CZU 327.5 **DOI 10.5281/zenodo.7184282**

Alexandru PARENIUC,
dr., conf. univ.
PhD,
associate professor

Vasili BEDA,
doctorand
PhD student

AMENINȚĂRI HIBRIDE ȘI METODELE DE REZISTENȚĂ ÎMPOTRIVA ACESTORA

În acest articol se efectuează o prezentare generală a fenomenului amenințărilor hibride, fiind analizată esența și conținutul strategiei și contrastrategiei utilizate de părțile opuse în pregătirea și în timpul războiului hibrid. Se arată că logica lor ar trebui reconstituită ținând cont de configurația neliniară a forțelor și capacităților strategice. Sunt oferite recomandări pentru neutralizarea amenințărilor hibride și organizarea de contramăsuri atunci când se declanșează un război hibrid.

Cuvinte cheie: amenințări hibride, riscuri hibride, măsuri psihologice strategice, model neliniar de război, acțiuni asimetrice, informare și presiune psihologică, atacuri cibernetice.

HYBRID THREATS AND METHODS OF RESISTANCE AGAINST THEM

This article gives an overview of the phenomenon of hybrid threats, analyzing the essence and content of the strategies and counterstrategies of the opposing sides when preparing and holding hybrid wars. It is shown that their logic should be built taking into account the nonlinear configuration of strategic forces and capabilities. Recommendations are given for neutralising hybrid threats and organising counteraction when unleashing a hybrid war.

Keywords: hybrid threats, hybrid risks, strategic psychological measures, nonlinear war model, asymmetric actions, information and psychological pressure, cyberattacks.

Introducere. Războiul hibrid, ca orice alt război, presupune redistribuirea rolurilor subiecţilor procesului politic la nivel global sau regional. Cu toate acestea, o asemenea conflagraţie se realizează în principal prin mijloace nemilitare, fără ocuparea ţării învinse, evitând distrugerea infrastructurii acesteia şi moartea în masă a populaţiei [4, p. 101].

Scopul studiului. Autorii trec în revistă fenomenului amenințărilor hibride, precum şi o analiză a esenţa şi conţinutul strategiei şi contrastrategiei utilizate de părţile opuse în pregătirea şi în timpul războiului hibrid.

Metode şi materiale aplicate. În calitate de metode de cercetare au fost folosite metoda logică, sistematică, descrierea, deducţia şi

de comparare. Materialele utilizate în vederea realizării studiului sunt publicaţiile cercetătorilor în domeniu, precum şi legislaţia relevantă. În baza analizei materialelor sunt formulate concluziile şi propunerile corespunzătoare.

Rezultate obţinute şi discuţii. Strategia şi contrastrategia războiului hibrid. Strategia integrează rezultatele analizei schimbărilor şi le transformă în paşi practici concreţi. Cunoscutul teoretician militar, şeful Statului Major al Prusiei, Helmuth von Moltke (senior), menţiona: *„Strategia este mai mult decât ştiinţă; este transferul de cunoştinţe în viaţa practică, dezvoltarea ulterioară a gândirii călăuzitoare originale în conformitate cu circumstanţe în continuă schimbare; strategia este arta de a acţiona sub jugul celor mai dificile condiţii"* [10].

Lista factorilor care determină evoluţia afacerilor militare s-a schimbat de-a lungul secolelor. Astăzi, procesele de globalizare şi revoluţia informaţiei şi comunicării, care formează noi mecanisme de interacţiune şi interdependenţă la scară globală şi regională, au cea mai profundă şi cuprinzătoare influenţă asupra dezvoltării strategiilor pentru conflictele militare moderne, precum şi asupra schimbării naturii şi conţinutului lor. Acoperind economia mondială, politica, domeniul militar, comunicaţiile, sportul, ştiinţa şi cultura, aceste procese foarte contradictorii şi dinamice afectează toate cele mai importante sfere ale societăţii moderne.

