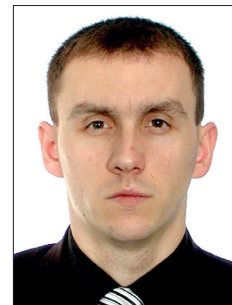


CZU 327.5

DOI 10.5281/zenodo.7184282



Alexandru PARENICU,
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 subiecților procesului politic la nivel global sau regional. Cu toate acestea, o asemenea conflagrație se realizează în principal prin mijloace nemilitare, fără ocuparea țării învinse, evitând distrugerea infrastructurii acesteia și moartea în masă a populației [4, p. 101].

Scopul studiului. Autorii trec în revistă fenomenului amenințărilor hibride, precum și o analiză a esența și conținutul strategiei și contrastrategiei utilizate de părțile opuse în pregătirea și în timpul războiului hibrid.

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

de comparare. Materialele utilizate în vederea realizării studiului sunt publicațiile cercetătorilor în domeniu, precum și legislația relevantă. În baza analizei materialelor sunt formulate concluziile și propunerile corespunzătoare.

Rezultate obținute și discuții. Strategia și contrastrategia războiului hibrid. Strategia integrează rezultatele analizei schimbărilor și le transformă în pași practici concreți. Cunoscutul teoretician militar, șeful Statului Major al Prusiei, Helmuth von Moltke (senior), menționa: „*Strategia este mai mult decât știință; este transferul de cunoștințe în viața practică, dezvoltarea ulterioară a gândirii călăuzitoare originale în conformitate cu circumstanțe în continuă schimbare; strategia este arta de a acționa sub jugul celor mai dificile condiții*” [10].

Lista factorilor care determină evoluția afacerilor militare s-a schimbat de-a lungul secolelor. Astăzi, procesele de globalizare și revoluția informației și comunicării, care formează noi mecanisme de interacțiune și interdependență la scară globală și regională, au cea mai profundă și cuprinzătoare influență asupra dezvoltării strategiilor pentru conflictele militare moderne, precum și asupra schimbării naturii și conținutului lor. Acoperind economia mondială, politica, domeniul militar, comunicațiile, sportul, știința și cultura, aceste procese foarte contradictorii și dinamice afectează toate cele mai importante sfere ale societății moderne.

Strategia conflictelor moderne, construită pe o combinație a unei game largi de forme și metode de luptă, conține un număr mare de semnificații. Cu această ocazie, președintele Academiei de Științe Militare, generalul de armată M.A. Gareev, afirma încă în 2003: „Autorii, lacomi de senzații, aproape în fiecare zi dau nume noi războaielor viitorului: tridimensional, de rețea, asimetric, fără contact, informațional etc. Da, toate aceste elemente vor avea loc, ele reflectă una dintre trăsăturile caracteristice ale confruntării militare, dar niciuna dintre ele nu caracterizează individual fața războiului în ansamblu” [8].

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

Prima este o formulare clară a sensului

și scopurilor războiului.

A doua este identificarea punctelor slabe și vulnerabilităților în sfera asigurării securității interne și externe a statului inamic.

A treia este formarea unui complex de amenințări hibride, ținând cont de specificul local pentru a influența obiectul agresiunii.

A patra este planificarea strategică bazată pe o relatare specifică a forțelor și mijloacelor naționale, menite să influențeze blocajele și vulnerabilitățile inamicului în sfera politică, administrativă, financiară, economică, culturală și ideologică, precum și o analiză a contracarării sale așteptate (*variante activității de contrastrategie*).

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

A șasea este desfășurarea ostilităților nedecarate, în timpul cărora statul-agresor atacă structurile țării și armata regulată a inamicului cu ajutorul rebelilor locali și separatiștilor susținuți cu armament și finanțe din străinătate. Un loc important este acordat acțiunilor „*coloanei a cincea*”, care dobândesc un caracter extremist, folosit pentru a lansa atacuri asupra autorităților în cursul uneia sau mai multor „*revoluții colorate*”.

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

Teoria descurajării. Metode de rezistență împotriva amenințărilor 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 forței are loc la o scară cunoscută.

În al doilea rând, această scară presupune că părțile au o bună înțelegere a mecanicii utilizării instrumentelor militare specifice și a consecințelor unei astfel de utilizări. Această

înțelegere este întărită de evaluarea de către rivali a raportului de putere, care, de regulă, se reduce la capacități pur militare. În cele din urmă, teoria descurajării militare nu ține cont de consecințele utilizării instrumentelor nemilitare în declanșarea unui război [3].

