UNIVERSITATEA NAȚIONALĂ DE APĂRARE „CAROL I”
CENTRUL DE STUDII STRATEGICE DE APĂRARE ȘI SECURITATE

IMPACT STRATEGIC

Nr. 2[63]/2017

Revistă ştiinţifică trimestrială, cu acces liber
şi prestigiu recunoscut de CNATDCU, indexată în baze de date
internaţionale (BDI): CEEOL, EBSCO, ProQuest, IndexCopernicus,
WorldCat, ROAD

EDITURA UNIVERSITĂŢII NAŢIONALE DE APĂRARE „CAROL I”
BUCUREŞTI

CONSILIUL EDITORIAL

Prof. univ. dr. Gheorghe CALOPĂREANU, Universitatea Naţională de Apărare „Carol I”, preşedintele Consiliului editorial
Prof. univ. dr. Daniel DUMITRU, Universitatea Naţională de Apărare „Carol I”
Prof. univ. dr. Valentin DRAGOMIRESCU, Universitatea Naţională de Apărare „Carol I”
Prof. univ. dr. Marian STANCU, Universitatea Naţională de Apărare „Carol I”
Prof. univ. dr. Vasile BUCINSCHI, Academia Forţelor Aeriene „Henri Coandă”
Prof. univ. dr. Florian RĂPAN, Universitatea Creştină „Dimitrie Cantemir”
Conf. univ. dr. Florin DIACONU, Universitatea din Bucureşti
Lect. univ. dr. Stan ANTON, Universitatea Naţională de Apărare „Carol I”
Prof. univ. dr. Dariusz KOZERAWSKI, Universitatea Naţională de Apărare, Polonia
Prof. univ. dr. Bohuslav PRIKRYL, Universitatea Naţională de Apărare, Cehia
Prof. univ. dr. ing. Pavel NECAS, Universitatea de Management al Securităţii, Slovacia
Prof. univ. dr. John L. CLARKE, Centrul European pentru Studii de Securitate „George C. Marshall”, Germania
Prof. univ. dr. Ilias ILIOPOULOS, Colegiul de Război al Forţelor Navale, Republica Elenă
Prof. univ. dr. ing. Adrian GHEORGHE, Universitatea „Old Dominion”, SUA
Conf. univ. dr. Georgi DIMOV, Colegiul Naţional de Apărare, Bulgaria
Dr. Gábor BOLDIZSÁR, Universitatea Naţională pentru Servicii Publice, Ungaria
Dr. Peter TÁLAS, Universitatea Naţională pentru Servicii Publice, Ungaria
Dr. Mircea TĂNASE, Statul Major General, Ministerul Apărării Naţionale
Dr. Igor SOFRONESCU, Academia Militară „Alexandru cel Bun”, Republica Moldova

REFERENŢI ŞTIINŢIFICI

CS II dr. Mirela ATANASIU
CS II dr. Cristian BĂHNĂREANU
CS III dr. Cristina BOGZEANU
Lect. univ. dr. Florian CÎRCIUMARU
ACS asoc. Valentin IACOB
CS I dr. Constantin MOŞTOFLEI
Prof. univ. dr. Visarion NEAGOE
CS III dr. Marius POTÎRNICHE
CS II dr. Alexandra SARCINSCHI
ACS Cătălina TODOR
CS dr. Mihai ZODIAN

COLEGIUL DE REDACŢIE

Redactor-şef: dr. Stan ANTON
Redactor-şef adjunct: dr. Daniela RĂPAN
Redactor „Colocviu strategic”: Cătălina TODOR

ADRESĂ

Şos. Panduri, nr. 68-72, sector 5,
Bucureşti, România
Telefon: (021) 319.56.49; Fax: (021) 319.57.80
Website: http//cssas.unap.ro
E-mail: impactstrategic@unap.ro

Responsabilitatea privind conţinutul articolelor publicate revine în totalitate autorilor, respectând prevederile Legii nr. 206 din 27 mai 2004 privind buna conduită în cercetarea ştiinţifică, dezvoltarea tehnologică şi inovare. Sunt autorizate orice reproduceri, fără perceperea taxelor aferente, cu condiţia precizării exacte a sursei.

Opiniile exprimate în materialele publicate aparţin strict autorilor şi nu reprezintă poziţia CSSAS/UNAp.

ISSN 1842-810X; ISSN-L 1582-6511

CUPRINS

EVENIMENT ȘTIINȚIFIC

AGENDA CSSAS

GHID PENTRU AUTORI

CUVÂNTUL EDITORULUI

Ediția a doua din anul 2017, cu numărul 63, cuprinde o colecție de șapte articole, la care se adaugă tradiționalele *Agenda CSSAS*, *Eveniment științific* și *Ghidul pentru autori*.

Revista este deschisă cu rubrica ***Actualitatea politico-militară***, unde domnul general (r) Teodor Frunzeti și domnul Cristian Bărbulescu ne relevă o serie de *determinări ale conduitei hibride în sistemul internațional actual și noile tipuri de amenințări derivate din conflictele emergente*.

Geopolitici și geostrategii – tendințe și perspective, unde colega noastră, ACS Cătălina Todor, împărtășește cu dumneavoastră rezultatele studiului său despre *actualitatea modelului spirală al dilemei securității în analiza mediului internațional*.

În continuare, dl. Răzvan Munteanu realizează o analiză a *rolului statului Bahrain în viziunea geostrategică a Iranului și Arabiei Saudite.*

Urmează rubrica ***Securitate și strategie militară***, la care puteți citi materialul elaborat în coautorat de domnul comisar-șef de poliție Ștefan Săvulescu împreună cu doamna comisar de poliție Mihaela Țone, referitor la *creșterea rezilienței instituționale în fața amenințărilor la adresa securității naționale*, ce a fost susținut la Simpozionul organizat de CSSAS în data de 25 mai 2017.

În continuare, domnul locotenent colonel Dan-Lucian Petrescu înaintează un *model avansat de configurare a agresiunii de tip hibrid.*

La rubrica intitulată ***Concepte de apărare și securitate***, am inclus două articole, primul aparținându-i colegei noastre, CS II dr. Mirela Atanasiu, referitor la *abordări conceptuale ale spațiului cibernetic în NATO, UE și România*.

În cel de-al doilea material, doamna lector universitar dr. Florentina Dragomir prezintă o serie de *modele matematice specifice domeniului militar*.

Noua noastră colegă, Andra Pînzariu vă prezintă, la rubrica ***Eveniment științific***, câteva concluzii în urma Simpozionului internațional „Cooperarea interinstituțională, – instrument de realizare a securității la nivel național și internațional”, organizat de CSSAS în data de 25 mai 2017.

Agenda CSSAS pentru perioada aprilie-iunie vă este adusă la cunoștință de către colega noastră, Raluca Stan.

În încheierea ediției, dna. dr. Daniela Răpan semnalează ***Ghidul pentru autori***, acesta fiind o lectură obligatorie pentru cei care doresc să disemineze rezultatele cercetării în *Impact strategic*.

Pentru cei care descoperă pentru prima dată *Impact strategic*, publicația, editată de Centrul de Studii Strategice de Apărare și Securitate, cu sprijinul Editurii Universității Naționale de Apărare „Carol I” este *revistă științifică cu prestigiu recunoscut din domeniul științe militare, informații și ordine publică*, conform Consiliului Național de Atestare a Titlurilor, Diplomelor și Certificatelor Universitare (CNATDCU).

Publicația apare de șaptesprezece ani în limba română și de doisprezece ani în limba engleză și

abordează o arie tematică complexă – actualitatea politico-militară, strategii de securitate, strategie militară, politici, strategii şi acţiuni NATO şi UE, problematica păcii şi a războiului viitorului, societatea informaţională, elemente şi aspecte privind comunitatea de informaţii. Cititorii găsesc în paginile publicaţiei analize, sinteze şi evaluări de nivel strategic, puncte de vedere în care se studiază impactul dinamicii acţiunilor pe plan naţional, regional şi global.

În ceea ce priveşte vizibilitatea pe plan internaţional – obiectiv primordial al publicaţiei –, recunoaşterea calităţii ştiinţifice a revistei este confirmată prin indexarea în bazele de date internaţionale CEEOL (Central and Eastern European Online Library, Germania), EBSCO (SUA), ProQuest (SUA) şi Index Copernicus International (Polonia), la acestea adăugându-se, recent, WorldCat şi ROAD ISSN, dar şi prin prezenţa în cataloagele virtuale ale bibliotecilor din instituţii prestigioase de peste hotare, precum NATO şi ale unor universităţi cu profil militar din Bulgaria, Polonia, Republica Cehă, Ungaria, Estonia etc.

Impact strategic se tipăreşte trimestrial, în două ediţii distincte: una în limba română şi alta în limba engleză. Revista este difuzată gratuit în principalele instituţii din sfera securităţii şi apărării, în mediul ştiinţific şi în cel academic din ţară şi din străinătate – în Europa, Asia, America.

În încheiere, îi încurajăm în continuare pe cei interesaţi să publice în paginile revistei să prospecteze şi să evalueze cu rigoare dinamica mediului de securitate şi, totodată, lansăm invitaţia către studenţii, masteranzii şi doctoranzii interesaţi să trimită articole spre publicare în suplimentul lunar al revistei, *Colocviu strategic*, disponibil pe internet la http://cssas.unap.ro/ro/cs.htm.

Redactor-şef, colonel dr. Stan ANTON
Directorul Centrului de Studii Strategice de Apărare şi Securitate

DETERMINĂRI ALE CONDUITEI HIBRIDE ÎN SISTEMUL INTERNAȚIONAL ACTUAL ȘI NOILE TIPURI DE AMENINȚĂRI DERIVATE DIN CONFLICTELE EMERGENTE

Dr. Teodor FRUNZETI*
Cristian BĂRBULESCU**

Evoluțiile recente din mediul de securitate global – precum criza din Ucraina și resurgența fenomenului terorist de factură fundamentalist-islamică – au reaprins dezbaterile în mediile de analiză specializate în domeniul relațiilor internaționale și studiilor de securitate pe tema reconfigurării sistemului internațional și apariției unor schimbări revoluționare în practica războiului modern.

Lucrarea de față evidențiază dintr-o perspectivă a teoriei relațiilor internaționale cum anume competiția geostrategică modelează formele hibride de manifestare a agresivității în relațiile dintre actorii sistemului internațional. În esență, vom arăta cum confruntările dintre actori sunt influențate de tendințele de remodelare și reașezare manifeste în sistemul internațional și vom evidenția faptul că acțiunile hibride și difuze, situate la limita dintre pace și război, reprezintă pentru puterile emergente o formă de contestare a influenței polului dominant la nivel global (scopul fiind de legitimare a multipolarității în sistemul internațional).

***Cuvinte-cheie**: sistem internațional multipolar, conflicte emergente, actor statal, actor non-statal, amenințare hibridă.*

1. Considerații preliminare

Actualul *sistem internațional* traversează o perioadă de *transformare structurală,* cu implicații asupra elementelor componente care îl definesc – actorii, dimensiunea, structura, procesele și capacitatea de interacțiune[1]. Procesul de transformare este ireversibil și este generat de discontinuitățile care apar permanent la nivelul

1 Cadrul conceptual propus de Barry Buzan este deosebit de util pentru înțelegerea evoluțiilor care modelează sistemul internațional. În esență, acesta evidențiază nivelurile de analiză (sistemul internațional, subsistemele, unitățile etc.), sectoarele de analiză (politic, militar, economic, socio-cultural și de mediu) și sursele de explicație (procesul, capacitatea de interacțiune și structura), ca părți ale cadrului conceptual necesar analizei și evaluării evoluțiilor în sistemul internațional.

[*] ***Dr. Teodor FRUNZETI, doctor în ştiinţe militare şi în ştiinţe politice, este profesor universitar în cadrul Univesității „Titu Maiorescu”, președintele secției de științe militare din cadrul Academiei Oamenilor de Știință din România. E-mail: tfrunzeti@gmail.com***

[**] ***Cristian BĂRBULESCU este doctorand în domeniul informații și securitate națională la Universitatea Națională de Apărare „Carol I” și asistent de cercetare în cadrul Academiei Oamenilor de Știință din România. E-mail: cebarbulescu@gmail.com***

actorilor (care le determină evoluția sau involuția) și cel al *relațiilor* care se stabilesc între aceștia, stare care conduce, finalmente, la regenerarea continuă a sistemului internațional.

Majoritatea relatărilor recente pe tema transformării sistemului internațional se reduce la ideea de schimbare a puterii dominante sau a polarității în interiorul acestuia, deși procesul *per se* (de transformare) vizează mult mai multe paliere (tehnologic, informațional, politic, economic și militar). Analiza noastră pornește de la premisa conform căreia schimbările care au loc în sistemul internațional vizează *procesele dominante* (politice, militare, economice, socio-culturale) existente în interiorul acestuia.

2. Tendințe de evoluție în relațiile internaționale

În actualul sistem internațional, coexistă și interferează reprezentarea celor trei curente dominante în teoria relațiilor internaționale – *realismul structuralist* (sau neorealismul), *neoliberalismul* și *constructivismul*. Diferențele de nuanță sunt cele care întrețin „concurența" dintre cele trei teorii. Perspectiva *realistă*, conform căreia într-un sistem anarhic actorul însuși este singurul care își poate asigura securitatea și contribui la menținerea echilibrului în sistemul internațional, se distinge de cea *liberală*, care susține ideea de normare internațională a relațiilor dintre actori, și de cea *constructivistă,* care promovează faptul că, în condiții de anarhie, identitatea și interesele actorilor derivă din interacțiunile acestora, derulate după regulile impuse de mediul în care au loc.

Teoria neorealistă pare a fi încă o dominantă în relațiile internaționale. Sistemul internațional actual rămâne dominat de capacitatea influență și de proiectare a puterii a actorilor de tip statal. Pe de o parte, ideea de haos în sistemul internațional este întreținută de conduita actorilor statali, circumscrisă necesității de satisfacere a intereselor proprii în relațiile pe care le stabilesc cu alți actori și de absența unei „instituții" suprastatale care să descurajeze perpetuarea tendințelor egocentriste ale acestora. Pe de altă parte, *creșterea exponențială a gradului de interconectare politică, economică și socială, odată cu accelerarea procesului de globalizare și avansul generat de inovațiile tehnologice, menține viabile opțiunile neoliberale*, fundamentate pe promovarea proiectelor integraționiste și a comunităților de valori și o mai mare deschidere pentru dezvoltarea cadrului de reglementare a interacțiunilor dintre actori, pe domeniile încă insuficient abordate, cum sunt, de exemplu, cel ecologic și cel cibernetic.

Imediat după încheierea Războiului Rece, Barry Buzan evidenția că „noua structură a relațiilor de putere este multipolară, prin faptul că mai multe mari puteri independente se află în joc, dar unipolarizată prin existența unei singure coaliții dominante (cea occidentală, condusă de SUA – n.n.), care guvernează relațiile internaționale"[2]. Prăbușirea URSS a pus punct epocii bipolare, a confruntării dintre cele două mari blocuri politico-militare, NATO și Tratatul de la Varșovia, și a marcat începutul unipolarității în sistemul internațional. *Unipolaritatea reprezintă*, în opinia noastră, *o fază tranzitorie către un sistem policentric de distribuție a puterii la nivel global*. Realitatea descrisă depinde de asumarea de către o singură mare putere a leadershipului la nivel global și rămâne valabilă dacă sunt îndeplinite două condiții esențiale: angajamentul să fie în interesul direct al actorului, prin beneficiile pe care acesta i le produce la nivel politic și economic și nicio altă mare putere să nu poată îndeplini și/sau să nu fie interesată de acest rol. Este dificil de evaluat, în prezent, dacă această etapă intermediară a fost sau nu parcursă integral. Din perspectivă militară, considerăm că actualul sistem internațional este încă unul *unipolar* fiind dominat de o singură mare putere, și anume SUA, care dispune de capacitatea de proiecție a forței la nivel global. Dacă, peste dimensiunea militară, suprapunem dimeniunile politică, economică și socio-culturală, obținem o imagine completă asupra sistemului internațional, care reflectă existența mai multor centre regionale de putere în competiție (SUA, Europa, Federația Rusă, India,

[2] Barry Buzan, „New Patterns of Global Security in the Twenty-First Century", în *International Affairs*, Royal Institute of International Affairs 1944-), Vol. 67, No. 3 (Jul.,1991), p. 437, URL: http://www.jstor.org/stable/2621945, accesat la 06.05.2017.

China și Extremul Orient) și surse de instabilitate (în Europa de Est, Caucaz, Orientul Mijlociu și Nordul Africii, Asia-Pacific).

Contestarea rolului hegemonic al polului de putere dominant (în prezent, asociat SUA și Occidentului) va influența cu certitudine configurarea aranjamentelor viitoare în interiorul sistemului internațional. *Scenariul realist al unei lumi multipolare bazată pe echilibrul de putere* între diferitele centre politico-economice și militare regionale este susținut de evoluțiile din sistemul internațional actual. În prezent, se remarcă tot mai acut dificultatea de punere în aplicare a politicilor și programelor liberale dedicate stabilității internaționale și regionale, promovate prin intermediul ONU și se constată o accentuare a politicilor asertive ale marilor puteri emergente (China și Federația Rusă), precum și o tendință de creștere a profilului regional și global al organizațiilor politico-economice suprastatale (*UE, Uniunea Economică Euroasiatică/UEE, Asociația Națiunilor din Sud-Estul Asiei/ASEAN*). Acest scenariu va fi acceptat chiar de actorii suprastatali (UE, ASEAN, UEE), constituiți pe baza principiilor *neoliberalismului*. Aceștia nu vor renunța la valorile care le definesc existența, dar vor căuta să capete „personalitate" în noul sistem de relații internaționale, devenind tot mai mult implicate politic la nivel regional și global. De altfel, definirea personalității în interiorul sistemului internațional este un obiectiv deja asumat la nivelul UE, cel mai avansat proiect regional de integrare politico-economică, fiind inclus în Strategia Globală asupra Politicii Externe și de Securitate a Uniunii Europene (2016)[3].

În opinia noastră, acreditarea *sistemului post-modern policentric de distribuție a puterii* nu va conduce, în mod obligatoriu, la decăderea ideilor liberale asupra relațiilor internaționale. Dimpotrivă, acest scenariu reflectă supraviețuirea *modelului liberal integraționist într-o lume multipolară*. *Noua ordine mondială post-modernă va funcționa ca un hibrid,* prin simbioza principiilor liberale și neorealiste aplicate în relațiile internaționale.

Noua configurație a sistemului mondial va conduce la o *translatare a competiției geostrategice de la nivel global la nivel regional*. Această perspectivă este favorizată de prezența mai frecventă a mizelor economice în interacțiunile dintre actori și a tendințelor de integrare a piețelor la nivel regional și inter-regional (ex.: inițiativa chineză „Drumul Mătăsii", Acordul economic și comercial cuprinzător/CETA dintre Uniunea Europeană și Canada, Acordul Transpacific). Spunem, prin urmare, că *sistemul internațional urmează o etapă de transformare structurală* pentru că, în cea mai mare parte, schimbarea majoră survine din concentrarea politicilor asupra dimensiunii politico-economice la nivel regional.

În acest scenariu, dimensiunea militară nu este minimizată, ci servește satisfacerii intereselor politice și economice ale actorilor în competiție. Complementaritatea celor două dimensiuni, economică și militară, în acțiunile de pe scena internațională, reflectată prin combinarea instrumentelor de putere de tip „*soft*" și „*hard*" constituie o tendință în relațiile internaționale. Schimbările rapide care au loc în domeniul tehnologic antrenează creșterea nivelului de interconectare globală, fenomen vizibil, cu precădere, în domenii conexe precum cel social și economic.

În plan social, multiplicarea posibilităților de comunicare în interiorul comunităților și statelor și în afara acestora descrie realitatea *societății informaționale* în care trăim. În plan economic, avansul relativ lent înregistrat de SUA (2,2%) și statele din Uniunea Europeană (2,3%) în comparație cu statele din Asia – China (6,8%), India (7,1%) și Indonezia (5,2%) – și menținerea aceleiași tendințe pentru următoarea decadă[4]

[3] Strategia Globală pentru Politica Externă și de Securitate a UE (2016) prevede promovarea valorilor și intereselor europene (pace și securitate, democrație și o ordine globală fundamentată pe reguli) în plan global. A se vedea: ***, A Global Strategy for the European Union's Foreign and Security Policy. Shared Vision, Common Action: A Stronger Europe, June 2016, p. 13, http://europa.eu/globalstrategy/sites/globalstrategy/files/regions/files/eugs_review_ web_0.pdf, accesat la 12.05.2017.

[4] Date exprimate pentru 2017, conform World Economic Outlook, October 2017, Fondul Monetar Internațional, http://www.imf.org/external/datamapper/NGDP_RPCH@WEO/OEMDC/WEOWORLD/CHN/USA/ADVEC/EU/AS5/DA/BRA/IND, accesat la 30.11.2017.

accentuează reflexele naționaliste și sentimentele protecționiste la nivelul societăților occidentale. Puterea economică nu este, însă, suficientă în reconfigurarea balanței de putere la nivel global, dar reprezintă, cu siguranță, unul dintre factorii determinanți ai acestui proces. Factorul economic contribuie într-o mare măsură la consolidarea și dezvoltarea puterii militare a marilor actori în competiție (SUA, pe de o parte, și China și Federația Rusă, pe de altă parte), ale căror cheltuieli militare s-au dublat în ultimii zece ani[5]. Pe cale de consecință, factorul economic are un aport și la accentuarea tendinței de redefinire a raporturilor de putere dintre aceștia.

Din această perspectivă, interesează modul în care se reflectă conflictualitatea în raporturile viitoare de confruntare, care sunt factorii care pot modela conduita agresivă a actorilor și cum se manifestă aceasta și dacă există o relație dintre conduita hibridă a actorilor internaționali și dinamica relațiilor din sistemul internațional.

3. Factori generatori de schimbare în sistemul internațional

3.1. Inovațiile tehnologice

Societatea informațională actuală este produsul inovațiilor generate de „*cea de-a patra revoluție tehnologică*”[6]. Fuziunea sistemelor fizice de calcul cu rețelele de prelucrare și comunicare a datelor și, în plus, gradul ridicat de interacțiune dintre tehnologiile inteligente și factorul uman pot genera schimbări în planul securității.

Produsele tehnologice avansate determină mutații în fizionomia războiului[7]. În conflictele moderne, distincția dintre pace și război, dintre combatanți și necombatanți, violență și non-violență (mai ales, în domeniul cibernetic) devine dificil de realizat. Această situație se poate explica și pe baza produselor tehnologice avansate care pot substitui dislocările de forțe în teren (ex.: un avion fără pilot poate neutraliza un obiectiv al adversarului, fără ca acesta să realizeze originea atacatorului). De asemenea, *existența sistemelor autonome comerciale face ca diversele produse nocive, accesibile pe piața liberă (ex.: chimice și biologice) să fie mai ușor de folosit la nivelul indivizilor și grupurilor de indivizi*. Așadar, există un risc ridicat ca astfel de „arme” să fie operate de actori non-statali[8] (ex.: grupări teroriste, forțe paramilitare) în acțiuni cu caracter destabilizator.

Dezvoltarea fără precedent a Internetului și accesul la mijloacele de comunicații mobile inteligente influențează nu doar *ceea ce facem* ci și *ceea ce suntem*. Viața privată, propriile nevoi (traduse în indicatori de consum), timpul liber, itinerariile de deplasare, disponibilitatea la socializare ș.a. sunt doar câteva caracteristici care ne definesc ca indivizi și care nu ne mai aparțin în exclusivitate odată cu dezvoltarea noilor aplicații inteligente. Tehnologiile sociale multiplică forța ideilor exprimate de grupruri restrânse de indivizi sau mișcări sociale, care devin capabile să influențeze semnificativ comportamentul comunităților și statelor din care fac parte.

3.2. Translatarea puterii economice globale pe axa vest - est și sud

Studiile recente indică o perspectivă de reechilibrare a economiilor la nivel global[9]. Dominația economică occidentală este amenințată de creșterea economică progresivă în statele din Asia Centrală și de Sud-Est. Statele în curs de dezvoltare din aceste regiuni vor manifesta o disponibilitate mai mare pentru a investi în apărare și securitate și pentru a-și dezvolta autonomia la nivel regional, eventual prin (re) evaluarea alianțelor cu marile puteri (ex.: SUA, Federația Rusă, China). Pe termen lung, creșterea

[5] ***, SIPRI Military Expenditure Database, Stockholm International Peace Research Institute, https://www.sipri.org/databases/milex, accesat la data de 30.05.2017.

[6] Klaus Schwab, „The Fourth Industrial Revolution - What It Means and How to Respond”, în Foreign Affairs, 12 December 2015, ediția online, https://www.foreignaffairs.com/articles/2015-12-12/fourth-industrial-revolution, accesat la data de 20.05.2017.

[7] *Ibidem.*

[8] ***, *Discussion Paper – The Impact of New Technologies on Peace, Security, and Development*, Independent Commission on Multilateralism, International Peace Institute, aprilie 2016, p. 10.

[9] ***, *The World in 2050 – The long view: how will the global economic order change by 2050?*, Princewaterhouse Cooper (PwC), UK, February 2017, http://www.pwc.com/gx/en/issues/economy/the-world-in-2050.html, accesat la 22.05.2017.

populației în zonele subdezvoltate[10] și scăderea și îmbătrânirea acesteia în cele dezvoltate (ex.: Europa) imprimă schimbări în distribuția creșterii economice, pe direcția Europa – Asia, și atrage după sine o creștere a consumului și a cererii de alimente, apă și energie[11] în zonele subdezvoltate din Africa și Asia. În acest scenariu, se accentuează competiția pentru accesul la aceste resurse, atât în interiorul statelor, cât și între acestea, conducând, în cazuri extreme, la apariția de conflicte armate.

3.3. Slaba / buna guvernare

Statele, de la cele cu economii avansate la cele emergente, se confruntă cu provocări în ceea ce privește asigurarea cadrului politic, economic, juridic și social favorabil dezvoltării propriilor societăți. Progresul și stabilitatea societăților sunt limitate de propagarea corupției, lipsa transparenței decizionale și abaterile de la respectarea drepturilor și libertăților omului. Aceste fenomene determină accentuarea decalajelor dintre societatea civilă și autorități și, pe cale de consecință, vulnerabilizarea acestora din urmă în fața șocurilor[12].

[10] Ultimul raport al ONU (publicat în anul 2015) privind *„Perspectivele Populației Mondiale"* indica o creștere medie a populației mondiale de aproximativ 83 de milioane de persoane în fiecare an. Prognozele stabilite în 2015 prevăd că populația umană va continua să crească ajungând la aproximativ 8 miliarde de oameni în 2024 și 9 miliarde în 2040. Pentru detalii, a se vedea: ***, World Population Prospects. Key Findings and Advance Tables, 2015 Revision, United Nations, URL: https://esa.un.org/unpd/wpp/Publications/Files/Key_Findings_WPP_2015.pdf, accesat la data de 21.05.2017.

[11] Organizația pentru Alimentație și Agricultură (*FAO*) estimează o creștere de 70% a producției alimentare totale până în anul 2050. Pentru detalii, a se vedea: ***, Global Agriculture Towards 2050, How to Feed the World 2050. High-Level Expert Forum, 12-13 October 2009, URL: http://www.fao.org/fileadmin/templates/wsfs/docs/ Issues_papers/HLEF2050_Global_Agriculture.pdf, accesat la 16.05.2017. De asemenea, Organizația pentru Cooperare și Dezvoltare Economică (*OCDE*) estimează că cererea globală de apă va crește cu 55% până în 2050. Pentru detalii, a se vedea:Helen Mountford, The Environmental Outlook to 2050, OECD Global Forum on Environment: Making Water Reform Happen, 25-26 October 2011, Paris, URL: https://www.oecd.org/env/ resources/49006778.pdf, accesat la data de 22.05.2017.

[12] ***, *Global trends – Paradox of Progress*, National Intelligence Council, January 2017, NIC 2017-001, p. 67, URL: www.dni.gov/nic/globaltrends, accesat la 22.05.2017

4. Emergența tiparelor acționale hibride în mediul de securitate global

4.1. Conduita actorilor nonstatali

Vidul de putere creat de prăbușirea statelor eșuate din Lumea a Treia determină apariția și perpetuarea crizelor de securitate regionale cu implicații la nivel global. Acțiunile recente ale *grupărilor teroriste* derulate atât în zonele de conflict din Orientul Mijlociu și Nordul Africii cât și pe teritoriul statelor vest europene[13] reflectă *caracterul hibrid și complex al fenomenului terorist actual*. La nivel global, potențialul de acțiune al grupărilor teroriste este în creștere odată cu dispariția liniei de demarcație între acțiunile executate în teatrul de confruntare și atacurile executate în exteriorul acestora, pe teritoriul statelor occidentale. Activitatea grupării ISIS în regiunea Orientului Mijlociu relevă o abordare nouă, de tip *centru – periferie*, în practica acțiunilor teroriste. Aceasta poate fi descrisă printr-o concentrare a efortului în *aria de operații de proximitate* și capitalizarea succesului operațional în *aria de influență extinsă*, la nivelul întregii lumi musulmane, și în *exteriorul zonelor controlate teritorial*, prin răspândirea ideologiei radicalismului islamic, atragerea de noi adepți/simpatizanți și folosirea acestora în executarea de atacuri teroriste. Acțiunile grupării produc efecte în plan global, în primul rând, pe fondul aderenței ridicate din partea simpatizanților acesteia la ideologia radicalismului islamic. Ia naștere, astfel, o formă de *terorism autohton,* în care prevalează amenințarea provenită din rândul elementelor radicalizate alogene.

Spre deosebire de grupările teroriste, al căror tipar operațional se limitează la escaladarea deliberată a nivelului de violență în zonele de acțiune și interes ale acestora, în ceea ce privește milițiile, grupările insurgente locale și formațiunile paramilitare, este dificil de realizat o distincție clară din punctul de vedere al obiectului de activitate. Conflictul din estul Ucrainei descrie un model de complex de insurgență, în

[13] A se vedea atacurile care au avut loc, începând cu anul 2015, pe teritoriul Europei (în Franța, Marea Britanie, Germania și Spania).

care miliţiile locale, constituite şi legitimate pe baza afilierii/apartenenţei etnolingvistice ruse, au jucat un rol central în destabilizarea situaţiei de securitate şi, ulterior, în definitivarea procesului de substituire a autorităţilor oficiale cu structuri administrative paralele. Miliţiile şi grupările insurgente locale iau naştere, se reproduc şi sunt dependente de anumiţi factori indigeni, care vulnerabilizează statul-gazdă, în timp ce grupările paramilitare există cu sprijinul politic şi logistic din partea unui stat-sponsor.

4.2. Conduita actorilor statali

Viziunea neoliberală asupra sistemului internaţional şi existenţa unor norme care reglementează conflictele armate dintre actori reduce, în continuare, riscul de apariţie a unui război clasic între actori, dar nu îl elimină în totalitate. O nouă conflagraţie mondială este dificil de imaginat în prezent, când *componenta militară se constituie, cu preponderenţă, în instrument de descurajare*. În acest context, *confruntarea devine mult mai probabilă la nivel regional, în zonele de interferenţă a intereselor marilor puteri, fără escaladarea într-un conflict armat de lungă durată*. Evoluţiile recente dezvăluie trei tipuri de „*tactici revizioniste*" utilizate mari puteri pentru atingerea avantajului competitiv în cadrul conflictelor regionale: evitarea „liniilor roşii" ale apărătorilor, angajarea actorilor intermediari ca agresori şi punerea apărătorilor în situaţii de tipul *fait acompli*[14].

4.2.1. Acţiunile Chinei în Marea Chinei de Est şi Marea Chinei de Sud

Pretenţiile Chinei şi Taiwanului asupra arhipelagului Senkaku/Diaoyu, din Marea Chinei de Est, sub controlul Japoniei, au devenit evidente după descoperirea, în anul 1968, a unor noi resurse de petrol în zonă. Conform datelor publicate de Garda de Coastă a Japoniei[15], începând cu anul 2012, China a sporit prezenţa navelor civile şi militare în apropierea insulelor japoneze. Acţiunile în domeniul naval au fost completate de acţiuni ale aviaţiei militare chineze. Majoritatea acestor acţiuni a constituit provocări lansate de partea chineză, probabil, pentru a identifica „liniile roşii" şi testa reacţiile Japoniei, fiind consumate fără escaladarea violenţelor. Constituirea de către China, în noiembrie 2013, a unei *„zone aeriene de identificare şi apărare"* în Marea Chinei de Est, cu includerea insulelor japoneze, a reprezentat o tentativă de schimbare a *statu quo-ului* în regiune şi de preluare a controlului asupra insulelor japoneze prin intimidarea Japoniei.