Strategia conflictelor moderne, construită pe o combinare a unei game largi de forme şi metode de luptă, conţine un număr mare de semnificaţii. Cu această ocazie, preşedintele Academiei de Ştiinţe Militare, generalul de armată M.A. Gareev, afirma încă în 2003: „Autorii, lacomi de senzaţii, aproape în fiecare zi dau nume noi războaielor viitorului: tridimensional, de reţea, asimetric, fără contact, informaţional etc. Da, toate aceste elemente vor avea loc, ele reflectă una dintre trăsăturile caracteristice ale confruntării militare, dar niciuna dintre ele nu caracterizează individual faţa războiului în ansamblu" [8].

Elaborarea şi realizarea strategiei de război hibrid include următoarele etape [7]:

Prima este o formulare clară a sensului şi scopurilor războiului.

A doua este identificarea punctelor slabe şi vulnerabilităţilor în sfera asigurării securităţii interne şi externe a statului inamic.

A treia este formarea unui complex de ameninţări hibride, ţinând cont de specificul local pentru a influenţa obiectul agresiunii.

A patra este planificarea strategică bazată pe o relatare specifică a forţelor şi mijloacelor naţionale, menite să influenţeze blocajele şi vulnerabilităţile inamicului în sfera politică, administrativă, financiară, economică, culturală şi ideologică, precum şi o analiză a contracarării sale aşteptate *(varianta activităţii de contrastrategie)*.

A cincea reprezintă un impact distructiv consistent asupra domeniilor cheie ale guvernării ţării-victime, concentrându-se în principal eforturile asupra factorilor cei mai critici care asigură securitatea militară a statului *(economia, finanţele, moralul armatei şi al populaţiei)*.

A şasea este desfăşurarea ostilităţilor nedeclarate, în timpul cărora statul-agresor atacă structurile ţării şi armata regulată a inamicului cu ajutorul rebelilor locali şi separatiştilor susţinuţi cu armament şi finanţe din străinătate. Un loc important este acordat acţiunilor *„coloanei a cincea"*, care dobândesc un caracter extremist, folosit pentru a lansa atacuri asupra autorităţilor în cursul uneia sau mai multor „revoluţii colorate".

A şaptea este înaintarea cererii de ultimatum pentru predarea completă a statului victimă.

Teoria descurajării. Metode de rezistenţă împotriva ameninţărilor de natură hibridă

Potrivit colonelului *John J. Neal*, expert american, mai multe aspecte ale descurajării militare trebuie revizuite atunci când se elaborează o viitoare politică de descurajare.

În primul rând, spectrul conflictului în **descurajarea militară** este privit ca un concept liniar, în care utilizarea forţei are loc la o scară cunoscută.

În al doilea rând, această scară presupune că părţile au o bună înţelegere a mecanicii utilizării instrumentelor militare specifice şi a consecinţelor unei astfel de utilizări. Această

înţelegere este întărită de evaluarea de către rivali a raportului de putere, care, de regulă, se reduce la capacităţi pur militare. În cele din urmă, teoria descurajării militare nu ţine cont de consecinţele utilizării instrumentelor nemilitare în declanşarea unui război [3].

Schema constă într-o aranjare liniară a nivelurilor de criză şi a nivelurilor de risc corespunzătoare. Subiecţii se deplasează în sus sau în jos pe această scară, efectuând acţiuni care măresc sau, respectiv, scad nivelul de ameninţare al inamicului. Acest concept a fost aplicat scenariilor Războiului Rece, în special scenariilor conflictuale dintre SUA şi URSS.

Metoda balanţei puterii a fost folosită pentru a determina preţul care trebuie plătit pentru o anumită acţiune, fiecare stat putând să-şi cuantifice punctele forte şi punctele slabe cu relativă uşurinţă.

Instrumentele non-militare, totuşi, nu sunt cuantificabile şi, prin urmare, consecinţele potenţiale ale utilizării acestor mijloace sunt mult mai abstracte. Există, de asemenea, un cadru general acceptat pentru costurile potenţiale ale unui conflict militar în creştere şi pentru răspunsul adversarului la o astfel de escaladare. Dar în cazul utilizării mijloacelor nemilitare, nu există un astfel de cadru. Toate acestea complică calculul efectului de descurajare al instrumentelor nemilitare.

