 2016. *Adaptable Architecture – Theory and Practice.* New York: Routledge.

SMFT [Statul Major al Forțelor Terestre]. 2022. „*Exercițiu în poligonul «Operații militare în teren urban» din Cincu.*" https://www.defense.ro/exercitiu-in-poligonul-operatii-militare-in-teren-urban-din-cincu.

Stârzioru, M. și S. Pădureanu. 1995. *Istoria construcțiilor și domeniilor militare.* București: Editura Militară.


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


Institutional Evaluation Programme
Performance in Research, Performance in Teaching – Quality, Diversity and Innovation in Romanian Universities Project

"CAROL I - NATIONAL DEFENCE UNIVERSITY"
BUCHAREST-ROMANIA

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: 09.04.2024
Lucrarea conține 144 de pagini.