Începând cu anul 2013, China s-a angajat într-un proces rapid de *aluvionare şi reconstruire artificială a unor recife din arhipelagul Spratly*, din Marea Chinei de Sud (revendicat de China, Filipine, Taiwan, Vietnam şi de Brunei). Ulterior, în cursul anului 2016, China a trecut la militarizarea insulelor artificiale Fiery Cross, Mischief şi Subi, prin construirea pe acestea a unor elemente de infrastructură, unele cu destinaţie militară[16]. Prin aceste acţiuni, China urmăreşte extinderea Zonei Economice Exclusive şi exercitarea controlului asupra liniilor maritime utilizate pentru transportul resurselor energetice în Asia de Sud-Est. Construirea artificială a insulelor în arhipelagul Spratly constituie o situaţie de tip *fait acompli* la adresa celorlalte state care îşi dispută controlul insulelor şi la adresa SUA prin afectarea libertăţii de mişcare a navelor sale militare în regiune şi extinderea controlului asupra uneia dintre cele mai importante rute comerciale maritime din Asia de Sud-Est.

4.2.2. Abordarea Federaţiei Ruse în conflictele din Georgia şi Ucraina

În anul 2008, Federaţia Rusă s-a angajat într-un conflict deschis cu Georgia. Etapa de escaladare a violenţelor a durat doar cinci zile, pe teritoriul Georgiei. Pe durata confruntării, Federaţia Rusă a combinat forţele militare

[14] Van Jackson, *Tactics of strategic competition - Gray Zones, Redlines, and Conflicts before War*, Naval War College Review, Summer 2017, Vol. 70, No. 3, URL: https://search.proquest.com/openview/38ffba5bf77fcfbcb87a9cdac1f5b1a3 /1?pq-origsite=gscholar&cbl=34989, accesat la data de 03.11.2017.

[15] Pentru detalii, a se vedea: ***, Trends in Chinese Government and Other Vessels in the Waters Surrounding the Senkaku Islands, and Japan's Response - Records of Intrusions of Chinese Government and Other Vessels into Japan's Territorial Sea, Ministry of Foreign affairs of Japan, http://www.mofa.go.jp/region/page23e_000021.html, accesat la data de 03.05.2017.

[16] Asia Maritime Transparency Initiative, https://amti.csis.org/chinas-sam-shelters-spratlys/, accesat la data de 03.06.2017

convenționale cu grupările locale de gherilă și operațiile informaționale[17]. Obiectivele strategice ale Federației Ruse au constat în protejarea separatiștilor georgieni pro-ruși din regiunile Osetia de Sud și Abhazia și descurajarea demersurilor georgiene de aderare la NATO[18]. Acțiunea Federației Ruse a reprezentat un mesaj de avertizare la adresa statelor din regiune cu aspirații de aderare la NATO (cazul Ucrainei) sau apropiere de Alianță (cazul Republicii Moldova) și o reacție fermă la adresa politicilor de extindere promovate de SUA, NATO și UE în estul Europei și Caucaz.

Anexarea peninsulei Crimeea la Federația Rusă (2014) a reprezentat, fără îndoială, un moment strategic de cotitură în relațiile ruso-occidentale, un *fait acompli* la adresa Ucrainei și o reactivare a comportamentului asertiv al Moscovei în raport cu SUA și aliații acesteia europeni. Pe fond, ceea ce a surprins în Ucraina a fost modul de acțiune implementat în anexarea peninsulei Crimea și destabilizarea regiunilor estice ucrainene. Spre deosebire de conflictul din Georgia, în Ucraina, instrumentul militar nu a fost utilizat la vedere pe fondul limitărilor impuse de condițiile din mediul operațional și consecințelor de ordin politic generate de un asemenea curs de acțiune. Ceea ce s-a evidențiat, în schimb, a fost principiul utilizării adaptative a factorului militar, introdus de șeful Marelui Stat Major al Forțelor Armate ruse, gl. Valeri Gherasimov[19] și antrenarea pe scară largă a instrumentelor subversive de natură informațională (propagandă, dezinformare, intoxicare) direcționate asupra populației locale ucrainene și opiniei publice internaționale.

Implicațiile acestor conflicte exced contextul regional de securitate. Observăm că aceste acțiuni difuze au fost inițiate de mari puteri în zonele de interferență a intereselor cu alți actori regionali și că prezența SUA este semnalată în fiecare dintre acestea.

5. Amenințările derivate din conflictele emergente

5.1. Imaginea hibridă a războiului în noul sistem internațional

Războiul este, fără îndoială, un fenomen generator de schimbare în sistemul internațional. Carl von Clausewitz afirma, pe bună dreptate, că „*fiecare epocă își are propriul tip de război, propriile condiții și limitări și propriile preconcepții neobișnuite*”[20]. În opinia noastră,conflictele actuale sunt *un produs al teoriei neoclausewitziene* asupra războiului cu toate particularitățile care decurg din aceasta:

- *Războiul, ca formă de escaladare a violenței, rămâne un instrument al politicii*. Cu alte cuvinte, politica stabilește oportunitatea și/sau intensitatea utilizării factorului militar în confruntare. În prezent și în perspectivă, confruntarea tinde să devină mult mai mult politică decât militară și să se desfășoare în zonele de interferență a intereselor diferiților actori. Intensificarea concurenței politice între marii actori pentru obținerea avantajului competitiv pe scena internațională devine posibilă în condițiile menținerii factorului militar ca instrument prevalent de descurajare, fiecare dintre marii actori preferând anihilarea propriilor adversari prin exploatarea instrumentelor de putere „soft” de care dispun în locul unei soluții militare care implică costuri politice și economice ridicate. În afara structurilor de cooperare regională politico-militare și economice deja consacrate după sfârșitul Războiului Rece, pe scena internațională, se manifestă, din ce în ce mai mult, tendința de apariție a unor *formate alternative de cooperare* destinate soluționării crizelor de securitate recente[21], care vizează

[17] Nathan P. Freier (coord.), *Outplayed: regaining strategic initiative in the gray zone*, United States Army War College Press, Carlisle, 2016, URL: https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=1325, accesat la data de 12.06.2017.

[18] *Ibidem.*

[19] Valeri Gherasimov, „The Value of Science is in the Foresight. New Challenges Demand Rethinking the Forms and Methods of Carrying Out Combat Operations”, în Military Review, January – February 2016, pp. 23-29, http://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/January-February-2016/, accesat la 22.02.2017.

[20] Carl Von Clausewitz, *On War*, Princeton University Press, Princeton, 1976, p. 593.

[21] *Negocierile de la Minsk* pentru soluționarea crizei din Ucraina, *negocierile de la Astana* privind reglemetarea conflictului sirian și posibila revitalizare a negocierilor în cadrul *Grupului celor șase* privind dosarul nuclear nord-

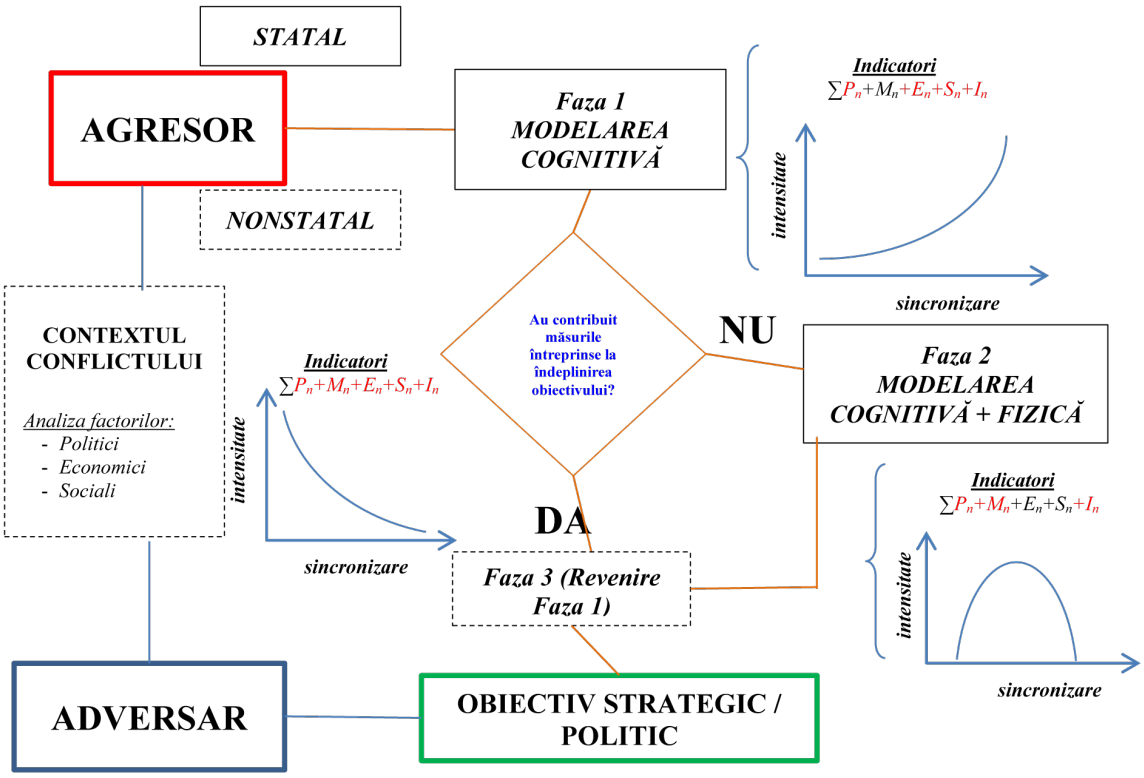

Figura nr. 1 - Matricea amenințărilor (în spectrul politic, militar, economic, social și informațional) în confruntările de tip hibrid

excluderea de la discuții a SUA, puterea dominantă din sistemul internațional. Acest fenomen reprezintă, de altfel, marca declinului autorității ONU și a influenței liberale la nivel global din partea polului de putere occidental (reprezentat de SUA și statele europene) și relansarea competiției politice între marii actori cu interese concurente la nivel regional și global (SUA, China și Federația Rusă).

- *Hibriditatea nu aduce schimbări în natura războiului, ci în fizionomia acestuia*. În esență, *„trinitatea remarcabilă"* a lui Clausewitz, interpretată ca relație între cei trei factori care influențează modalitatea de ducere a războiului – politic, militar și social – se aplică și în cazul *conflictelor actuale*.
- *Războiul hibrid nu este doar un instrument al statelor, ci și al actorilor nonstatali*. Toate cele trei elemente invocate de Clausewitz în descrierea fenomenului se regăsesc și în cele mai recente forme de insurgență sau în practica *grupărilor cu profil terorist*. Astfel, *rațiunea* (politica) acestora se reflectă în aspirațiile de constituire a unor organizări de tip pseudostatal sau de extindere a influenței la nivel transfrontalier, *violența* este alimentată de curentele ideologice radicale promovate în rândul populației-țintă (emoția) și *incertitudinea* (șansa) regăsită în reușita acțiunilor derulate în raport cu adversarul.
- Chiar dacă factorul militar nu este cel dominant, războiul hibrid rămâne *„un act de violență, pentru a sili adversarul să ne îndeplinească voința"*[22], numai că agresivitatea și violența se manifestă pregnant într-o nouă dimensiune, cea cognitivă și/sau informațională. *Violența activă* a maselor pseudo-organizate în cadrul mișcărilor de protest și/sau *violența pasivă* a grupurilor de influență, în mediul online, pe lângă violența clasică determinată de uzul forței militare sau în conjuncție cu aceasta, pot fi esențiale în obținerea succesului în cadrul scenariilor hibride.
- *„Decăderea din drepturi" a factorului militar face dificilă delimitarea clară între cele două stări: pacea și războiul*. Agresiunea militară este un atribut al războiului. Aceasta nu se manifestă decât într-o etapă superioară

corean.

[22] Carl von Clausewitz, *op.cit.*, p. 13.

de evoluție a conflictului în criză, în timp ce *agresiunea simbolică* și cea *informațională*, *diplomația coercitivă* și *atacurile cibernetice*, spre exemplu, se pot manifesta în întreg spectrul de confruntare, pe timp de pace, tensiune/conflict, criză și război.

- *Direcționarea energiei în scopul anihilării centrelor de greutate ale adversarului se menține și în scenariile hibride,* numai că, în acestea din urmă, *efortul se concentrează în zona vulnerabilizării și limitării funcționalității acestora*.

5.2. Modelul conceptual al amenințării în scenariile de confruntare de tip hibrid

Modelul de acțiune aplicat de Federația Rusă în Ucraina nu se pliază, în mod obligatoriu, pe un alt actor expus aceluiași tipar acțional hibrid deoarece caracteristicile mediului operațional nu sunt identice. În scopul decelării acestei prejudecăți (care ne determină, în mod eronat, să ne pregătim pentru a lupta războaie trecute) și pentru o mai bună înțelegere a particularităților conflictelor emergente, considerăm util și oportun efortul de *conceptualizare a amenințărilor derivate din actualitatea confruntărilor difuze și hibride* (a se vedea Figura nr. 1). În opinia noastră, amenințările manifeste în noile scenarii de confruntare de tip hibrid integrează un ansamblu de acțiuni/măsuri întreprinse de un potențial agresor la adresa țintei sale în diferitele stadii posibile de confruntare.

În faza preliminară a confruntării, sunt derulate, după caz, acțiuni non-kinetice în mediul politic, economic și diplomatic, activități specifice de intelligence (culegere de informații, dezinformare) și operații psihologice (de influențare și descurajare a adversarului), acțiuni militare de descurajare activă (utilizarea capabilităților proprii în spațiul aerian și maritim controlat de adversar) și pasivă (evidențierea pericolului unei intervenții militare sau a unor lovituri preemptive) desfășurate planificat, simultan și coordonat asupra unui potențial adversar pentru atingerea obiectivelor politice strategice ale potențialului agresor. Această primă etapă vizează preponderent dimensiunea cognitivă a războiului.

Utilizarea componentei militare, a forțelor și capabilităților armate devine efectivă, ulterior, *în faza activă a confruntării*. Această etapă vizează preponderent dimensiunea materială/fizică a războiului (și se adaugă măsurilor specifice primei faze care rămân active) și poate include, după caz, impunerea unor blocade/zone de interdicție aeriană asupra zonelor care deservesc obiectivele strategice vizate de agresor, executarea de lovituri de înaltă precizie de pe platformele aeriene, navale și/sau terestre, sprijinirea forțelor neregulate de opoziție/grupărilor proxy care acționează pe teritoriul adversarului, dislocarea de forțe de operații speciale (acoperit sau la vedere) pentru neutralizarea obiectivelor dispuse pe teritoriul adversarului.

În final, în faza de detensionare sunt reactivate acțiunile non-kinetice (prezentate în faza preliminară) și, după caz, dislocate forțe regulate la vedere sub diferite pretexte (spre exemplu forțe de menținere a păcii) și, disimulat, pentru desfășurarea activităților de instruire a grupărilor proxy.

Concluzii

Schimbările din interiorul sistemului internațional vizează preponderent *procesele* care modelează *relațiile* dintre actori pe diferitele domenii de interacțiune (politic, economic, militar, socio-cultural) și care contribuie la menținerea echilibrului relativ în interiorul acestuia. În acest context, nu se poate vorbi de o transformare sistemică similară celei care a dat naștere bipolarității de după cel de-al Doilea Război Mondial și mecanismelor și instituțiilor internaționale de reglementare a conflictelor dintre actori.

Conduita hibridă a actorilor internaționali este determinată de accentuarea competiției geostrategice dintre aceștia și tacticile revizioniste ale puterilor emergente (precum China și Federația Rusă) de legitimare a unui sistem internațional policentric. Interesele concurente ale acestora afectează demersurile organizațiilor internaționale implicate în procesul de soluționare a crizelor și contribuie la perpetuarea și extinderea instabilității în afara zonelor afectate (noile crize de securitate capătă caracter global, prin efectele pe care le produc și actorii implicați).

Acest lucru induce imaginea unei ineficiențe a organizațiilor internaționale care, astfel, par desuete, nereformate sau incapabile să răspundă scopului pentru care au fost create, ceea ce nu face decât să accentueze tendința de resetare a sistemului internațional, după principiile *realismului structuralist* al echilibrului de putere asigurat de către mai multe state sau poli regionali de putere.

Perioada de dominație a Vestului sau era „*globalismului centralizat*"[23] este supusă unor presiuni care se manifestă prin tendința de reechilibrare a inegalității distribuției nivelului de dezvoltare economică între „centru" („Lumea Întâi") și zonele de „periferie" („Lumea a Doua" și „Lumea a Treia"). Interdependențele de natură economică și tehnologică manifeste din ce în ce mai pregnant în relațiile dintre actorii sistemului internațional definesc „noul globalism" care, însă, nu mai este atât de puternic influențat de un singur actor internațional cu statut de „superputere". SUA va rămâne, cu siguranță, *primus inter pares* sau actorul care va avea un cuvânt de spus în orice dosar aflat pe agenda internațională. Influența acesteia va fi, însă, contestată de tendințele revizioniste ale actorilor competitori atât în „centru", pe fondul fragilizării coeziunii transatlantice tradiționale, cât și în zonele de „periferie". Această tendință nu reprezintă decât expresia *regionalizării competiției geostrategice* și a emergenței *complexelor regionale de securitate*. Conduita actorilor concurenți integrează un ansamblu de *instrumente legale și ilegale* și *mijloace convenționale și neconvenționale* de exprimare a puterii, utilizate difuz, *la limita dintre starea de pace și cea de război*.

Actorii care contestă actuala ordine mondială vor identifica acele mijloace din „*zonele gri*" (politice, economice, sociale, militare etc.) a căror combinare și sincronizare vor contribui la obținerea avantajului competitiv sau la asigurarea unor mize care vizează controlul zonelor contestate, nu în mod obligatoriu teritorial (deși cazul Crimeii sau al insulelor artificiale chineze din arhipelagul Spratly confirmă această ipoteză) cât, mai ales, politic, economic și informațional.

Creșterea relevanței globale a actorilor nonstatali cu profil insurgent cu concursul statelor-sponsor constituie un factor de multiplicare a complexității în mediul global de securitate. Rolul acestora va crește pe măsură ce competiția geostrategică dintre actorii statali se accentuează. Implicarea diferitelor grupări paramilitare și miliții locale în conflicte de partea și cu sprijinul unor state-sponsor contribuie la menținerea unui nivel relativ de autonomie a acestora la nivel regional (cazul Ucrainei, Yemenului, Siriei și Irakului).

Delimitarea între diferitele stări care pot caracteriza relațiile dintre actori – *pace, criză, conflict sau război* – va fi dificil de realizat cât timp tendința care se manifestă la nivelul actorilor statali este de evitare a escaladării violenței. *Hibriditatea se manifestă în toate din cele patru stări anterior descrise, ceea ce diferă în fiecare dintre acestea fiind doar natura consecințelor produse de agresor prin strategia de combinare a diferitelor instrumente pe care le are la dispoziție*. Distincția dintre pace și război este din ce în ce mai dificil de realizat deoarece, de cele mai multe ori, relațiile dintre părți exced *domeniul fizic* de confruntare (în care se desfășoară operațiile militare clasice). Acestea au loc preponderent în domeniul *cognitiv* (în care cunoașterea asigură implementarea deciziei strategice) și *informațional* (în care se creează și manipulează informația), situație în care consecințele acțiunilor agresorului pot fi dificil de identificat în mod oportun de către țintei, pe fondul deficitului de percepție sau a unei stări de confuzie generalizată.

Evitarea escaladării violenței în cadrul unui conflict armat de amploare din partea actorilor statali cu tendințe revizioniste accentuează latura politică a relațiilor internaționale (în special a celor derulate cu puterea dominantă din sistemul internațional). Accentuarea multipolarității în sistemul internațional poate crește riscul de confruntare armată dintre actori în regiunile în care interesele ale acestora sunt divergente și interferează. Transformarea în sistemul internațional nu este o problemă a zilelor noastre, ci este o constantă care reclamă o permanentă capacitate de adaptare din partea actorilor, mai

[23] Barry Buzan, *The global transformation – history, modernity and the making of international relations*, Cambridge University Press, 2015, p. 274.

ales a celor fără o influență ridicată la nivel regional, dar care sunt poziționate la confluența intereselor unor mari puteri.

BIBLIOGRAFIE:

1. *** *Global trends – Paradox of Progress*, National Intelligence Council, 2017, NIC 2017-001, URL: www.dni.gov/nic/globaltrends.
2. ***, A Global Strategy for the European Union's Foreign and Security Policy. Shared Vision, Common Action: A Stronger Europe, June 2016, URL: http://europa.eu/globalstrategy/sites/ globalstrategy/files/regions/files/eugs_review_web_0.pdf.
3. ***, *Discussion Paper – The Impact of New Technologies on Peace, Security, and Development*, Independent Commission on Multilateralism, International Peace Institute, April 2016, URL: https://www.icm2016.org/IMG/pdf/new_tech_paper.pdf.
4. ***, *Global trends – Paradox of Progress*, National Intelligence Council, 2017, NIC 2017-001, URL: www.dni.gov/nic/globaltrends.
5. ***, *SIPRI Military Expenditure Database*, Stockholm International Peace Research Institute, URL: https://www.sipri.org/databases/milex.
6. ***, *The World in 2050 – The long view: how will the global economic order change by 2050?*, Princewaterhouse Cooper (PwC), URL: http://www.pwc.com/gx/en/issues/economy/the-world-in-2050.html.
7. ***, *World Economic Outlook, October 2017*, Fondul Monetar Internațional, URL: http://www.imf.org/external/datamapper/NGDP_RPCH@WEO/OEMDC/WEOWORLD/CHN/USA/ADVEC/EU/AS5/DA/BRA/IND.
8. ***, World Population Prospects. Key Findings and Advance Tables, 2015 Revision, United Nations, URL: https://esa.un.org/unpd/wpp/Publications/Files/Key_Findings_WPP_2015.
9. BUZAN, Barry, „*New Patterns of Global Security in the Twenty-First Century"*, în *International Affairs* (Royal Institute of International Affairs 1944-), Vol. 67, No. 3 (Jul.,1991), URL: http://www.jstor.org/stable/2621945.
10. CLAUSEWITZ, Carl Von, *On War*, Princeton University Press, Princeton, Princeton, 1976.
11. FREIER, Nathan P. (coord.), *Outplayed: regaining strategic initiative in the gray zone*, United States Army War College Press, Carlisle, 2016, URL: https://ssi.armywarcollege.edu/pubs/ display.cfm?pubID=1325.
12. GHERASIMOV, Valeri, „The Value of Science is in the Foresight. New Challenges Demand Rethinking the Forms and Methods of Carrying Out Combat Operations", în *Military Review*, January – February 2016, URL: http://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/January-February-2016/.
13. GORDEEVA, Evgenia, „Transforming international system and the three approaches to the security dilemma", în *European Journal Of Futures Research,* Vol. 4/2016, URL: https://link.springer.com/article/10.1007/s40309-016-0088-y.
14. HOFMANN, Frank. G., „Hybrid wars and challenges", JFQ, issue 52, 1st quarter 2009, URL: www.ndupress.ndu.edu.
15. JACKSON, Van, *Tactics of strategic competition – Gray Zones, Redlines, and Conflicts before War*, Naval War College Review, Summer 2017, Vol. 70, No. 3, URL: https://search.proquest.com/openview/38ffba5bf77fcfbcb87a9cdac1f5b1a3 /1?pq-origsite=gscholar&cbl=34989.
16. KANT, Immanuel, *Toward Perpetual Peace and other writings on politics, peace and history: a philosophical essay*,. Yale University Press, 2006.
17. KEOHANE, Robert, *After Hegemony: Cooperation and Discord in the World Political Economy*, Princeton University Press, Princeton, 1984.
18. SCHWAB, Klaus, „The Fourth Industrial Revolution - What It Means and How to Respond", în *Foreign Affairs*, 12 December 2015, URL: https://www.foreignaffairs.com / articles/2015-12-12/fourth-industrial-revolution.

ACTUALITATEA MODELULUI SPIRALĂ AL DILEMEI SECURITĂŢII ÎN ANALIZA MEDIULUI INTERNAȚIONAL

Cătălina TODOR*

Cu toate că, în actualitate, interdependenţele şi interconexiunile internaţionale se află la niveluri fără precedent - la această stare aducându-şi contribuţia toate acele fenomene asociate globalizării, ce a determinat diluarea reprezentării spaţio-temporale ca urmare a evoluţiilor din ultimul secol, precum cele din domeniul transporturilor şi comunicaţiilor - nu asistăm la creşterea stabilităţii mediului internaţional, ci la emergenţa a numeroase provocări în înţelegerea dinamicilor sale specifice.

De aceea, constructe teoretice precum dilema securităţii sunt extrem de utile pentru că pot explica, măcar parţial, dezvoltarea unor anumite tipuri de relaţii tensionate între actori geopolitici/actori ai mediului de securitate internaţional. Astfel, cercetarea de faţă îşi propune să aducă în actualitate acest concept, apărut în anii '50 şi să sublinieze utilitatea sa în prezent. Pentru îndeplinirea acestui obiectiv, cercetarea se bazează, în special, pe analiza literaturii de specialitate, dar şi a unor date statistice cu privire la conflictualitate.

Cuvinte-cheie: *dilema securităţii, model spirală, tensiune, amplificare, ameliorare.*

Introducere

Mediul de securitate internaţional este din ce în ce mai dificil de analizat din cauza complexităţii sale şi a creşterii în amploare a unor fenomene, precum diversificarea ameninţărilor neconvenţionale şi a tensionării unor relaţii guvernate de poziţii divergente (spre exemplu relaţia NATO-Rusia, relaţia SUA-Rusia, inclusiv cu privire la zonele „fierbinţi" − Siria, sau cu privire la actori cu acţiuni provocatoare − Coreea de Nord).

Prezentul articol şi-a propus ca, în cele ce urmează, să prezinte succint şi neexhaustiv conceptul dilemei de securitate, ca un posibil concept ce poate oferi un model spirală de analiză a dinamicilor mediului de securitate, în special acelea care privesc doi actori cu poziţii divergente.

Cercetarea porneşte de la creionarea necesităţii unui asemenea model teoretic şi apoi dedică o a doua parte aducerii în actualitate a ancorei teoretice reprezentată de cele mai importante elemente constitutive ale conceptului „dilema securităţii". O ultimă parte oferă un potenţial cadru metodologic pentru dezvoltarea studiilor de caz, prin explicarea elementelor constitutive pe care o relaţionare trebuie să le conţină pentru a se încadra în modelul spirală oferit de dilema securităţii.

1. Elemente ale contextului internaţional ca obiect de analiză pentru modelul spirală al dilemei de securitate

Evenimentele recente ne creionează anul 2017 ca pe o continuare a unei perioade caracterizate de o amplificare treptată a tensiunilor la nivel regional şi global. Câteva

**** Cătălina TODOR este asistent de cercetare ştiinţifică în cadrul Centrului de Studii Strategice de Apărare şi Securitate (CSSAS) din Universitatea Naţională de Apărare „Carol I", Bucureşti. E-mail: todor.catalina@unap.ro***

exemple în acest sens ar putea fi tensiunea generată de relaţia dificilă dintre NATO şi Rusia, dintre SUA şi Rusia (chiar şi după instalarea noii administraţii prezidenţiale Trump), de imposibilitatea comunităţii internaţionale de a adopta o poziţie unitară pentru ameliorarea unor zone de conflict (spre exemplu Siria) sau a acţiunilor belicoase specifice unor state (spre exemplu Coreea de Nord). Pe de altă parte, persistența anumitor zone de conflict sau acţiunile provocatoare ale unor ţări pot servi drept debuşeu geopolitic, prin care se manifestă dorinţa unor actori de a-şi arăta prezenţa în anumite regiuni sau de a avea un cuvânt de spus în soluţionarea problemelor regionale/globale.

Acest barometru oferă o clasificare a conflictelor în funcţie de cinci niveluri de intensitate: dispute, crize nonviolente, conflicte violente, războaie limitate, războaie, ce sunt încadrate în două mari categorii: (A) conflictele nonviolente: 1. disputele, 2. crizele nonviolente; (B) conflictele violente: 3. crizele violente, 4. războiul limitat, 5. război.

Revenind la tensiunile globale, observarea acestora ne arată că, de-a lungul ultimilor ani, numărul total de conflicte a înregistrat în general o creştere, chiar dacă, în particular, în 2016 observăm o uşoară scădere numerică: în 2016 se constata existența a 402 conflicte, din care 226 erau violente şi 176 nonviolente. Pe categorii de

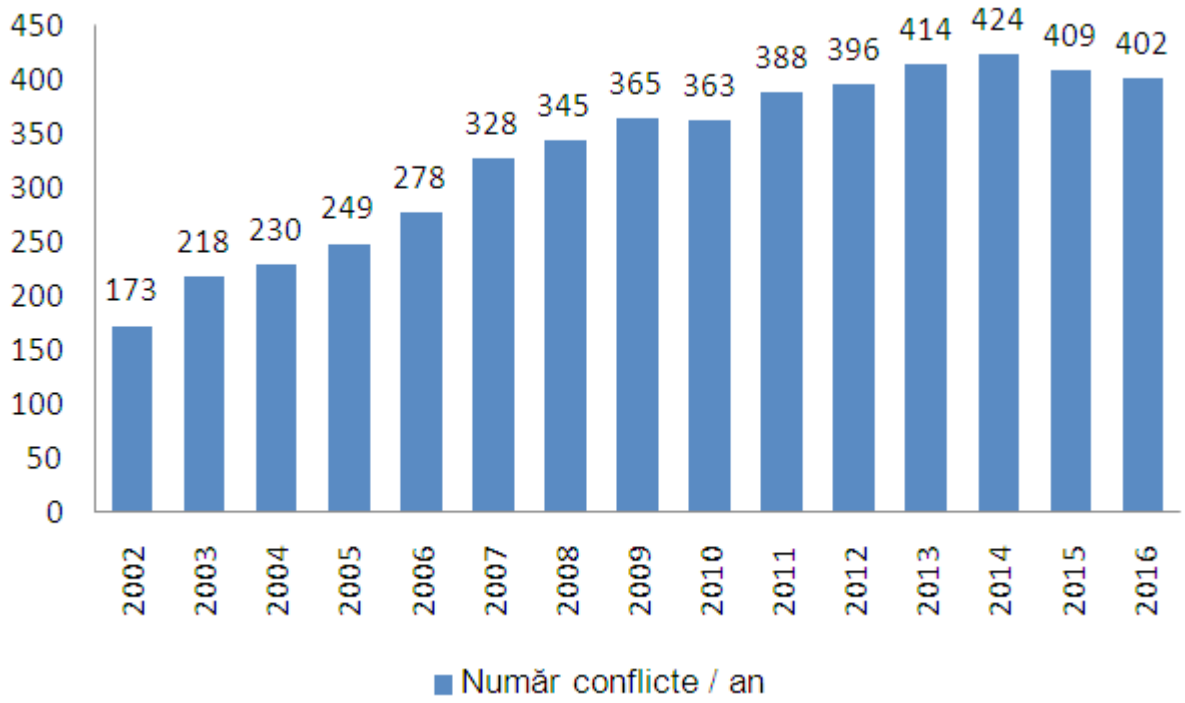

Figura nr. 1: Evoluţia numărului de conflicte în perioada 2002-2016

SURSA: Grafic realizat pe baza datelor cu privire la numărul total de conflicte la nivel mondial selectate din fiecare raport anual al *Barometrului conflictualităţii*; cele 15 rapoarte se găsesc online la https://www.hiik.de/en/konfliktbarometer/, accesat la data de 22.06.2017.

Dacă studiem ideea de tensiune/conflict la nivel global din punct de vedere statistic, cele mai recente date centralizate în acest sens sunt cele prezentate în *Barometrul conflictualităţii 2016*[1].

intensitate ale conflictualităţii, în 2016, observăm o creştere faţă de 2015, după cum urmează: în ceea ce priveşte numărul disputelor, de la 90 la 98, iar al crizelor violente, de la 183 la 188. Pe de altă parte, a scăzut numărul crizelor nonviolente, de la 88 la 78, numărul războaielor limitate, de la 24 la 20 şi numărul războaielor de la 19 la 18.

[1] ***, *Conflict Barometer 2016*, Heidelberg Institute for International Conflict, 2017, URL: https://www.hiik.de/en/konfliktbarometer/pdf/ConflictBarometer_2016.pdf, accesat la data de 07.07.2017.

La o analiză a evoluției numărului total de conflicte la nivel mondial din primii ani ai publicaţiei şi până în prezent, constatăm că deşi, la nivel global, interdependențele şi interconexiunile sunt la o scară fără precedent şi continuă să se intensifice (diluarea noţiunilor de timp şi spaţiu ca urmare a fenomenului globalizării, avansului tehnologic, evoluţiei căilor de transport şi comunicaţii etc.), noţiunea de pace este foarte greu de atins, conflictualitatea chiar amplificându-se, per total, în ultimul deceniu. Aceasta se poate constata prin analiza datelor din Figura nr. 1.

În acest context, în care conflictualitatea persistă şi se intensifică, sunt necesare modelele teoretice care să poată explica, măcar parţial, cauzele amplificării unor stări de tensiune (în cazul de față, cele care privesc relaţia dintre actorii statali/actorii internaţionali). Acestea pot oferi cunoaşterea mai bună a realităţii curente, în special în ceea ce privește amplificarea, dar și ameliorarea tensiunilor regionale şi internaţionale.

Astfel, dilema de securitate este un concept asociat unui cadru de analiză pentru relaţii tensionate cum este, spre exemplu, cea dintre NATO şi Rusia, cea dintre comunitatea internaţională (în speţă SUA) şi Coreea de Nord, cele geopolitice dintre actorii care acționează în Siria etc.