Conceptele din trecut au fost sub forma unei scale mobile şi s-au concentrat pe utilizarea forţei militare, mijloacele nemilitare fiind o componentă auxiliară a celor militare *(Figura 1)*.

Aceasta a reflectat ideea că acţiunea militară are o ierarhie de escaladare bine definită, cu caracteristici distinctive clare şi că mijloacele nemilitare au un rol de susţinere prost definit şi cu greu reprezintă o ameninţare.

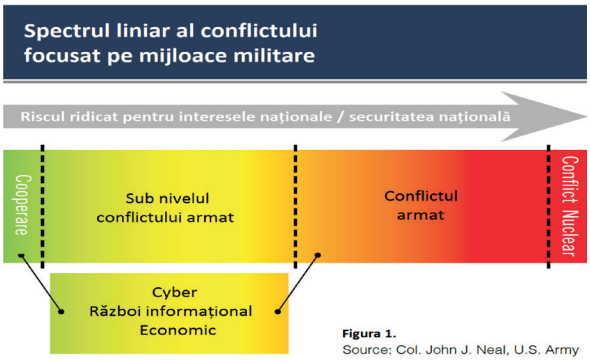

Figura 1.
Source: Col. John J. Neal, U.S. Army

Acum recunoaştem că mijloacele non-militare reprezintă o mare ameninţare la adresa securităţii naţionale şi, în viitor, pot reprezenta aceeaşi ameninţare ca şi instrumentele militare. Cu toate acestea, aceste zone sunt adesea considerate izolat şi li se aplică scara teoretică a potenţialei escalade *(Figura 2)*.

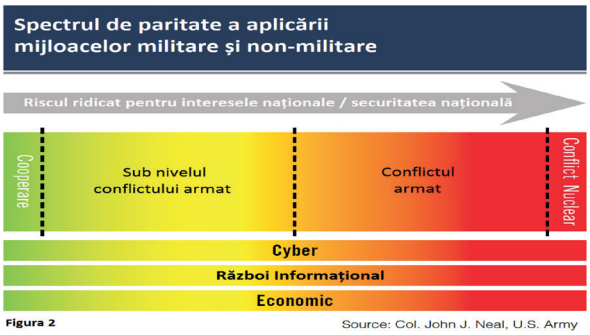

Figura 2
Source: Col. John J. Neal, U.S. Army

Aceasta este o reflectare a concentrării actuale asupra descurajării atacurilor în fiecare zonă specifică, fără a înţelege modul în care acţiunile din fiecare dintre aceste zone se adaugă la deteriorarea mediului de securitate.

Modelul de concept în evoluţie se îndepărtează de scara de escaladare pe măsură ce nevoia de această scară scade din cauza că părţile opuse caută modalităţi de a ocoli normele stabilite. În acest model, mijloacele militare şi nemilitare sunt prezentate ca fiind egale în capacitatea lor de a reprezenta o ameninţare la adresa intereselor naţionale şi a securităţii naţionale.

Astfel, sunt definite praguri pentru utilizarea forţei militare, iar pragurile pentru mijloacele nemilitare vor fi luate în considerare în caz dacă acestea vor fi clar definite *(Figura 3)*.

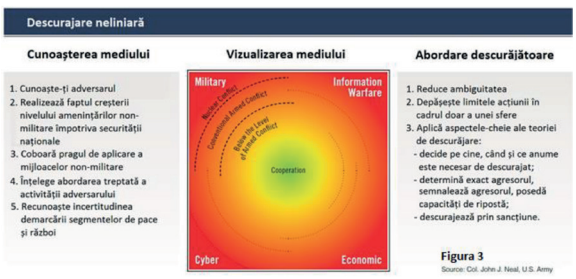

Figura 3
Source: Col. John J. Neal, U.S. Army

Abordări descurajatoare

Primul principiu al abordărilor descurajatoare este ***reducerea ambiguității***. Ambiguitatea este un factor critic al strategiilor concurenților. Scăderea acestuia va influența semnificativ scăderea capacității unui agresor pentru a-și atinge obiectivele. Realizarea acestei sarcini implică stabilirea unor parametri definiți și norme de comportament, provocând adversarii atunci când una din părți le încalcă.

