

Anul XIV nr. 3/2022

# INFOSFERA

Revistă de studii de securitate și informații pentru apărare

Publicație indexată în bazele de date internaționale EBSCO și CEEOL

Revistă cu prestigiu științific recunoscut de Consiliul Național de Atestare  
a Titlurilor, Diplomelor și Certificatelor Universitare (CNATDCU)

Direcția Generală de Informații a Apărării



# CUPRINS

## PERSPECTIVE GEOPOLITICE ȘI GEOSTRATEGICE

<b>Reziliența contemporană: competitivitatea națiunilor, capabilitatea statelor și securitatea societală .....</b>	<b>5</b>
<i>Iulian CHIFU</i>	
<b>NATO post-Madrid și Conceptul Strategic 2022: între continuitate și schimbare .....</b>	<b>15</b>
<i>Vasile CREȚU</i>	
<b>Federația Rusă: Vectori ai politicii externe pe direcțiile strategice Vest și Sud-Vest .....</b>	<b>29</b>
<i>Gheorghe MATEI</i>	

## RĂZBOAIELE SECOLULUI XXI

<b>Impactul conflictului ruso-ucrainean asupra Regiunii Balcanilor de Vest .....</b>	<b>36</b>
<i>Florin-Vasile GROZA</i>	
<b>Efectele războiului din Ucraina asupra Regiunii Arctice .....</b>	<b>41</b>
<i>Iohana-Georgia BURCEA</i>	
<b>Militarizarea Peninsulei Crimeea – capabilități de război electronic ale Federației Ruse .....</b>	<b>49</b>
<i>Simion-Călin GHEORGHIȚĂ</i>	
<b>Virtualizarea mediului operațional .....</b>	<b>59</b>
<i>Marian ȘTEFAN</i>	

**AMENINȚĂRI HIBRIDE**

<b>Provocări hibride de natură biologică .....</b>	<b>69</b>
<i>Paul MIHAI</i>	
<b>Tehnologiile cuantice și impactul lor asupra securității informatice .....</b>	<b>80</b>
<i>Sergiu Beniamin MĂLUȚAN</i>	
<b>Metacogniții și nivel ierarhic .....</b>	<b>85</b>
<i>Cristian ILIE</i>	

**ISTORIA SERVICIILOR DE INFORMAȚII**

<b>Serviciile de informații românești și franceze – parteneri în combaterea pericolului comunist în anii '20 ai secolului trecut .....</b>	<b>92</b>
<i>Ioan-Codruț LUCINESCU</i>	

**RECENZII ȘI SEMNALĂRI**

<b>Food for thought .....</b>	<b>104</b>
<i>Vasile CREȚU</i>	

# REZILIENȚA CONTEMPORANĂ: COMPETITIVITATEA NAȚIUNILOR, CAPABILITATEA STATELOR ȘI SECURITATEA SOCIETALĂ

*Iulian CHIFU\**

## **Abstract**

*Contemporary international turbulence has created a wide range of uncertainty and launched the concept of societal resilience, as a possibility to deal with the turbulences and tectonic changes of the international relations and global security. But how do we measure and how do we enforce the resilience stay remains an important issue for researchers. Therefore we tried to enter into the depth of the resilience studies and approaches and use what we have in hand as studies in sociology, history of conflicts and economic turbulences, geopolitical capability of the states and specially societal security. The paper emphasizes also the main points of a RAND Corporation study on the societal foundation of nations competitiveness as a mean to identify criteria and indicators for societal resilience.*

**Keywords:** *resilience; competitiveness; geopolitical capability; societal security.*

## REZILIENȚA ÎN DOCUMENTELE NATO ȘI UE

În numărul anterior al acestei publicații am avut ocazia să facem o trecere în revistă a conceptelor de „reziliență”, așa cum apar ele în documentele NATO și UE<sup>1</sup>. Pe fond, reziliența este capacitatea de a gestiona perioadele de criză și de a reveni cât mai repede la *business as usual* după momentul de criză. Reziliența presupune reacția potrivită la amenințări și riscuri și compensarea sau limitarea vulnerabilităților<sup>2</sup>. Desigur, atunci când vorbim despre reziliență, avem în vedere multiplele aspecte la nivelul statelor, ca actori ai relațiilor internaționale și ai securității globale, dar și ceea ce numim **reziliență națională**, adică reziliența instituțiilor naționale, a patrimoniului,

bunurilor și proprietăților materiale și imateriale ale națiunii, dar și cea a societății, deopotrivă, pe care o regăsim, în fapt, în *reziliența societală*. În același timp, reziliența se poate extinde și la nivelul companiilor, orașelor, regiunilor, familiilor sau al comunităților umane de orice tip.

Reziliența societală este componenta care se referă la societate. La nivelul securității societale, componentele de apărare sunt coeziunea societală și identitatea<sup>3</sup>. Însă, acestora li se adaugă și alte elemente care țin de *leadership*, încrederea în autoritate, calitatea democrației, a statului de drept, patriotismul, dorința de a-și apăra statul, modul de viață și proprietatea, precum și accesul egal la oportunități.