2. Utilitatea dilemei securităţii în actualitate[2]

Pornim de la premisa că dilema securităţii a apărut din necesitatea practică de a înţelege dinamica mediului de securitate. Valenţa sa pozitivă poate fi regăsită în cunoaşterea pe care acest model o oferă pentru a descifra modul în care se poate ajunge de la cele mai slabe stări de tensiune la cele mai intense trepte ale conflictualităţii[3].

Dilema securităţii propune un model spirală de amplificare a insecurităţii unui sistem, din aproape în aproape, bazat pe interacţiunea dintre acţiuni şi reacţii ale unor actori. Pentru realitatea internaţională, dilema securităţii ar putea oferi explicaţia măcar secvenţială sau parţială a cauzelor şi modului în care s-a ajuns la o stare de tensiune la nivel regional/global la un moment dat.

Ca şi în cazul altor concepte ce ţin de sfera relaţiilor internaţionale, geopoliticii şi studiilor de securitate, nici pentru dilema securităţii nu există un consens academic asupra elementelor şi raţionamentelor sale constitutive, cum, de altfel, nu există nici o definiţie universală acceptată a sa. Acest termen apare în anii ’50, avându-i ca „părinţi” pe John Hertz (1950), care, de altfel, îi oferă denumirea de „dilema securităţii”, pe Herbert Butterfield (1951) şi Robert Jervis (anii ’70) – chiar dacă Jervis dezvoltă idei în acest sens la două decenii după primii doi, îl putem considera, totuşi, printre pionierii dilemei securităţii pentru că îi asociază noţiunea de model spirală şi, de asemenea, are meritul încorporării conceptului în teoria relaţiilor internaţionale.

De-a lungul timpului şi până în prezent, dilema securităţii a fost tratată din mai multe perspective, dintre care putem aminti:

- *perspectiva realismului ofensiv*: într-un sistem internaţional anarhic, frica generată de intenţiile statelor rivale poate îndepărta de la cooperare chiar şi două state aflate în căutarea securităţii[4];
- *perspectiva realismului defensiv* pune la îndoială puterea legăturii dintre anarhie, incertitudine şi cooperare: două state ce caută securitate nu ar trebui să găsească dificilă cooperarea, dacă se recunosc fiecare ca făcând parte din această categorie de state; incertitudinea nu este suficientă pentru ca adepţii realismului ofensiv să formuleze predicţii pesimiste, chiar dacă incertitudinea cu privire la motivaţiile unui stat poate, într-adevăr, complica problemele[5];

[2] Menţionăm că această cercetare are la bază un studiu anterior, diseminat printr-o comunicare susţinută în cadrul *Conferinţei internaţionale „Mediul strategic de securitate: provocări şi tendinţe”*, organizată la 18 mai 2017 de către Centrul de Studii Strategice de Apărare şi Securitate al Academiei Militare a Forţelor Armate „Alexandru cel Bun” din Chişinău, Republica Moldova, în curs de publicare.

[3] A se vedea cele cinci trepte ale conflictualităţii oferite de *Barometrul conflictualităţii*.

[4] Avidit Acharya, Kristopher W. Ramsay, „The Calculus of the Security Dilemma”, Quarterly Journal of Political Science, Vol. 8, nr. 2, pp. 183-203, URL: http://stanford.edu/~avidit/security.pdf, accesat la data de 22.05.2017.

[5] *Ibidem.*

▪ *perspectiva realismului bayesian:* în timp ce abordările anterioare au în vedere două state aflate în căutarea securităţii, această perspectivă aduce în discuţie alte variabile, precum state cu preferinţe diferite privind revizuirea statu quoului şi nivelul de încredere dintre state; apar două categorii distincte de ţări - cele demne de încredere şi cele nedemne de încredere.[6]

În Tabelul nr. 1 sunt sistematizate unele dintre cele mai importante demersuri conceptuale în direcţia dilemei securităţii, care arată continuitatea preocupărilor în acest domeniu şi actualitatea noţiunii.

AUTOR	AN*	ELEMENTELE ŞI ALGORITMUL DILEMEI SECURITĂŢII	INOVAŢIE
John Herz	1950	1. Sistem anarhic 2. Nesiguranţa şi frica faţă de intenţiile unui actor 3. Acumularea de putere ca răspuns la frică 4. Ciclul competiţiei de putere poate duce la creşterea insecurităţii în sistem 5. Dilema securităţii poate duce la război, dar nu este cauza tuturor războaielor 6. Dilema securităţii se autoalimentează, rezultând un cerc vicios	1. Concepţie realistă 2. Anarhia sistemului 3. Neîncrederea dintre actori DILEMA SECURITĂȚII
Herbert Butterfield	1951	1. Frica 2. Incertitudine faţă de intenţiile unui actor 3. Lipsa intenției 4. Rezultate tragice 5. Amplificată de factori de natură psihologică 6. Cauza fundamentală a conflictelor omenirii	Caracterul neintenţionat
Robert Jervis	1976-1978	1. Într-un sistem anarhic, state cu obiective compatibile pot ajunge la competiţie sau chiar război 2. Două variabile dau natura şi intensitatea dilemei: diferenţa ofensiv-defensiv şi echilibrul ofensiv-defensiv	Încorporarea dilemei securităţii în teoria relaţiilor internaţionale
Charles L. Glaser	1997	Două variabile esenţiale: 1. motivaţiile dincolo de nevoia de securitate: lăcomia unui actor 2. cunoaşterea unitară a adversarului despre motivaţiile unei ţări	Conceptul de „stat lacom”

[6] *Ibidem.*

AUTOR	AN*	ELEMENTELE ŞI ALGORITMUL DILEMEI SECURITĂŢII	INOVAȚIE
Andrew Kydd	1997-2005	1. Problematicile de încredere stau la baza dilemei securităţii; nivelul încrederii poate determina dacă, într-un sistem anarhic, cooperarea este posibilă sau nu 2. Încrederea interacţionează cu două variabile: puterea relativă şi costul conflictului. În funcţie de interacţiunea lor, cooperarea se poate amplifica sau înrăutăţii 3. Incertitudinea asupra informaţiilor deţinute de către actori şi în ceea ce priveşte preferinţele acestora 4. Teoria jocului bayesian pentru a analiza problematica încrederii /neîncrederii. Patru tipuri de actori ce variază în funcţie de două axe (axa 1: nivelul agresiunii/lăcomiei; axa 2: nivelul fricii) şi două reprize de luarea a deciziei (atac/apărare) 5. Statele de încredere sunt adesea capabile să se separe de cele nedemne de încredere. 6. Statele lacome sunt mult mai susceptibile de a-şi consolida puterea în scopul expansiunii (indiferent de natura adversarului), în timp ce statele aflate în căutarea securităţii vor opta pentru consolidare numai dacă ajung să îşi considere adversarul ca stat lacom 7. Spirala înarmării poate fi evitată de către statele aflate în căutarea securităţii, prin abţinerea de la acumularea de armament. Statele lacome sunt predispuse spre a purta un război, mai ales în cazul în care costul acestuia sau al cursei înarmării este mai scăzut	Prima abordare cunoscută a problematicii informaţiilor incomplete în dilema securităţii
Shiping Tang	2009	1. Punctul de plecare: anarhia politicii internaţionale 2. Nesiguranţa aspra intenţiilor actorilor 3. Caracterul neintenţionat 4. Incertitudinea şi frica duc la acumularea de putere, ce conţine, invariabil, şi componente ofensive 5. Model spirală de înrăutăţire a relaţiilor; cursă a înarmării 6. „Mai multă putere, mai puţină securitate” 7. Cerc vicios cu potenţiale rezultate grave (războiul) 8. Severitatea dilemei poate fi amplificată de factori materiali şi psihologici	1. Anarhia 2. Caracterul neintenţionat: lipsa de intenţii maligne 3. Acumularea puterii DILEMA SECURITĂŢII

AUTOR	AN*	ELEMENTELE ŞI ALGORITMUL DILEMEI SECURITĂŢII	INOVAŢIE
AvidAcharya, Kristopher W. Ramsay	2013	1. Problema încrederii stă la baza dilemei securităţii (în mod special, incertitudinea asupra elementelor fundamentale strategice: tehnologia militară a actorilor; beneficiile relative ale unei acţiuni ofensive militare; stimulentele pentru cooperarea reciprocă); mediul valorilor comune 2. Validitatea logicii realismului ofensiv: chiar şi atunci când statele ştiu că sunt din categoria celor aflate în căutarea securităţii, încrederea se poate afla la un nivel atât de scăzut, încât cooperarea poate deveni imposibilă 3. Dilema securităţii nu este neapărat ameliorată de discuţiile premergătoare unor acţiuni (încadrate la capitolul diplomaţie)	Model formal ce arată probabilitatea redusă a cooperării în anumite situaţii; rolul diplomaţiei: în multe cazuri, discuţiile premergătoare unor acţiuni nu duc neapărat la o îmbunătăţire a cooperării

Tabelul nr. 1: Raţionamentul şi elementele principale ale dilemei de securitate. Perspectivă evolutivă

SURSE:

Shiping Tang, „The Security Dilemma: A Conceptual Analysis", *Security Studies*, 18:587–623, Editura Taylor & Francis Group, LLC, 2009, p. 587, disponibil online la https://www.researchgate.net/publication/242166630_The_Security_Dilemma_A_Conceptual_Analysis, accesat la data de 02.03.2017.

Charles L. Glaser, „The Security Dilemma Revisited", *World Politics*, Vol. 50, No. 1, Fiftieth Anniversary Special Issue (Oct., 1997), pp. 171-201, Cambridge University Press, disponibil online la http://www.jstor.org/stable/25054031, accesat la data de 12.04.2017.

John H. Herz, „Idealist Internationalism and the Security Dilemma", *World Politics*, Vol. 2, No. 2 (Jan., 1950), pp. 157-180, 1950, p. 157, disponibil online la https://www.jstor.org/stable/2009187, accesat la data de 02.03.2017.

Evan Braden Montgomery, „Breaking Out of the Security Dilemma - Realism, Reassurance, and the Problem of Uncertainty", *International Security*, Vol. 31, No. 2 (Fall 2006), pp. 151–185, disponibil online la https://www.jstor.org/stable/4137519, accesat la data de 19.04.2017.

Avidit Acharya, Kristopher W. Ramsay, „The Calculus of the Security Dilemma", *Quarterly Journal of Political Science*, Vol. 8, 2013, disponibil online la http://stanford.edu/~avidit/security.pdf, accesat la data de 15.08.2017.

Andrew Kydd, „Game Theorz and the Spiral Model", *World Policies*, vol. 49, nr. 2, aprilie 1997, pp. 371-400.

Andrew Kydd, „Trust and Mistrust in International Relations", Princeton, New Jersey, Princeton University Press, 2005.

N.A.: Unele informaţii se regăsesc, sub altă formă, şi în Cătălina Todor, „Dilema securităţii în actualitate. Spirala tensiunilor NATO-Rusia", material susţinut în cadrul *Conferinţei internaţionale „Mediul strategic de securitate: provocări şi tendinţe*" organizată de către Centrul de Studii Strategice de Apărare şi Securitate al Academiei Militare a Forţelor Armate „Alexandru cel Bun", 18 mai 2017, Chişinău, Republica Moldova, în curs de publicare.

*N.A.: Anul de apariție al dezvoltărilor teoretice.

În linii mari, chiar dacă unele variabile pot să difere în funcţie de perspectiva şi evoluţia conceptului[7], logica dilemei securităţii porneşte de la un sistem internaţional anarhic[8], în care tensiunile dintre actori se pot amplifica treptat până la cel mai grav nivel (reprezentat de război), într-un model spirală al acumulării de putere. Acumularea de putere (din dorinţa actorilor de a-şi asigura securitatea) poate duce la insecuritatea sistemului.

Desigur, acumularea de putere (atât „soft", cat şi „hard") poate avea ca motivaţie fie frica şi incertitudinea cu privire la intenţiile unui actor, fie o gândire geopolitică specifică unui naţionalism expansionist (în această categorie putem încadra imperialismele, panideile). Acestea ar fi cele două extreme ce aparţin unor tipologii de state: cele în căutarea securităţii şi statele lacome (categorii evidenţiate de către C.L. Glaser încă din anii 1990). Considerăm că, totuşi, pe lângă aceste două tipologii, ar putea exista şi state mixte din perspectiva motivaţiei ce stă la baza acumulării puterii. Spre exemplu, un aşa-zis stat lacom poate să fie motivat în acumularea de putere şi de o concepţie geopolitică expansionistă, dar şi de ameninţarea pe care acesta o resimte ca reală şi ce rezidă din pierderea unor zone de influenţă tradiţionale şi considerate vitale pentru el (un exemplu, în acest sens, ar putea fi Rusia). De aici derivă şi dificultatea în a încadra ca tipologie acţiunile unui stat: dacă acestea sunt intenţionate sau neintenţionate, agresive/ofensive sau motivate de frică/defensive. Astfel, dacă avem în discuţie un stat cu motivaţie mixtă (aflat între definirea propriei securităţi şi o istorie ce evidenţiază o concepţie geopolitică expansionistă), atunci acţiunile acestuia pot fi o împletire între intenţionat şi neintenţionat, între defensiv şi ofensiv. Prin urmare, este foarte dificil de realizat o delimitare clară a situaţiilor şi de conchis că anumite evoluţii nu se încadrează în dilema securităţii (situaţii tensionate cauzate de acumularea de putere a unor state lacome).

Ipoteza informaţiilor incomplete (asupra căreia atrage atenţia Andrew Kydd) accentuează această dificultate. De asemenea, şi în virtutea posibilei existenţe a statelor unde motivaţia este un mix între frică şi o gândire geopolitică specifică marilor puteri, adesea marcată de expansionism (chiar dacă nu în sensul tradiţional pur teritorial, ci expansionism manifestat la nivelul sferelor de influenţă), considerăm că majoritatea situaţiilor tensionate/conflictuale regionale şi globale se încadrează în logica dilemei securităţii.

Prin această expunere, am urmărit două obiective.

- Să evidenţiem faptul că acest concept este de actualitate şi evoluează, comportând diferite variabile. Aceasta din două motive distincte: a fost creat să servească înţelegerii modului în care se poate ajunge în situaţii ce ameninţă securitatea unui sistem şi pentru că evoluţia lui este în relaţie cu mediul de securitate pe care încearcă să îl explice, mediu aflat într-o continuă mişcare şi transformare.
- Să arătăm care sunt cele mai importante elemente constitutive ale dilemei securităţii.

3. Cadru teoretic de validare a încadrării unei relaţii între actori în dilema securităţii

În urma analizei realizate la punctul anterior, putem să extragem cele mai importante şase elemente ale dilemei securităţii în actualitate. Astfel, în momentul în care constatăm că o relaţionare dintre anumiţi actori întruneşte toate cele şase condiţii (elemente) din Figura nr. 2, putem afirma că acea dinamică se încadrează în raţionamentul dilemei de securitate.

Din acel moment, modelul spirală poate să se constituie într-un veritabil cadru teoretic de analiză a dezvoltărilor acelei relaţionări. Ea poate să meargă în trei tipuri de direcţii: în cea a ameliorării acumulării de putere şi insecurităţii (detensionarea relaţiilor), a amplificării acumulării de putere şi insecurităţii sistemului (tensionarea relaţiilor) şi în cea a menţinerii fără fluctuaţii semnificative a gradului de putere şi

[7] Acest concept (dilema securităţii) a evoluat de-a lungul timpului, aşa cum se întâmplă, de cele mai multe ori, cu noţiunile specifice ariei relaţiilor internaţionale, geopoliticii şi studiilor de securitate. Pe de altă parte, evoluţia unor concepte este dictată şi de evoluţiile societale complexe la nivel global.

[8] Definit prin inexistenţa unei unităţi finale, căreia să i se subordoneze multitudinea de state şi grupuri/blocuri/organizaţii internaţionale.

securitate (îngheţarea dezvoltărilor în model spirală a unei relaţii).

Studierea fiecăruia dintre cele şase elemente în cadrul unor raporturi specifice între anumiţi actori ne poate aduce informaţii cu privire la direcţia (dintre cele trei expuse anterior) în care se poate îndrepta interacţiunea dintre părţi.

Figura nr. 2: Elementele constitutive ale dilemei de securitate în actualitate

Menţionez, în continuare, câteva completări care ar putea aduce o şi mai mare claritate cu privire la unele dintre aceste şase elemenete constitutive ale dilemei securităţii, mai exact, referitor la componentele trei, cinci şi şase:

▪*Componenta nr. 3:* actorii să fie din categoria celor aflaţi în căutarea securităţii, pentru care există şi predomină caracterul neintenţionat al acţiunilor, chiar dacă unele dintre acestea pot duce la amplificarea unei tensiuni. Aici îi includem şi pe acei actori pentru care motivaţia poate fi un mix de căutare a securităţii şi a menţinerii unor obiective geopolitice specifice logicii expansioniste în temenii sferelor de influenţă; ameninţarea unor obiective de acest gen poate să se transforme pentru unii actori într-o reprezentare a ameninţării la adresa propriei securităţi.

▪*Componenta nr. 5:* acumularea de putere în înţelesul complex al conceptului de putere. Acesta trebuie văzut ca mixul dintre componenta sa – hard – componentele tangibile/ indicatori cantitativi precum forţa militară, capacitatea economică, demografică, resursele naturale, teritoriul, infrastructura, tehnica – şi cea soft – componenta intangibilă/indicatorii calitativi – coeziunea naţională, reprezentarea la nivel regional/mondial, liderii politici, capacitatea de a organiza şi conduce eficient societatea, nivelul culturii şi civilizaţiei, puterea tradiţiei, determinarea populaţiei în atingerea obiectivelor, educaţia, pregătirea profesională, componenta informaţională, propaganda etc.[9]

▪*Componenta nr. 6:* creşterea insecurităţii sistemului se produce ca urmare a acumulării de putere din partea actorilor pentru a-şi asigura propria securitate. Aşa se ajunge la un cerc vicios, la o spirală a acumulărilor de putere, pentru că ceilalţi actori implicaţi în ecuaţie resimt o potenţială ameninţare, ca urmare a sporirii puterii primilor, şi atunci pot decide să îşi mărească, la rândul lor, puterea. Acest tip de dinamică poate rezulta într-o cursă a înarmărilor, noţiune care, de altfel, a fost şi este asociată acestui concept al dilemei de securitate. Pe de altă parte, având în vedere faptul că puterea nu constă doar în componenta sa hard, pe lângă această cursă a înarmării, se poate produce şi o cursă a întăririi componentei intangibile a puterii (cea „soft"), a consolidării competenţelor şi capabilităţilor care să sprijine capacitatea de a stăpâni şi controla propria securitate, dar şi de a o influenţa pe cea regională sau chiar internaţională. De multe ori, aceasta duce la potenţarea unui actor în a impune sau a juca un rol important geopolitic în diferite spaţii (de la cele tradiţionale: terestru, maritim, aerian, la cele emergente, precum spaţiul cibernetic şi sfera reprezentărilor în conştiinţa unei populaţii). Mai ales în actualitate,

[9] Informaţii la care am mai facut apel şi cu ocazia altor cercetări, spre exemplu: Cătălina Todor, „Dilema securităţii în actualitate. Spirala tensiunilor NATO-Rusia", material susţinut în cadrul cadrul Conferinţei internaţionale „Mediul strategic de securitate: provocări şi tendinţe"organizată de către Centrul de Studii Strategice de Apărare şi Securitate al Academiei Militare a Forţelor Armate „Alexandru cel Bun", 18 mai 2017, Chişinău, în curs de publicare, şi Cătălina Todor, „From Clasical Geopolitics to Contemporary Geopolitics. Statutory Elements of a Strong Grounded Science in Reality and Actuality", Geopolitical Perspectives and Development EUBSR 2013 International Conference Volume, 2013, Italian Academic Publishing, p. 168.

componenta soft a puterii capătă noi valenţe, societatea informaţională oferind un nou spaţiu în care se pot manifesta atât poziţiile convergente, cât şi cele divergente, şi anume spaţiul cibernetic (ştirile false, propaganda etc.). Acumularea de putere în ambele sale componente de către actorii implicaţi într-o relaţionare, în model spirală, poate duce la o deteriorare a relaţiilor şi la o potenţială degradare a mediului de securitate regional/global.

Dacă o situaţie/o relaţionare întruneşte toate cele şase componente, o putem încadra în logica dilemei de securitate. Cunoaşterea generată de acest algoritm poate contribui la înţelegerea neexhaustivă a amplificării/ameliorării stării de tensiune la nivel regional şi internaţional. De aceea, considerăm că acest concept poate fi utilizat metodologic pentru analiza dinamicii unei relaţionări dintre actorii participanţi ai mediului internaţional de securitate.

Concluzii

Aşa cum se poate observa din prima parte a acestui articol, mediul de securitate actual nu este unul mai stabil, în ciuda interdependenţelor şi interconexiunilor crescute la nivel internaţional. De aceea, orice concept sau cadru metodologic ce vine în sprijinul înţelegerii dinamicilor de securitate are o utilitate imediată. Acesta este şi cazul dilemei de securitate.

Partea a doua a cercetării arată faptul că modelul spirală oferit de dilema securităţii a evoluat de-a lungul timpului, autorii care l-au studiat adăugându-i noi variabile sau aducând în atenţie posibile argumente ce l-ar putea demonta (spre exemplu dezvoltările lui Glaser cu privire la existenţa statelor lacome ce anulează dilema securităţii). Totuşi, aproape constante rămân câteva elemente ale dilemei de securitate: sistemul anarhic, neîncrederea, acumularea de putere şi creşterea insecurităţii sistemului.

În urma studiului literaturii de specialitate, am ajuns la concluzia că un model de actualitate pentru dilema securităţii ar putea fi format din existenţa a şase condiţii: 1. sistemul anarhic, 2. neîncrederea, 3. actorii statali aflaţi în căutarea securităţii (inclusiv cei cu motivaţie mixtă), 4. informaţiile incomplete, 5. acumularea de putere şi 6. creşterea insecurităţii sistemului.

Considerăm că, dacă în cadrul unei relaţionări dintre doi sau mai mulţi actori ai mediului de securitate internaţional există toate aceste caracteristici, atunci relaţionarea se încadrează în modelul spirală oferit de dilema securităţii.

Conchidem prin a aprecia faptul că valenţa practică a acestei cercetări este posibilitatea utilizării logicii existenţei celor şase caracteristici în studiile de caz. De altfel, ne propunem, ca o continuare a acestei cercetări, să oferim un exemplu prin studierea relaţiei dintre NATO şi Rusia prin prisma acestor şase elemente pentru a demonstra dacă putem discuta sau nu de o dilemă a securităţii în acest caz.

BIBLIOGRAFIE:

1. ***, Conflict Barometer (*Barometrul conflictualităţii*); Institutul Heidelberg pentru Cercetarea Conflictelor Internaţionale (HIIK), URL: https://www.hiik.de/en/konfliktbarometer/.

2. ACHARYA, Avidit; RAMSAY W. Kristopher, „The Calculus of the Security Dilemma”, *Quarterly Journal of Political Science*, Vol. 8, nr. 2, pp. 183-203, URL: http://stanford.edu/~avidit/security.pdf.

3. BRADEN MONTGOMERY, Evan, „Breaking Out of the Security Dilemma - Realism, Reassurance, and the Problem of Uncertainty”, *International Security*, Vol. 31, No. 2 (Fall 2006), pp. 151–185, URL: https://www.jstor.org/stable/4137519.

4. GLASER, L. Charles, „The Security Dilemma Revisited”, *World Politics*, Vol. 50, No. 1, Fiftieth Anniversary Special Issue (Oct., 1997), pp. 171-201, Cambridge University Press, URL: http://www.jstor.org/stable/25054031.

5. HERZ, H. John, „Idealist Internationalism and the Security Dilemma”, *World Politics*, Vol. 2, No. 2 (Jan., 1950), pp. 157-180, 1950, URL:

https://www.jstor.org/stable/2009187.

6. KYDD, Andrew, „Game Theorz and the Spiral Model", *World Policies,* vol. 49, nr. 2, aprilie 1997, pp. 371-400.

7. KYDD, Andrew, „Trust and Mistrust in International Relations", Princeton, New Jersey, Princeton University Press, 2005.

8. TANG, Shiping, „The Security Dilemma: A Conceptual Analysis", *Security Studies*, 18:587–623, Editura Taylor & Francis Group, LLC, 2009, p. 587, URL: https://www.researchgate.net/publication/242166630_The_Security_Dilemma_A_Conceptual_Analysis.

9. TODOR, Cătălina, „Dilema securității în actualitate. Spirala tensiunilor NATO-Rusia" material susţinut în cadrul *Conferinţei internaţionale „Mediul strategic de securitate: provocări şi tendinţe"*, organizată la 18 mai 2017 de către Centrul de Studii Strategice de Apărare şi Securitate al Academiei Militare a Forţelor Armate „Alexandru cel Bun" din Chişinău, Republica Moldova, în curs de publicare.

10. TODOR, Cătălina, „From Clasical Geopolitics to Contemporary Geopolitics. Statutory Elements of a Strong Grounded Science in Reality and Actuality", *Geopolitical Perspectives and Development EUBSR 2013 International Conference Volume*, Italian Academic Publishing, 2013.

ROLUL STATULUI BAHRAIN ÎN VIZIUNEA GEOSTRATEGICĂ A IRANULUI ȘI A ARABIEI SAUDITE

Răzvan MUNTEANU*

Chiar dacă, după Revoluția Islamică din Iran, din 1979, Riyadul și Teheranul s-au angrenat într-o competiție geopolitică pentru supremație în lumea musulmană, înainte, cele două state erau parteneri strategici, ce împărtășeau interese comune, precum combaterea ideologiei comuniste sau a pan-arabismului. Cu toate acestea, și înainte de 1979, și după, Bahrainul, un stat format din 33 de insule, dintre care doar două locuibile, a reprezentat un punct de dispută al intereselor saudito-iraniene.

Astfel, acest articol își propune să înțeleagă importanța strategică a Bahrainului, atât pentru Arabia Saudită, cât și pentru Iran, în contextul rivalității geopolitice dintre acestea, cu atât mai mult cu cât Bahrainul reprezintă un stat majoritar șiit condus de către o minoritate sunnită. Începând cu 1979, șiiții din Bahrain au fost motivați, de către Revoluția Islamică, să ceară noi drepturi, precum accederea în funcții guvernamentale superioare, însă marginalizarea acestora a continuat, această politică a regimului de la Manama fiind sprijinită de către Riyad. Astfel, Bahrainul a devenit un câmp al unui conflict proxy desfășurat între Arabia Saudită - care susține monarhia sunnită - și Iran, a cărui strategie s-a axat asupra susținerii unor actori nonstatali care să destabilizeze Bahrainul pentru ca șiiții să preia apoi puterea. Un asemenea scenariu este însă privit de către saudiți ca o amenințare asupra securității naționale și a status quoului regional.

Cuvinte-cheie: *geopolitică, Bahrain, Golful Persic, Arabia Saudită, Iran, Primăvara Arabă, război proxy.*

Introducere

Cu o populație de 1.410.942 locuitori[1], micul stat Bahrain reprezintă un important punct geostrategic pentru balanța de putere din Golful Persic, în contextul actualei competiții geopolitice dintre Arabia Saudită și Iran.

Arhipelagul format din 33 de insule, dintre care doar două locuibile, a fost ocupat de către portughezi în perioada 1522-1602, apoi a intrat, pe rând, în posesia triburilor arabe și persane[2]. Influența Iranului în Bahrain începe încă din anul 1602, în timpul Dinastiei Safavide, și durează până în 1782, atunci când are loc expansiunea militară a tribului sunnit al-Khalifa. Pe acest fond, au loc și mișcările demografice ale populației șiite, care se deplasează ca urmare a conflictelor sectare în zonele de nord și vest[3], acolo unde a

[1] ***, „Bahrain", CIA The World FactBook, URL: https://www.cia.gov/library/publications/the-world-factbook/geos/ba.html, accesat la data de 01.06.2017.

[2] ***, „The Strategic Importance of Bahrain to Saudi Arabia", în *The Oil Price*, 29.07.2011, URL: http://oilprice.com/Geopolitics/Middle-East/The-Strategic-Importance-Of-Bahrain-To-Saudi-Arabia.html, accesat la data de 03.06.2017.

[3] Jason Rivera, „Iran's Involvement in Bahrain: A Battleground as Part of the Islamic Regime's Larger Existential Conflict", în *Small Wars Journal*, URL: http://smallwarsjournal.com/printpdf/22533, accesat la data de 01.06.2017.

Răzvan MUNTEANU este doctorand în domeniul Științelor politice în cadrul Școlii Naționale de Studii Politice și Administrative (SNSPA), București, România. E-mail:razvan.munteanu@newsint.ro; r.munteanu88@yahoo.com

rămas poziționată până în zilele noastre. Al-Khalifa, care provine din peninsula qatareză, a reușit să conducă Bahrainul până în prezent, folosindu-se inclusiv de sprijinul britanicilor, care au transformat țara în protectorat începând cu anul 1830[4], dar și de sprijinul americanilor, care au preluat rolul britanicilor în regiune după descoperirea resurselor energetice din Golful Persic.

Cu toate acestea, deși prezența americană în regiune datează încă din 1948, primul acord militar între SUA și Bahrain a fost semnat în 1971, pentru ca, începând cu anul 1977, marina SUA să primească acces în Portul Salman iar, începând cu 1995, americanii să mute Flota a V-a în Bahrain[5], în scopul de a menține status quoul și arhitectura de securitate regională.

Dar, încă înainte de sosirea americanilor în regiune, imediat după retragerea britanicilor din Golful Persic, atât Iranul, cât și Arabia Saudită au revendicat teritorialitatea arhipelagului, ceea ce a condus către impunerea unui mandat ONU de observare, prin care s-a luat decizia, în cele din urmă, să se acorde independență statului Bahrain[6]. Familia al-Khalifa, ale cărei rădăcini istorice se regăsesc în Casa Saud, a menținut totdeauna o politică apropiată de Arabia Saudită, ceea ce a făcut ca Bahrainul să fie un stat aflat în sfera de influență saudită, aceasta deși este o țară majoritar șiită, condusă de către o minoritate sunnită.

De altfel, dincolo de rădăcinile istorice și ideologice, legăturile dintre cele două țări au fost consolidate și prin căsătoria fiului regelui saudit Abdullah cu fiica regelui Hamad al-Khalifa[7].

În tot acest timp, șiiții au rămas o populație marginalizată, membrii acestei comunităţi neputând accede, spre exemplu, în funcţii politice superioare, în timp ce guvernul duce o politică de oferire a cetăţeniei expaților arabi sunniți, în scopul de a modifica raportul demografic[8], ceea ce a condus către adâncirea clivajului sectar și către escaladarea tensiunilor sociale.

Deși populația șiită din Bahrain este divizată în două mari ramuri, respectiv *Baharna*, în cazul celor ce au origini arabe, și *Howala or 'Ajams*, în cazul celor ce au rădăcini persane, aceasta s-a dovedit a fi în strânsă legătură cu Iranul și fidelă regimului de la Teheran[9], un lucru datorat, foarte probabil, marginalizării la care șiiții au fost supuși în Bahrain de-a lungul timpului, inclusiv în perioada otomană, aceștia fiind încurajați și susținuți pentru a cere noi drepturi abia odată cu Revoluția Islamică din 1979[10]. De altfel, Revoluția Islamică a determinat guvernul saudit să accelereze construcția sistemului de poduri și șosele *King Fahd Causeway*, ce leagă pe cale maritimă Arabia Saudită de Bahrain[11].

Figura nr. 1: King Fahd Causeway

SURSA: Al Arabiya, https://english.alarabiya.net/, accesat la data de 28.05.2017.

Finalizat în 1986, King Fahd Causeway era prezentat ca un proiect ce avea drept scop îmbunătățirea relațiilor economice dintre cele două state, însă, în realitate reprezintă și

[4] „The Strategic Importance...", *op. cit.*
[5] Delshad Khezri, „The Islamic Awakening in Bahrain and Geopolitical Developments in Persian Gulf", în *Indian Journal of Scientific Research*, 1/ 2014, pp. 300-306.
[6] Simon Mabon, „The Battle for Bahrain: Iranian-Saudi Rivalry", în *Middle East Political Council*, Volume XIX, Summer, Number 2, URL: http://www.mepc.org/battle-bahrain-iranian-saudi-rivalry, accesat la data de 02.05.2017.
[7] *Idem.*
[8] *Ibidem.*
[9] Jacques Neriah, „Iranian-Saudi Tensions Are Played Out in Bahrain", în *Institute for Contemporary Affairs*, Vol. 17, No. 1, URL: http://jcpa.org/article/iranian-saudi-tensions-played-bahrain/, accesat la data de 01.05.2017
[10] Jason Rivera, *op. cit.*
[11] Simon Mabon, *op. cit.*

o infrastructură militară care poate permite intervenția armatei saudite în Bahrain[12], lucru dovedit, de altfel, în timpul Primăverii Arabe, atunci când trupele militare saudite, împreună cu forțele speciale ale Emiratelor Arabe Unite au intrat în Bahrain pentru a sprijini regimul al-Khalifa în fața protestatarilor șiiți.