Thomas Schelling menționează în lucrarea „Strategia conflictului" [5, p. 177], că atunci când este pornită progresiunea unei amenințări, atacarea punctată și selectivă a unor elemente ale obiectivului inamicului este mai eficientă decât atentarea asupra obiectivului în general.

Folosind această metodă, statele treptat pot crea impedimente pentru a preveni condițiile în care situația operativă și tactică se va schimba irevocabil în favoarea adversarului.

O modalitate de a defini parametrii este stabilirea unor indici (marcheri) clari pentru acțiunile care amenință interesele naționale. Procedând astfel, statele pot contesta definitiv comportamentul adversarului. Marcherii sunt definiți ca poziția declarată a unei entități, care urmează a fi atacată în caz de încălcarea ei de către entitatea adversară.

Un exemplu este articolul 5 din Tratatul Atlanticului de Nord, care prevede că *un atac armat împotriva unui membru al Alianței va primi răspuns din partea tuturor aliaților* [6].

Cu toate acestea, există vulnerabilități inerente în indicii menționați mai sus.

Daniel Altman a remarcat în studiul său „Linii roșii și fapte realizate în constrângere și criză interstatală" [1], că marcherii roșii sunt arbitrari și pot să nu aibă o precizie definitivă, fiind incompleți și neverificabili.

Articolul 5 al tratatului NATO ilustrează unele dintre aceste vulnerabilități.

În 2014, membrii NATO au convenit asupra faptului că atacurile cibernetice întrunesc acele criterii conform cărora se declară încălcarea prevederilor articolului 5 al Tratatului. Aceste argumente au avut relevanță, luând în considerare creșterea nivelului amenințărilor cibernetice. Totodată, s-au evidențiat și unele elemente vulnerabile, incluse în noțiunea de

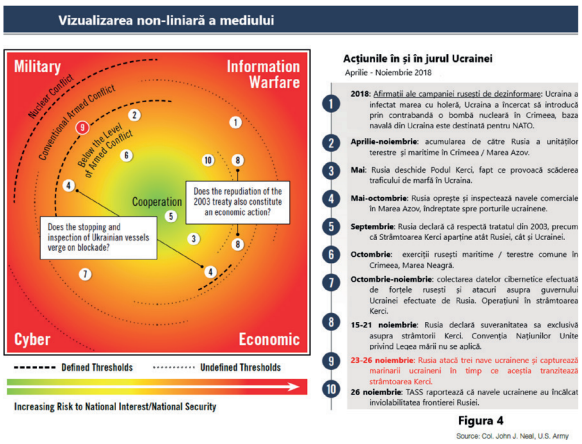

Figura 4
Source: Col. John J. Neal, U.S. Army

„linie roșie" sau „marcher (indice) roșu".

În acest sens remarcăm faptul că poziția față de atacurile cibernetice este nu doar imprecisă, ci și incompletă, deoarece Alianța nu a definit clar ce acțiuni anume constituie un atac cibernetic. De asemenea, este greu de verificat cât de exact se încadrează o acțiune sau alta în noțiunea atacului cibernetic, dat fiind faptul că unul dintre avantajele acestei infracțiuni este posibilitatea inerentă de negare a efectuării unui atac cibernetic.

În sfârșit, începând cu anul 2014, de când NATO a luat această poziție, până în prezent au avut loc mai multe atacuri cibernetice asupra membrilor săi, fără represalii clare și fără invocarea încălcării articolului 5 al Tratatului Nord-Atlantic. De aici deducem că pentru a fi eficienți, indicii roșii trebuie să fie clar definiți, manifestați prin amenințări credibile și, cel mai important, aceștia trebuie puși în aplicare.