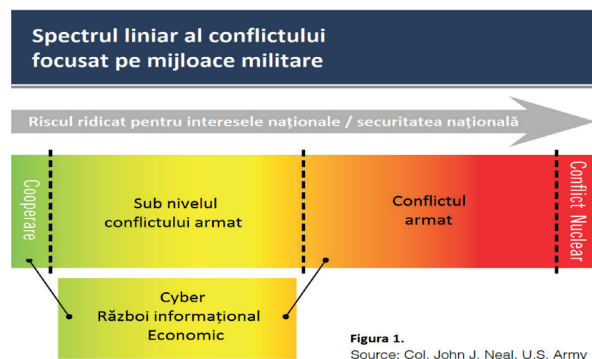
Schema constă într-o aranjare liniară a nivelurilor de criză și a nivelurilor de risc corespunzătoare. Subiecții se deplasează în sus sau în jos pe această scară, efectuând acțiuni care măresc sau, respectiv, scad nivelul de amenințare al inamicului. Acest concept a fost aplicat scenariilor Războiului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

Metoda balanței puterii a fost folosită pentru a determina prețul care trebuie plătit pentru o anumită acțiune, fiecare stat putând să-și cuantifice punctele forte și punctele slabe cu relativă ușurință.

Instrumentele non-militare, totuși, nu sunt cuantificabile și, prin urmare, consecințele potențiale ale utilizării acestor mijloace sunt mult mai abstracte. Există, de asemenea, un cadru general acceptat pentru costurile potențiale ale unui conflict militar în creștere și 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.

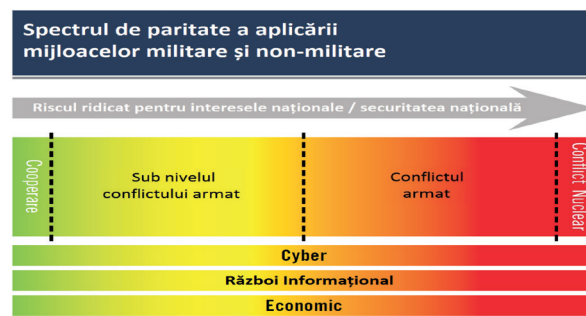
Conceptele din trecut au fost sub forma unei scale mobile și s-au concentrat pe utilizarea forței militare, mijloacele nemilitare fiind o componentă auxiliară a celor militare (Figura 1).

Aceasta a reflectat ideea că acțiunea mi-



litară are o ierarhie de escaladare bine definită, cu caracteristici distinctive clare și că mijloacele nemilitare au un rol de susținere prost definit și cu greu reprezintă o amenințare.

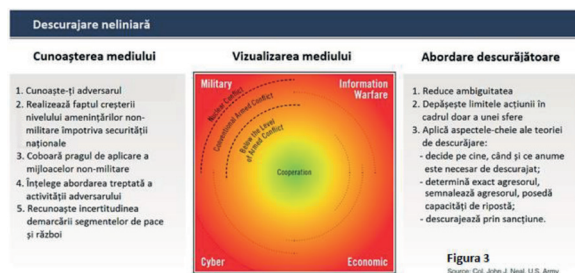
Acum recunoaștem că mijloacele non-militare reprezintă o mare amenințare la adresa securității naționale și, în viitor, pot reprezenta aceeași amenințare ca și instrumentele militare. Cu toate acestea, aceste zone sunt adesea considerate izolat și li se aplică scara teoretică a potențialei escalade (Figura 2).



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

Modelul de concept în evoluție se îndepărtează de scara de escaladare pe măsură ce nevoia de această scară scade din cauza că părțile opuse caută modalități de a ocoli normele stabilite. În acest model, mijloacele militare și nemilitare sunt prezentate ca fiind egale în capacitatea lor de a reprezenta o amenințare la adresa intereselor naționale și a securității naționale.

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



Abordări descurajatoare

Primul principiu al abordărilor descurajatoare este **reducerea ambiguității**. Ambiguitatea este un factor critic al strategiilor concurențiale. 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 estepornită 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.