După cum am mai precizat, NATO își are propriile definiții și referințe la reziliență și

\* Iulian Chifu este președintele Centrului de prevenire a Conflictelor și Early Warning, București, profesor la Universitatea Națională de Apărare Carol I din București și profesor asociat la SNSPA. În prezent, îndeplinește funcția de consilier de stat în cadrul Cancelariei Prim-ministrului Guvernului României.

reziliență societală. Conținutul rezilienței în cazul NATO vizează protecția infrastructurii critice pe teritoriul aliat și asigurarea că armatele statelor membre pot să opereze oricând și pe întreg teritoriul Alianței. Securitatea societală este definită în documentele NATO drept limitarea vulnerabilităților societății în fața atacurilor și coerciției<sup>4</sup> și salvagardarea societăților, populațiilor și valorilor comune<sup>5</sup>. Există șapte cerințe de bază cuantificate ca atare la nivelul Alianței:

- 1) asigurarea continuității guvernării și a serviciilor guvernamentale critice;
- 2) aprovizionarea constantă și sustenabilă, la prețuri acceptabile, cu energie;
- 3) abilitatea de a răspunde eficient mișcărilor necontrolate (ex.: migrații) ale oamenilor;
- 4) resurse constante de apă și alimente pentru populație;
- 5) abilitatea de a face față crizelor cu număr mare de victime;
- 6) sisteme de comunicații funcționale și reziliente;
- 7) asigurarea sistemelor de transport reziliente<sup>6</sup>.

Și Uniunea Europeană și-a pregătit documentul strategic, *Busola Strategică*, care are prevederi referitoare la modul în care privesc cei 30 de membri reziliența<sup>7</sup>. Și temele explicite se referă la schimbările climatice, dezastre, urgențe civile. Pe dimensiunea rezilienței economice, temele sunt lanțurile de aprovizionare, rutele de transport, libertatea navigației, securitatea furnizorilor. La capitolul reziliență societală, atenția se concentrează pe întărirea accesului la informație credibilă, media independentă și contracararea manipulării și interferenței străine la nivel informațional. Regăsim, de asemenea, în același document, reziliența societăților și a proceselor democratice, a instituțiilor politice, ca și reziliența în fața tehnologiilor disruptive și a utilizării acestora de către competitorii strategici ai UE sau terțe state.

## O AGENDĂ PENTRU REZILIENȚA SOCIETALĂ

Preocupările asociate conceptului de reziliență se regăsesc în nenumărate studii

și cercetări aprofundate, pe dimensiuni distincte. Astfel, studiile referitoare la modul în care putem compara națiunile<sup>8</sup>, care sunt trăsăturile caracteristice naționale, elementele definitorii, care sunt valorile și axiologia națională dominantă și cum influențează acestea supraviețuirea și prosperitatea națiunilor (azi am spune reziliența națională) sunt extrem de actuale<sup>9</sup>. De asemenea, avem o întreagă literatură privind dezvoltarea democratică și aspirația pentru libertățile individuale, care definesc lumea în care suntem, bazată pe reguli și modul nostru de viață, dar și relația dintre guvernare, democrație și reziliență<sup>10</sup> – decantată inclusiv de la actuala competiție declarată între democrații și autocrații și pretenția unor regimuri autocratice de a genera modele de guvernare mai reziliente prin represiune, centralizarea puterii și eficiența deciziei.

Pe de altă parte, așa cum am văzut și în definițiile rezilienței și în explicitarea lor la nivelul UE și al NATO, reziliența se relaționează direct cu *dimensiunea de securitate*, cu precădere cu amenințările, riscurile și vulnerabilitățile identificate, pe diferite generații succesive, la zi. Practic, reziliența presupune construirea instrumentarului de reacție la diferitele categorii de elemente ce afectează securitatea, în scopul creșterii capacității de a absorbi șocurile și, eventual, de a preveni ca evenimentele ce afectează securitatea să se producă pe aceeași direcție; pasul ulterior a vizat interesul pentru studiile prospective<sup>11</sup> și adaptarea societăților, națiunilor, instituțiilor și a statelor la amenințările și evoluțiile viitoare, de „dincolo de orizont”. Prin urmare, reziliența este privită, într-o mare măsură, ca produs al planificării securitare. Aici este importantă și preocuparea pentru avertizarea timpurie - *early warning*.

Desigur, atunci când vorbim despre reziliența societală trebuie să o legăm direct de securitatea societală, așa cum am văzut mai sus, care are la bază drept principale componente *identitatea* și *coeziunea*<sup>12</sup>, pe lângă multe alte elemente și componente ce determină osatura internă a națiunilor. Securitatea societală se raportează și la elementele caracteristice națiunii titulare –

așa cum le-am văzut definite mai sus, la nivelul rezilienței națiunilor, dar și la propensiunea și caracteristicile societății la un moment dat. Nu trebuie să uităm, din nou, că securitatea societală are și ea o raportare directă la modul și nivelul respectării drepturilor omului.