În așa mod, din 2014 noțiunile ***„război hibrid"*** și ***„amenințări hibride"*** au fost utilizate tot mai des în discursul politicii internaționale de securitate. Cu toate acestea, cu mici excepții, nu există o definiție sau un concept comun în practica politică sau în mediul academic care să poată fi utilizat pentru a desemna în mod fiabil o situație drept război hibrid – și, prin urmare, niciun set de măsuri și proceduri politice, militare sau juridice pe care statele sau organizațiile să le poată invoca ca răspuns la amenințare.

Războiul hibrid poate fi descris ca o combinație de forță militară – deschisă și ascunsă – și orice mijloace nemilitare care ar

putea aduce daune unui stat, societăți sau organizații internaționale precum UE sau NATO. În timp ce astfel de mijloace completează adesea operațiunile militare clasice în războaiele convenționale, ele sunt instrumente esențiale în războiul hibrid și adesea depășesc eforturile militare.

La conferința militaro-științifică a Academiei de Științe Militare a Federației Ruse din 24 martie 2018, generalul de armată V. V. Gherasimov, șef al Marelui Stat Major al Forțelor Armate ale Federației Ruse, a conturat elementele unui posibil viitor război. El a afirmat că fiecare conflict militar are propriile sale trăsături distinctive.

Principalele trăsături ale războaielor viitorului vor include utilizarea pe scară largă a armelor noi de înaltă precizie și a altor tipuri de arme, inclusiv a tehnologiilor laser, spațiale și robotice, atribuindu-i un rol special combaterii comunicațiilor, informațiilor și navigației. Iar pe lângă domeniile tradiționale ale luptei armate vor fi implicate activ sfera și spațiul cosmic [9].

Potrivit lui Gherasimov, raportul dintre mijloacele militare și cele nemilitare ar trebui să fie de 1 la 4. Ca elemente ale unei strategii integrate, mijloacele militare sunt aplicate sistematic și flexibil acolo unde se potrivesc cel mai bine.

În cazul acțiunilor militare, acestea pot fi operațiuni ale forțelor speciale ale „omuleților verzi" fără însemne de identificare, acordând sprijin ascuns insurgenților. Astfel de operațiuni permit atacatorului să nege implicarea directă și să facă situația cât mai neclară.

Spațiul cibernetic este un tărâm ideal pentru războiul hibrid. El transcende granițele clasice, interconectează zone private, publice, economice și administrative și este greu de controlat, în ciuda eforturilor enorme ale statelor puternice precum SUA și China. Cyberspațiul oferă bunuri convenabile, cum ar fi infrastructura interconectată la nivel global, permițând comunicarea în timp real pentru actorii publici, privați sau individuali, ceea ce stimulează schimburile internaționale și comerțul. În același timp, dependența extinsă de aceste tehnologii în toate domeniile relevă vulnerabilități existențiale din ce în ce mai semnificative. Natura virtuală a spațiului cibernetic permite unui spectru larg de militanți să lanseze atacuri grave care provoacă daune considerabile indivizilor, organizațiilor și statelor, prezentând un risc scăzut de a fi identificați și urmăriți.

Ca instrument de război hibrid, atacurile cibernetice pot deruta sau perturba infrastructura de comunicații, pot provoca paralizii temporare vieții publice și contribui la un climat general de incertitudine și frică. De asemenea, astfel poate fi subminată legitimitatea guvernelor care nu sunt în stare să protejeze societățile de amenințări cibernetice reale. Apărarea infrastructurii publice și economice împotriva unor asemenea atacuri a devenit o provocare zilnică.

Spionajul cibernetic și crimele cibernetice reprezintă amenințări tot mai mari pentru națiuni, întreprinderi și persoane. Dezvăluirea informațiilor piratate din comunicațiile electronice ale politicienilor poate influența alegerile, la fel ca și atacurile asupra sistemelor electronice de vot. După cum au arătat alegerile prezidențiale din SUA din 2016, țările democratice trebuie să devină mai atente la pericolele interferenței din spațiul cibernetic.