Chiar dacă rezervele petroliere din Bahrain sunt aproape epuizate[13], influența asupra acestui stat încă reprezintă un motiv de dispută între Arabia Saudită și Iran. În aceste condiții, articolul își propune să demonstreze importanța strategică a Bahrainului, în contextul rivalității geopolitice saudito-iraniene, precum și cauzele pentru care regimul de la Manama adoptă o anumită poziționare față de statele din regiune.

1. Rivalitate prin *proxy*

Implicarea iraniană în Bahrain a fost realizată în mod indirect, prin crearea unor actori *proxy*, dar și în mod direct, prin mesaje de susținere pentru unii lideri șiiți sau prin continuarea mesajelor de revendicare teritorială.

Spre exemplu, în 2007, ziarul iranian Kayhan, cunoscut ca fiind o publicație apropiată liderului suprem de la Teheran, a publicat un articol în care se menționa că Bahrainul, ca urmare a „unor documente incontestabile", a reprezentat un „teritoriu iranian până în urmă cu 46 de ani", în timp ce, doi ani mai târziu, Akbar Nateq Nuri, fostul președinte la Parlamentului iranian (Majlis), a declarat că „Bahrain a reprezentat cea de-a paisprezecea provincie iraniană până în anul 1970[14]".

În esență, Revoluția Islamică a promovat trezirea comunității șiite, coalizarea acesteia sub formațiuni politice și încercarea de a juca un rol important în structurile politice din țările de care aparține[15], motiv pentru care, după 1979, Iranul a sprijinit crearea unor actori nonstatali care să formeze mișcări revoluționare în Bahrain, inclusiv prin recurgerea la acțiuni teroriste[16].

Doi ani mai târziu, în 1981, regimul de la Manama acuza gruparea intitulată Frontul Islamic pentru Eliberarea Bahrainului[17] (*The Islamic Front for the Liberation of Bahrain* – IFLB) pentru încercarea de a orchestra o lovitură de stat.

IFLB a fost înființată la jumătatea anilor '70 cu scopul de a instaura un stat teocratic în Bahrain, în timp ce unul dintre liderii săi, Hadi al-Modarresi, a afirmat că dorește importarea revoluției islamice[18], studiile arătând că gruparea era influențată de către Iran prin ideologie, leadership, sprijin mediatic și suport logisitic și militar[19]. Un alt exemplu al acțiunilor proxy întreprinse de Iran pentru destabilizarea regimului sunnit din Bahrain pot fi evidențiate prin crearea și finanțarea grupării Hezbollah al-Hejah, care se dorea a fi o replică a Hezbollahului libanez în zona Golfului, pentru a destabiliza regimurile din Arabia Saudită, Kuweit și Bahrain[20].

În 2013, o altă grupare paramilitară șiită lua naștere în Bahrain. Intitulată Saraya al-Mukhtar, făcând trimitere prin numele său la o importantă figură istorică șiită, gruparea folosește un logo asemănător celui utilizat de către Garda Revoluționară Iraniană, în timp ce acțiunile sale sunt axate asupra propagandei online fiind implicată și în acțiuni de conflict cu forțele de ordine și poliția statală[21]. De altfel, tot în 2013, în data de 25 septembrie, Muhammad Abdul Ghaffar, consilierul regal din Bahrain privind afacerile diplomatice, a acuzat, cu ocazia unui summit ONU, în termeni duri Iranul pentru acțiunile sale, afirmând: „Regatul Bahrain suferă de foarte mult timp din cauza interferențelor iraniene în politica sa internă. Sunt multe canale

[12] *Ibidem.*
[13] Simon Henderson, „Saudi Arabia's Fears for Bahrain", în The Washington Institute,Policy Analysis, 17 februarie 2011, URL: http://www.washingtoninstitute.org/policy-analysis/view/saudi-arabias-fears-for-bahrain, accesat la data de 28.05.2017.
[14] Simon Mabon, *op. cit.*
[15] Delshad Khezri, *op. cit.*
[16] Jason Rivera, *op.cit.*
[17] IFLB este cunoscută în lumea arabă și sub denumirea *Al-Jabha al-Islamiyya li Tahrir al-Bahrayn.*
18 Kevin Downs, „A Theoretical Analysis of the Saudi-Iranian Rivalry in Bahrain", în *Journal of Politics & International Studies*, Vol. 8, Winter 2012/13, p. 214.
[19] Simon Mabon, *op. cit.*
[20] Jason Rivera, *op. cit.*
[21] Abbas Qaidaari, „Does Iran have a card to play in Bahrain?", în *Al Monitor*, 17 martie 2015, URL: http://www.al-monitor.com/pulse/originals/2015/03/iran-bahrain-saraya-mukhtar.html#ixzz4sZVXwmlX, accesat la data de 09.06.2017.

TV care reprezintă influența iraniană, concomitent cu existența unui număr mare de posturi radio, ziare sau instituții media afiliate Iranului[22]".

Cu toate acestea, punctul culminant al rivalității saudito-iraniene privind Bahrain a fost atins în timpul Primăverii Arabe, atunci când peste 200.000 de șiiți[23] au luat cu asalt străzile marilor orașe pentru a protesta împotriva familiei al-Khalifa. Pe fondul acelor proteste, saudiții au oferit ajutor financiar către Manama pentru ca guvernul să poată dezvolta unele politici sociale, trimițând totodată 1.200 de soldați, cărora li s-au alăturat alți 800 de membri ai forțelor speciale din Emiratele Arabe Unite, care au traversat King Fahd Causeway, strivind cu violență mișcările antiregim din Bahrain[24]. Deși, la nivel declarativ, a existat un discurs dur venit din partea ambelor tabere, acolo unde Bahrain și Arabia Saudită acuzau Iranul pentru susținerea protestelor și ingerința în afacerile interne ale altui stat, în timp ce Teheranul milita pentru respectarea drepturilor șiiților din Bahrain, regimul iranian nu a trimis trupe militare la rândul său în Bahrain, arătând că preferă conflictele de tip proxy pentru a-și atinge interesele strategice, în timp ce o confruntare militară cu Arabia Saudită și mai ales cu SUA, care deține la rândul său trupe în arhipeleag, reprezintă o linie roșie ce nu poate fi încălcată.

Evident, tensiunile dintre Bahrain și Iran sunt departe de a se încheia, nefiind stopate nici măcar de semnarea acordului nuclear de către Teheran și statele occidentale.

Un exemplu constă în anunțul guvernului de la Manama din data de 25 iulie 2015, la aproape o săptămână de la semnarea acordului, atunci când autoritățile din Bahrain au descoperit o încercare de contrabandă cu armament iranian, dar și o fabrică clandestină de explozibil[25].

Tot în 2015, SUA elaborează un raport în care se menționează că Iranul „a oferit arme, bani și antrenament militar militanților șiiți din Bahrain[26]".

Nu în cele din urmă, în același an, în timp ce regimul din Bahrain sărbătorea împlinirea a patru ani de la intervenția militară saudită, șiiții au realizat mitinguri în capitala Manama și orașul Sitra, unde au promovat sloganuri precum „Suntem toți membri ai rezistenței", ceea ce se traduce, în termeni generali ai zonei Orientului Mijlociu, prin mișcări de opoziție, aflate în sfera iraniană de influență, precum Hezbollah sau Hamas[27].

2. Importanța geostrategică a statului Bahrain

Escaladarea acestor tensiuni sociale are la bază marginalizarea și discriminarea comunității șiite din Bahrain, politică susținută și de Arabia Saudită față de propria minoritate șiită, care reprezintă aproximativ 10-15% din populația totală[28].

Atât Arabia Saudită, cât și Bahrain privesc comunitățile proprii de șiiți drept o posibilă Coloană a V-a iraniană[29], ceea ce le alimentează neîncrederea și, implicit, privarea șiiților de anumite drepturi socio-politice.

Populația șiită din Arabia Saudită se regăsește în Provincia de Est, care se află în proximitatea Bahrainului (vezi Figura nr. 2), iar o posibilă emancipare politică a șiiților din statul vecin sau preluarea puterii de către aceștia printr-o revoluție va conduce la stimularea propriei comunități șiite către revolte și chiar către cererea secesiunii. Așadar, Riyadul percepe evenimentele din Bahrain implicit ca o amenințare la adresa propriei integrități teritoriale.

[22] Jason Rivera, *op. cit.*

[23] Tali Rachel Grumet, „New Middle East Cold War: Saudi Arabia and Iran 's Rivalry", University of Denver, URL: http://digitalcommons.du.edu/cgi/viewcontent.cgi?article=2027&context=etd, accesat la data de 01.05.2017.

[24] René Rieger, „In Search of Stability: Saudi Arabia and the Arab Spring", Gulf Research Center, 2014, URL: https://www.files.ethz.ch/isn/182104/GRM_Rieger_final__09-07-14_3405.pdf, accesat la data de 07.02.2017, p. 6.

[25] Tzvi Kahn, „Iran'a Proxy War in Bahrain", în The Foreign Policy Initiative, URL: http://www.foreignpolicyi.org/content/fpi-bulletin-iran%E2%80%99s-proxy-war-bahrain, accesat la data de 18.05.2017.

[26] *Ibidem.*

[27] Abbas Qaidaari, *op. cit.*

[28] CIA Factbook.

[29] Laurence Louër, „Sectarianism and Coup-Proofing Strategies in Bahrain", în *Journal of Strategic Studies*, 36:2, p. 246.

Figura nr. 2: Populația șiită din Arabia Saudită și proximitatea vecinătății cu Bahrain

SURSA: *Oil Price,* http://oilprice.com/, accesat la data de 28.05.2017.

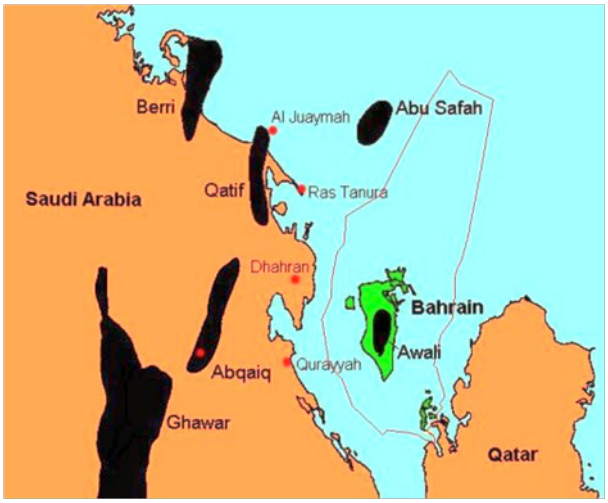

Figura nr. 3: Infrastructura critică saudită și proximitatea statului Bahrain

SURSA: *Oil Price,* http://oilprice.com/, accesat la data de 28.05.2017.

Mai apoi, intrarea Bahrainului în sfera iraniană de influență ar echivala fie cu părăsirea regiunii de către Statele Unite, fie cu o alianță iraniano-americană, ceea ce ar contraveni intereselor saudite, cu atât mai mult cu cât, după 1979, SUA a influențat în mod direct relația dintre Arabia Saudită și Iran, devenind un actor cheie în limitarea influenței iraniene în cadrul statelor membre ale Consiliului de Cooperare a Golfului (Arabia Saudită, Qatar, Emiratele Arabe Unite, Bahrain, Oman, Kuwait), precum și în limitarea influenței iraniene în comunitățile șiite din aceste țări.

Proximitatea celor două țări plasează Bahrainul la aproximativ 20 km distanță de infrastructura critică petrolieră a Arabiei Saudite, după cum rezultă și din Figura nr. 3, infrastructură critică alcătuită din:

- câmpurile petroliere: Ghawar, Abqaiq, Abu Safah, Qatif, și Berri;
- terminalele de export petrolier: Ras Tanura, Al Juaymah;
- facilitățile de procesare a apei de la Abqaiq;
- instalațiile de tratare a apei din Qurayyah[30].

Vulnerabilitatea saudită este cu atât mai ridicată cu cât infrastructura critică petrolieră se regăsește în Provincia ce Est, zonă populată cu precădere de către minoritatea șiită, care ar putea fi mobilizată de către Iran într-un posibil atac convențional sau neconvențional, prin luptă de gherilă sau terorism.

În cele din urmă, deși Arabia Saudită reprezintă, din punct de vedere cultural, cel mai conservator stat al lumii arabe, Bahrainul este, în contrapondere, o țară cu mult mai liberală, ceea ce conferă o supapă socială pentru saudiți, care trec cu regularitate King Fahd Causeway pentru a ajunge în arhipeleag, unde pot consuma alcool, carne de porc sau se pot bucura de viața de noapte[31].

La rândul său, pentru Iran, controlul căilor navigabile din Golf este percepută ca o problemă de securitate națională, motiv pentru care niciodată de-a lungul istoriei Teheranul nu s-a simțit confortabil cu prezența unei puteri militare străine în Golful Persic, fie că a fost vorba de britanici sau americani[32]. În final, impunerea unui regim apropiat Teheranului în Bahrain ar legitima politica iraniană în regiune și ar oferi Iranului o capacitate de proiecție a puterii mult mai mare, în scopul atingerii statutului de hegemon regional, putând influența inclusiv politicile petroliere ale statelor riverane Golfului Persic, de altfel cea mai bogată regiune în hidrocarburi la nivel global.

[30] *„The Strategic Importance...", op. cit.*

[31] Simon Mabon, *op. cit.*

[32] Sina Azodi, „Iran, the US, and the Persian Gulf", în *The Diplomat*, 05.11. 2016, URL: http://thediplomat.com/2016/11/iran-the-us-and-the-persian-gulf/, accesat la data de 08.05.2017.

Considerații finale

Bahrain reprezintă o zonă tampon atât din punct de vedere militar, cât și strategic, ce desparte Arabia Saudită de Iran, rolul său fiind unul fundamental în ceea ce privește arhitectura de securitate a Golfului Persic, iar dacă orice pas către instabilitatea acestei țări reprezintă o vulnerabilitate pentru Riyad, pentru Tehran va reprezenta o oportunitate, care ar putea conduce către schimbarea status quoului regional.

Strategia Iranului este axată atât pe factorul cultural, acolo unde se urmărește influențarea în propriul scop al comunității șiite din Bahrain, cât și pe factorul istoric, prin reinterpretarea trecutului și revendicarea teritorială a arhipelagului, scopul final fiind acela de a penetra Consiliul de Securitate a Golfului, slăbind influența Arabiei Saudite și obținerea hegemoniei regionale.

Pentru saudiți, evenimentele petrecute în Bahrain sunt considerate ca putând afecta în mod direct securitatea națională, cu atât mai mult cu cât Riyadul privește comunitățile șiite din Golf drept o unealtă a Teheranului de a destabiliza Monarhiile, ceea ce ar conduce către importul clivajului sectar din Bahrain, situație ce poate da naștere inclusiv secesiunii teritoriale a Arabiei Saudite.

Bahrain este, așadar, un teatru al războaielor proxy, acolo unde saudiții susțin financiar și militar regimul de la Manama condus de către familia al-Khalifa, în timp ce iranienii susțin activități subversive, în scopul de a destabiliza guvernarea. Ținând cont de acestea, marginalizarea șiiților în Bahrain dar și în Arabia Saudită va continua atât timp cât Riyadul și Manama privesc cu neîncredere aceste comunități, iar clivajul sectar se va accentua în întregul Orient Mijlociu.

Disputa regională va alimenta inclusiv divergențe privind opțiunile arhitecturii de securitate din Golful Persic, acolo unde, de teama unei posibile expansiuni a influenței iraniene, Arabia Saudită va milita în continuare pentru prezența unei puteri militare externe, așa cum este cazul prezenței americane, în timp ce, în contrapondere, Iranul își va menține poziția pentru promovarea unui mediu de securitate realizat doar de către statele riverane.

În tot acest context, în Bahrain, puterea politică, economică și militară aparține comunității sunnite, care reprezintă o minoritate de doar 25% din totalul populației, în timp ce șiiții alcătuiesc o majoritate covârșitoare de 75 procente, motiv pentru care alianța familiei al-Khalifa cu Arabia Saudită nu este motivată numai istoric sau ideologic, ci este mai ales o alianță ce permite supraviețuirea actualei monarhii ce guvernează la Manama.

BIBLIOGRAFIE:

1. AZODI, Sina, „Iran, the US, and the Persian Gulf", în *The Diplomat*, 05.11.2016, URL: http://thediplomat.com/2016/11/iran-the-us-and-the-persian-gulf/.
2. COATES, Kristian, *Insecure Gulf*, Oxford, Oxford University Press, 2015.
3. DOWNS, Kevin, „A Theoretical Analysis of the Saudi-Iranian Rivalry in Bahrain", în *Journal of Politics & International Studies*, Vol. 8, Winter 2012/13.
4. GRUMET, Tali Grumet, „New Middle East Cold War: Saudi Arabia and Iran's Rivalry", University of Denver, URL: http://digitalcommons.du.edu/cgi/viewcontent.cgi?article=2027&context=etd.
5. HENDERSON, Simon, „Saudi Arabia's Fears for Bahrain", în *The Washington Institute*, Policy Analysis, 17 februarie 2011, URL: http://www.washingtoninstitute.org /policy-analysis/view/saudi-arabias-fears-for-bahrain.
6. HOURANI, Albert, *Istoria Popoarelor Arabe*, Iași, Polirom, 2010.
7. JOYCE, Miriam, *Bahrain from the Twenthieh Century to the Arab Spring*, New York, Palgrave Macmillan, 2012.
8. KAHN, Tzvi, „Iran'a Proxy War in Bahrain", în *The Foreign Policy Initiative*, URL: http://www.foreignpolicyi.org/content/fpi-bulletin-iran%E2%80%99s-proxy-war-bahrain, accesat la 18.07.2017.
9. KHEZRI, Khezri, „The Islamic Awakening in Bahrain and Geopolitical

Developments in Persian Gulf", în *Indian Journal of Scientific Research*, 1/2014, pp. 300-306.

10. LEWIS, Bernard, *Istoria Orientului Mijlociu*, Iași, Polirom, 2014.

11. LOUËR, Laurence, „Sectarianism and Coup-Proofing Strategies in Bahrain", în *Journal of Strategic Studies*, 36:2, pp. 245-260.

12. MABON, Simon, „The Battle for Bahrain: Iranian-Saudi Rivalry", în Middle East Political Council, Volume XIX, Summer, Number 2, URL: http://www.mepc.org/battle-bahrain-iranian-saudi-rivalry.

13. NERIAH, Jacques, „Iranian-Saudi Tensions Are Played Out in Bahrain", Institute for Contemporary Affairs, Vol. 17, No. 1, URL: http://jcpa.org/article/iranian-saudi-tensions-played-bahrain/.

14. QAIDAARI, Abbas, „Does Iran have a card to play in Bahrain?", în *Al Monitor*, 17 martie 2015, URL: http://www.al-monitor.com/pulse/originals/2015/03/iran-bahrain-saraya-mukhtar.html#ixzz4sZVXwmlX.

15. RIEGER, René, „In Search of Stability: Saudi Arabia and the Arab Spring", Gulf Research Center, 2014, URL: https://www.files.ethz.ch/isn/182104/GRM_Rieger_final__09-07-14_3405.pdf.

16. RIVIERA, Jason, „Iran's Involvement in Bahrain: A Battleground as Part of the Islamic Regime's Larger Existential Conflict", în *Small Wars Journal*, URL: http://smallwarsjournal.com/printpdf/22533.

17. WEHREY, Frederic ... [et al.], *Saudi-Iranian Relations Since the Fall of Saddam*, RAND Corporation, Report, 2009.

18. ***, „The Strategic Importance of Bahrain to Saudi Arabia", în *Oil Price*, 29.07.2011, URL: http://oilprice.com/Geopolitics/Middle-East/The-Strategic-Importance-Of-Bahrain-To-Saudi-Arabia.html.

CREȘTEREA REZILIENȚEI INSTITUȚIONALE ÎN FAȚA AMENINȚĂRILOR LA ADRESA SECURITĂȚII NAȚIONALE

Ștefan SĂVULESCU*
Mihaela ȚONE**

Dinamica securității la nivel global, coroborată cu accentuarea efectelor globalizării, pune atât statele, alianțele militare, cât și celelalte formate de cooperare în fața unor provocări serioase pentru menținerea nivelului de securitate atins în ultimul deceniu. Aceste evoluții au determinat statele membre NATO și UE să adopte măsuri de natură a schimba paradigma în care erau gândite o parte din mecanismele de asigurare a protecției propriilor cetățeni și apărarea drepturilor fundamentale ale omului. Dacă NATO a stabilit ca prioritate adoptarea de măsuri la nivelul statelor pentru dezvoltarea rezilienței în fața amenințărilor, în corelare cu prevederile articolului 3 al Tratatului Alianței, UE a luat în dezbatere serioasă opțiunea constituirii unei forțe militare la nivel european. Pe de altă parte, la nivelul statelor membre, a fost dezvoltată cooperarea efectivă dintre structurile militare și cele de aplicare a legii. Această tendință s-a manifestat și la nivelul țării noastre. România a dezvoltat mecanismele instituționale necesare gestionării amenințărilor la adresa securității naționale, în corelare cu cerințele NATO și UE în materia rezilienței și menținerea la un nivel superior al gradului de siguranță al propriilor cetățeni, similar statelor europene.

Cuvinte-cheie: *reziliență, cooperare interinstituțională, migrație, mecanisme europene și naționale, Uniunea Europeană, NATO, amenințări hibride.*

1. Evoluția securității și adaptabilitatea instituțională (la nivel aliat, european și național)

Evoluția securității, înregistrată de la finele secolului al XX-lea, a cunoscut o dinamică fără precedent, ceea ce a impus regândirea paradigmei de acțiune, atât la nivelul statelor și al alianțelor militare, cât și al formatelor de cooperare internaționale.

Căderea Cortinei de Fier în anii 1990, atacurile teroriste din 11 septembrie 2001 asupra Turnurilor Gemene ale World Trade Center din New York, evoluția situației de securitate din Orientul Mijlociu, începând cu anul 2010, odată cu declanșarea „Primăverii arabe” și dinamizarea fenomenului migraționist reprezintă principalele repere ale ultimelor trei decenii. Derularea acestora, concomitent cu dinamizarea acțiunilor, pe plan extern, a unor actori statali, în vederea extinderii sau consolidării spațiului de influență, în special Federația Rusă, contestarea

Comisar-șef de poliție Ștefan SĂVULESCU este șeful Direcției operații din cadrul Ministerului Afacerilor Interne, București. E-mail: stefan.savulescu@mai.gov.ro
****Comisar de poliție Mihaela ȚONE este specialist în cadrul Serviciului Cooperare Interinstituțională de la nivelul Direcției Generale Management Operațional a Ministerului Afacerilor Interne, București. E-mail: mihaela.tone@mai.gov.ro***

limitelor frontierelor statelor și menținerea interesului populației din diferite regiuni pentru obținerea autonomiei pe criterii etnice, precum și extinderea acțiunilor teroriste au impus adaptarea mecanismelor destinate gestionării acestor tipuri de fenomene.

Perioada de extindere a NATO, de după căderea Cortinei de Fier, respectiv atentatele teroriste din septembrie 2001 și consolidarea poziției în țările membre și zonele de acțiune, a fost urmată de una în care „NATO își reevaluează și transformă constant politicile, capabilitățile și structurile, pentru a se asigura că poate continua să abordeze provocările actuale și viitoare, pentru libertatea și securitatea membrilor săi”[1]. Alianța și-a adaptat capabilitățile, acționând pentru extinderea sferei de acțiune, de la cele militare la combaterea terorismului și managementul situațiilor de criză. Astfel, pe lângă reevaluarea politicilor acționale, NATO a urmărit suplimentarea bugetelor alocate ministerelor de resort și creșterea rezilienței statelor membre.

Înțeleasă ca un corolar al măsurilor de descurajare și reasigurare în sfera militară clasică a strategiei cuprinzătoare de securitate, reziliența este evaluată pe baza a șapte cerințe de bază[2]:

- asigurarea continuității guvernării și serviciilor critice ale serviciilor guvernamentale critice;
- reziliența surselor de energie;
- capacitatea de a gestiona eficient mișcări masive de populație;
- asigurarea resurselor de apă și alimente;
- capacitatea de a trata un număr mare de victime;
- reziliența sistemelor de comunicații;
- reziliența sistemelor de transport.

Uniunea Europeană a cunoscut schimbări profunde, transformându-se, treptat, dintr-o uniune pur economică, la o organizație care acționează în numeroase domenii: politică, schimbări climatice, protecția mediului, sănătate, relații externe, securitate, justiție și migrație.

Securitatea propriilor cetățeni a cunoscut un nivel ridicat, fără precedent, comparativ cu multe alte regiuni ale globului, ca efect al măsurilor de securitate adoptate de fiecare stat membru și aplicarea de mecanisme de cooperare internaționale, dar și ca urmare a manifestării efectelor pozitive ale globalizării în domeniile tehnologic, politic sau economic. Cu toate acestea, evoluțiile recente ale situației de securitate din proximitatea și din interiorul continentului european, acțiunile unor actori statali/nonstatali sau ale unor exponenți ai mișcărilor extremiste au condus la schimbarea granițelor unor state, persistența unor conflicte înghețate și sădirea unui sentiment de insecuritate în rândul europenilor.

Aceste evoluții, coroborate cu accentuarea efectelor negative ale globalizării au determinat statele să identifice soluții pentru interconectarea elementelor militare și nonmilitare, creșterea rezilienței instituționale și dezvoltarea cooperării pe toate palierele relevante, respectiv militar, ordine publică, economic, informații, tehnică, știință, educație etc.

Cele opt atacuri teroriste comise în Europa, în mai puțin de șase luni, în Franța, Suedia, Rusia, Marea Britanie, Turcia și Germania în perioada decembrie 2016-mai 2017, inițiate în contextul aplicării măsurilor subsecvente unui nivel ridicat de alertă al instituțiilor de aplicare a legii, demonstrează, pe de o parte, adaptabilitatea acțiunilor derulate de exponenții organizațiilor extremiste, iar, pe de altă parte, și necesitatea adoptării de măsuri complementare, de natură a conduce la menținerea nivelului de securitate, atins la începutul acestui deceniu.

Acțiunile instituțiilor cu responsabilități directe sunt insuficiente fără adaptarea permanentă a mecanismelor de cooperare internațională, implicarea coordonată a resurselor pe care le are la dispoziție fiecare stat și continuarea proceselor derulate pentru educarea propriilor cetățeni, în abordarea unei atitudini de sprijin a organelor de aplicare a legii.

În căutarea unor soluții echilibrate de gestionare a situației actuale de securitate, preocupările la nivel european s-au reorientat către amenințările complexe, interconectate și

[1] The Secretary General”s Annual Report 2016, Investing in Security, p. 28, URL: http://www.nato.int/cps/en/natohq/opinions_142149.htm#sg2, accesat la data de 12.05.2017.
[2] Resilience: a core element of collective defence, URL: http://www.nato.int/docu/Review/2016/Also-in-2016/nato-defence-cyber-resilience/EN/index.htm, accesat la data de 12.05.2017.

transnaționale, discutându-se din ce în ce mai aplicat despre lansarea, în viitorul apropiat, a unei forțe armate la nivelul Uniunii Europene. De asemenea, la nivel european, se apreciază, mai mult ca oricând, că „aspecte precum drepturile omului, degradarea mediului înconjurător, stabilitatea politică și democrația, problemele sociale, identitatea culturală și religioasă sau migrația ar trebui avute în vedere”[3] .

În ultimul deceniu, principala provocare cu care statele europene s-au confruntat a fost reprezentată de migrația neregulată, fie datorată dorinței de a avea un trai mai bun, fie evitării conflictelor armate, însă punctul culminant a fost înregistrat în anul 2015, când numărul de imigranți care au intrat în Europa a depășit 1.000.000[4], pe fondul conflictelor militare din Orientul Mijlociu și Nordul Africii.

Acest fenomen a testat atât solidaritatea la nivel european și mecanismele de cooperare, cât și nivelul de pregătire al autorităților naționale pentru gestionarea unei situații de criză.

Cu toate că migrația regulată are multiple implicații pozitive asupra pieței forței de muncă, prin scăderea nivelului de șomaj și atragerea de specialiști în anumite domenii vitale sau asupra demografiei negative a Europei[5], de peste 8% până în anul 2050, în comparație cu creșterea estimată pentru SUA și Canada, de aproximativ 31%, în contextul actual în care numărul de migranți ilegali a crescut semnificativ, Uniunea Europeană nu își poate permite ca fenomenul migrației să se deruleze necontrolat și fără respectarea cadrului normativ internațional și național aplicabil în materie.

Pentru gestionarea fenomenului, Uniunea Europeană a adoptat o serie de măsuri, destinate în special creșterii nivelului de securitate la frontierele externe, relevantă fiind adoptarea Regulamentului (UE) 2016/1624 al Parlamentului European și al Consiliului din 14 septembrie 2016 privind Poliția de frontieră și garda de coastă la nivel european[6]. Pe de altă parte, statele membre au reevaluat cadrul normativ în materie de migrație și azil și au adoptat o serie de măsuri în plan operațional. Totodată, în sprijinul eforturilor UE și al statelor afectate de fenomenul migraționist au acționat și organizații guvernamentale și neguvernamentale (Organizația Internațională pentru Imigrație, Înaltul Comisariat pentru refugiați al Națiunilor Unite, Medici Fără Frontiere etc.).

Potrivit Regulamentului 1624, măsurile adoptate la nivel comunitar au vizat gestionarea integrată a frontierelor la nivel național și la nivelul Uniunii Europene, ca o componentă fundamentală a unui spațiu de libertate, securitate și justiție, pe patru niveluri, respectiv: măsuri în țări terțe (cum ar fi cele din cadrul politicii comune în domeniul vizelor); măsuri cu țările terțe vecine; măsuri de control la frontierele externe, analiză de risc; măsuri în spațiul Schengen și în domeniul returnării persoanelor.

În urma impactului acțiunilor derulate de FRONTEX la frontiera Uniunii Europene, s-a decis extinderea domeniului de acțiune al principalelor operațiuni și a duratei misiunilor Triton și Poseidon. Numai în perioada ianuarie - august 2016, ambarcațiunile care au acționat în coordonarea FRONTEX au salvat 76.229 de vieți omenești în Marea Mediterană, din care 38.750 în proximitatea Italiei și 37.479 în proximitatea Greciei[7].

Concomitent, la nivelul UE, au fost adoptate măsuri privind relocarea solicitanților de azil aflați în statele membre, cele mai importante vizând reinstalarea pe criterii voluntare a persoanelor

[3] European Commission, HORIZON 2020, The EU Framework Programme for Research and Innovation, Security, URL: https://ec.europa.eu/programmes/horizon2020/en/area/security.

[4] Conform Risk Analysis for 2016, FRONTEX, p. 5, URL: http://frontex.europa.eu/publications/?p2, accesat la data de 12.05.2017.

[5] Demographic Future. Growing Imbalances, redactat de Berlin Institute - Europe’s, p. 3.

[6] Regulamentul (UE) 2016/1624 al Parlamentului European și al Consiliului din 14 septembrie 2016 privind Poliția de frontieră și garda de coastă la nivel european și de modificare a Regulamentului (UE) 2016/399 al Parlamentului European și al Consiliului și de abrogare a Regulamentului (CE) nr. 863/2007 al Parlamentului European și al Consiliului, a Regulamentului (CE) nr. 2007/2004 al Consiliului și a Deciziei 2005/267/CE a Consiliului, URL: https://publications.europa.eu/ro/publication-detail/-/publication/65db3442-7bcf-11e6-b076-01aa75ed71a1/language-ro, accesat la data de 12.05.2017.

[7] EU operations in the Mediterranean Sea, URL: https://ec.europa.eu>fact-sheets>docs,
accesat la data de 12.05.017.

în dificultate din țările învecinate, returnarea persoanelor care nu îndeplinesc condițiile pentru azil, încheierea Acordului UE-Turcia, în vederea limitării fluxului de migranți, pe una dintre principalele rute de la Marea Egee și crearea de rețele de centre de primire în Grecia și Italia (așa-numitele hotspoturi).

Efortul legislativ și operațional derulat la nivel european a fost completat cu măsurile adoptate de statele membre afectate, acestea fiind extrem de eterogene. Unele state, ca de exemplu România și Bulgaria, au încercat să gestioneze fenomenul prin angajarea progresivă a resurselor instituțiilor de aplicare a legii responsabile și consolidarea capabilităților destinate gestionării acestuia, iar altele au introdus controale la frontieră și, în ciuda faptului că fac parte din Spațiul Schengen, au implicat Forțele Armate în securizarea frontierelor sau au construit bariere artificiale (spre exemplu, între Ungaria, Serbia, Slovenia și Croația; între Macedonia și Grecia; între Bulgaria și Turcia).

Pe lângă măsurile instituite pentru securizarea frontierelor, pentru statele aflate la frontiera maritimă a Europei (Turcia, Grecia și Italia) și cele aflate pe rutele de deplasare ale migranților (Serbia, Croația, Ungaria, Austria și Slovenia), alocarea de alimente, apă, adăpost și servicii medicale migranților a reprezentat o provocare enormă.

În ciuda eforturilor uriașe depuse la nivelul Uniunii Europene și al statelor membre pentru securizarea frontierelor și respectarea principiilor fundamentale ale drepturilor omului prin protejarea persoanelor aflate în dificultate, atât la nivel comunitar, cât și la nivelul unor state membre au fost luate în discuție și analiză mecanismele de acțiune pentru asigurarea managementului integrat și coerent a situațiilor de criză.