În ceea ce privește raportul dintre reziliența societală și reziliența democratică, ca și în cazul școlii de gândire care privește în mod absolut drepturile individuale și respinge organizarea puternică instituțională și statală, și aici putem găsi elemente care pot contrapune reziliența societală – supraviețuirea societății la crize și la șocuri – cu cea democratică. Desigur lucrurile pot migra în zonele mai filosofice, axiologice și etice, ale unei posibile competiții sau ale unui conflict de valori<sup>13</sup>. Din nou, trebuie menționat faptul că o majoritate relevantă a autorilor evidențiază nu numai compatibilitatea dintre reziliența democratică și cea societală, ci și similitudinea dintre cele două, tot astfel cum securitatea societală într-un stat democratic presupune și apărarea drepturilor individuale ale membrilor națiunii (cetățenii statului în cauză). Astfel, democrația presupune drepturi individuale, dar asumate liber și în cunoștință de cauză, de unde introducerea în elementele de taxonomie a rezilienței, la nivelul Uniunii Europene, a componentelor de *război informațional* (care urmăresc alterarea opțiunilor, cunoașterii și a acțiunilor liber determinate ale cetățenilor, lucru fundamental în alegerile lor libere, și îmbrățișarea unor alternative privitoare la modul de viață și politicile publice în statele democratice)<sup>14</sup>.

Nu în ultimul rând, democrația a avut formule de alunecare de factură populistă, cu precădere în ultimii 20 de ani, cu relevanță majoră la nivelul spectrului politic. Francis Fukuyama<sup>15</sup> a reușit să studieze fenomenul și a relevat preocuparea oricărui individ pentru identitatea personală și de grup, caracterul omului de ființă socială și nevoia de recunoaștere, demnitate, respect, incluziune, coexistență și coeziune. Toate acestea – *identitatea* cu precădere – sunt parte a securității societale și trebuie deopotrivă studiate, aprofundate și dezvoltate în paralel cu evoluția societății și a conceptelor definitorii ale securității societale, care se regăsesc, firește, în reziliență.

## PROIECTE DE ABORDARE A REZILIENȚEI SOCIALE

Dintre categoriile de proiecte care interesează studiile de reziliență, le putem reține, pentru moment, pe cele referitoare la ***criterii și indicatori pentru compararea națiunilor***, pe cele referitoare la securitate și securitate societală, respectiv proiecte de întărire a rezilienței referitoare la diferitele amenințări, riscuri și vulnerabilități, ***studiile prospective*** și amenințările de viitor la adresa securității, în general, și a securității societale, în special atunci când ne concentrăm pe reziliența societală. Dar, profund legate de reziliență s-au dovedit, așa cum am ales noi să definim reziliența în acest articol, reacțiile la crize și conflicte, decizia în condiții de criză, ***gestionarea crizelor și reziliența în criză*** a societăților, națiunilor și a statelor<sup>16</sup>.

Dacă decizia în contextul unei crize am evaluat-o prin abordare cognitiv-instituțională, reziliența o legăm indisolubil de criză și turbulență, de capacitatea de adaptare și, mai mult, de ceea ce Zygmunt Bauman numea „*societatea lichidă*”<sup>17</sup> și ceea ce am identificat drept capacitate de adaptare și separare a continuității guvernării (continuitate a serviciilor și nu neapărat continuitate a instituțiilor).<sup>18</sup> Din această perspectivă, rămâne deschisă discuția vizând primatul continuității instituționale, ca efect al rezilienței și forței de a recupera valorile societale și bunurile după criză, sau al continuității serviciilor, ca atribut și obiectiv al instituțiilor. Disputa este cea a *diferenței dintre anti-fragil și robust*<sup>19</sup>: rezistența în fața amenințării și a vicisitudinilor justifică efortul menținerii formulei fizice de reprezentare a statului și instituției sau trebuie asigurată doar supraviețuirea și continuitatea serviciilor asigurate populației?

La această agendă mai putem adăuga câteva elemente care țin de ***competitivitatea națiunilor***, un unghi de abordare altfel îngust al realităților<sup>20</sup>, dar care se dovedește interesant și plin de resurse. Astfel, un studiu recent, elaborat de RAND Corporation, aduce în discuție perspectiva competiției ca și tendință a epocii care vine în



relațiile internaționale, studiile de securitate și studiile strategice, așa cum subliniază, de altfel, și *U.S. National Security Strategy*<sup>21</sup>. Autorii utilizează baza teoretică și contextul istoric care ar explica modul în care s-ar dezvolta această competiție în prezent și în viitor.

Caracteristicile relevante desprinse din studiul competitivității și care vizează reziliența se referă la democrație și libertăți *versus* autoritarism și regimuri închise, dictatoriale, la naționalism și profunzimea identității naționale, la gradul de revizionism, toate măsurate la nivelul actorilor internaționali, și se apleacă asupra următorilor *posibili indicatori*: creșterea accesului la distribuția de bunuri; creșterea relevanței relative a statului; creșterea relevanței și influenței globale a propriului sistem de valori și ideologie; schimbarea regulilor ce guvernează sistemul; creșterea relevanței proprii în instituirea noului set de reguli.

Apoi, baza teoretică a competiției între actorii internaționali introduce diferențierea între aceste abordări moderate și cele militarist-revizioniste: violarea repetată a normelor internaționale în beneficiul unilateral al actorului în cauză; ambiții teritoriale și dorința creării unei sfere de influență prin agresiune militară, care să fie dominată militar; considerarea ordinii internaționale ca fiind profund ilegală, creată împotriva lor, de unde nevoia nu a reformei, ci a schimbării depline și profunde, chiar a distrugerii acestei ordini cu totul. Studiul abordează și gradul de compatibilitate, acceptabilitate și spațiul de dialog între diferiții actori, nivelul de competiție și revizionism, precum și elementele de incompatibilitate majoră ce induc cadrul pentru declanșarea conflictului deschis<sup>22</sup>.