Dezvăluirile, precum cele de la *WikiLeaks*, pot avea un impact negativ asupra securității naționale. Programele distructive – precum *Stuxnet*, care se presupune că a fost lansat de SUA pentru a distruge părți centrale ale programului nuclear iranian – s-au dovedit a fi o armă letală în arsenalele militare, din nou fără posibilitatea unei clasificări clare [2].

În scopul prevenirii utilizării tehnologiilor subversive moderne împotriva țării, trebuie acordată o atenție deosebită dezvăluirii setului de măsuri implementate de agresor în pregătirea și desfășurarea unui război hibrid. Pentru aceasta, activitatea contrainformativă trebuie organizată ținând cont de următoarele caracteristici principale ale unui război hibrid:

– ***războiul hibrid nu se declară oficial***, ostilitățile pot să nu se desfășoare pentru o perioadă lungă de timp, nu există frontul de față și spatele, iar operațiunile acoperă întreg teritoriul statului țintă (statului victimă);

– ***statul agresor nu se dezvoltă o anumită perioadă de timp***, nu efectuează măsuri de mobilizare pe scară largă, tinde spre ducerea războiului indirect, utilizând ţările sau formaţiunile terţe, foloseşte mercenari, companii militare private, activizează formaţiunile interne neregulate, „coloana a cincea" şi agenţi de influenţă;

– ***formal, în cazul războiului hibrid lipseşte aparatul central de conducere şi dirijare a acţiunilor ostile***. Scopul comun pentru distrugerea statului inamic este dezvoltat şi convenit la nivelul organismelor guvernamentale, conducerii corporaţiilor transnaţionale, structurilor financiare şi bancare, precum şi persoanelor influente;

– ***planurile de acţiune pentru destabilizarea sferelor administrativ-politice, socio-economice, culturale şi ideologice*** prevăd crearea unor structuri de reţea distribuite pe teritoriul inamic cu un grad ridicat de independenţă şi capacitate de autosincronizare. Sunt elaborate în prealabil canalele pentru sprijinul lor financiar, logistic, informaţional şi de personal, sunt create depozite pentru arme, muniţii, comunicaţii, sunt selectate locuri pentru pregătirea militanţilor;

– ***se folosesc catalizatori-acceleratori ai proceselor subversive***, în special demersurile diplomatice, sancţiunile economice, umplerea de informaţii şi acţiunile de succes ale forţelor neregulate împotriva unor obiecte importante. Un catalizator puternic în acest sens sunt „revoluţiile colorate", organizate într-un punct de cotitură important al războiului, pentru a accelera procesul de destabilizare a statului, asemănător avalanşelor. Descoperirea la timp a pregătirii operaţiunilor care vizează accelerarea proceselor de prăbuşire a statului este cea mai importantă sarcină a serviciilor de intelligence;

– ***forţele de operaţiuni speciale sunt folosite împotriva obiectelor importante din punct de vedere strategic***, pentru a răpi şi asasina lideri politici şi pentru a oferi sprijin formaţiunilor neregulate;

– ***forţele armate regulate încep să opereze în fazele finale ale unui război hibrid*** sub diferite pretexte, cum ar fi „intervenţii umanitare", operaţiuni de impunere a păcii, misiuni pacificatoare etc. Obţinerea unui mandat ONU în acest sens este de dorit, dar nu obligatoriu [7].

Concluzii. Ameninţările hibride nu sunt un fenomen nou, dar în această lume globalizată, cu dezvoltarea uluitoare a comunicaţiilor din ce în ce mai rapide, impacturile acestor ameninţări devin masive şi periculoase. Ele ridică noi provocări pentru politicile şi agenţiile de securitate naţională, dar, în acelaşi timp, măsurile defensive adecvate deschid oportunităţi imense pentru societăţi.