Deși, la nivel european, unele state nu au fost puternic afectate de fenomenul migraționist sau nu au fost puse în situația de a gestiona situații de criză în domeniul securității, ca, spre exemplu, România, dinamica mediului de securitate și evoluțiile recente din flancul estic al NATO și UE, precum și previziunile sumbre privind o posibilă detensionare a conflictelor din țările de proveniență a migranților impun adoptarea de măsuri preventive pe toate palierele pentru asigurarea de capabilități suficiente și mecanisme calibrate de reacție.

2. Contextul actual și proiecții privind cooperarea în zona operațională, pe componente din responsabilitatea MAI

Dacă până acum un deceniu, majoritatea forțelor armate erau antrenate pentru ducerea unor acțiuni pur militare în medii ostile, familiare doctrinelor în materie, iar instituțiile de aplicare a legii erau pregătite să facă față provocărilor de securitate din partea unor indivizi organizați sau nu în grupări infracționale, sau să gestioneze situații de urgență, evoluțiile recente ale mediului de securitate au demonstrat că nu mai poate fi stabilită o graniță acțională clară între cele două domenii majore ale securității din responsabilitatea ministerelor apărării și al afacerilor interne.

Tendința înregistrată în materie este reprezentată de recalibrarea capabilităților structurilor militare naționale și a NATO pentru a putea face față unui spectru mai larg de acțiune și asigurarea interoperabilității cu celelalte instituții cu responsabilități în domeniul securității.

Măsurile adoptate de forțele armate sunt dublate de cele demarate la inițiativa NATO, de către instituțiile naționale, pentru creșterea nivelului de reziliență al statelor, sens în care au fost definite cele șapte domenii de acțiune menționate.

În cazul României, cooperarea între structurile Ministerului Apărării Naționale și Ministerul Afacerilor Interne a cunoscut o dinamizare accentuată în ultimii ani, atât la nivel conceptual, cât și operațional. Deși încheiate cu succes, acțiunile reale sau de exercițiu derulate în comun au adus în atenție nevoia de creștere a nivelului de interoperabilitate și înțelegere amănunțită a provocărilor care stau în fața fiecărei structuri din cadrul acestor instituții. Ministerul Afacerilor Interne, pe lângă *împrumutarea* unor bune practici uzitate la nivelul NATO și, implicit, al MApN, și-a dezvoltat componenta structurală de planificare a misiunilor și operațiilor, înființând,

în cadrul aparatului central al ministerului, Direcția Operații. Prin această măsură, s-a reușit dezvoltarea capacității instituționale de planificare a misiunilor complexe și crearea premiselor necesare asigurării unei interoperabilități sporite cu celelalte instituții din Sistemul Național de Apărare, Ordine Publică și Securitate Națională.

Pe de altă parte, analizând responsabilitățile stabilite în sarcina instituțiilor de aplicare a legii pentru asigurarea managementului unei situații speciale sau de criză, inclusiv pe timpul stărilor excepționale (urgență, asediu, mobilizare și război) rezultă că, deși responabilitatea principală este transferată între instituțiile responsabile, acestea rămân solidare în efortul național de gestionare a acestora.

Astfel, apreciem că nici statele membre și nici NATO, și respectiv, UE nu își pot permite să nu utilizeze toate capabilitățile pe care le au la dispoziție pentru gestionarea unei situații de criză, indiferent de caracterul acesteia, militar sau nonmilitar.

3. Aspecte și implicații generale privind cooperarea interinstituțională în domeniul securității naționale

În prezent, nu avem o imagine coerentă a mediului de securitate viitor; cu toate acestea, un lucru este cert: amploarea, scopul și complexitatea amenințărilor la adresa securității au atins punctul în care nici un sector – guvernamental, societate civilă, economic, social, academic, nu poate gestiona de unul singur transformările apărute[8].

Dacă la nivelul Uniunii Europene nu mai vorbim de conflicte armate, amenințările actuale sunt circumscrise atât sectorului militar, cât și celui civil, căpătând din ce în ce mai mult un caracter hibrid. Astfel, ultimele evenimente care au avut loc pe spațiul european (anexarea Crimeei de către Federația Rusă, afluxul de migranți proveniți din Orientul Mijlociu și statele din Nordul Africii, atentatele teroriste, precum și atacurile cibernetice) confirmă caracterul hibrid al amenințărilor la adresa securității europene și securității naționale.

În acest context, pentru a face față tuturor acestor provocări, se impune realizarea de alianțe între diferiți actori și cooperarea interinstituțională a acestora, context în care este absolut necesară cooperarea și coordonarea la nivel ministerial, în vederea obținerii de rezultate care nu pot fi obținute în mod individual.

Potrivit Strategiei Naționale de Apărare (2015)[9], obiectivele și direcțiile de acțiune care privesc securitatea națională urmăresc consolidarea atât a capacităților militare, cât și a celor civile la standarde care să permită prevenirea, descurajarea și apărarea împotriva oricăror acțiuni agresive la adresa țării noastre, inclusiv împotriva celor hibride.

Deși cooperarea interinstituțională pare a fi răspunsul potrivit pentru a face față amenințărilor actuale, este de amintit faptul că, de fiecare dată, cooperarea eficientă implică costuri, în special în ceea ce privește timpul. Semnarea unor acorduri/protocoale de cooperare nu asigură premisele necesare unui răspuns eficient în fața amenințărilor la adresa securității, însă operaționalizarea și testarea practică a acestor protocoale, încă din timp de pace, sunt premise ce pot îmbunătății răspunsul instituțional la nivel național.

Din experiența practică în domeniul securității naționale, am dedus faptul că, pentru a fi eficientă, cooperarea interinstituțională presupune respectarea unor principii:

- valori comune;
- înțelegerea așteptărilor, capabilităților și limitărilor comune;
- angajament reciproc;
- platforme speciale pentru schimb de informații;
- leadership;
- planificare pe timp de pace;
- exerciții comune.

Totodată, în mod particular, cooperarea interinstituțională între MAI și MApN poate presupune sprijinirea autorităților civile cu operații militare, în anumite situații, precum

[8] National security, URL: https://en.m.wikipedia.org/wiki/National_security, accesat la data de 12. 05. 2017.

[9] The Secretary General`s Annual Report 2016, Investing in Security, p. 28, URL: http://www.nato.int/cps/en/natohq/opinions_142149.htm#sg2, accesat la data de 12.05.2017.

dezastre, aflux de migranți, acțiuni paramilitare ale unor actori nonstatali. În acest context, este important ca fiecare parte implicată să înțeleagă delimitarea propriilor atribuții, în funcție de domeniul de competență, precum și responsabilitățile ce revin fiecăruia, printr-un proces continuu de planificare și exerciții, dat fiind că într-o situație de criză nu poate fi crescut imediat gradul de încredere.

Un rol prioritar în promovarea și asigurarea cooperării interinstituționale privind securitatea națională este deținut de către Consiliul Suprem de Apărare a Țării (CSAT), autoritate administrativă autonomă care coordonează unitar activitățile care privesc apărarea țării și securitatea națională, în conformitate cu prevederile Constituției României.

Pentru prima dată, la nivel național, conceptul unui organism de cooperare și coordonare interinstituțională în domeniul securității naționale a fost prevăzut de Constituția din anul 1923, care, la art. 122 prevedea faptul că „se va înființa un Consiliu Superior al Apărării Țării, care va îngrijii, în mod permanent, de măsurile necesare pentru organizarea apărării naționale”[10].

În prezent, responsabilitățile și activitatea CSAT sunt reglementate de *Legea nr. 415/2002, privind organizarea și funcționarea CSAT*; MAI și MApN, alături de alte instituții, sunt componente ale acestui format colaborativ.

Fiecare instituție membră în CSAT are un mod propriu de gestionare a hotărârilor/documentelor și a activității în acest domeniu. Instituțiile membre CSAT participă la ședințele acestui for, pentru asigurarea securității naționale; cu toate acestea, se impune dezvoltarea de formate de cooperare interinstituțională, la niveluri diferite și în funcție de tematicile specifice, CSAT neavând rol de celulă de criză.

CSAT, prin atribuțiile exercitate, are un rol bine determinat, în special în ceea ce privește analiza și aprobarea documentelor strategice care vizează securitatea națională, a măsurilor privind respingerea unor agresiuni armate îndreptate împotriva României, dar și în ceea ce privește coordonarea unor activități subsecvente integrării țării noastre în structurile de securitate europene și euroatlantice. Conform prevederilor Legii 415/2002, CSAT „coordonează activitatea de integrare în structurile de securitate europene și euroatlantice, monitorizează procesul de adaptare a forțelor armate la cerințele NATO și formulează recomandări în concordanță cu standardele Alianței”; prin urmare, rolul CSAT este acela de instrument de decizie în politica de securitate națională.

Totodată, proiectarea climatului de securitate la nivel național este o responsabilitate comună a tuturor instituțiilor membre, nu doar a CSAT sau a celor două ministere amintite, iar o parte importantă în acest proces este sectorul civil. Este necesară dezvoltarea culturii de securitate atât la nivelul instituțiilor, cât și la nivelul sectorului privat și a cetățenilor.

Având în vedere considerentele prezentate, putem concluziona că, în ceea ce privește securitatea națională, cooperarea interinstituțională reclamă acțiuni integrate, capabilități robuste, inclusiv de ISR (intelligence, surveillance, reconnaissance), precum și operații ample și complexe, pentru abordarea contextualizată a amenințărilor actuale de securitate.

4. Implementarea celor șapte cerințe de bază în reziliență exemplu de cooperare interinstituțională

Pentru creșterea rezilienței naționale, Consiliul Nord-Atlantic a stabilit șapte cerințe de bază menționate în capitolul întâi, încă din februarie 2016; subsecvent, la nivelul Alianței au fost dezvoltate ghiduri și criterii de evaluare, care să asiste fiecare stat membru în procesul de evaluare și planificare/pregătire pentru gestionarea situațiilor de criză[11].

Având în vedere faptul că, prin reziliență se înțelege capacitatea unui sistem de a face față unor situații, prezente sau posibile, de criză, ce pot

[10] Resilience: a core element of collective defence, URL: http://www.nato.int/docu/Review/2016/Also-in-2016/nato-defence-cyber-resilience/EN/index.htm, accesat la data de 12.05.2017.

[11] Allies move forward on enhancing NATO”s resilience, URL: www.nato.int/cps/en/natohq/news_135288.htm?selectedLocale=en , accesat la data de 12.05.2017.

apărea, continuând să se dezvolte, putem aprecia că dezvoltarea rezilienței naționale, pentru a face față oricăror tipuri de amenințări este un proces continuu, fără termen de finalitate.

Ținând cont de importanța acordată dezvoltării la nivelul Alianței, de către fiecare stat membru, a rezilienței naționale, în cadrul Summitului NATO de la Varșovia din iulie 2016, șefii de state și de guverne și-au asumat, ca prioritate, implementarea celor șapte cerințe de bază.

România se înscrie acestui demers; la nivel național, instituția responsabilă pentru coordonarea implementării conceptului de reziliență privind urgențele civile este Ministerul Afacerilor Interne. În procesul de implementare a acestui concept, au fost invitate să-și aducă contribuția mai multe instituții: Administrația Prezidențială, Secretariatul General al Guvernului, Ministerul Afacerilor Externe, Ministerul Apărării Naționale, Ministerul Afacerilor Interne, Ministerul Agriculturii și Dezvoltării Rurale, Ministerul Sănătății, Ministerul Energiei și Ministerul Transporturilor, reușindu-se astfel dezvoltarea unui mecanism național de cooperare interinstituțională.

Ministerele de resort și-au asumat responsabilitatea dezvoltării de mecanisme specifice, potrivit domeniului de competență, pentru creșterea rezilienței sectorului comunicațiilor, transporturilor și resurselor de apă și de hrană. În ceea ce privește stabilirea unor mecanisme naționale pentru gestionarea deplasării necontrolate a populației și a victimelor multiple responsabilitatea a fost asumată de către Ministerul Afacerilor Interne.

Prin implementarea rezilienței, la nivel național, se are în vedere dezvoltarea capacității instituționale de a face față oricăror amenințări, inclusiv celor hibride, dar și dezvoltarea interoperabilității capabilităților naționale cu cele ale NATO, astfel încât să poată fi asigurat sprijinul națiunii gazdă pentru forțele aliate, în caz de necesitate.

Totodată, în contextul în care 90% din resursele și logistica necesară forțelor NATO provine de la companii private sau se asigură prin contracte cu operatorii din sectorul privat, în acest proces au fost implicați, subsecvent, și operatori privați, fie de transport, de comunicații sau din domeniul alimentar, încercându-se atingerea unui nivel comun de înțelegere a cerințelor militare la nivelul sectorului civil/privat.

Suplimentar, în contextul actual, în care nu mai există o delimitare clară a conceptelor de pace și război prin apariția amenințărilor de tip hibrid, acțiunile singulare ale forțelor statului au devenit insuficiente, necesitând acțiuni conjugate cu actori din sectorul civil (spre exemplu, din domeniul comunicațiilor). De asemenea, amenințările hibride reclamă nu doar cooperare între sectorul militar și cel civil[12], dar și cooperare între organizații, precum cea dintre NATO și UE, în special în ceea ce privește creșterea rezilienței și contracararea amenințărilor hibride, prin utilizarea în comun atât a capabilităților militare, cât și a altor resurse, inclusiv legislative, ale UE.

La nivel național, în ceea ce privește amenințările hibride, în practica profesională, am identificat principalele responsabilități instituționale, desprinse din corelarea tipurilor de amenințări hibride cu măsurile necesare pentru contracararea acestora, ce au în vedere o serie de aspecte:

- cunoașterea permanentă a situației operative, potrivit sferei de competență;
- prevenirea acțiunilor de tip hibrid, prin creșterea măsurilor de protecție fizică a obiectivelor aflate în responsabilitate, precum și securizarea rețelelor informatice și de comunicații;
- conducerea și executarea acțiunilor de contracarare a acestora, în cazul apariției pe teritoriul național;
- creșterea nivelului de interoperabilitate și a schimbului de informații între structurile din cadrul Sistemului Național de Apărare;
- întocmirea documentelor de planificare, instruire și cooperare interinstituțională, în scopul creșterii capacității de acțiune, în mod integrat, a

[12] Cătălin Alexandru, Patrick Turner, (NATO): România, unul din cei mai puternici aliați NATO în măsurile de creștere a rezilienței, URL: https://www.agerpres.ro/politica/2017/03/28/patrick-turner-nato-romania-unul-din-cei-mai-puternici-aliati-nato-in-masurile-de-crestere-a-rezilientei-12-54-13, 28.03.2017, accesat la data de 29.03.2017.

instituțiilor din cadrul SNA;

- participarea la forme de pregătire interinstituțională, pe palierul de competență, prin planificarea, organizarea și desfășurarea de exerciții.

Concluzii

Noile provocări la adresa securității statelor, cum ar fi fenomenul migrației neregulate, atacurile teroriste repetate, dar și efectele negative ale globalizării impun măsuri de natură a schimba paradigma în care erau gândite parte din mecanismele de asigurare a protecției propriilor cetățeni și apărarea drepturilor fundamentale ale omului.

Astfel, statele au fost determinate să identifice soluții pentru interconectarea elementelor militare și nonmilitare, creșterea rezilienței instituționale și dezvoltarea cooperării pe toate palierele relevante, respectiv militar, ordine publică, economic, informații, tehnică, știință, educație etc.

Atât la nivel aliat, cât și la nivel național, acțiunile forțelor de apărare/aliate necesită adaptarea continuă la vulnerabilitățile și amenințările actuale, generate inclusiv de actori nonstatali, iar în ceea ce privește acțiunile reale sau de exercițiu derulate în comun de către Ministerul Afacerilor Interne și Ministerul Apărării Naționale, acestea au adus în atenție nevoia de creștere a nivelului de interoperabilitate și înțelegere amănunțită a provocărilor care stau în fața fiecărei structuri din cadrul acestor instituții.

În acest context, creșterea rezilienței naționale, în fața oricărui tip de amenințări, inclusiv hibride, este un pilon central al apărării, care contribuie la reducerea riscurilor de securitate și la menținerea coeziunii statale, a independenței și securității naționale.

BIBLIOGRAFIE:

1. Agenția de presă Agerpres, URL: https://www.agerpres.ro/politica/2017/03/28/patrick-turner-nato-romanaia-unul-dintre-cei-mai-puternici-aliati-nato-in-masurile-de-crestere-a-rezilientei-12-54-13.
2. Agenția de presă Reuters, URL: www.reuters.com.
3. Agenția pentru drepturi fundamentale a Uniunii Europene, *Fundamental rights of migrants in an irregular situation in the European Union*, 2011.
4. Agenția pentru drepturi fundamentale a Uniunii Europene, *Manual de drept european în materie de azil, frontiere și imigrație*, 2014.
5. ALEXE, Iris şi PĂUNESCU, Bogdan (coordonatori), *Studiu asupra fenomenului imigrației în România. Integrarea străinilor în societatea românească*, Editor Fundația Soros România, 2011.
6. Allies move forward on enhancing NATO"s resilience, URL: www.nato.int/cps/en/natohq/news_135288.htm?selectedLocale=en.
7. Berlin Institute for Population and Development, *Europe's Demographic Future. Growing Imbalances*, 2016.
8. BRETTELL, Caroline B., HOLLIFIELD, James F., *Migration theory*, Publisher New York: Routledge, 2015.
9. CASTLES, Stephen; MILLER, MARK J., *The Age of Migration. International Population Movements in the Modern World*, Fourth Edition, revised and updated, Palgrane Macmillon, 2009.
10. Center for Global Constitutionalism, Communication from the Commission to the European Parliament and the Council on Guidance for Application of Directive 2003/86/EC on the Right to Family Reunification, 2014.
11. Constituţia României, republicată, 2003.
12. Department of Economic and Social Affairs din cadrul Organizației Națiunilor Unite, *International Migration Report 2015*, 2016.
13. EU operations in the Mediterranean Sea, URL: https://ec.europa.eu>fact-sheets>docs.
14. FAUDE, Benjamin, How Is Inter-Institutional Order Possible In Global Governance, aprilie 2016, URL: https://lawlog.blog.wzb.eu/2016/04/18/how-is-inter-institutional-order-possible-in-global-governance/.
15. Fondul Națiunilor Unite pentru populație și Organizația internațională pentru migrație, *International Migration and Development:*

Contributions and Recommendations of the International System, 2013.

16. Hotărârea Guvernului 1152/2014 privind organizarea, funcţionarea şi compunerea Centrului Naţional de Conducere a Acţiunilor de Ordine Publică.

17. Hotărârea Guvernului nr. 117/2014 privind organizarea şi funcţionarea Centrului operaţional de comandă al Guvernului, cu modificările şi completările ulterioare.

18. Hotărârea Guvernului nr. 572/2008, privind constituirea Grupului de coordonare a Implementării Strategiei naţionale privind migraţia, cu modificările şi completările ulterioare.

19. Hotărârea Guvernului nr. 780/2015 pentru aprobarea Strategiei naţionale privind imigraţia pentru perioada 2015-2018 şi a Planului de acţiune pe anul 2015 pentru implementarea Strategiei naţionale privind imigraţia pentru perioada 2015-2018.

20. Hotărârea Guvernului nr. 94/2014 privind organizarea, funcţionarea şi componenţa Comitetului naţional pentru situaţii speciale de urgenţă, cu modificările şi completările ulterioare.

21. Hotărârea Guvernului nr. 943/2001 privind înfiinţarea Grupului Interministerial Român pentru Managementul Integrat al Frontierei de Stat, republicată.

22. Institutul pentru politici publice București, *Consiliul Suprem de Apărare a Țării, principal instrument de decizie în politica de securitate a României*, București 2005.

23. KING, Russell, *Theories and Typologies of Migration: An Overview and a Primer*, Malmö Institute for Studies of Migration, Diversity and Welfare, Malmö University, 2012.

24. KING, Russell, *Theories and Typologies of Migration: An Overview and a Primer*, 2012.

25. Legea apărării naţionale nr. 45/1994, cu modificările şi completările ulterioare.

26. Legea nr. 122/2006 privind azilul în România, cu modificările şi completările ulterioare.

27. Legea nr. 346/2006 privind organizarea şi funcţionarea Ministerului Apărării Naţionale, cu modificările şi completările ulterioare.

28. Legea nr. 415/2002 privind organizarea şi funcţionarea Consiliului Suprem de Apărare a Ţării, cu modificările şi completările ulterioare.

29. Legea nr. 51/1991 privind securitatea naţională a României, republicată.

30. Legea nr. 90/2001 privind organizarea şi funcţionarea Guvernului României şi ministerelor, cu modificările şi completările ulterioare.

31. Legea planificării apărării nr. 203/2015.

32. MARENIN, Otwin, *Challenges for Integrated Border Management in the European Union* - Geneva Centre for Democratic Control of Armed Forces - DCAF 2010.

33. MOREHOUSE, Christal; BLOMFIELD, Michael, *Irregular migration in Europe*, Migration Policy Institute, 2011.

34. NATO sees resilience as key issue in AWACS replacement, URL: http://www.reuters.com/article/us-nato-arms-idUSKBN0L51SE20150201.

35. Ordonanţa de urgenţă a Guvernului nr. 1/1999 privind regimul stării de asediu şi regimul stării de urgenţă, aprobată cu modificări şi completări prin Legea nr. 453/2004.

36. Ordonanţa de urgenţă a Guvernului nr. 194/2002 privind regimul străinilor în România, republicată, cu modificările şi completările ulterioare.

37. Ordonanţa de urgenţă a Guvernului nr. 30/2007 privind organizarea şi funcţionarea Ministerului Afacerilor Interne, aprobată cu modificări prin Legea nr. 15/2008, cu modificările şi completările ulterioare.

38. Ordonanţa de Urgenţă nr. 105/2001 privind frontiera de stat a României, aprobată cu modificări prin Legea nr. 243/2002, cu modificările şi completările ulterioare.

39. Organizaţia internaţională pentru migraţie, *Migration and the United Nations post-2015 development agenda*, 2013.

40. Organizaţia internaţională pentru migraţie, *Migration Initiatives 2016. Migration governance and sustainable development*, 2016.

41. Organizaţia internaţională pentru migraţie, *World Migration Report 2015. Migrants and Cities: New partnerships to*

Manage Mobility, 2016.

42. Reglementări UE, URL: https://publications.europa.eu.

43. Resilience: a core element of collective defence, URL: http://www.nato.int/docu/Review/2016/Also-in-2016/nato-defence-cyber-resilience/EN/index.htm.

44. Risk Analysis for 2016, FRONTEX, p. 5, URL: http://frontex.europa.eu/publications/?p2.

45. SARCINSCHI, Alexandra, *Migraţie şi securitate*, Editura Universității Naționale de Apărare „Carol I", București, 2008.

46. SKELDON, Ronald, *Global Migration: Demographic Aspects and Its Relevance for Development, UN Population Division*, Technical Paper no. 2013/6.

47. Strategia Națională de Apărare a Țării pentru perioada 2015-2019, O Românie puternică în Europa și în lume, București, 2015.

48. The Secretary General"s Annual Report 2016, Investing in Security, pag. 28, URL: http://www.nato.int/cps/en/natohq/opinions_142149.htm#sg2.

49. UNHCR, *Global trends forced displacement in 2015.*

50. VOINESCU, Sever și DUDU IONESCU, Constantin, Consiliul Suprem de Apărare a Țării, principal instrument de decizie în politica de securitate a României, Institutul pentru Politici Publice, București, 2005.

51. Website NATO, URL: http://www.nato.int/docu/review/2016/Also-in-2016/nato-defence-cyber-resilience/EN/index.htm.

MODEL AVANSAT DE CONFIGURARE A AGRESIUNII DE TIP HIBRID

Dan-Lucian PETRESCU*

Ţinând cont de complexitatea mediului de securitate contemporan şi de nivelul ridicat de incertitudine pe care îl presupune, consider că cea mai potrivită abordare a eforturilor integrate de identificare şi contracarare a ameninţării de tip hibrid şi de soluţionare a crizelor pe care le generează este abordarea proactivă. Aceasta trebuie să fie fundamentată pe un mod de gândire prospectiv, susţinut cu argumente ştiinţifice, care să contribuie semnificativ la determinarea coordonatelor dinamicii probabile sau dorite ale quo vadisului situaţiei de securitate actuale.

În acest context, aprofundarea cunoaşterii conceptului de ameninţare de tip hibrid, care conturează aspectul modern al fenomenului război, constituie un demers de importanţă majoră în domeniul ştiinţelor militare. În acest articol, am urmărit proiectarea unui algoritm avansat, puternic, controlabil, eficient şi flexibil de configurare a agresiunii de tip hibrid, care să vină în sprijinul previzionării situaţiilor de criză viitoare şi planificării modului de prevenire sau rezolvare a lor.

***Cuvinte-cheie**: ameninţare hibridă, agresiune hibridă, măsuri proactive, analiza structurală, impact încrucişat.*

Introducere

Ameninţarea de tip hibrid este extrem de complexă, iar modalitatea de contracarare a acesteia trebuie să fie pe măsură. Răspunsul adecvat acestui tip de ameninţare trebuie să fie configurat prin realizarea în mod ingenios şi inteligent a unor conexiuni transdisciplinare reale între domeniile de vârf ale ştiinţei militare.

Este important să precizăm faptul că, în prezent, în mediul internaţional ştiinţific, dar şi în cel operaţional, se depune un efort semnificativ în scopul definirii ameninţării de tip hibrid şi modalităţilor în care aceasta se poate pune în aplicare, devenind, astfel, agresiune. Ţinând cont de definiţiile date de către diferiţi cercetători care au inventat − James N. Mattis şi Frank G. Hoffman − şi au studiat conceptul − Russel W. Glenn, Valery Gherasimov, Andrew Korybko −, ameninţarea de tip hibrid se defineşte ca *o acţiune posibilă a unui adversar de tip statal sau nonstatal care întrebuinţează în mod adaptiv şi concertat mijloace politice, militare, economice, sociale sau informaţionale, în cadrul unor combinaţii de metode neconvenţionale şi convenţionale, în scopul realizării obiectivelor urmărite*.

Urmând modelul Quad chart al lui Nathan Freier[1], dinamica ameninţării de tip hibrid presupune acţiunea concertată a patru tipuri de ameninţări – *tradiţionale* (convenţionale), *neregulate* (neconvenţionale), *catastrofice* şi *disruptive*[2] – asupra centrului de greutate

[1] Nathan P. Freier, „Present at the Counterrevolution: An Essay on the 2005 National Defense Strategy and Its Impact on Policy", *United States Army War College Guide to National Security Issues*, Vol. 2: *National Security Policy and Strategy*, pp. 120-121. Editor J. Boone Bartholomees, Jr., 4th edition, iulie, 2010.

[2] N.A. Termenul *disruptiv* provine din *disruptive* (en.) şi este considerat cu sensul de scoatere din funcţiune, afectare a funcţionării unui sistem, fără a-l distruge.

Locotenent-colonel Dan-Lucian PETRESCU este instructor superior în cadrul Facultății de Securitate și Apărare, Universitatea Națională de Apărare „Carol I" din București.

E-mail: dan_petrescu1@yahoo.com

al actorului ţintă, ceea ce duce la distrugerea acestuia.

Adiţional, se poate desprinde o caracteristică importantă conform căreia, în mediul operaţional de tip hibrid, ponderea acţiunilor, din perspectiva tipologiei, prezintă o puternică migraţie de la cele regulate spre cele neconvenţionale, în special către cele de tip asimetric.

În literatura de specialitate se utilizează foarte des termenul de *ameninţare hibridă* în locul celei de *agresiune hibridă*. Consider că motivele ar putea proveni din următoarele două situaţii. Pe de o parte, se doreşte evidenţierea caracterului proactiv al acţiunilor de contracarare a agresiunii de tip hibrid, prin eliminarea ameninţării, înainte ca acesta să se manifeste, devenind agresiune (totuşi, nu se ia în consideraţie situaţia în care o ameninţare poate deveni, în sine, agresiune). Pe de altă parte, lipsesc reglementările prin care un complex de acţiuni să poată fi declarat, în mod oficial, agresiune de tip hibrid. În măsura în care, în documentele oficiale din domeniul dreptului internaţional public, agresiunea de tip hibrid nu a fost definită complet, se deduce ideea conform căreia criteriile prin care se poate identifica agresorul şi dovedi agresiunea lipsesc sau sunt neclare. În consecinţă, se preferă termenul *ameninţare*, întrucât acesta oferă cadrul oficial desfăşurării unor măsuri preventive împotriva unor acţiuni potenţiale, considerate agresiuni.

Configurarea agresiunii de tip hibrid presupune un efort considerabil; ea trebuie să fie realizată printr-un proces complex, similar celui de planificare operaţională (produsul se constituie într-o serie de acţiuni în toate domeniile asimilate operaţiilor militare) şi care trebuie desfăşurat de către un actor cel puţin raţional, dacă nu chiar super-raţional. Dacă ţinta percepe acţiunile agresorului ca fiind iraţionale, înseamnă că agresiunea de tip hibrid care le subsumează este bine configurată şi aplicată. Cu cât mai iraţională pare agresiunea, cu atât mai mult aceasta creşte în valoare şi îşi amplifică efectele, iar ţintei îi va fi mai dificil să genereze un răspuns adecvat.

Dezvoltarea modelului de configurare a agresiunii de tip hibrid

Considerând un mediu operaţional în care coexistă mai mulţi actori de tip statal sau nonstatal, configurarea ameninţărilor pe care le poate genera fiecare dintre aceştia şi, în final, a celor pe care un agresor le poate aplica asupra unei ţinte, necesită o atenţie deosebită, un mare nivel de cunoaştere a posibilităţilor de acţiune ale fiecăruia, o capacitate ridicată de sinteză şi chiar o imaginaţie bogată.

Pentru a oferi un model teoretic complet, în cele ce urmează, considerăm că suntem în afara mediului analizat şi, astfel, excludem posibilitatea plasării noastre în rolul agresorului sau al ţintei. Obiectivele urmărite vizează obţinerea de date eficient structurate pentru a estima impactul pe care îl pot avea acţiunile agresorului în mediul operaţional asupra ţintei, compunerea lor şi modul în care se realizează conexiunile între diferite tipuri de agresiuni (componente) pentru a se obţine configuraţia de tip hibrid. Pentru ca acest proces să se desfăşoare în mod eficient, este necesară parcurgerea a şapte etape, pe care le voi expune în cele ce urmează.

1. Prima etapă constă în ***identificarea ameninţărilor ce pot apărea în mediul operaţional şi redarea lor într-o formă tabelară***, alături de caracteristici specifice acestora, astfel: domeniu, ameninţare, mijloace, efecte, risc, importanţă (impactul asupra ţintei), probabilitate şi frecvenţă de apariţie.

Aceasta se realizează prin analiza mediului operaţional şi de securitate în care se află actorii. Pentru operativitate, se poate utiliza o listă standard care să fie adaptată şi completată corespunzător mediului respectiv şi caracteristicilor actorilor. Se recomandă ca primul criteriu de ordonare descrescătoare a ameninţărilor să fie cel al nivelului de risc, şi anume al produsului dintre impactul şi probabilitatea de apariţie a fiecărei ameninţări. Lista va fi definitivată după parcurgerea etapelor de analiză a actorilor, în ce priveşte capabilităţile şi vulnerabilităţile lor.

În Tabelul nr. 1 este prezentat câte un exemplu pentru fiecare domeniu: politic, militar, economic, social, informaţii, infrastructuri şi securitate (PMESII-S).

DOMENIU	AMENINŢARE/ AGRESIUNE	MIJLOACE	EFECTE	R	I	PI	FA
POLITIC	Subminarea încrederii populaţiei în autorităţile de guvernare	Formatori de opinie, informaţii, timp	Diminuarea/ pierderea controlului asupra politicii interne şi externe	R	4	0,75	P
MILITAR	Inserţia unor forţe pentru operaţii speciale (FOS) fără însemne care să joace rolul unor miliţii locale	FO, mercenari	Fabricarea unui motiv pentru intervenţia militară sau destabilizarea ordinii interne	R	4	0,75	M
ECONOMIC	Subminarea relaţiilor economice externe ale ţintei pe domeniile critice ale acesteia (cum ar fi exportul de resurse) prin concurenţă neloială sau alte mijloace	Resurse economice, influenţă	Reducerea veniturilor la bugetul de stat, afectarea procesului de dezvoltare economică	R	4	0,75	P
SOCIAL	Infiltrarea unor formatori de opinie care să polarizeze populaţia din statul ţintă	Personal specializat, informaţii, timp	Afectarea coeziunii sociale	S	2	0,5	P
INFORMAŢII	Promovarea prin formatori de opinie (în mass-media sau mediul virtual) a ineficienţei autorităţilor sau a incompetenţei clasei politice	Formatori de opinie, informaţii, circumstanţe, timp	Diminuarea sprijinului acordat de populaţie autorităţilor şi structurilor de guvernare	M	3	0,75	P
INFRA STRUCTURĂ	Distrugerea unor elemente de infrastructură critică (centrale electrice, treceri permanente etc.)	FOS, mercenari, informaţii	Distrugeri, victime sau afectarea vieţii societăţii	R	4	0,75	R
SECURITATE	Subminarea autorităţilor statului ţintă (sistemul de securitate internă cel de impunere a legii, sistemul de justiţie etc.	Agenţi infiltraţi, resurse financiare, informaţii, timp	Diminuarea capacităţii statului de a-şi asigura securitatea proprie	R	4	0,75	P

Tabelul nr. 1: Model privind identificarea ameninţărilor ce pot apărea în mediul operaţional

Gradul de risc (**R**) reprezintă produsul între probabilitatea de apariţie şi impactul asupra ţintei şi poate avea valorile: **S**căzut (0-1,25), **M**ediu (1,25-2,75), **R**idicat (2,75-4). Impactul (**I**) poate fi **1**=*slab*, **2**=*mediu*, **3**=*ridicat*, **4**=*critic*. Probabilitate independentă (**PI**) este de forma **0,xx** şi se exprimă în multipli de 0,25. Frecvenţa de apariţie (**FA**) poate avea valorile: **S**ingulară, **R**edusă, **M**edie, **M**are, **P**ermanentă.