Un alt proiect relevant este *indicele capabilității geopolitice a statelor*. Este cea mai inedită evaluare a capabilității statelor, pe baza unei metodologii ce conține indicatori și proporții prestabilite pe baza experienței în timp a acestui tip de studii<sup>23</sup>. Este un proiect al Henry Jackson Society și vine după un studiu elaborat în 2017 și rafinat în 2019. Se concentrează pe G20, în care UE e înlocuită cu Nigeria (mai degrabă din nevoia echilibrului geografic).

Actualul Indice compozit al capabilității geopolitice<sup>24</sup> conține patru indici, combinați prin medie ponderată, după cum urmează: *baza națională* – reprezentând 20% – alcătuită din bunăstarea națională (10%), structura populației (6%), răspândirea națională (3%) și auto-suficiența resurselor și capabilităților (1%); *structura națională* – reprezentând 40% – cu trei piloni a câte cinci indicatori: economic (15%), activitate și realizări tehnologice (10%) și prestigiu cultural (15%); *instrumentele naționale* – reprezentând 30% – cu doi piloni a câte cinci indicatori: diplomația (15%) și instrumentul militar (15%); *determinarea națională* (în fapt măsurarea *voinței*) – reprezentând 10% și format din patru indicatori: eficacitatea guvernării (7%), determinarea economică, determinarea strategică și determinarea altruistă (câte 1%).

Desigur, cel mai interesant și recent este studiul RAND Corporation despre *fundamentele societale ale competitivității națiunilor*<sup>25</sup>, asupra căruia ne vom concentra atenția mai detaliat în rândurile următoare. Agenda proiectelor în materie nu ar fi completă dacă nu am adăuga *tehnologia, inovația și antreprenoriatul* în dezvoltarea rezilienței societale, elemente care se dovedesc a fi o eternă verigă lipsă. Securitatea tehnologică<sup>26</sup> este un important punct de plecare în abordarea rezilienței legată de securitate și a componentelor rezilienței în fața tehnologiilor disruptive, care includ deopotrivă evoluțiile din *social media* și legăturile cu războiul informațional. Desigur, alte elemente pot fi adăugate agendei noastre prezente.

## FUNDAMENTELE SOCIETALE ALE COMPETITIVITĂȚII NAȚIUNILOR

RAND Corporation a produs și lansat recent, după o cercetare de peste 15 luni, un studiu despre elementele care fac o societate competitivă. Citisem despre modul în care putem compara națiunile, despre națiuni de succes și națiuni care se sting, despre legătura dintre prezervarea națiunii și statalitate, dar ceea ce ne propune acum acest studiu este mult mai important și mai relevant pentru lumea contemporană, pentru



traversarea crizelor suprapuse și pentru reziliența societală în întregul său. Este vorba despre *formulele de organizare și coeziunea societăților capabile să manifeste reziliență* și acest pas este de primă importanță.

Desigur, forța unei națiuni și capacitatea de a marca lumea de astăzi sunt judecate în câteva clișee clasice, extrem de utile: capacitatea militară și tehnologică de vârf, capacitatea economică de a susține puterea militară, capacitatea de proiecție a puterii la distanță și anduranța consumării și desfășurării unui război lung. Însă, actualul studiu este cu adevărat remarcabil pentru că este făcut la adâncimea istoriei, luând în discuție toate exemplele trecutului, de la războaiele peloponesiace și Tucidide<sup>27</sup> până în actualitate, deci un spațiu al lecțiilor învățate mult mai vast, care oferă idei noi. În plus, studiul în sine subliniază și limitele metodologiei utilizate, ceea ce este cu adevărat remarcabil prin conținutul simultan al tezei și, dacă nu al antitezei, măcar al estimării corecte a erorilor de model ale produsului oferit.

Astfel, dacă proiectul Indicilor Capabilității Geopolitice introducea, în mod natural, statul ca instrument, proiectul experților de la RAND se concentrează cel mai mult pe *societăți*, pe comunitățile organizate și caracteristicile lor, evitând și caracterizarea diferitelor sisteme de guvernare, dar și capcana caracteristicilor etnice colective sau naționale ale popoarelor, concentrându-se pe trăsături și comportamente societale avantajoase sau, din contra, nefaste pentru sustenabilitatea discutată.

În competiția strategică a contemporaneității, componentele caracteristice statului sunt extrem de importante, indiferent dacă vorbim despre capabilități militare, întărirea apărării, investițiile în tehnologii cheie și capacități economice, toate făcând diferența crucială. Totuși, studiul aduce în atenție cazuri multiple în care aceste caracteristici sunt insuficiente pentru a defini reziliența sau câștigătorul competiției și evidențiază nevoia unor calități fundamentale ale societății, care să genereze *productivitate economică, coeziune societală și voință națională*, caracteristici ce se dovedesc mai importante și definitorii pentru obiectivele rezilienței și câștigării competiției.

Există un număr mare de studii care abordează *puterea*, cu tot atâtea critici și contraexemple. În fapt, nu există nici la nivelul specialiștilor zonei academice și universitare și nici la nivelul cercetătorilor o accepțiune generală a puterii și a măsurării ei. Abordarea lui Joseph Nye Jr.<sup>28</sup> este cea mai în vogă la nivelul consilierilor celor mai importante cancelarii ale lumii, cu modul său de a defini tipurile de putere: *hard, soft* și *smart*. Dar când depășim dimensiunea filosofică și intrăm în spațiul indicilor și al determinantilor puterii, controversile apar la fiecare pas și la fiecare actor care încearcă să-și valorifice propriile avantaje naționale.