Rezilienţa adevărată necesită un anumit grad de satisfacţie şi fericire în rândul tuturor cetăţenilor. Guvernele responsabile şi actorii societăţii civile trebuie să ţină cont de legătura strânsă dintre securitatea societală şi naţională şi să depună eforturi pentru a-şi face cetăţenii mai fericiţi şi naţiunile mai puternice.

Natura conflictelor se schimbă. Statele recurg din ce în ce mai mult la mijloace nonmilitare pentru a-şi atinge obiectivele, schimbând pe parcurs conceptul de escaladare a conflictului. Această utilizare interdependentă a mijloacelor militare şi non-militare a condus la o estompare a graniţei dintre război şi pace. Aceşti factori au creat condiţii în care părţile opuse exploatează nedemonstrabilitatea atacurilor lor şi absenţa normelor internaţionale de conduită în avantajul lor, ameninţând statele cu acţiuni care în trecut erau de neimaginat. Pentru a-şi asigura interesele în viitor, statele trebuie să îşi adapteze înţelegerea privind activitatea de descurajare la noile condiţii.

Descurajarea neliniară implică realizarea conceptului de descurajare, ceea ce va contribui la înţelegerea mediului de securitate actual. Este o fuziune a gândirii trecute şi actuale, precum şi a ideilor generate de doctrina şi comportamentul recent adoptat de inamic. Este, de asemenea, un punct de plecare pentru discuţii ulterioare şi eforturi suplimentare în ceea ce ţine de dezvoltarea descurajării interstatale, care pot fi aplicate în formularea politicilor naţionale.

Referințe bibliografice

1. Daniel W. Altman. Red Lines and Faits Accomplis in Interstate Coercion and Crisis. Massachusetts Institute of Technology 2015.
2. Gareis Sven Bernhard. Hybrid War and Hybrid Threats: Coping with conventional and unconventional security challenges. Gheorghe C. Marshall European Center for Security Studies. 25.08.2017.
3. John J. Neal, colonel U.S. Army. Deterrence in a Hybrid Environment. Concordiam, vol.10, №1, 2020.
4. Pareniuc A., Beda V. Basic concepts of the hybrid threat phenomenon. Analele ştiinţifice ale Academiei „Ştefan cel Mare" a MAI al Republicii Moldova, Ştiinţe juridice// Legal Sciences, nr. 15/ 2022, ISSN 1857-0976.
5. Thomas C. Schelling. The Strategy of Conflict. Harvard University Press, 1981, ISBN 9780674251861.
6. Tratatul Atlanticului de Nord. Washington DC, 4 aprilie 1949.
7. Бартош А.А. Стратегия и контрстратегия гибридной войны. 10 октября 2018. https://vm.ric.mil.ru/Stati/item/138034/ [data accesării: 06.04.2022].
8. Гареев М.А. Характер будущих войн // Право и безопасность. 2003. № 1-2 (6-7). URL: http://dpr.ru/pravo/pravo_5_4.htm [data accesării: 15.04.2022].
9. Герасимов В.В. Горячие точки науки // Военно-промышленный курьер. № 12 (725). 2018. 27 марта. URL: https://vpk-news.ru/articles/41870 [data adresării: 17.08.2022].
10. Мольтке Г. фон (старший). О стратегии. // Стратегия в трудах военных классиков. Т. II. М.: Госвоениздат, 1926. URL: http://militera.lib.ru/science/classic2/15.html [data accesării: 15.04.2022].

DESPRE AUTORI

Alexandru PARENIUC,
dr., conf. univ.,
şef-adjunct al Direcţiei studii
şi management al calităţii
a Academiei „Ştefan cel Mare" a MAI,
e-mail:alexandru.pareniuc@mai.gov.md,
ORCID: https://orcid.org/0000-0002-6642-4610

Vasili BEDA,
doctorand,
Academia „Ştefan cel Mare " a MAI,
e-mail:vasili.beda@gmail.com,
ORCID: https://orcid.org/0000-0002-7873-371X