2. Cea de a doua etapă presupune ***analiza capabilităţilor actorilor*** din mediul operaţional (din punctul de vedere al instrumentelor, resurselor, pregătirii, doctrinei, acţiunilor anterioare) de a genera agresiunile ce pot compune o ameninţare de tip hibrid. De aici rezultă (se poate selecta dintr-o listă constituită apriori) setul de agresiuni independente pe care fiecare actor le poate aplica asupra unei ţinte oarecare. Pentru a sprijini etapele următoare, se recomandă consemnarea, în dreptul fiecărei ameninţări, a actorilor ce se pot constitui în potenţiale ţinte.

3. Cea de a treia etapă constă în ***identificarea agresorului şi a ţintei***. Considerând cazul general ce implică posibilitatea declanşării confruntării de tip hibrid între oricare dintre actorii existenţi în mediul operaţional, în acest stadiu se realizează analiza relaţiilor dintre actori, pentru care se recomandă utilizarea metodei MACTOR[3] inventată de către analistul francez Michel Godet. Rezultatele obţinute oferă posibilitatea stabilirii argumentate a alianţelor şi conflictelor ce pot apărea între actori şi, în consecinţă, permit identificarea agresorului şi a ţintei. Strategiile determinate pot include realizarea de alianţe între diferiţi actori, caz în care rezultă noi actori cu capacităţi combinate şi care pot genera ameninţări de tip hibrid în configuraţii sau cu ponderi ale elementelor componente specifice acestora. Pentru a avea imaginea corectă, este necesar să se analizeze agresiunile şi efectele compuse aferente părţilor rezultante implicate în conflict. De asemenea, nu trebuie uitat faptul că structura ameninţării de tip hibrid (din punct de vedere cantitativ şi calitativ) depinde fundamental, în afară de capacităţile generatorului, de vulnerabilităţile, dar şi de punctele tari ale ţintei (se recomandă evitarea/erodarea punctelor tari şi „ochirea" vulnerabilităţilor).

4. În următoarea etapă se realizează ***analiza ţintei*** (analiza SWOT şi analiza structurală), urmărindu-se identificarea vulnerabilităţilor şi, respectiv, a variabilelor operaţionale cheie ce direcţionează acţiunile agresorului.

Din analiza SWOT, rezultă vulnerabilităţile ţintei care, aşa cum am precizat, vor constitui obiective pentru agresor. Vulnerabilităţile determină o a doua selecţie a acţiunilor pe care agresorul are posibilitatea şi trebuie să le aplice asupra ţintei pentru a-şi atinge scopul. Prin urmare, rezultatul analizei SWOT a ţintei determină în mod decisiv stabilirea setului de agresiuni care se adresează ţintei şi, în plus, alături de rezultatele analizei structurale, contribuie la cristalizarea strategiilor de combinare a acestora pentru maximizarea efectelor (în special rezultatele relaţiilor puncte tari – oportunităţi şi ameninţări – puncte slabe).

Analiza structurală[4] a ţintei permite descrierea stării actorului ţintă prin prezentarea caracteristicilor acestuia ca variabile de sistem şi a relaţiilor dintre ele, precum şi prin identificarea aspectelor relevante în măsură să justifice strategii posibile ale agresorului care nu pot fi deduse pe cale intuitivă. Trebuie specificat faptul că variabilele de intrare sunt, în primul

[3] N.A.: MACTOR reprezintă matricea alianţelor şi conflictelor: tactici, obiective, recomandări. Metoda a fost prezentată în original în lucrarea *From anticipation to action – a handbook of strategic prospective*, United Nations Educational, Scientific and Cultural Organization, Paris, 1994, p. 105. În formă adaptată, am prezentat-o în comunicarea cu titlul „The prospective analysis of strategic relations between geopolitical actors in the contemporary security environment - the MACTOR method", în cadrul Conferinţei internaţionale *Strategies XXI – Strategic Changes in Security and International Relations*, organizată de către Facultatea de Securitate şi Apărare şi Şcoala Doctorală din Universitatea Naţională de Apărare „Carol I" în perioada 14-15 aprilie 2016, vol. 1, pp. 62-72.

[4] N.A. Metoda a fost inventată de către Michel Godet şi J.C. Duperrin în 1973 şi este denumită MICMAC (*Matrice d'Impacts Croisés – Multiplication Appliquée à un Classement*). În formă adaptată, am prezentat-o în comunicarea cu titlul „*Structural analysis of hybrid aggression target*", în cadrul Conferinţei internaţionale „*Strategies XXI – Strategic Changes in Security and International Relations*", organizată de către Facultatea de Securitate şi Apărare şi Şcoala Doctorală din Universitatea Naţională de Apărare „Carol I" în perioada 06-07 aprilie 2017, vol. 1, pp. 87-94.

rând, vulnerabilităţile ţintei determinate din analiza SWOT. Pe lângă acest produs de natură descriptivă, rezultatele obţinute evidenţiază variabilele cheie prin intermediul cărora agresorul poate influenţa dinamica stărilor ţintei astfel încât să o dezechilibreze. Nu trebuie uitat faptul că „*unul dintre obiectivele principale urmărite de ameninţările de tip hibrid este destabilizarea guvernării şi instituţiilor principale ale oponentului, prin aceasta creându-se haos şi vacuum de putere*”[5]. De asemenea, analiza structurală a actorului ţintă prezintă concluzii privind stabilitatea acestuia, deduse din dispunerea variabilelor de sistem în cadrul *Graficului relaţiilor directe* şi *Graficului relaţiilor directe şi indirecte*. Graficele relaţiilor reprezintă câte o „hartă” a influenţelor şi dependenţelor dintre factorii care definesc actorul ţintă şi îi evidenţiază pe aceia (*variabilele cheie*) pe care agresorul trebuie să îi exploateze pentru a genera perturbaţii semnificative în sistem. Factorii vor desemna, cu prioritate, obiectivele vizate de către acţiunile ce compun agresiunea de tip hibrid, într-o configuraţie bazată pe efecte. Produsele analizei structurale depind calitativ de obiectivitatea cu care se realizează determinarea variabilelor de sistem şi a relaţiilor dintre acestea.

Cu ajutorul produselor rezultate din analiza structurală a ţintei şi din analiza SWOT, agresorul poate determina o „hartă” a efectelor necesare a fi generate asupra ţintei pentru exploatarea vulnerabilităţilor şi destabilizarea acesteia. Mai mult ca orice, agresorul caută să controleze efectele acţiunilor sale pentru a le putea combina şi focaliza asupra ţintei. Agresorul trebuie să aibă în permanenţă în vedere faptul că rezultatul urmărit constituie configurarea setului de acţiuni care, prin integrarea efectelor, să ducă la atingerea scopului, adică impunerea voinţei proprii asupra ţintei fără a o distruge şi fără a fi sancţionat, în conformitate cu dreptul internaţional.

5. În continuare, ***analiza de impact încrucişat***[6] ***a agresiunilor*** oferă o imagine a interdependenţei lor, luând în considerare probabilitatea condiţională dintre acestea. Aplicarea metodei create de către Michel Godet (1974) presupune întocmirea pentru actorul agresor a matricei de impact încrucişat privind agresiunile pe care le poate aplica asupra ţintei, considerând cele două criterii: capabilităţile agresorului şi vulnerabilităţile ţintei. Aceasta este o matrice pătratică de forma ($\mathbf{A_n}\times\mathbf{A_n}$), unde $\mathbf{A_1}$, …, $\mathbf{A_n}$ reprezintă acţiunile agresorului. Elementele matricelor sunt de forma $\mathbf{a_{i/j}}/\mathbf{a_{i/\bar{j}}}$, unde:

- $\mathbf{a_{i/j}}$ reprezintă probabilitatea de manifestare a ameninţării $\mathbf{A_i}$ dacă se manifestă $\mathbf{A_j}$;
- $\mathbf{a_{i/\bar{j}}}$ reprezintă probabilitatea de manifestare a ameninţării $\mathbf{A_i}$ dacă **nu** se manifestă $\mathbf{A_j}$.

Considerând agresiunea de tip hibrid ca un complex de acţiuni cu diferite probabilităţi de manifestare, se poate calcula probabilitatea ca agresorul să genereze în mediul operaţional toate combinaţiile posibile. Pentru operativitatea execuţiei se poate utiliza aplicaţia informatică *Smic*[7], dezvoltată de către *Heurisco*. Interpretarea rezultatelor analizei de impact încrucişat presupune şi identificarea unor concluzii care să completeze rezultatele obţinute în etapa de determinare a strategiilor actorilor prezenţi în mediul operaţional (etapa nr. 3). Mai exact, concluziile rezultate din analiza impactului încrucişat dintre ameninţări oferă informaţii extrem de valoroase în crearea conexiunilor dintre acţiunile ce compun strategia agresorului şi obiectivele pe care acesta le urmăreşte, prin prisma efectelor pe care le generează.

Configuraţiile agresiunilor de tip hibrid se ordonează în ordine descrescătoare a probabilităţii de manifestare. Rezultatul oferă, astfel, variantele cele mai probabile de combinare a acţiunilor pe care agresorul este în măsură să le desfăşoare pentru a genera efecte asupra ţintei. Ţinând cont de definiţia ameninţării de tip hibrid, este evident că aceasta, în forma ei ideală şi completă, conţine, în proporţii corespunzătoare şi într-o manieră de manifestare coerentă, toate tipurile de agresiuni pe care agresorul este în măsură să le aplice asupra ţintei. Arta constă în identificarea strategiei în care agresiunile să fie aplicate astfel încât să

[5] Valery Gherasimov, „Valoarea ştiinţei în predicţie”, revista *VPK*, nr. 8(476), februarie-martie 2013, URL: http://vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf

[6] Michel Godet, *From anticipation to action – a handbook of strategic prospective*, United Nations Educational, Scientific and Cultural Organization, Paris, 1994.

[7] URL: http://en.laprospective.fr/methods-of-prospective/softwares/62-smic-prob-expert.html

producă efectul maxim asupra ţintei. Această activitate se desfăşoară în pasul următor.

6. Configurarea agresiunii de tip hibrid (sub aspect temporal şi spaţial) şi planificarea acţiunilor care o compun constituie cea mai importantă etapă. După determinarea componentelor agresiunii de tip hibrid, configurarea acesteia presupune stabilirea proporţiilor, resurselor, locului, succesiunii şi momentelor în care agresiunile, ca manifestări ale ameninţărilor, să fie aplicate astfel încât să producă efectul maxim asupra ţintei. Pentru a determina modalitatea cea mai eficientă de acţiune se pot utiliza diferite metode de asistare a procesului de luare a deciziei, cum ar fi aplicaţia informatică *ORANetScenes*[8] în care se consideră ca date de intrare setul instrumente, obiective, strategii, astfel:

- *instrumente* – instrumentele de care dispune agresorul;
- *obiective* – vulnerabilităţile cheie ale ţintei;
- *strategii* – configuraţiile agresiunii de tip hibrid.

Aplicaţia are posibilitatea să realizeze o reprezentare grafică a triadei *instrumente-strategii-obiective* şi să determine care dintre strategii (în acest caz, configuraţii ale agresiunii de tip hibrid) sunt cele mai eficiente (utilizează mai puţine resurse pentru atingerea obiectivelor) şi mai eficace (duc la atingerea a cât mai multe obiective dintre cele propuse). Pe lângă precizarea tuturor instrumentelor, obiectivelor şi strategiilor, utilizatorul trebuie să introducă şi datele referitoare la relaţia *instrumente-strategii* (ce instrumente se utilizează pentru aplicarea fiecărei configuraţii a agresiunii de tip hibrid) şi la relaţia *strategii-obiective* (ce obiective sunt atinse de către fiecare agresiune de tip hibrid).

Fiecare configuraţie poate fi reprezentată sub forma unui graf care să evidenţieze relaţiile cauzale (în strânsă legătură cu efectele pe care le generează fiecare) ce se stabilesc între acţiunile ce le compun. Astfel, pentru o agresiune de tip hibrid analizată, nodurile grafului reprezintă acţiunile, iar legăturile dintre noduri reprezintă existenţa unei relaţii de tip cauzal dintre ele (elementele matricei pătratice $\mathbf{A_n}\times\mathbf{A_n}$ din cadrul analizei de impact încrucişat). Prin aceasta, artizanul agresiunii de tip hibrid are posibilitatea de a estima (şi controla) efectul rezultant al fiecărei configuraţii de tip hibrid în urma analizei modului în care se compun efectele fiecărei componente din cadrul acesteia.

Configuraţiile obţinute constituie esenţa planificării agresiunii de tip hibrid. Ele se pot materializa printr-o reprezentare de tip „design operaţional", adică o reprezentare în timp a succesiunii acţiunilor componente (cu resursele necesare şi efectele rezultante ale acestora) şi a atingerii obiectivelor urmărite de către agresor. De asemenea, agresorul poate realiza o selecţie a configuraţiei convenabile utilizând un criteriu oarecare, care poate fi cel al probabilităţii, cel al timpului la dispoziţie pentru pregătirea şi executarea acţiunilor etc. Ulterior, el va dezvolta acest produs într-un plan, realizând conexiunea în dimensiunea temporală şi cea spaţială între resurse şi obiective prin acţiuni (agresiuni) şi efecte.

7. Etapa a şaptea constă în ***interpretarea rezultatelor analizei ameninţării***. Trebuie menţionat faptul că metoda elaborată nu oferă un rezultat cuantificat în ceea ce priveşte efectul rezultant al unei agresiuni hibride. Efectul compus al unui set de agresiuni care se manifestă în mod simultan asupra unei ţinte este extrem de imprevizibil, iar aplicarea unor metode matematice care să determine valoarea interferenţelor dintre ele ar putea duce la rezultate înşelătoare. Totuşi, după stabilirea configuraţiilor agresiunii de tip hibrid, prin analiza structurală a acestora, se poate determina o hartă a efectelor, care să fie comparată cu „imaginea" ce prezintă efectele necesare exploatării cu succes a vulnerabilităţilor ţintei şi care a fost realizată în etapele iniţiale. Astfel, luând în considerare instrumentele la dispoziţia agresorului şi acţiunile pe care acesta le poate desfăşura pentru a exploata vulnerabilităţile ţintei, prin adaptarea metodei de analiză structurală MICMAC, se pot determina componentele principale ale agresiunii de tip hibrid (înlocuind variabilele

[8] URL: http://ora-netscenes-st-iw-32.updatestar.com/

operaţionale cu acţiuni), precum şi modul în care acestea facilitează (influenţează) sau sunt favorizate (dependente) de celelalte componente. De asemenea, rezultatele conduc la concluzii ce pot fi utilizate în identificarea celor mai probabile componente ale agresiunii de tip hibrid, precum şi în determinarea modului de desfăşurarea în timp a acestora (succesiv/simultan, periodic/ permanent). În ceea ce priveşte stabilitatea/ instabilitatea agresiunii hibride (considerată ca sistem) metoda MICMAC oferă posibilitatea determinării vulnerabilităţilor acesteia din care derivă modalităţi de contracarare, informaţii extrem de utile în stabilirea acţiunilor ţintei.

Concluzii

Ameninţarea de tip hibrid se manifestă în mediul operaţional într-o configuraţie de o complexitate deosebită, mereu diferită, adaptată vulnerabilităţilor actorului ţintă şi într-o manieră care, de cele mai multe ori, produce un efect de dezechilibru ce uzează capabilităţile lui în toate domeniile, diminuându-i puterea de a riposta. Contracararea ameninţării de tip hibrid devine, astfel, una dintre cele mai complexe probleme privind asigurarea securităţii actorilor de pe mapamond la început de secol XXI. De aceea, conflictul în care este prezentă agresiunea de tip hibrid nu mai este o problemă de apărare naţională, ci devine una de securitate naţională.

Măsurile şi acţiunile care compun contracararea ameninţării de tip hibrid trebuie să înceapă înainte ca aceasta să se materializeze în agresiune, trebuie să fie gândite şi desfăşurate într-o abordare proactivă. În caz contrar, actorul ţintă va întâmpina dificultăţi majore în configurarea răspunsului, dificultăţi care vor escalada exponenţial, pe măsură cu puterea sa se diminuează. Augmentarea capabilităţilor necesare combaterii ameninţării de tip hibrid se poate face prin previzionarea situaţiilor de criză, prin pregătirea corespunzătoare a forţei şi prin desfăşurarea de acţiuni eficiente şi eficace care să compună răspunsul adecvat. Aceste secvenţe trebuie să fie conectate între ele printr-un proces de planificare eficient, care trebuie desfăşurat în mod conjugat la toate nivelurile părţilor implicate în conflict. Un instrument util este metoda scenariilor, care pune la dispoziţie un cadru flexibil şi controlat, un „laborator" ce permite utilizarea coerentă unei game variate de algoritmi şi proceduri pentru identificarea răspunsului optim, precum şi pentru antrenarea şi verificarea forţelor.

În funcţie de modul de aplicare, metoda scenariilor poate declanşa procesul de planificare sau îl poate sprijini pe parcursul întregii perioade de desfăşurare. Scopul utilizării ei este eliminarea incertitudinii sau, cel puţin, stabilirea unor limite controlabile în jurul incertitudinilor generate de mediul operaţional de tip hibrid şi concentrarea efortului planificatorilor înspre soluţionarea problemei. În plus, întrebuinţarea metodei scenariilor în cadrul procesului de planificare facilitează utilizarea de procedee avansate de cercetare operaţională care, corelate cu utilizarea modelării şi simulării, contribuie la crearea unor planuri viabile şi valide necesare generării unei capacităţi de ripostă flexibilă şi eficientă.

BIBLIOGRAFIE:

1. ARCADE, Jaques; GODET, Michel; MEUNIER, Francis; ROUBELAT, Fabrice, *Structural analysis with the MICMAC method & Actors' strategy with MACTOR method*, AC/ UNU Millennium Project - Laboratory for Investigation in Prospective and Strategy (LIPS), Paris, 2003.

2. DUŢU, Petre, *Ameninţări asimetrice sau ameninţări hibride: delimitări conceptuale pentru fundamentarea securităţii şi apărării naţionale*, Editura Universităţii Naţionale de Apărare „Carol I", Bucureşti, 2013.

3. GHERASIMOV, Valery, „Valoarea ştiinţei în predicţie (traducere din limba rusă)", Revista *VPK*, nr. 8(476), februarie-martie 2013, URL: http://vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf.

4. GLENN, Russel, „Thoughts on <Hybrid> Conflict", *Small Wars Jurnal*, Editura Small Wars Journal LLC, 2 martie 2009, URL:http://smallwarsjournal.com/jrnl/art/thoughts-on-hybrid-conflict

5. GODET, Michel, *From anticipation to action – a handbook of strategic prospective*, UNESCO, Paris, 1994.

6. GORDON, Theodore Jay, *Cross-Impact Method*, AC/UNU Millennium Project, Paris, 1994.

7. HOFFMAN, Frank, Hybrid *Threats: Reconceptualizing the Evolving Character of Modern Conflict*, Institute for National Strategic Studies, National Defense University, Strategic Forum No. 240, aprilie, 2009.

8. HOFFMAN, Frank, MATTIS James, „Future Warfare: The Rise of Hybrid Wars", *Proceedings Magazine*, vol. 132/II/1,233, US Naval Institute, noiembrie 2005.

9. HOFFMAN, Frank, „Hybrid vs. compound war", *Armed Forces Journal*, 1 octombrie 2009, URL: http://armedforcesjournal.com/hybrid-vs-compound-war/

10. OMRAN, Ahmed; KHORISH, Motaz; SALEH, Mohamed, *Structural Analysis with Knowledge-based MICMAC Approach*, International Journal of Computer Applications, Volumul 86, Nr. 5, 2014, URL:https://pdfs.semanticscholar.org/9515/b310ab104da6f2c2116fb6a42e19ade6adb5.pdf

ABORDĂRI CONCEPTUALE ALE SPAȚIULUI CIBERNETIC ÎN NATO, UE ȘI ROMÂNIA

Dr. Mirela ATANASIU*

Odată cu extinderea utilizării tehnologiilor informațiilor și comunicațiilor în toate domeniile vieții sociale, inclusiv în cel militar, organizațiile și statele de pe teritoriul european au remarcat necesitatea sporirii conștientizării asupra riscurilor spațiului cibernetic și acționării în direcția prevenirii și combaterii lor. De exemplu, pe de o parte, NATO – organizație politico-militară – a inclus spațiul cibernetic printre domeniile operaționale, considerându-l spațiu de luptă, pe lângă cele trei deja tradiționale − aerian, terestru și naval. Uniunea Europeană – organizație politico-economică −, pe de altă parte, se preocupă mai mult de securitatea informatică și criminalitatea informatică, conștientizând faptul că asigurarea sistemelor de rețea este esențială pentru menținerea economiei online și asigurarea prosperității statelor și cetățenilor săi. Și la nivelul României au fost lansate o serie de inițiative ce vizează spațiul digital, atât de sensibil.

În materialul de față, fără pretenția de a avea o abordare exhaustivă, dorim să prezentăm cadrul conceptual actual al securității cibernetice în plan euroatlantic, european și național și, foarte pe scurt, unele inițiative convergente domeniului.

Cuvinte-cheie: *securitate cibernetică, vulnerabilitate, dimensiune a războiului, NATO, UE, România.*

Introducere

În ultimele decade, tehnologia informației s-a dezvoltat foarte mult. De la o unealtă pur administrativă care ajuta la optimizarea proceselor birocratice, a devenit un instrument strategic utilizat în industrie, transporturi, medicină, biologie, administrație, armată etc., aceasta în contextul în care, înainte de 11 septembrie 2001, riscurile și provocările legate de securitatea cibernetică erau discutate numai în grupuri restrânse de experți tehnici. Dar, din acea zi, a devenit evident că lumea cibernetică atrage provocări serioase de securitate pentru societățile din ce în ce mai interdependente.

În prezent, companii, state și organizații internaționale sunt implicate în permanenta activitate de contracarare a riscurilor, amenințărilor și vulnerabilităților la adresa securității lumii digitale. Spre exemplu, actorii statali sau nonstatali pot exploata complexitatea și conectivitatea sporită a rețelelor de sisteme de infrastructură critică cibernetizate (sisteme bancare, sisteme de transport public, sisteme de energie electrică etc.) puse în funcțiune și controlate cu ajutorul tehnologiei informației și comunicațiilor, având potențialul de a provoca daune materiale și pierderi financiare majore și, astfel, de a pune în pericol securitatea, economia, siguranța publică a unor state și bunăstarea cetățenilor lor.

Dr. Mirela ATANASIU este cercetător ştiinţific gr. II la Centrul de Studii Strategice de Apărare şi Securitate din cadrul Universităţii Naţionale de Apărare „Carol I”, Bucureşti. E-mail: atanasiu.mirela@unap.ro

1. Spațiul cibernetic – a patra dimensiune euroatlantică a războiului

De-a lungul istoriei, conflictele militare au variat în sferă și complexitate, strategie și tactică, dar un element constant al tuturor acestor ciocniri militare rămâne necesitatea mobilizării de către un actor a infrastructurii și capacității sale cu scopul de a ataca un altul în vederea obținerii victoriei. Același lucru este valabil pentru instrumentul cibernetic care se raportează direct la capacitatea unui adversar de a-și utiliza capabilitățile informaționale proprii pentru a exploata vulnerabilitățile oponenților. De asemenea, similar conflictelor armate, și în războiul cibernetic, fiecare adversar folosește tactici, tehnici și proceduri diferite pentru obținerea supremației în luptă, iar logistica, comunicarea și cunoașterea câmpului de luptă devin elemente esențiale pentru atingerea scopului final – înfrângerea adversarului.

Amenințările cibernetice sunt parte a războiului hibrid[1]. Acestea pot fi, deopotrivă, înșelătoare și toxice pentru civili, state sau grupări de state. Amenințările au potențialul de a avaria, distruge sau anula funcționarea unor infrastructurii critice, vitale pentru bunul mers al unor state, pentru că folosindu-se de mijloacele informatice avansate la dispoziție, grupurile de interese statale sau nonstatale pot controla rețelele energetice și sistemele de electricitate, conglomeratele industriale informatizate, sistemele de plată electronică, datele private ale civililor și proprietatea intelectuală a unor instituții sau organizații naționale sau internaționale.

NATO este printre organizațiile internaționale care a conștientizat amploarea impactului și consecințelor pe care le poate avea acest tip de amenințare. În acest sens, într-un document public, se afirmă că „atacurile cibernetice devin tot mai frecvente, sofisticate și dăunătoare. Alianța se confruntă cu un mediu în care amenințările de securitate cibernetică se dezvoltă exponențial. Actorii statali și nonstatali pot utiliza atacuri cibernetice în contextul operațiunilor militare. […] NATO trebuie să fie pregătită să-și apere rețelele și operațiunile împotriva amenințărilor cibernetice și al atacurilor tot mai sofisticate cu care se confruntă”[2]. Dar, conștientizarea nu a rămas doar la nivel de discurs, organizația reacționând proactiv pentru a ține pasul cu dinamica accelerată a amenințărilor provenite din rețelele virtuale.

Una dintre multele acțiuni în acest sens este cea de la momentul Summitului NATO din Țara Galilor, din septembrie 2014, când, în contextul îmbunătățirii capabilităților organizației de combatere a noilor sau vechilor amenințări la adresa securității euroatlantice, statele membre s-au pus de acord în ce privește realizarea „unui pachet de planificare a apărării care să includă o serie de priorități, în arealele consolidării programelor de formare și a exercițiilor; comenzii și controlului, inclusiv pentru operațiuni aeriene solicitante; intelligenceului, supravegherii și recunoașterii (ISR); capacității NATO de apărare împotriva rachetelor balistice, […]; apărării cibernetice”[3]. Așadar, printre domeniile cheie ale NATO, a fost inclus și cel cibernetic.

Cu această ocazie, NATO a adoptat o politică și un plan de acțiune consolidate în domeniul apărării cibernetice, care au fost aprobate de statele membre. De asemenea, prin politica de securitate cibernetică a Alianței se stabilește că apărarea cibernetică reprezintă una dintre principalele sarcini de apărare colectivă, o prioritate esențială identificată la nivel organizațional fiind protejarea sistemelor de comunicații și informatice deținute și operate de NATO.

Ulterior, la Summitul NATO de la Varșovia, din 2016, șefii de stat și de guvern ai NATO au recunoscut spațiul cibernetic drept „un domeniu operațional, pe lângă cele tradiționale – aerian,

[1] ***, *Cyber defence*, North Atlantic Treaty Organization, 17 februarie 2017, URL: http://www.nato.int/cps/on/natohq/ topics_78170.htm, accesat la data de 02.05.2017.

[2] ***, *NATO Cyber Defence*, North Atlantic Treaty Organization, URL: http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf, accesat la data de 06.05.2017.

[3] ***, *Wales Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales*, September 5, 2014, URL: http://www.nato.int/cps/ic/natohq/official_texts_ 112964.htm, accesat la data de 05.05.2017.

terestru și naval”[4]. Motivația acestei recunoașteri a constituit-o faptul că „tratarea spațiului cibernetic ca domeniu operațional va permite Alianței să își protejeze mai bine misiunile și operațiunile, concentrându-se mai mult pe formarea și planificarea militară”[5], concomitent cu oferirea „unui cadru mai propice pentru gestionarea resurselor, abilităților, capacităților și coordonarea deciziilor”[6]. Instrumentul principal de implementare a acestui cadru este reprezentat de *Politica consolidată a NATO privind apărarea cibernetică* coroborată inițiativei de întărire a capacităților NATO de apărare cibernetică cu tehnologii de ultimă oră.

Până la declararea spațiului cibernetic ca nouă dimensiune de ducere a războiului, securitatea informatică a Alianței a parcurs un traseu împărțit de unii specialiști[7] în trei etape.

• Prima s-a derulat când securitatea informatică era tratată mai mult ca o provocare tehnică ce trebuia confruntată atât la nivel colectiv, prin intermediul NATO, cât și individual, de fiecare dintre statele sale membre. Astfel, inițiativa era văzută ca activitate de securizare a infrastructurii de tehnologia comunicațiilor și informaticii (TIC) utilizată de NATO cu contribuția colectivă a statelor sale membre, iar cea de securizare a rețelelor naționale de TIC era realizată la nivelul național al statelor membre.

• A doua etapă a fost inițiată în momentul în care problematica cibernetică a devenit o chestiune politică importantă (procesul a fost inițiat în timpul reuniunii la nivel înalt de la Riga și, ulterior, a fost intensificat, în urma atacurilor cibernetice împotriva Estoniei din anul 2007).

• Cea de a treia etapă, încă în derulare, a început în 2014, în cadrul Summit-ului NATO din Țara Galilor, când securitatea informatică a fost declarată ca fiind o provocare strategică de interes comun la adresa membrilor Alianței, necesitând o reacție coordonată din partea întregii comunități euroatlantice de securitate și a tuturor statelor membre NATO, punând în discuție chiar „invocarea articolului 5 din Tratatul de la Washington, dacă atacurile cibernetice ajung la un prag care amenință prosperitatea, securitatea și stabilitatea națională a statelor membre și euro-atlantică”[8], pe ansamblu. De altfel, în etapa actuală, prioritățile NATO în materie de securitate cibernetică sunt două, respectiv, protejarea propriilor rețele informatice specifice Alianței și asistarea statelor membre în dezvoltarea propriilor capabilități cibernetice. Activitățile circumscrise acestor priorități sunt abordate de această dată întrunit, și nu separat.

La momentul actual, diversitatea modurilor în care pot fi utilizate capabilitățile cibernetice reprezintă una dintre cele mai mari provocări pentru NATO în a-și înțelege propriul rol în ceea ce privește apărarea cibernetică. Două tipuri principale de atacuri cibernetice sunt deosebit de relevante în privința rolului NATO în domeniul cibernetic[9]. În primul rând, spionajul cibernetic – de la nivel strategic sau operațional – poate compromite confidențialitatea sistemelor informatice și de comunicații, având capacitatea de a dezvălui adversarilor secrete și informații sensibile. În al doilea rând, sabotajul cibernetic poate provoca daune materiale importante, mai ales când sunt vizate infrastructuri critice, precum rețelele de energie sau de transport sau baze de date pe care un adversar le poate ataca prin blocarea accesului, mutarea sau modificarea acestora cu potențialul de a crea daune majore țintei vizate și chiar de a submina procesul asistat (sau nu) de luare a deciziilor de comandă și control.

[4] ***, *NATO Cyber Defence*, Fact Sheet, North Atlantic Treaty Organization, July 2016, URL: http://www.nato.int/ nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf, accesat la data de 08.05.2017.

[5] *Ibidem*.

[6] *Ibidem*.

[7] Joanna ŚWIĄTKOWSKA, „NATO's Road to Cybersecurity – towards bold decisions and decisive actions”, în *NATO Road to Cybersecurity*, The Kosciuszko Institute, Kraków, Poland, 2016, p. 5, URL: http://www.ik.org.pl/wp-content/uploads/nato_road_to_cybersecurity_the_kosciuszko_institute_2016.pdf, accesat la data de 11.05.2017.

[8] ***, *Wales Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales*, Press Release, North Atlantic Treaty Organization, 5 septembrie 2014, punctul 72, URL: http://www.nato.int/cps/en/natohq/official_texts_112964.htm#cyber, accesat la data de 11.05.2017.

[9] ***, „NATO: changing gear on cyber defence”, în *NATO Review Magazine*, URL: http://www.nato.int/docu/Review/2016/Also-in-2016/cyber-defense-nato-security-role/EN/index.htm, accesat la data de 10.05.2017.

2. Amenințarea cibernetică și securitatea internă a Uniunii Europene

Securitatea cibernetică este o preocupare majoră și a Uniunii Europene. În acest sens, în cadrul Uniunii, se acționează pe mai multe direcții pentru a asigura protejarea acestei dimensiuni de securitate, de la îmbunătățirea capabilităților statelor membre în plan intern, până la punerea în aplicare a cooperării internaționale privind securitatea informatică și criminalitatea informatică. Aceasta este o activitate primordială în contextul în care se conștientizează faptul că securizarea sistemelor de rețea și informatice din spațiul UE este esențială pentru buna desfășurare a comerțului efectuat în mediul virtual și pentru asigurarea prosperității cetățenilor și statelor.