Totuși, punctul unanim de convergență este faptul că *o națiune dinamică și rezilientă, coerentă și coezivă pe plan intern, este fundamentul succesului internațional*. De aici înainte, când se evaluează indicii care ar defini aceste elemente, încep să se arate diferențele semnificative. Din această perspectivă ni se relevă importanța studiului realizat de RAND Corporation, comandat de către Pentagon, care vizează identificarea acelor caracteristici ce au determinat succesul competițional în istorie. Între acestea, evident, *o ambiție națională puternică, o cultură a învățării și adaptării continue și o manifestare largă a diversității și pluralismului inclusiv*. Obiectivul este transferul către stat a caracteristicilor puterii dinamice, inovative și adaptabile ale societății, în același timp.

Istoria a dovedit că armele, tehnologia, strategia, pregătirea, reflexele militare, împreună cu o economie serioasă, capabilă să susțină un efort de război, sunt caracteristici importante pentru victoria în competiții, cel puțin pe termen scurt. Dar, aceeași Istorie ne învață, din cele mai vechi timpuri, că victoria pe termen lung, cea reală și definitivă, vine din *calitatea superioară a sistemelor social și politic* și, cu precădere, din *caracteristicile societății*, care influențează sistemul de guvernare și statul care le administrează.

Cele mai recente exemple, precum Războiul Rece, au relevat că victoria merge către actorul mai energic, mai inovativ, mai productiv, mai legitim în acțiunea și politicile sale<sup>29</sup>. În plus, s-a

dovedit în ciclurile istorice și în succesiunea de hegemoni și structuri ale sistemului internațional că națiunile cresc și se prăbușesc ca urmare a unui *set complex de caracteristici sociale interdependente* și care produc dinamismul național și avantajele competitive. Aceasta este teoria prezentată de Michael J. Mazarr, care susține că statele cu prea puțină ambiție, diversitate sau dorință de a se adapta riscă să alunece în spirala declinului.

## EXEMPLE ȘI CONTRAEXEMPLE ALE PUTERII SOCIALE

Între factorii fundamentali identificați de studiul RAND Corporation, care a apelat la un număr mare de istorici în faza inițială, urmând ca decantarea să se facă de specialiști în studii de securitate, se numără cei care generează dezvoltarea economică, inovarea, sofisticarea militară, productivitatea, caracteristici asociate dinamismului național și competitivității. Totuși, există state care îndeplinesc aceste caracteristici și care nu ajung în topul ierarhiei globale. Este cazul, de exemplu, al Țărilor de Jos și Singapore, care sunt prea mici ca dimensiuni pentru a putea proiecta puterea la nivel global, sau al Suediei și Coreei de Sud, care nu au avut ambiții și dorințe de a se implica și a conduce destine la nivel global. Caracteristicilor sociale li se adaugă puterea geopolitică și capacitatea influenței culturale, dar și factori de criză naturali, precum pandemii sau erori strategice umane fundamentale.

Totuși, concluzia este că longevitatea unui sistem verificat și adaptabil și abilitatea de a oferi securitate și prosperitate propriei societăți sunt elementele fundamentale ale succesului în rivalitățile bilaterale sau la nivel global. Studiul a adus în prim-plan *șapte caracteristici sociale fundamentale*:

- *ambitiția națională;*
- *oportunități împărtășite cu toți cetățenii;*
- *o identitate națională comună și coerentă;*
- *un stat activ;*
- *instituții sociale eficiente;*
- *un interes major pe învățare și adaptare;*
- *diversitate și pluralism semnificative în societate*<sup>30</sup>.

Studiul nu neagă și alți factori, precum dezastrele naturale, pandemiile sau geografia, care joacă rolul lor în evaluarea capacităților sociale ce pot duce la succes. Și ele nu sunt implicite, nici nu se reflectă automat în cele șapte caracteristici sociale evocate. Totuși, studiul relevă o caracteristică mai importantă pentru toate cele precedente: *echilibrul*. Echilibrul între susținerea uneia sau alteia dintre caracteristici la nivelul politicilor publice, pentru că excesul în fiecare dintre aceste direcții poate duce la efecte negative cel puțin la fel de importante.

De exemplu, dacă este să vorbim despre *ambitiția națională puternică*, ea se poate traduce prin simțul unei „misiuni naționale” sau al unei „relevanțe excepționale”, care induce nevoia de a influența politica globală. Dar, mitologia națională excepționalistă poate lesne devia de la dorința de a învăța, de a realiza și de a avea succes în orice (de la cercetare științifică, afaceri, industrie sau arte, la competiții sportive) către ambiții naționale excesive, excepționalism, unilateralism, precum și către tendința de a impune și de a te considera superior celorlalte națiuni și societăți<sup>31</sup>, ceea ce împinge societatea respectivă către eșec major, ba chiar cu costuri de prestigiu și de justificare a locului în lume extrem de mari și care se perpetuează pe perioade lungi de timp.