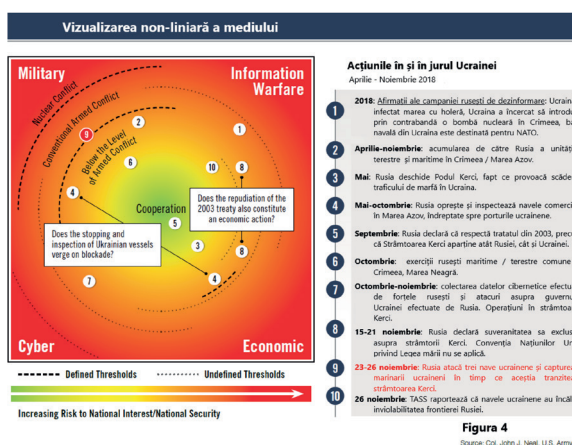
Un exemplu este articolul 5 din Tratatul Atlanticului de Nord, care prevede că *un atac armat împotriva unui membru al Alianței va primi răspuns din partea tuturor aliaților* [6].

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



„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 infrafracțiuni 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 politicianilor 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 *Wiki-Leaks*, 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 țările sau formațiunile terțe, folosește mercenari, companii militare private, activează formațiunile interne neregulate, „coloana a cincea” și agenți de influență;

– **formal, în cazul războiului hibrid lipsește aparatul central de conducere și dirijare a acțiunilor ostile**. Scopul comun pentru distrugerea statului inamic este dezvoltat și convenit la nivelul organismelor guvernamentale, conducerii corporațiilor transnaționale, structurilor financiare și bancare, precum și persoanelor influente;

– **planurile de acțiune pentru destabilizarea sferelor administrativ-politice, socio-economice, culturale și ideologice** prevăd crearea unor structuri de rețea distribuite pe teritoriul inamic cu un grad ridicat de independență și capacitate de autosincronizare. Sunt elaborate în prealabil canalele pentru sprijinul lor financiar, logistic, informațional și de personal, sunt create depozite pentru arme, muniții, comunicații, sunt selectate locuri pentru pregătirea militanților;

– **se folosesc catalizatori-acceleratori ai proceselor subversive**, în special demersurile diplomatice, sancțiunile economice, umplerea de informații și acțiunile de succes ale forțelor neregulate împotriva unor obiecte importante. Un catalizator puternic în acest sens sunt „revoluțiile colorate”, organizate într-un punct de cotitură important al războiului, pentru a accelera procesul de destabilizare a statului, asemănător avalanșelor. Descoperirea la timp a pregătirii operațiunilor care vizează accelerarea proceselor de prăbușire a statului este cea mai importantă sarcină a serviciilor de intelligence;

– **forțele de operațiuni speciale sunt folosite împotriva obiectelor importante din punct de vedere strategic**, pentru a răpi și asasina lideri politici și pentru a oferi sprijin formațiunilor neregulate;

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

Concluzii. Amenințările hibride nu sunt un fenomen nou, dar în această lume globalizată, cu dezvoltarea uluitoare a comunicațiilor din ce în ce mai rapide, impacturile acestor amenințări devin masive și periculoase. Ele ridică noi provocări pentru politicile și agențiile de securitate națională, dar, în același timp, măsurile defensive adecvate deschid oportunități imense pentru societăți.

Reziliența adevărată necesită un anumit grad de satisfacție și fericire în rândul tuturor cetățenilor. Guvernele responsabile și actorii societății civile trebuie să țină cont de legătura strânsă dintre securitatea societală și națională și să depună eforturi pentru a-și face cetățenii mai fericiți și națiunile mai puternice.

Natura conflictelor se schimbă. Statele recurg din ce în ce mai mult la mijloace non-militare pentru a-și atinge obiectivele, schimbând pe parcurs conceptul de escaladare a conflictului. Această utilizare interdependentă a mijloacelor militare și non-militare a condus la o estompare a graniței dintre război și pace. Acești factori au creat condiții în care părțile opuse exploatează nedemonstrabilitatea atacurilor lor și absența normelor internaționale de conduită în avantajul lor, amenințând statele cu acțiuni care în trecut erau de neimaginat. Pentru a-și asigura interesele în viitor, statele trebuie să își adapteze înțelegerea privind activitatea de descurajare la noile condiții.

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

Referințe bibliografice

1. Daniel W. Altman. Red Lines and Facts 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 științifice ale Academiei „Ștefan cel Mare” a MAI al Republicii Moldova, Științe 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.,
șef-adjunct al Direcției studii
și management al calității
a Academiei „Ștefan cel Mare” a MAI,
e-mail:alexandru.pareniuc@mai.gov.md,
ORCID: <https://orcid.org/0000-0002-6642-4610>*

Vasili BEDA,

*doctorand,
Academia „Ștefan cel Mare ” a MAI,
e-mail:vasili.beda@gmail.com,
ORCID: <https://orcid.org/0000-0002-7873-371X>*