În anul 2004 a fost înființată Agenția Uniunii Europene pentru Securitatea Rețelelor și Informațiilor (ENISA) care sprijină procesul de implementare al legislației UE relevantă în domeniu la nivelul statelor membre și acționează pentru îmbunătățirea rezilienței infrastructurilor și a rețelelor critice informatice din Europa. Astfel, ENISA a demarat o primă definire a unui set minim de capabilități pe care o Echipă de Răspuns în caz de Urgență în domeniul Informatic (CERT) responsabilă cu protejarea infrastructurii critice de informații (CIIP) din statele membre UE trebuie să îl posede, inițiativă materializată în anul 2009 prin documentul „Baseline capabilities for national/governmental CERTs (Part 1 Operational Aspects)". Un astfel de document a fost realizat și în limba română în decembrie 2010 în intenția constituirii unei astfel de echipe la nivel național.

Ca urmare a percepției europene cu privire la importanța domeniului cibernetic în contextul asigurării spațiului de securitate și prosperitate, un document important arondat acestuia este *Strategia de securitate cibernetică a Uniunii Europene*, din anul 2013, care „stabilește strategia UE de prevenire și reacție la perturbările și atacurile care afectează rețeaua De telecomunicații a Europei"[10], ca urmare a constatării că „în ultimii ani (…) lumea digitală aduce beneficii enorme, însă este în același timp vulnerabilă. Numărul incidentelor de securitate cibernetică, fie ele intenționate sau accidentale, crește într-un ritm alarmant și ar putea perturba furnizarea unor servicii esențiale a căror existență o considerăm de la sine înțeleasă, și anume, aprovizionarea cu apă sau energie electrică, asistența medicală sau serviciile de telefonie mobilă. Amenințările pot veni din surse diverse – cum ar fi atacurile criminale, teroriste, motivate politic sau comandate de adversari (n.a. actori statali și nonstatali), precum și catastrofele naturale sau greșelile neintenționate"[11].

De asemenea, în corpusul *Comunicării Comisiei Europene către Parlamentul European, Consiliul European, Comitetul Economic și Social și Comitetul Regiunilor de la Strasbourg din 28 aprilie 2015*[12] a fost stabilită *Agenda europeană de securitate pentru perioada 2015-2020*, „cu rolul de a sprijini cooperarea statelor membre în combaterea amenințărilor la adresa securității și intensificarea eforturilor comune în lupta împotriva terorismului, a crimei organizate și a criminalității informatice"[13]. Așadar, Agenda arată clar cele trei amenințări de securitate care, în ultima perioadă, se îmbină cu rezultate grave în plan internațional, ceea ce poate deveni, în timp, o problemă majoră și în plan european.

Strategia de securitate cibernetică a Uniunii Europene și *Agenda europeană pentru securitate* oferă cadrul strategic general pentru inițiativele UE privind securitatea informatică și criminalitatea informatică. *Strategia privind piața unică digitală* recunoaște importanța încrederii și a securității în spațiul digital. Un studiu arată că prin realizarea pieței unice digitale, UE ar putea

[10] ***, *Îmbunătățirea securității cibernetice în întreaga UE*, Consiliul Uniunii Europene, 2013, URL: http://www.consilium.europa.eu/ro/policies/cyber-security/, accesat la data de 14.05.2017.

[11] ***, *Strategia de securitate cibernetică a Uniunii Europene: un spațiu cibernetic deschis, sigur și securizat*, Comunicare Comună către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor join/2013/01 final.

[12] ***, *The European Agenda on Security*, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Strasbourg, 28.04.2015 COM (2015) 185 final.

[13] ***, *Commission takes steps to strengthen EU cooperation in the fight against terrorism, organized crime and cybercrime, Strasbourg*, 28 April 2015, p. 1.

să își dezvolte economia cu aproape 415 miliarde de euro pe an și să creeze sute de mii de noi locuri de muncă[14]. Dar, pentru ca europenii să agreeze implementarea unor astfel de noi tehnologii digitale și a serviciilor lor conexe la scară largă în interiorul societăților lor trebuie să primească semnale care să le crească încrederea în existența unui nivel ridicat de securitate cibernetică în plan european.

Date fiind aceste sincope legate de nivelul de securitate acceptat de comunitatea europeană pentru a spori încrederea în utilizarea tehnologiilor și comunicațiilor informatice, printre principalele obiective ale Comisiei Europene în materie de securitate cibernetică se numără[15]:

- *sporirea capacităților și a cooperării în domeniul securității cibernetice*, cu scopul de a aduce capacitățile de securitate digitală la același nivel de dezvoltare în toate statele membre ale UE și de a asigura că schimburile de informații și cooperarea sunt eficiente, inclusiv la nivel transfrontalier. În acest domeniu, directiva privind securitatea sistemelor de rețea și de informații (Directiva NIS) este principalul instrument care sprijină reziliența cibernetică a Europei;
- *constituirea din UE a unui jucător puternic în domeniul securității informatice*, prin promovarea avantajului competitiv al organizației politico-economice în domeniul securității cibernetice pentru a se asigura că cetățenii europeni, întreprinderile și administrațiile publice au acces la cea mai recentă tehnologie digitală de securitate, interoperabilă, competitivă, demnă de încredere și respectând drepturile fundamentale ale indivizilor, inclusiv dreptul la intimitate;
- *integrarea securității informatice în politicile UE*, în special în politicile referitoare la noile tehnologii și sectoarele emergente, cum ar fi mașinile conectate, rețelele inteligente și internetul obiectelor (*Internet of Things - IoT*).

După realizarea Strategiei de securitate cibernetică a Uniunii Europene în anul 2013, a fost creată Platforma de securitate a informațiilor (NISP)[16], realizată în parteneriat public-privat, cu ajutorul căreia părțile interesate pot să identifice bunele practici de securitate cibernetică pentru securitatea informațiilor și a tehnologiilor de informații și de comunicare (TIC), creând condiții favorabile de piață pentru dezvoltarea și adoptarea unor soluții tehnologice sigure.

Ulterior, în iulie 2016, a fost adoptată *Directiva privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune*, în care se prevede că „ar trebui să se instituie un grup de cooperare, compus din reprezentanți ai statelor membre, Comisiei Europene și Agenției Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor pentru a sprijini și a facilita cooperarea strategică dintre statele membre în ceea ce privește securitatea rețelelor și a sistemelor informatice”[17]. De asemenea, până în septembrie 2017, Comisia Europeană urmărește revizuirea Strategiei de securitate cibernetică și mandatul ENISA pentru a le alinia la noul cadru european privind securitatea informatică.

3. Cadrul național de securitate cibernetică

România nu poate ignora dezvoltările în materie cibernetică și nici nu o face, fapt reliefat în strategiile și politicile sale arondate domeniului. Astfel că, în *Strategia Națională de Apărare a Țării pentru perioada 2015-2019 – O Românie puternică în Europa și în lume* – printre tendințele pe termen mediu și lung cu potențial de a afecta mediul global de securitate sunt identificate și „atacurile cibernetice”[18]. În același cadru strategic, se conștientizează faptul că

[14] ***, *Cybersecurity,* Digital Single Market, URL: https://ec.europa.eu/digital-single-market/en/cybersecurity, accesat la data de 10.05.2017.
[15] *Ibidem*.
[16] ***, *NIS Platform. Network and Information Security Risk Management Organisational Structures and Requirements,* Final Draft, 22.05.2015, p. 3, URL: https://resilience.enisa.europa.eu/nis-platform/shared-documents/ 5th-plenary-meeting/chapter-1-nis-risk-management-organisational-structures-and-requirements-v2/view, accesat la data de 21.02.2017.
[17] ***, *Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune,* publicată în Jurnalul Oficial al Uniunii Europene
[18] ***, *Strategia Națională de Apărare a Țării pentru perioada 2015-2019* – O Românie puternică în Europa și în lume, Administrația Prezidențială, București, 2015, p. 11.

„ameninţările cibernetice lansate de entităţi ostile, statale sau nonstatale, asupra infrastructurilor informaţionale de interes strategic ale instituţiilor publice şi companiilor, atacurile cibernetice desfăşurate de grupări de criminalitate cibernetică sau atacurile cibernetice extremiste lansate de grupuri de hackeri afectează direct securitatea naţională”[19]. Ca urmare, printre obiectivele naționale de securitate internă, se pune accent, printre altele, pe „consolidarea securității și protecției infrastructurilor critice – energetice, de transport şi cibernetice –, precum şi a securităţii alimentare şi a mediului”[20]. Ulterior, în cadrul aceluiași document se stabilește ca direcție de acțiune „asigurarea mecanismelor de prevenire şi contracarare a atacurilor cibernetice la adresa infrastructurilor informaţionale de interes strategic, asociată cu promovarea intereselor naţionale în domeniul securităţii cibernetice”[21]. Aşadar, aceste elemente prezentate în strategie, scot în evidență conștientizarea la nivel politic a prezenței amenințărilor de natură cibernetică, dorința de a acționa în sensul combaterii acestei amenințări și inițierea implementării unui cadru normativ și desemnarea unor organisme de prevenție aferente care să asigure echilibrul de securitate în spațiul virtual românesc, cel puțin în ce privește protejarea infrastructurilor critice și a informațiilor strategice vehiculate în acest mediu fluid.

Prin Hotărârea Consiliului Suprem de Apărare a Țării nr. 16/2013 şi Hotărârea de Guvern nr. 271/ 2013 a fost aprobată *Strategia de securitate cibernetică a României*, care stabilește cadrul conceptual, organizatoric și de acțiune necesar asigurării securității cibernetice și care vizează protecția infrastructurilor cibernetice în concordanță cu noile concepte și politici din domeniul apărării cibernetice elaborate și adaptate la nivelul NATO și al Uniunii Europene.

În cadrul acestui document, pe de o parte, securitatea cibernetică este definită ca fiind „starea de normalitate rezultată în urma aplicării unui ansamblu de măsuri proactive și reactive prin care se asigură confidențialitatea, integritatea, disponibilitatea, autenticitatea și nonrepudierea informațiilor în format electronic, a resurselor și serviciilor publice sau private, din spațiul cibernetic”[22]. Apărarea cibernetică, pe de altă parte, este definită ca fiind un cumul de „acțiuni desfășurate în spațiul cibernetic în scopul protejării, monitorizării, analizării, detectării, contracarării agresiunilor şi asigurării răspunsului oportun împotriva amenințărilor asupra infrastructurilor cibernetice specifice apărării naționale”[23]. Se realizează astfel o separare a tipurilor de activități specifice pentru securitatea cibernetică și apărarea cibernetică, respectiv între măsurile generice luate pentru asigurarea cadrului de securitate a infrastructurilor de tehnologia comunicațiilor și informațiilor în general și acțiunile specifice desfășurate în domeniul cibernetic pentru asigurarea apărării naționale.

Conform Hotărârii Guvernului nr. 271/2013, „Ministerul pentru Societatea Informaţională (Ministerul Comunicațiilor și Societății Informaționale, n.a.) şi celelalte autorităţi publice responsabile au obligaţia de a duce la îndeplinire obiectivele şi direcţiile de acţiune prevăzute în Strategia de securitate cibernetică a României şi în Planul de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică, cu respectarea prevederilor legale în vigoare”[24]. De asemenea, în același document sunt explicate și o serie de alte sintagme arondate domeniului securității și apărării cibernetice, precum „amenințare cibernetică”, „atac cibernetic”, „incident cibernetic”, „terorism cibernetic”, „spionaj cibernetic”, „criminalitate informatică”, „vulnerabilitate în spațiul cibernetic”, „risc de securitate în spațiul cibernetic”, ajungându-se la identificarea a patru categorii majore de provocări cibernetice pentru securitatea națională: primele două asociate în

[19] *Ibidem,* pp. 14-15.
[20] *Ibidem* p. 9.
[21] *Ibidem*, p. 20.

[22] ***, *Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică* publicată în Monitorul Oficial nr. 296, Partea I din 23.05.2013, p. 7, URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf, accesat la 26.05.2017.
[23] *Ibidem.*
[24] *Ibidem.*

mare parte cu statele, respectiv războiul cibernetic și spionajul economic, următoarele două, în mare parte, asociate cu actorii nonstatali – criminalitatea cibernetică și terorismul cibernetic.

În România, conform Strategiei de securitate cibernetică, acoperirea domeniului este asigurată prin intermediul *Sistemului național de securitate Cibernetică* (SNSC), ce reprezintă „cadrul general de colaborare care reunește instituții și autorități publice cu responsabilități și capabilități în domeniu, în vederea coordonării acțiunilor la nivel

Așadar, CERT-RO este entitatea organizațională specializată care dispune de capacitatea necesară pentru prevenirea, analiza, identificarea și reacția la incidentele cibernetice. În cadrul CERT-RO, se analizează disfuncționalitățile procedurale și tehnice la nivelul infrastructurilor cibernetice naționale[27]. De asemenea, CERT-RO reprezintă un punct național de contact cu structurile de tip similar din străinătate.

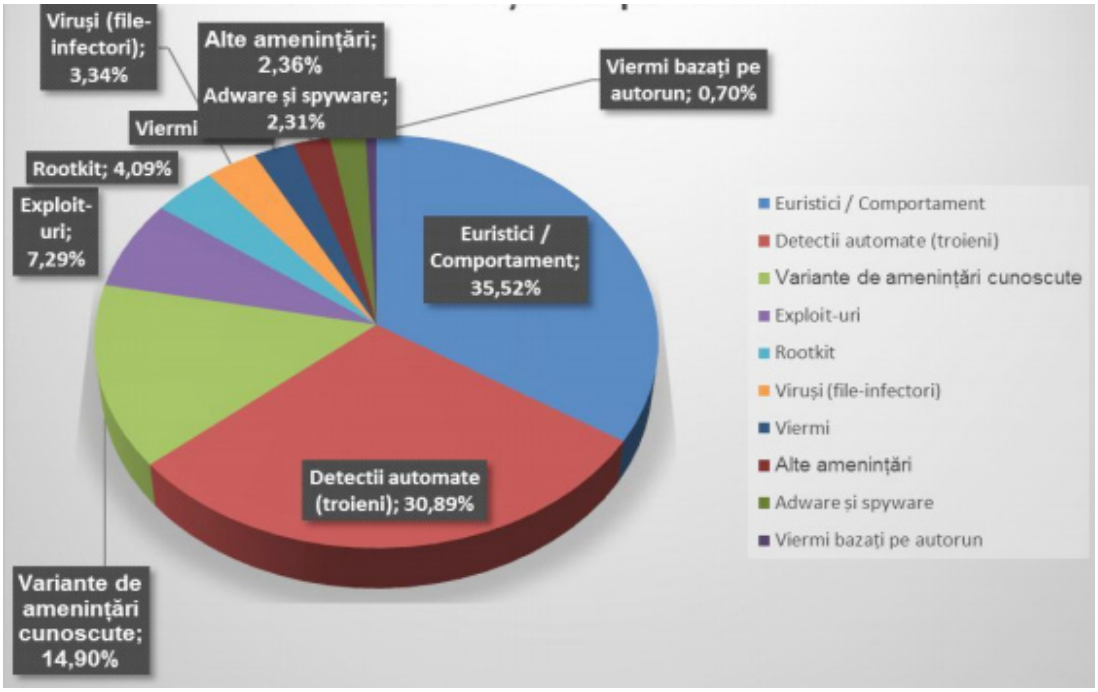

Figura nr. 1: Distribuția amenințărilor informatice în primele 6 luni ale anului 2013.

SURSA: *Raport. Amenințări cibernetice la adresa utilizatorilor din România*, Bitdefender, 2016, p. 6, URL: https://www.cert.ro/vezi/document/amenintari-cibernetice-la-adresa-utilizatorilor-romani, accesat la data de 25.05.2017.

național pentru asigurarea spațiului cibernetic românesc, inclusiv prin cooperarea cu mediul academic și cel de afaceri, asociațiile profesionale și organizațiile neguvernamentale”[25].

În cadrul Sistemului, Centrul Național de Răspuns la Incidente de Securitate Cibernetică (CERT-RO), constituit după modelul promovat de UE, asigură „elaborarea şi diseminarea politicilor publice de prevenire şi contracarare a incidentelor din cadrul infrastructurilor cibernetice, potrivit ariei de competenţă”[26].

Această entitate organizațională emite o serie de documente care sprijină creșterea conștientizării cu privire la riscurile de securitate cibernetică și diseminarea culturii de securitate în domeniul cibernetic în plan național. Printre aceste documente se află îndrumare, ghiduri de bună practică, proceduri de gestionare a datelor,

[25] *Ibidem,* p. 12.

[26] ****, CCS146 – Securitatea Cibernetică – Securitatea Rețelelor și Sistemelor Informatice: „Scenarii și soluții privind soluționarea incidentelor de securitate – gestionarea incidentelor la nivel național cu potențial impact pe scară largă”,* proiect elaborat în cadrul Planului Sectorial *MSI,* 2015, p. 26, URL: https://www.comunicatii.gov.ro/wp-content/ uploads/2016/02/CyberSec_nov2015.pdf, accesat la data de 23.05.2017.

[27] Centrul Național de Răspuns la Incidente de Securitate Cibernetică, URL: http://internship.gov.ro/informatii/centrul-national-de-raspuns-la-incidente-de-securitate-cibernetica/#null, accesat la data de 24.05.2017.

idei și sfaturi de protecție cibernetică, rapoarte, documentele cu privire la tipurile și formele de amenințări cibernetice ce apar noi. Un astfel de document este Raportul „Amenințări cibernetice la adresa utilizatorilor din România", realizat pentru prima jumătate a anului 2013 de Bitdefender, unde se arăta că „în prima jumătate a anului 2013, cele mai importante amenințări cu malware în România au fost troienii, urmați de variante ale unor amenințări cunoscute deja, dar refolosite de atacatori prin tehnici specifice"[28].

În același Raport, erau prezentate și o serie de instrumente utile în activitatea de protecție a confidențialității, o listă a centrelor de securitate cibernetică împotriva amenințărilor și o serie de resurse guvernamentale care pot sprijini indivizi, companii și organisme ale statului în prevenirea criminalității informatice.

În prezent, România nu dispune de o lege a securității cibernetice, dar, în ultimii ani, s-au făcut eforturi în această direcție. O primă inițiativă a fost în 2014, însă a fost respinsă în Senatul României, ca urmare a obiecțiilor de neconstituționalitate acceptate de Curtea Constituțională, prin Decizia nr. 17/ 21 ianuarie 2015 publicată în Monitorul Oficial nr.79 din 30.01.2015[29].

Ulterior, la finele lunii ianuarie 2016, Ministerul Comunicațiilor lansa în dezbatere publică un alt proiect de Lege privind Securitatea Cibernetică a României, îmbunătățit prin considerarea criticilor aduse prin Decizia anterioară a Curții Constituționale a României (CCR) asupra obiecției de neconstituționalitate ca urmare a încălcării prevederilor constituționale privind statul de drept și principiul legalității, precum și cele privind viața intimă, familială și privată, respectiv secretul corespondenței[30]. În februarie 2017, ministrul Comunicațiilor și Societății Informaționale declara că „Legea securității cibernetice nu este printre priorități (…) și nu va pleca mai departe către Parlament (…)"[31], justificând această poziție prin existența Directivei europene nr. 1148/2016, *NIS — Networking Information Security*, adoptată în Parlament, prin care oficialul considera că acoperă deja domeniul securității cibernetice așa cum este prezentat în proiectul de lege aferentă. Personal, consider că emiterea respectivei legi este necesară și nu se suprapune cu directiva europeană.

Concluzii

Amenințările cibernetice nu țin cont de limitele geografice naționale, europene sau internaționale, pentru că sistemele informatice sunt interconectate în rețele, depășind aceste niveluri, astfel, sistemul informatic național este interconectat cu cel european și cu cel al NATO. Aceasta face ca o vulnerabilitate minoră a unui microsistem informatic să poată crea, ca urmare a „efectului de rețea", probleme majore unei părți mai mari sau în ansamblul unui sistem, ceea ce necesită coerență la nivel internațional în stabilirea reglementărilor și măsurilor de prevenire și combatere a acestora.

În acest sens, România – stat membru al NATO și al UE – trebuie să își ralieze politica de securitate cibernetică la politicile în domeniu ale ambelor organizații. Pe de o parte, trebuie să acționeze în direcția continuei revizuiri a documentelor strategice arondate dimensiunii securității cibernetice, iar, pe de altă parte, în dezvoltarea capabilităților cibernetice naționale, astfel încât să fie compatibile și securizate conform celor aflate la nivelul organizațiilor din care face parte.

Așa cum am prezentat în materialul de față, preocupările în materie cibernetică sunt reale la toate nivelurile abordate: euroatlantic, european și

[28] ***, *Raport. Amenințări cibernetice la adresa utilizatorilor din România,* Bitdefender, 2016, p. 6, URL: https://www.cert.ro/vezi/document/amenintari-cibernetice-la-adresa-utilizatorilor-romani, accesat la data de 25.05.2017.

[29] *Proiect de lege privind securitatea cibernetică a României,* URL: https://www.senat.ro/Legis/Lista.aspx?cod=18494, accesat la data de 22.05.2017.

[30] *Cosmoiu (SRI): Noua Lege a securității cibernetice nu are un caracter intruziv,* Agerpress, 14 iunie 2016, URL: https://www.agerpres.ro/cybersecurity/2016/06/14/cosmoiu-sri-noua-lege-a-securitatii-cibernetice-nu-are-un-caracter-intruziv-11-25-15, accesat la data de 23.05.2017.

[31] *Jianu (MCSI): Legea securității cibernetice nu se află printre prioritățile mele; România trebuie să implementeze legi pe baza Directivei NIS,* Agerpress, 15 februarie 2017, URL: https://www.agerpres.ro/economie/2017/02/15/jianu-mcsi-legea-securitatii-cibernetice-nu-se-afla-printre-prioritatile-mele-romania-trebuie-sa-implementeze-legi-pe-baza-directivei-nis-11-36-50, accesat la data de 26.05.2017.

național. Totuși, există unele sincope între gradul de intensificare și diversificare a amenințărilor cibernetice și viteza de implementare la nivelul sistemelor informatice și de comunicații a unor măsuri preventive adecvate, și acest lucru este resimțit pe toate palierele amintite, nu numai la nivel național.

Considerăm că pentru asigurarea unui nivel de securitate ridicat al spațiului cibernetic pe ansamblul unor organizări de state precum EU sau NATO, principalul rol revine statelor naționale, fiind necesară o abordare de jos în sus, cel puțin în ce privește înzestrarea cu mijloace de tehnologia informației și comunicațiilor performante, mai reziliente la vulnerabilități și amenințări. Pentru aceasta, este necesar a se investi masiv în astfel de sisteme, cu atât mai mult cu cât majoritatea statelor avansate tehnologic consideră capabilitățile cibernetice ca fiind o parte legitimă și necesară a setului lor de instrumente strategice, alături de diplomație, forță economică și putere militară. Totuși, această abordare ridică îngrijorări cu privire la faptul că, în viitorul apropiat, am putea fi martorii unui război total între state, dus în spațiul cibernetic. În plus, observăm un interes ocazional în utilizarea capacităților cibernetice de către actorii nonstatali – în prezent, cu dovezi limitate în ceea ce privește utilizarea lor efectivă. De altfel, experiența actuală cu privire la utilizarea reală a capacităților cibernetice de către state sugerează că astfel de capabilități sunt încadrate în categoria instrumentelor specifice spionajului sau sabotajului, ceea ce face ca angajarea lor să treacă dincolo de simplul atac armat. Deși există o anumită logică a acestui argument, este din ce în ce mai clar că unele state consideră capabilitățile cibernetice drept parte integrantă a capacității militare operaționale și nu se tem să le folosească ca atare, chiar dacă sunt reticente să recunoască o astfel de utilizare în mod public.

Experiența României demonstrează că este necesară o îmbunătățire continuă a reglementărilor relevante în ceea ce privește securitatea cibernetică. În același timp, dinamica reglementărilor legislative privind domeniul securității cibernetice este mai lentă, nu numai la nivel național, ci și la alte niveluri superioare, comparativ cu dinamica de perpetuare și dezvoltare a amenințărilor informatice, ceea ce poate duce la sincope în acoperirea eficientă a domeniului.

BIBLIOGRAFIE:

1. ***, *CCS146 – Securitatea Cibernetică – Securitatea Rețelelor și Sistemelor Informatice: „Scenarii și soluții privind soluționarea incidentelor de securitate – gestionarea incidentelor la nivel național cu potențial impact pe scară largă”*, proiect elaborat în cadrul Planului Sectorial MSI, 2015.
2. ***, *Commission takes steps to strengthen EU cooperation in the fight against terrorism, organized crime and cybercrime,* Strasbourg, 28 April 2015.
3. ***, *Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune*, publicată în Jurnalul Oficial al Uniunii Europene
4. ***, *Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică*, publicată în Monitorul Oficial nr. 296, Partea I din 23.05.2013.
5. ***, *Îmbunătățirea securității cibernetice în întreaga UE*, Consiliul Uniunii Europene, 2013.
6. ***, *NATO Cyber Defence*, Fact Sheet, North Atlantic Treaty Organization, July 2016.
7. ***, *NIS Platform. Network and Information Security Risk Management Organisational Structures and Requirements*, Final Draft, 22.05.2015.
8. ***, *Raport. Amenințări cibernetice la adresa utilizatorilor din România*, Bitdefender, 2016.
9. ***, *Strategia de securitate cibernetică a Uniunii Europene: un spațiu cibernetic deschis, sigur și securizat*, Comunicare Comună către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul

Regiunilor 2013/01 final.

10. ***, *Strategia Națională de Apărare a Țării pentru perioada 2015-2019 – O Românie puternică în Europa și în lume*, Administrația Prezidențială, București, 2015.

11. ***, *The European Agenda on Security,* Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Strasbourg, 28.4.2015 COM (2015) 185 final.

*12. ***, Wales Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales*, 5 septembrie 2014.

*13. ***, Wales Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales,* Press Release, North Atlantic Treaty Organization, 5 septembrie 2014.

14. Site-ul agenției de știri Agerpress, www.agerpres.ro.

15. Site-ul oficial al Centrului Național de Răspuns la Incidente de Securitate Cibernetică (CERT-RO), https://cert.ro.

16. Site-ul oficial al Comisiei Europene, https://ec.europa.eu.

17. Site-ul oficial al NATO, www.nato.int

18. Site-ul oficial al Senatului României, www.senat.ro.

19. Site-ul oficial al Uniunii Europene, www.europa.eu.

20. ŚWIĄTKOWSKA, Joanna, „NATO's Road to Cybersecurity – towards bold decisions and decisive actions", în *NATO Road to Cybersecurity*, The Kosciuszko Institute, Kraków, Poland, 2016.

MODELE MATEMATICE SPECIFICE DOMENIULUI MILITAR

Dr. Florentina-Loredana DRAGOMIR*

Pentru a identifica tendinţele existente în evoluţia unor procese, a conexiunilor dintre acestea, precum şi implicaţiile viitoare asupra desfăşurării activităţii, este necesară o limitare a numărului de alternative (soluţii) ce privesc modul de desfăşurare a evenimentelor. Pornind de la alternativele (soluţiile) posibile, o putem identifica pe cea mai bună, având la bază anumite criterii, tehnici, procedee, metode. Procesul de identificare a variantei optime, în rapot cu anumite criterii, implică răspundere şi, de cele mai multe ori, asumarea unui risc. Riscul poate fi însă diminuat prin formalizarea procesului decizional cu ajutorul unor modele şi metode matematice.

***Cuvinte-cheie**: model, model matematic, fazele modelării, modelare, model militar, decizie.*

1. Delimitări conceptuale

Conceptul de „model" folosit în sfera academică are ca scop cunoaşterea în detaliu a realităţii, a procesului însuşi, necesar fundamentării şi elaborării deciziilor. Modelul devine un instrument de lucru pentru evaluarea efectelor potenţiale ale alternativelor decizionale.

Modelarea matematică reprezintă trecerea de la fenomenul în sine la relaţiile matematice care caracterizează conexiunile între componentele sale, precum şi conexiunile cu alte fenomene. Modelarea matematică este o problemă analitică şi experiment de cercetare a diferitelor procese dinamice.

Baza reală a modelării matematice este izomorfismul fenomenelor din natură, prin aceasta înţelegându-se o formă comună de descriere a lor prin relaţii de calcul adecvate. De aici, rezultă posibilitatea de a reduce studiul unuia din sistemele izomorfe la studiul altui sistem, de a modela comportarea unui sistem cu ajutorul altuia. Izomorfismul relevă unitatea, legătura şi interacţiunea, în limitele determinate, ceea ce permite ca analiza unui proces să se facă prin intermediul altuia, asemănător ca formă şi structură, dar mai uşor de studiat.

Modelul matematic este constituit din relaţiile logico-matematice (formule, ecuaţii, inegalităţi, condiţii logice, operatori etc.) care oglindesc raporturile cantitative (caracteristicile stării sistemului, ieşirile acestuia în funcţie de parametrii şi intrările sale, condiţiile iniţiale şi de timp) din desfăşurarea fenomenului analizat.

2. Principale caracteristici ale modelelor

Modelele au următoarele trăsături definitorii[1]:

- Cu cât relaţia de similitudine cuprinde mai multe caracteristici generale ale

[1] Gheorghe Ilie; Ion Stoian; Gelu, Alexandrescu, *Modelarea sistemelor şi proceselor*, Editura Universităţii Naţionale de Apărare „Carol I", Bucureşti, 2005, p. 41.

Dr. Florentina-Loredana DRAGOMIR este lector universitar la Departamentul Sisteme informaţionale militare şi informaţii pentru apărare din cadrul Facultăţii de Securitate şi Apărare, Universitatea Naţională de Apărare „Carol I" din Bucureşti. E-mail: dragomir.florentina@myunap.net

ambelor sisteme (original şi model), cu atât posibilitatea de a cunoaşte originalul prin modelul său creşte;
- Cu cât proprietăţile care formează obiectul relaţiei de similitudine sunt mai importante pentru cele două sisteme, cu atât probabilitatea obţinerii unor concluzii adevărate referitoare la original, deduse prin modelul său, este mai mare;
- dacă în model există o proprietate generală care nu apare în original, atunci concluziile deduse din acestea pot fi fără valoare pentru sistemul real;
- Cu cât conexiunea reciprocă a caracteristicilor generale de similitudine aparţinând celor două sisteme este cunoscută mai profound, cu atât concluziile referitoare la original, deduse din modelul său, sunt mai apropiate de certitudine.

Un model trebuie să îndeplinească următoarele cerinţe:
- Simplitate - este necesar să conţină numai informaţiile stricte procesului descris;
- supleţe - caracteristică cerută de necesitatea de a descrie cu ajutorul modelului orice comportare a sistemului la variaţiile datelor de intrare între anumite limite;
- adaptabilitate - caracteristică ce impune a se lua în consideraţie noile informaţii ce pot apărea la un moment dat;
- robusteţe - rezultatele obţinute prin crearea modelului trebuie să fie credibile;
- totalitate - să reflecte toate problemele principale ale sistemului;
- facilitate - dialogul dintre utilizator şi model să se efectueze uşor.

Modelul, ca instrument al sferei ştiinţifice, este folosit în variate discipline din diferite domenii de activitate. În funcţie de metoda pentru construirea modelelor, de natura elementelor care intră în compunerea lor, de particularităţile acestora există o mare diversitate de modele şi, de aici, o oarecare dificultate în clasificarea lor şi, mai ales, în identificarea unui anumit tip de model.

Astfel, după *natura elementelor componente*, modelele pot fi[2]:
- Fizice, ale căror componenete sunt de natură fizică (de exemplu machete, simulatoare etc.);
- abstracte, care cuprind elemente de natură abstractă (variabile, ecuaţii, funcţii);
- hibride, având combinaţii de elemente de natură fizică şi de natură abstractă.

După *modelul de reprezentare a sistemelor*, fenomenelor sau proceselor reale se pot distinge:
- modele analogice, care folosesc unele proprietăţi fizice, de o anumită natură, în scopul reprezentării altor proprietăţi fizice, de natură diferită;
- modele simbolice sau matematice, în care proprietăţile sistemului sunt exprimate printr-un set de parametrii, iar relaţiile care descriu funcţionalitatea acestuia, prin funcţii matematice logice sau cantitative;
- modele iconice, ce reprezintă imaginea acestuia (hărţi, miniaturi, machete etc.) la alte dimensiuni.

După *natura şi gradul de cunoaştere a relaţiilor* dintre elementele componente ale sistemului real, modelele pot fi deterministe sau probabilistice.

În cazul modelelor deterministe, relaţia de cauzalitate este o corespondenţă biunivocă, ce poate fi descrisă cu suficientă exactitate, iar valorile luate de variabilele de ieşire şi relaţiile dintre parametrii definitorii ai sistemului modelat, precum şi funcţia care defineşte interacţiunea acestora sunt determinate şi cunoscute. Ca urmare, unor parametrii de intrare stabiliţi le corespund parametrii de ieşire determinaţi, ori de câte ori se repetă procesul caracteristic sistemului.

În cazul modelelor probabilistice (stochastice), cunoaşterea sistemului prin modelul său are caracter probabilistic, generat de faptul că variabilele ce descriu sistemul, fenomenul sau procesul modelat au aspect aleatoriu cu o distribuţie cunoscută.