În al doilea rând, pe lângă ambiția națională comună, de a reuși împreună, societățile competitive au *tendința de a împărtăși oportunitățile* cu toți cetățenii lor; de a oferi cât mai multora căile spre succes și de a exclude cât mai puține segmente din populația lor de la perspectivele de a câștiga. Efortul național nu se poate realiza dacă nu sunt implicate toate segmentele societății, un număr cât mai mare de cetățeni, dacă nu există conștiința nevoii de a reuși prin efortul comun, al tuturor. Iar acest efort poate fi angajat doar dacă există *un țel comun coerent și major* și dacă perspectiva succesului este împărtășită cu toți, în mod egal și potrivit propriilor abilități, fără a lăsa pe nimeni în urmă. Mobilitatea socială este, de asemenea, un mecanism de coeziune și implicare necesar, pentru că asigură tuturor un drum spre vârf, spre succes intern în societate, pentru că există o speranță îndreptățită pentru fiecare membru al

societății, și cu o probabilitate mai mare decât cea de a juca la loterie.

*Identitatea națională coerentă și împărtășită* este o altă caracteristică relevantă a perspectivei de a reuși împreună<sup>32</sup>. Exemplele în direcția aceasta vin de la identitatea națională unificatoare a Japoniei, după cel de-al Doilea Război Mondial, care a dat imboldul de a reuși după dezastru, de a se reconstrui și de a se afirma în lumea post-război. Statul activ, implicat, este o altă caracteristică, subliniată o dată mai mult în situații de criză, precum cele pe care le-am traversat, când rolul statului rămâne crucial. Dar un stat activ presupune și o guvernare coerentă, puternică, direcționată spre obiective și eficiență, care știe și reușește să investească capabilități naționale și calități societale benefice în viitorul propriei țări<sup>33</sup>. Și astăzi perspectivele de succes în tehnologia informației, energie verde și cuceriri farmaceutice de vârf țin de stat (vezi rolul U.S. Defense Advanced Research Projects Agency).

*Instituțiile sociale eficiente* se referă la instituții puternice și inclusive care determină creștere economică, îmbunătățesc legitimitatea statului și răspund provocărilor sociale, producând, totodată, putere militară coerentă. Un Parlament relevant și puternic, un sector financiar puternic și o putere navală capabilă au dus, de exemplu, Imperiul Britanic, la creștere economică și geopolitică. Din contra, preocuparea de sine, nu față de cetățeni și de țară, a conducătorilor și instituții corupte și ineficiente au determinat prăbușirea URSS și, de ce nu, actuala prăbușire a forței armate a F.Ruse în războiul din Ucraina.

Sublinierea ca valori societale majore a *învățării și adaptării* este cel puțin la fel de importantă ca triada de a crea, explora și învăța, ca obiectiv major pentru societățile cu competitivitate majoră, care îmbrățișează cu precădere dezideratele adaptării și experimentării și sunt deschise inovării în politicile publice, modelele de afaceri, conceptele și doctrinele militare, artă și cultură. Curiozitatea intelectuală răspândită, angajamentul de a învăța, înclinația spre educație tehnologică modernă, creștere și inovare sunt modele majore și de neocolit pentru o societate competitivă.

Cel de-al șaptelea criteriu identificat este despre gradul semnificativ de *diversitate și pluralism*, dar la un nivel suficient pentru a menține coerența și identitatea comună a societății. Totuși, un set larg de experiențe și perspective ajută la generarea unei multitudini de idei și la atragerea de talente care pot susține puterea națională. Aici intervine, cu precădere, pentru societățile occidentale, din care și România face parte, abilitatea de a asimila și integra străinii, refugiații, migranții, de a folosi avantajele diversității în sens modern, de susținere a competiției și inovării contra delăsării și complacerii într-o situație comodă, poate, la un moment dat. Pentru că unul dintre motivele prăbușirii imperiilor, hegemonilor și a societăților de succes s-a dovedit exact această complacere a elitelor (a clasei de vârf), în special, de unde și prăbușirea în timp a acestor societăți, state și actori internaționali.

---

## CONCLUZII

---

*Avertismentul studiului* lui Michael J. Mazarr este drastic: fiecare dintre cele șapte caracteristici identificate, asociate cu competitivitatea națională, sunt obligatorii, dar nici societățile care le au pe toate șapte nu pot fi sigure de succes pe termen lung. Motivul este echilibrul în fiecare caz în parte, pentru ca avantajele să nu se transforme în excese și vulnerabilități, ba chiar impedimente<sup>34</sup>. Iar exemplele sunt multiple în acest sens, inclusiv cele care au stat la baza studiului RAND Corporation. Efortul de a construi un stat activ poate să genereze o agendă de centralizare, autoritarism sau intoleranță. Instituțiile eficiente pot determina birocrății enorme și greoaie, blocante, și care frânează inovația și adaptarea. Prea mult pluralism poate dizolva unitatea națională. Competitivitatea vine, la națiunile de succes, de la îngrijirea și promovarea cu atenție a caracteristicilor esențiale, dar cu moderație sănătoasă și menținând echilibrele fragile și esențiale ale societății.

O discuție aparte trebuie purtată în ceea ce privește *rolul elitei* pentru promovarea unei societăți care să fie competitivă și rezilientă

deopotrivă, capabilă să asigure, pe termen lung, structurarea și funcționarea unui stat care să furnizeze securitatea și prosperitatea națiunii. Studiul realizat de către RAND Corporation arată că cele șapte caracteristici, tratate echilibrat, se susțin și se întăresc reciproc. Ambiția națională și cultura educației și adaptării se întăresc reciproc, tot astfel cum un stat activ și instituții eficiente au roluri complementare și se autosusțin. Împărtășirea oportunităților, diversitatea și pluralismul dau măsura valorii adevărate<sup>35</sup>.

Aceasta ar fi rețeta succesului național, în momentul în care există *o elită acceptată și recunoscută societal*. Atunci când elita devine coruptă și înclinată spre modele personale rentiere, se erodează și valorile de competitivitate, reziliența și dinamismul națiunii<sup>36</sup>. Elitele sunt cruciale, ele conduc națiunile, sunt exemple de urmat, dar trebuie să fie devotate binelui public și societății, pentru a fi acceptate și urmate cu entuziasm de către societate. Aceasta este cheia esențială a ingredientelor ce determină competitivitatea și reziliența unei națiuni.

## BIBLIOGRAFIE

1. ACEMOGLU Daron, Robinson A. James, *Why Nations Fail. The Origins of Power, Prosperity and Poverty*, Profile Books, London, 2013, ISBN 978-1-84668-430-2, 529 p. (versiunea în limba română - *De ce eșuează națiunile. Originile puterii, ale prosperității și ale sărăciei*, Editura Litera, 2016, ISBN 978-606-33-0025-7, 527 p.).
2. PLATIAS G. Athanassios, Constantinos Koliopoulos, *Thucydides on Strategy. Grand Strategies in the Peloponnesian War and their Relevance Today*, Columbia University Press, 2010, ISBN 978-0-231-70133-4, 197 p.
3. BAUMAN Zygmunt, *Globalizarea și efectele ei sociale*, Ed. Antet, 2005, ISBN: 973-8203-57-0, 128 p.
4. BREMMER Ian, *Every Nation for Itself. Winners and Losers in a G0 World*, Portfolio Penguin, 2012, ISBN 978-1-59184-468-6, 229 p.
5. CHIFU Iulian, *Decizia în criză*, Editura RAO, București, 2019, ISBN 978-606-006-349-0, 335 p.
6. CHIFU Iulian, „Lecțiile conflictului din Ucraina și perspectiva rezilienței societale”, *Infosfera*, vol. 14, nr. 2, 2022, ISSN 2065-3395, pp. 5-12.
7. CHIFU Iulian, Nantoi Oazu, Sushko Oleksandr, *Societal Security in the trilateral Region Romania-Ukraine-Republic of Moldova/ Securitate societală în regiunea trilateralei România – Ucraina - Republica Moldova*, ediție bilingvă, Editura Curtea Veche, București, 2008, ISBN 978-973-1983-00-4, 320 p.
8. CHIFU Iulian, ”Prospective Analysis of Ukrainian Crisis: Scenarios for mid-long term evolution”, *Ukraine Analytica*, Nr.1/9 octombrie 2015, Odessa, ISSN 2518-7481.
9. CHIFU Iulian, Ramberg Britta, *Crisis management in Transitional Societies*, Editura CRISMART SNDC, Stockholm, 2007, ISBN 978-91-85401-64-2, 387 p.
10. CHIFU Iulian, Ramberg Britta, *Managementul crizelor în societățile în tranziție, Cazul României*, Editura RAO, București, 2008, ISBN 978-973-103-687-8, 352 p.
11. CHIFU Iulian, „Războiul hibrid și reziliența societală. Planificarea apărării hibride”, *Revista Infosfera*, vol.10, nr. 1, 2018, ISSN 2065-3395, pp. 23-30.
12. CHIFU Iulian, *Reconfigurarea securității și a relațiilor internaționale în secolul 21*, Editura ISPRI, 2022 (în curs de apariție).
13. CHIFU Iulian, „Securitatea tehnologică. Un nou domeniu de strictă actualitate a securității viitorului”, *Infosfera*, vol. 13, nr. 2, 2021, ISSN 2065-3395, pp.13-23.
14. CHIFU Iulian, *Studii prospective și metodologii alternative. Eșafodajul de securitate în secolul 21*, Editura RAO, 2022 (în curs de apariție).
15. CHIFU Iulian, Nantoi Oazu, *Război informațional: tipizarea agresiunii informaționale a Federației Ruse*, Editura ISPRI, București, 2016.