[2] *Ibidem*, p. 42.

3. Modelul militar

Fundamentarea ştiinţifică a deciziei necesită efectuarea unui mare volum de calcule complexe cu ajutorul metodelor (modelelor) matematice probabilistice, care ţin seama de factorii aleatori în desfăşurarea acţiunilor de luptă. Modelele constituie instrumente utile ce pot fi folosite de comandanţi şi statele majore pentru identificarea unor soluţii la problemele care apar în toate etapele de instruire şi desfăşurare a operaţiei şi luptei. Multitudinea informaţiilor culese sunt prelucrate şi diseminate întrucât succesul operaţiei şi luptei revine celui care stăpâneşte informaţia, celui care culege un volum complet de informaţii, le prelucrează oportun, ia decizii fundamentate ştiinţific, formulează şi transmite la timp misiunile subordonaţilor.

3.1. Principiile modelării matematice în sistemul militar

Cadrul metodologic de abordare a modelării matematice a operaţiei şi luptei are la bază o serie de şase principii[3] (a se vedea *Figura nr. 1*).

Principiul descompunerii

Acest principiu impune analiza unei probleme mari de optimizare prin studiul subproblemelor locale şi rezolvarea independentă a acestora fără a se ţine cont de soluţiile celorlalte activităţi (optimul global). Ca urmare a introducerii unor restricţii artificiale subproblemelor rezultate în urma descompunerii, se poate obţine o soluţie suboptimală (satisfăcătoare).

Principiul coordonabilităţii

Acest principiu are în vedere conducerea sistemelor mari compuse din subsisteme interconectate în mod ierarhizat şi descentralizat; aceasta poate fi la fel de eficientă ca şi conducerea centralizată, cu condiţia să existe un sistem complex. Chiar dacă este posibilă, nu este avantajoasă din pricina numărului mare de bucle de reacţie „feed-back" a neliniarităţii şi a altor factori, inclusiv a unităţilor de măsură diferită. Pe de altă parte, nici conducerea descentralizată (independentă) nu este o soluţie, din cauza tendinţei inerente proprii sistemelor de a nu ţine cont de cerinţele celorlalte subsisteme.

Principiul armonizării obiectivelor conflictuale existente la nivelul subsistemelor, în scopul asigurării îndeplinirii obiectivelor globale.

Acest principiu generează o serie de metode şi tehnici de abordare a modelării matematice a operaţiei şi luptei, în sensul că obiectivul unui eşalon superior devine normă de control la nivelul eşaloanelor subordonate, deciziile fiind luate la nivelul ierarhic superior, în funcţie de situaţia globală şi de restricţiile sistemului.

Principiul incompatibilităţii

Acest principiu este caracterizat prin faptul că, atunci când complexitatea sistemului este mare, posibilitatea de a analiza comportamentul sistemului cu un instrument de modelare se reduce până la un anumit nivel, astfel, precizia şi relevanţa se pot exclude reciproc.

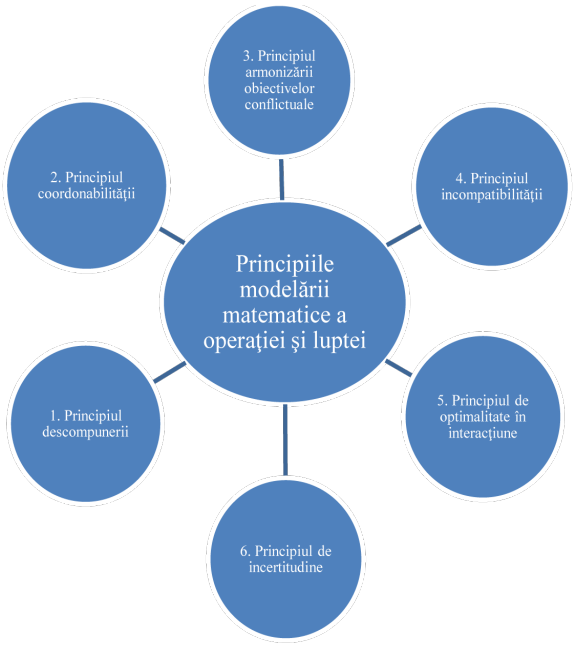

Figura nr. 1. Principiile modelării matematice în sistemul militar

Principiul de optimalitate în interacţiune

Când un sistem complex, compus din sisteme de optimalitate este optimal, atunci fiecare subsistem se consideră optimal în interacţiune, şi reciproc.

[3] Fang Deng, Lin Zhu, Jie Chen, „Application of cellular automata in military complex system", *31st Youth Academic Annual Conference of Chinese Association of Automation (YAC)*, Wuhan, 2016, pp. 281-285.

Principiul de incertitudine

Într-un sistem complex, format din mai multe subsisteme corelate, starea *i* a subsistemului „*i*" şi corelaţia lui cu celelalte subsisteme pot fi determinate simultan, până la un anumit grad de precizie.

Prin modelul matematic specific domeniului militar se înţelege, în general, o descriere formalizată (analitică sau logică) a unei acţiuni militare, astfel încât să reflecte în suficientă măsură particularităţile acestei acţiuni, să ia în considerare caracteristicile ei principale şi să permită obţinerea rezultatelor cu precizia impusă.

Modelele matematice ale acţiunilor militare trebuie să conţină cerinţe[4] care să ţină cont de principiile generale ale tacticii, strategiei şi artei militare, precum şi de compunerea de luptă a dispozitivului tactic şi operativ necesar îndeplinirii misiunii. Modelele trebuie să fie opeartive, acestea furnizând permanent date necesare comandantului. Ele se elaborează anticipat şi trebuie să reprezinte analogiile matematice şi logice ale unei acţiuni militare tipice, în care se iau în considerare elemente specifice din domeniul militar, ca spre exemplu: structura organizatorică reală a forţelor participante, compunerea organică cantitativă şi calitativă a acestora, normele operativ-tactice prevăzute în regulamente, instrucţiuni şi alte acte normative. Autorii studiului „Modelling earthquake activity features using cellular automata" recomandă realizarea unor modele care să ţină cont şi de caracteristicile geografico-militare ale direcţiilor de acţiune care să fie limitate la o anumită parte a acţiunii militare.

3.2. Fazele elaborării unui model militar

Eficienţa modelării trebuie să fie o caracteristică a fiecărei etape de proiectare a noului sistem. În acelaşi timp, se desfăşoară o serie de operaţii care au loc în cadrul analizei de sistem.

În cele ce urmează, vom prezenta o etapizare a diferitelor faze[5] ale elaborării unui model matematic, etapizare aflată în strânsă legătură cu alte faze ale analizei de sistem (a se vedea *Figura nr. 2*).

Faza 1

Faza întâi cuprinde acţiuni care au caracter pregătitor, având, în principal, menirea de a cunoaşte realităţile organismului militar.

În cadrul acestei faze, pot fi remarcate o serie de etape.

Analiza sistemului

Prin folosirea scopului şi a destinaţiei modelului, se pot preciza principalii parametrii ce pot fi luaţi în calcul ţinând cont de datele iniţiale ce vor face obiectul acţiunii militare. Parametrii incumbă principiile generale ale tacticii, strategiei şi artei militare, norme operativ-tactice prevăzute în regulamente şi instrucţiuni, precum şi alte elemente caracteristice luptei armate.

Modelul matematic se elaborează de către un colectiv multidisciplinar format din analişti de stat major sau specialişti militari în domeniul în care se simulează, matematicieni şi programatori. Rolul analistului de stat major constă în a stabili cât mai corect scopul modelului şi formularea principalelor cerinţe tactico-operative ce se impun modelului care se va elabora.

În cele mai frecvente cazuri, se pot urmări:

- simularea luptei armate în diverse condiţii;
- organizarea conducerii la diferite eşaloane, în raport cu unul sau mai mulţi factori obiectivi;
- descompunerea sistemului în subsisteme are în vedere criteriile după care se pot face acestea; ele sunt fizice sau funcţionale;
- explicitarea limitelor sistemului militar;
- determinarea variabilelor sistemului militar – acestea, asemeni tuturor sistemelor, au variabile exogene care provin din exterior, cu influenţe asupra variabilelor endogene variabile determinate de componentele din interiorul sistemului.

Ca o caracteristică pentru această fază este specificul metodologiilor informaţional-decizionale care prevăd necesitatea unei descrieri mai detaliate a proceselor decizionale axate, în principal, pe înţelegerea luării deciziilor de către

[4] G. Ioakeim Georgoudas, Georgios Sirakoulis, I. Andreadis, „Modelling earthquake activity features using cellular automata", *Math. Comput. Model*, 2007, vol. 46, pp. 124-137.

[5] Ion Stoian, *Elemente de programare liniară – aplicaţii în domeniul militar*, Editura Academiei de Înalte Studii Militare, Bucureşti, 2002, pp. 16-19.

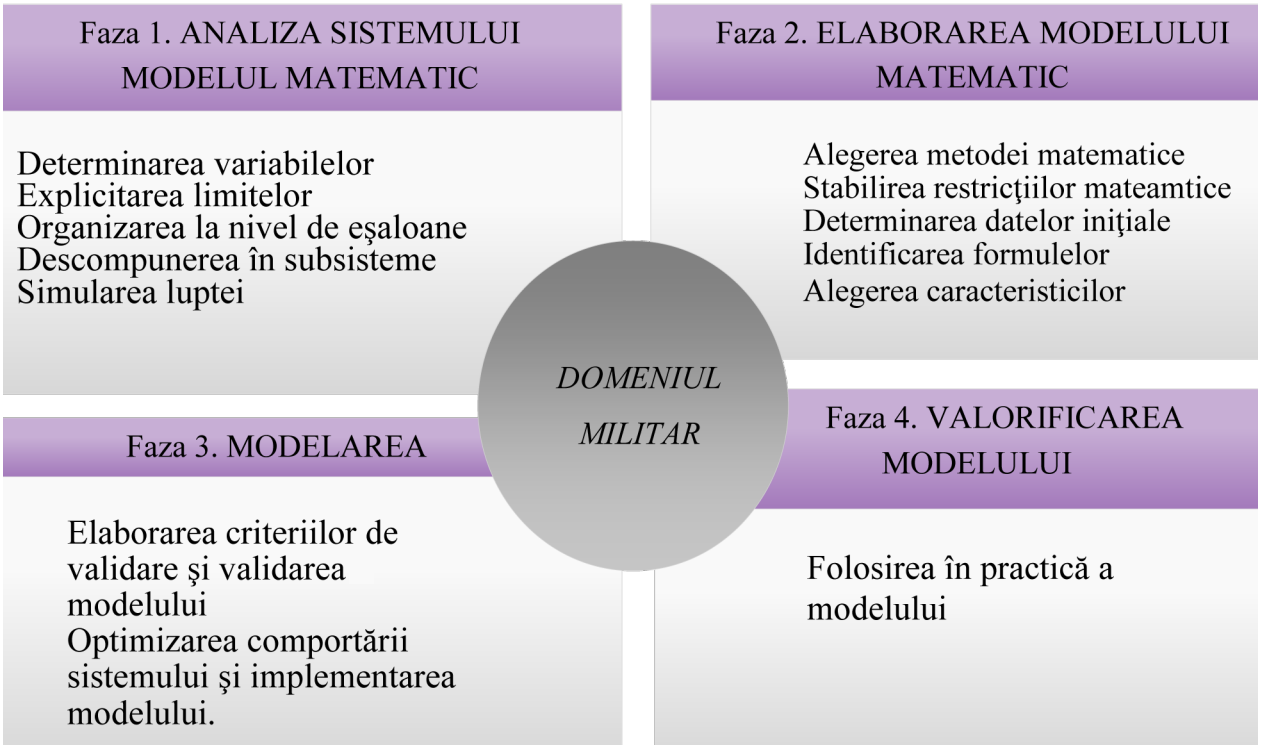

Figura nr. 2: Cele patru faze ale domeniului militar

comandanţi. Ca urmare, principalele elemente ale cunoaşterii realităţii necesare modelării sunt descrierea logicii proceselor decizionale şi obiectivele sistemului.

Faza a 2-a

Faza a doua constă în elaborarea propriu-zisă a *modelului*. Această operaţie se reflectă în folosirea unui instrument specific de modelare, ales din multitudinea foarte variată pe care ne-o pune la dispoziţie cercetarea operaţională. Modelul este inseparabil de abordarea raţională a conducerii sistemului atât în cadrul proceselor programabile, cât şi a celor neprogramabile.

Elaborarea modelelor matematice de ansamblu permite desfăşurarea următoarelor activităţi esenţiale:

- fundamentarea şi alegerea metodei matematice de rezolvare a problemelor militare prin: metode analitice; metode stochastice (probabilistice); metode mixte; alegerea principalelor dependenţe (restricţii) matematice pe baza cărora se apreciază acţiunile unităţilor luptătoare în fiecare etapă de conducere sau în fiecare etapă a confruntării în luptă;
- determinarea datelor iniţiale necesare alcătuirii modelului;
- deducerea sau identificarea formulelor matematice pentru restricţii;
- alegerea caracteristicilor de probabilitate ce definesc: eficacitatea componentelor sistemului în fiecare etapă de conducere; determinarea şi normalizarea restricţiilor şi toleranţelor; formularea matematică a problemei; elaborarea listei datelor de intrare şi ieşire din sistem; identificarea parametrilor modelului prin metoda directă sau indirectă; elaborarea algoritmilor şi programului de calcul.

Faza a 3-a

Faza a treia, cea a modelării, constă din compararea modelului obţinut cu realitatea. Ca etape pentru această fază sunt relevante: elaborarea criteriilor de validare şi validarea modelului; optimizarea comportării sistemului şi implementarea modelului. Cum se ţine cont şi de personalizarea deciziei, se verifică setul de variabile care fac referire la manager şi variabilele contextuale referitoare la influenţele sociale ale contextului organizaţional.

Datele necesare implementării trebuie să îndeplinească următoarele cerinţe: corectitudine; facilitate; frecvenţă mare a culegerii datelor şi să reflecte abordări manageriale participative.

În acestă etapă, incertitudinea şi riscul deciziei, inerente în condiţiile actuale, sunt minimizate, datorită preciziei şi completitudinii ridicate ale datelor constituite în model. Factorul care creează greutăţi în obţinerea unei precizii sporite este dat de complexitatea sistemelor militare abordate. Dacă orice informaţie culeasă ar avea o acurateţe perfectă, s-ar opera cu variabile şi modele deterministe, situaţie respinsă de condiţiile reale.

Faza a 4-a

Faza a patra – constă în valorificarea modelelor elaborate şi folosirea lor în practică. Avantajele modelării matematice sunt subliniate de micşorarea substanţială a caracterului subiectiv al deciziei, iar valorificarea modelelor concepute cu instrumentarul decizional modern creşte calitatea deciziei şi asigură o soluţionare competentă a unor situaţii de mare complexitate. Această fază a modelării se răsfrânge prin amplificarea funcţionalităţii şi eficacităţii managementului decizional. Folosirea în practică a modelului oferă o imagine a informaţiilor cu pregnante funcţii decizionale şi o eficientizare decizională multidimensională. În mod sintetic, se oglindesc rezultatele activităţii trecute, ce constituie şi baza unor direcţii normative pentru activităţile decizionale viitoare.

Pe baza celor patru faze ale modelării matematice se încearcă, practic, obţinerea unor soluţii optime sau cel puţin aproape de optim, aspect care, de fapt, se constituie ca obiectiv principal al modelării matematice.

În vederea atingerii acestui obiectiv, în principal, se pot utiliza trei metode:

- *Procedeele de optimizare exacte*, ce implică, de fapt, obţinerea celei mai bune soluţii din punct de vedere al unui criteriu formulat, lucru ce presupune, în subsidiar, că nu ar exista soluţii mai bune; în acest caz, eroarea este nulă;
- *metode euristice*, care conduc la obţinerea unei soluţii satisfăcătoare, bune sau chiar foarte bune, ceea ce nu presupune însă certitudinea optimului şi nici posibilitatea de a estima abaterea de la optim. Din acest motiv, eroarea modelelor nu poate fi ţinută sub control;
- *metode aproximative*, care presupun obţinerea unei soluţii apropiate de optim prin intermediul unor iteraţii succesive; în acest caz, eroarea poate fi controlată.

Scopul principal al oricărui model este de a descrie structura internă, elementele (fluxurile) de intrare şi de ieşire, relaţiile, tipurile de legături între elementele constitutive, restricţiile impuse funcţionării modelului. Comportarea modelului este evaluată prin starea variabilelor de ieşire, care este determinată logic de variabilele şi parametrii de intrare, precum şi de structura internă şi de restricţiile impuse funcţionării modelului. De regulă, dependenţa variabilelor de ieşire de variabilele de intrare este stabilită de structura logică a modelului adoptat.

Concluzii

Modelarea este o metodă de cercetare a unor sisteme, procese sau fenomene, prin substituirea obiectului real, având la bază identificarea unor asemănări fizice sau matematice între două sisteme, în raport cu anumite caracteristici stabilite.

Printr-o structură judicioasă, modelele matematice specifice domeniului militar permit să se furnizeze, direct şi cu suficientă exactitate, soluţii optime în ducerea şi desfăşurarea acţiunilor militare.

Modelarea şi modelul se împletesc între ele în diferite etape ale cercetării, ele nu trebuie limitate la cele existente la un moment dat, ci trebuie studiate şi modernizate cu alte metode noi care apar în alte domenii ale ştiinţei şi care pot oferi soluţii interesante pentru problemele studiate.

Este esenţial ca alegerea metodelor să ţină seama nu numai de aspectul matematic, ci, mai ales, de specificul problemelor tactice şi de artă operativă, de practică, de activitatea de luptă. Aceste cerinţe pot fi îndeplinite apelând la metodele de cercetare specifice teoriei deciziilor.

Este esenţial ca alegerea metodelor să ţină seama nu numai de aspectul matematic.

BIBLIOGRAFIE:

1. BRYDE, Daniel; BROQUETAS, Michael; VOLM, John M, „The project benefits

of Building Information Modelling (BIM)", *International Journal of Project Management*, 2013.

2. DENG, Fang; ZHU, Lin; CHEN, Jie „Application of cellular automata in military complex system", *31st Youth Academic Annual Conference of Chinese Association of Automation (YAC)*, Wuhan, 2016.

3. GEORGOUDAS, Ioakeim G.; SIRAKOULIS, Georgios. C.; ANDREADIS, I. Th; „Modelling earthquake activity features using cellular automata", *Math. Comput. Model*, vol. 46, 2007.

4. ILIE, Gheorghe; STOIAN, Ion; ALEXANDRESCU, Gelu, *Modelarea sistemelor şi proceselor*, Editura Universităţii Naţionale de Apărare „Carol I", Bucureşti, 2005.

5. STOIAN, Ion, *Elemente de programare liniară – aplicaţii în domeniul militar*, Editura Academiei de Înalte Studii Militare, Bucureşti, 2002.

Simpozionul internațional „COOPERAREA INTERINSTITUȚIONALĂ – INSTRUMENT DE REALIZARE A SECURITĂȚII LA NIVEL NAȚIONAL ȘI INTERNAȚIONAL”

25 mai 2017

Centrul de Studii Strategice de Apărare și Securitate a organizat, în data de 25 mai 2017, Simpozionul internațional cu tema „Cooperarea interinstituțională – instrument de realizare a securității la nivel național și internațional”. Evenimentul s-a desfășurat în sala Senatului din Universitatea Națională de Apărare „Carol I” și a fost onorat de prezența unor specialiști din Ministerul Apărării Naționale, Ministerul Afacerilor Interne și Ministerul Afacerilor Externe, contribuind astfel la consolidarea unei cooperări interinstituționale solide si coerente.

Pe parcursul activității, a fost reliefată necesitatea dezvoltării si consolidării cooperării interinstituționale în domeniul securității și apărării, ca răspuns la riscurile și amenințările la adresa securitatății naționale și internaționale.

Fotografie de grup cu participanții la Simpozion

În cadrul evenimentului, moderat de dl. colonel lector univ. dr. Florian Cîrciumaru, au fost prezentate trei lucrări, după cum urmează:

- „Cooperarea în cadrul SNMSU - o perspectivă a Centrului Operativ pentru Situații Speciale de Urgență, Ministerul Afacerilor Externe”, susținută de către domnul general de brigadă (r) dr. Liviu-Mihai DĂNILĂ, Șeful Centrului Operativ pentru Situații Speciale de Urgență din cadrul Ministerul Afacerilor Externe.

- „Cooperarea internaţională în domeniul controlului armamentelor şi CSBM. Tendinţe recente la nivelul OSCE”, prezentată de către domnul colonel Ovidiu FIZEŞAN, din partea Centrului Naţional Militar de Comandă (Nucleu).

- „Creşterea rezilienţei instituţionale în faţa ameninţărilor la adresa securităţii naţionale”, elaborată de către domnul comisar-şef de poliţie Ştefan SĂVULESCU şi doamna comisar-şef de poliţie Mihaela ŢONE, din cadrul Ministerului Afacerilor Interne.

Foto: Aspect de la Simpozionul ştiinţific

Considerăm că evenimentul şi-a atins obiectivele propuse, şi anume: de a facilita înţelegerea aprofundată a unor aspecte arondate problematicii cooperării interinstituţionale la nivel naţional şi internaţional; de a contribui la constituirea unui cadru de îndrumare şi schimb de opinii între specialişti; de a promova cultura strategică şi de securitate şi de a disemina rezultatele expertizei profesionale şi cercetării ştiinţifice a practicienilor şi teoreticienilor în domeniul securităţii şi apărării.

Foto: Aspect de la Simpozionul ştiinţific

Andra PÎNZARIU*

Andra PÎNZARIU, Compartimentul Manifestări Ştiinţifice, CSSAS.
E-mail: pinzariu.andra@unap.ro

ACTIVITĂȚI ALE CENTRULUI DE STUDII STRATEGICE DE APĂRARE ȘI SECURITATE

(aprilie-iunie)

APRILIE - IUNIE 2017

În cele ce urmează, vom prezenta activitățile organizate de Centrul de Studii Strategice de Apărare și Securitate (CSSAS) în perioada analizată, precum și publicațiile apărute.

În data de 25 mai 2017, CSSAS a organizat, în sala Senatului din Universitatea Națională de Apărare „Carol I", Simpozionul internațional cu tema *„Cooperarea interinstituțională - instrument de realizare a securității la nivel național și internațional"*. Activitatea a fost onorată de prezența unor specialiști din Ministerul Apărării Naționale, Ministerul Afacerilor Interne și Ministerul Afacerilor Externe, contribuind astfel la consolidarea unei cooperării interinstituționale solidă si coerentă.

În suplimentul revistei *Impact strategic*, *Colocviu strate*gic nr. 4/2017, a fost publicat un articol intitulat *Implicaţiile de securitate ale malware-ului W32.Stuxnet*, elaborat de domnul Robert Dragoș, care a efectuat un stagiu de voluntariat la CSSAS în perioada aprilie-iunie.

Cei interesați să publice în *Colocviu strategic* pot trimite propuneri la adresa de e-mail: catalina.todor@unap.ro și cssas@unap.ro.

Prelegerile publice lunare desfășurate la Cercul Militar Național în această perioadă au abordat următoarele teme: în luna aprilie, CS III dr. Cristina Bogzeanu a vorbit despre *Securitate și apărare în UE în contextul Brexit. Concepte centrale și evoluții recente*; în luna mai, CS II dr. Cristian Băhnăreanu a ținut o prelegere despre *Cheltuielile de apărare în ecuaţia securităţii inter(naţionale)*, iar în luna iunie, CS III dr. Marius Potîrniche a abordat *Terminologia războiului – clarificare, confuzii, utilitate*.

În primul trimestru al anului universitar 2017-2018, CSSAS organizează două ateliere de lucru tematice și Conferința științifică internațională *STRATEGII XXI.*

Astfel, în data de 19 octombrie, la sediul UNAp se va desfășura Atelierul de lucru cu tema *Ştiinţe militare - ştiinţe ale securităţii - clarificări conceptuale*, iar în data de 14 noiembrie va avea loc la Cercul Militar Național un Atelier de lucru cu tema *Satellite as an enabler for C4ISR*, organizat în parteneriat cu compania SES TECHCOM S.A.

Conferința științifică internațională anuală *STRATEGII XXI*, cu tema „*Complexitatea şi dinamismul mediului de securitate*", se va desfășura în perioada 07-08 decembrie. Mai multe detalii despre conferință gasiți la www.strategii21.ro, selectând linkul CSSAS, iar detalii despre toate activitățile științifice organizate de CSSAS, pe site-ul web: http://cssas.unap.ro/en/events.htm.

Raluca STAN*

**** Raluca STAN, Compartimentul Manifestări Științifice, CSSAS. E-mail: stan.raluca@unap.ro***

GHID PENTRU AUTORI

Le mulţumim celor interesaţi să publice în revista ştiinţifică bilingvă *Impact strategic* şi le supunem atenţiei, totodată, aspectele pe care trebuie să le aibă în vedere la redactarea articolelor.

CRITERIILE DE SELECŢIE a articolelor sunt următoarele:

- **circumscrierea în aria tematică a revistei**: actualitatea politico-militară; tendinţe şi perspective în domeniile securitate, apărare, geopolitică şi geostrategie, relaţii internaţionale, societatea informaţională;
- **originalitate** – caracterul de noutate; argumentare proprie; să nu fi fost publicat anterior;
- **valoarea conţinutului ştiinţific** – caracterul ştiinţific este conferit de un stil obiectiv, neutru, argumentarea afirmaţiilor şi precizarea tuturor resurselor întrebuinţate;
- **o bibliografie relevantă,** care să cuprindă lucrări de prestigiu şi surse recente, redactată conform modelului prezentat în Ghid;
- **redactarea în limba română şi în limba engleză să corespundă standardelor academice**;
- **adecvarea la normele editoriale adoptate de revistă**.

DIMENSIUNEA ARTICOLULUI ŞI NORME DE EDITARE: dimensiunea articolului poate varia între minim 6 – maxim 12 pagini (inclusiv notele de subsol, bibliografia şi imaginile). Setări pagină: margini 2 cm, format A 4. Articolul se va scrie cu **font Times New Roman, dimensiune corp 12, spaţiere la un rând, cu diacritice**. Salvarea se va face ca document Word 2003 (.doc). Titlul fişierului în limba română trebuie să conţină numele autorului şi nu se scrie cu diacritice.

STRUCTURA ARTICOLULUI

- Titlul articolului (centrat, scris cu majuscule, bold, font 24)
- O succintă prezentare de autor, care să cuprindă următoarele elemente (după caz): grad militar, titlu didactic /cercetare, titlu ştiinţific, prenume, nume, funcţia deţinută la principala afiliere instituţională, în cazul doctoranzilor – domeniul cercetării, universitatea – oraşul, ţara de reşedinţă, e-mail.
- Un rezumat relevant, de circa 150 de cuvinte (caractere italice)
- 6 - 8 cuvinte-cheie (caractere italice)
- Introducere/Consideraţii preliminare
- Două-patru capitole, eventual subcapitole
- Concluzii
- Tabelele/graficele/imaginile se trimit şi separat, în format .jpeg/png./.tiff.

În cazul tabelelor, deasupra se scrie „**Tabelul nr. X,** titlu", iar în cazul imaginilor, hărţilor etc., dedesubt se scrie **Figura nr. X**: titlu". În ambele cazuri se menţionează sursa (dacă este cazul) în notă de subsol.

NOTE DE SUBSOL: toate sursele bibliografice citate se indică în limba în care au fost consultate; (prenume, nume autor) (la notele de subsol se indică şi nr. paginii/paginilor).

Exemplu de carte: Joshua S. Goldstein, Jon C. Pevenhouse, *Relaţii internaţionale*, Iaşi, Editura Polirom, 2007, pp. 37-45.

Exemplu de articol: Gheorghe Calopăreanu, „Securitate prin educaţie şi instruire în UE", în *Impact Strategic* nr. 2/2013, Bucureşti, Editura Universităţii Naţionale de Apărare „Carol I", p. 15.

Sursele electronice se citează cu link-ul întreg, menţionând titlul cărţii/articolului (între ghilimele) şi numele publicaţiei (se indică şi data la care a fost accesată).

Exemplu: John N. Nielsen, „Strategic Shock in North Africa", în *Grand strategy: the View from Oregon*, disponibil la http://geopolicraticus.wordpress.com/2011/03/03/strategic-shock-in-north-africa/, accesat la data de 10.03.2015.

BIBLIOGRAFIE: se vor menţiona toate lucrările studiate. Sursele se ordonează alfabetic, după numele autorului (NUME, prenume autor), şi se numerotează.

Exemplu de carte: GOLDSTEIN, Joshua S.; PEVENHOUSE, Jon C., *Relaţii internaţionale*, Iaşi, Editura Polirom, 2007.

Exemplu de articol: CALOPĂREANU, Gheorghe, „Securitate prin educaţie şi instruire în UE" în *Impact Strategic* nr. 2 /2013, Bucureşti, Editura Universităţii Naţionale de Apărare „Carol I".

Sursele electronice se citează cu link-ul întreg, menţionând titlul cărţii/articolului (între ghilimele) şi numele publicaţiei.

Exemplu: NIELSEN, John N., „Strategic Shock in North Africa", în *Grand strategy: the View from Oregon*, disponibil la http://geopolicraticus.wordpress.com/2011/03/03/strategic-shock-in-north-africa/, accesat la 10.03.2015.

EVALUAREA ŞTIINŢIFICĂ a articolelor se realizează conform procesului *double blind peer review*, de către cadre didactice universitare şi cercetători ştiinţifici specialişti în domeniul în care se circumscrie articolul. Identitatea autorilor nu este cunoscută de evaluatori, iar numele evaluatorilor nu este dezvăluit autorilor. Concluziile raportului de evaluare sunt aduse la cunoştinţa autorilor, ele reprezentând argumentul pentru acceptarea/respingerea articolelor. În urma evaluării, există trei posibilităţi: *a) acceptarea articolului spre publicare ca atare sau cu modificări minore; b) acceptarea articolului spre publicare cu modificări/completări de substanţă; c) respingerea articolului.* Aducem la cunoştinţa autorilor că, anterior evaluării, articolele sunt supuse unui proces de *analiză antiplagiat* (www.sistemantiplagiat.ro).

TERMENE DE PREDARE: articolele vor fi trimise în format electronic la adresa de e-mail a redacţiei, impactstrategic@unap.ro, până la: 15 decembrie (nr. 1); 15 martie (nr. 2); 15 iunie (nr. 3) şi 15 septembrie (nr. 4).

NOTA BENE: Redacţia îşi rezervă dreptul de a face sau de a solicita autorilor modificări ce se impun pe text.

Versiunea în limba engleză a articolului se predă redacţiei în termenul agreat şi va corespunde formei finale a materialului în limba română. Traducerea în limba engleză (British English sau American English, respectând principiul consecvenţei) trebuie să fie completă şi corectă, corespunzătoare standardelor academice, întrucât ediţia în limba engleză este indexată în prestigioase baze de date internaţionale şi difuzată comunităţii ştiinţifice internaţionale. Citatele din lucrări/documente oficiale (legi, tratate etc.) şi din declaraţiile existente în limba engleză ale unor personalităţi trebuie preluate ca atare din original. Ghilimelele se notează astfel: în limba română „…", iar în limba engleză"…".

Materialele nu vor conţine informaţii clasificate. Personalul militar şi civil angajat al MApN va trimite materialele destinate publicării însoţite de avizul structurii de securitate al unităţii în care este încadrat autorul/sunt încadraţi autorii.

Responsabilitatea privind conţinutul articolelor revine în totalitate autorilor, în conformitate cu *Legea nr. 206 din 27 mai 2004 privind buna conduită în cercetarea ştiinţifică, dezvoltarea tehnologică şi inovare*.

Articolele publicate sunt supuse legii copyright. Toate drepturile sunt rezervate Universităţii Naţionale de Apărare „Carol I", indiferent dacă se are în vedere întregul material sau numai o parte a acestuia, în special drepturile privind traducerea, retipărirea, reutilizarea ilustraţiilor, citatele, difuzarea prin mass-media, reproducerea pe microfilme sau orice alt mod şi stocarea în baze de date. Sunt autorizate orice reproduceri, fără perceperea taxelor aferente, dacă este precizată sursa.

Nerespectarea acestor instrucţiuni va atrage respingerea articolului. Trimiterea articolului către redacţie presupune acordul autorului în privinţa celor expuse.

Pentru mai multe detalii despre publicaţie, puteţi accesa site-ul nostru, http://impactstrategic.unap.ro/index.html, sau puteţi contacta redacţia la adresa de e-mail: impactstrategic@unap.ro.

Dr. Daniela RĂPAN

EDITURA UNIVERSITĂŢII NAŢIONALE DE APĂRARE „CAROL I”

Director: Colonel lector univ. dr. Alexandru STOICA

Corector: Carmen IRIMIA
Tehnoredactor: Elena PLEȘANU

Lucrarea conţine 76 pagini.

Tipografia Universităţii Naţionale de Apărare „Carol I”
Şoseaua Panduri, nr. 68-72, sector 5, Bucureşti
e-mail editura@unap.ro
Tel: 021/319.40.80/215

1635/2017

C. 119/2017