16. ECO Umberto, *Cronicle unei societăți lichide*, Editura Polirom, Iași, 2016, ISBN 978-973-46-6063-6, 363 p.
17. EU, "A strategic compass for security and defense, For an European Union that protects its citizens, values and interests and contributes to international peace and security", 2022. [https://www.eeas.europa.eu/sites/default/files/documents/strategic\\_compass\\_en3\\_web.pdf](https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf).
18. FUKUYAMA Francis, *Identity: Contemporary Identity Politics and the Struggle for Recognition*, Profile Books Ltd, Londra, 2019, 240p.
19. KISSINGER Henry, *Ordinea Mondială. Reflecții asupra specificului națiunilor și a cursului istoriei*, Editura RAO, 2015, ISBN 978-606-609-867-0, 350 p.
20. LYALL Jason, "How Inequality Hobbles Military Power. Divided Armies Struggle to Win", *Foreign Affairs*, July 22, 2022, at <https://www.foreignaffairs.com/ukraine/how-inequality-hobbles-military-power>.
21. MAZARR J. Michael, Blake Jonathan, Casey Abigail, McDonald Tim, Pezard Stephanie, Spirtas Michael, "Understanding the Emerging Era of International Competition Theoretical and Historical Perspectives", RAND Corporation, Research Report, 2018, [https://www.rand.org/pubs/research\\_reports/RR2726.html](https://www.rand.org/pubs/research_reports/RR2726.html).
22. MAZARR J. Michael, *The Societal Foundation of National Competitiveness*, RAND Corporation, 2022, ISBN: 978-1-9774-0939-3.
23. NATO documents, "Strengthen Resilience Commitment", 15 June, 2021, at [https://www.nato.int/cps/en/natohq/official\\_texts\\_185340.htm](https://www.nato.int/cps/en/natohq/official_texts_185340.htm).
24. NATO, "Preparing for the Future: NATO 2030", p.14, at [https://www.nato.int/nato\\_static\\_fl2014/assets/pdf/2022/3/pdf/sgar21-en.pdf#page=15](https://www.nato.int/nato_static_fl2014/assets/pdf/2022/3/pdf/sgar21-en.pdf#page=15).
25. NYE Joseph S. Jr., *Viitorul puterii*, Editura Polirom, Iași, 2011.
26. ROGER James, "Audit of Geopolitical Capability. An assessment of 20 major powers", Henry Jackson Society, January 2019, ISBN: 978-1-909035-50-8, 64 p., la <https://henryjacksonsociety.org/wp-content/uploads/2019/01/HJS-2019-Audit-of-Geopolitical-Capability-Report-web.pdf>.
27. RUDD Kevin, "Rivals Within Reason? U.S.-Chinese Competition Is Getting Sharper—but Doesn't Necessarily Have to Get More Dangerous", *Foreign Affairs*, July 20, 2022, at <https://www.foreignaffairs.com/china/rivals-within-reason>.
28. SHEA Jamie, "Resilience, a core element of collective defense", <https://www.nato.int/docu/Review/2016/Also-in-2016/nato-defence-cyber-resilience/EN/index.htm>.
29. SIMONS Greg, Chifu Iulian, *The Changing Face of Warfare in the 21st Century*, Routledge, London and New York, 2017, ISBN 978-1-472-48212-9, 278 p.
30. STERN Eric, *Designing Crisis Management Training and Exercises for Strategic Leaders*, National Defense College, Stockholm, 2014, ISBN 978-91-86137-39-7, 112 p.
31. TALEB Nassim Nicolas, *Antifragil - ce avem de câștigat de pe urma dezordinii*, Editura Curtea Veche, 2014.
32. White House, *National Security Strategy of the United States*, decembrie 2017, <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>.

- <sup>1</sup> Iulian Chifu, „Lecțiile conflictului din Ucraina și perspectiva rezilienței societale”, *Revista Infosfera*, vol. 14, nr. 2, 2022, ISSN 2065-3395, p.p 5-12.
- <sup>2</sup> Idem.
- <sup>3</sup> Iulian Chifu, Oazu Nantoi, Oleksandr Sushko, *Societal Security in the trilateral Region Romania-Ukraine-Republic of Moldova/Securitate societală în regiunea trilateralei România-Ucraina-Republica Moldova*, ediție bilingvă, Editura Curtea Veche, București, 2008, ISBN 978-973-1983-00-4, 320 p.
- <sup>4</sup> NATO, ”Preparing for the Future: NATO 2030”, p.14, [https://www.nato.int/nato\\_static\\_fl2014/assets/pdf/2022/3/pdf/sgar21-en.pdf#page=15](https://www.nato.int/nato_static_fl2014/assets/pdf/2022/3/pdf/sgar21-en.pdf#page=15).
- <sup>5</sup> NATO documents, ”Strengthen Resilience Commitment”, 15 June, 2021, [https://www.nato.int/cps/en/natohq/official\\_texts\\_185340.htm](https://www.nato.int/cps/en/natohq/official_texts_185340.htm).
- <sup>6</sup> Jamie Shea, ”Resilience, a core element of collective defense”, <https://www.nato.int/docu/Review/2016/Also-in-2016/nato-defence-cyber-resilience/EN/index.htm>.
- <sup>7</sup> EU, ”A strategic compass for security and defense, For an European Union that protects its citizens, values and interests and contributes to international peace and security”, 2022. [https://www.eeas.europa.eu/sites/default/files/documents/strategic\\_compass\\_en3\\_web.pdf](https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf).
- <sup>8</sup> Daron Acemoglu, James A. Robinson, *De ce eșuează națiunile. Originile puterii, ale prosperității și ale sărăciei*, Editura Litera, 2016, ISBN 978-606-33-0025-7, 527 p.
- <sup>9</sup> Henry Kissinger, *Ordinea Mondială. Reflecții asupra specificului națiunilor și a cursului istoriei*, Editura RAO, 2015, ISBN 978-606-609-867-0, 350 p.
- <sup>10</sup> Iulian Chifu, „Războiul hibrid și reziliența societală. Planificarea apărării hibride”, *Revista Infosfera*, vol. 10, nr. 1, 2018, ISSN 2065-3395, pp. 23-30.
- <sup>11</sup> Iulian Chifu, ”Prospective Analysis of Ukrainian Crisis: Scenarios for mid-long term evolution”, *Ukraine Analytica*, Nr.1/ octombrie 2015, Odessa, ISSN 2518-7481, pp.38-45.
- <sup>12</sup> Iulian Chifu, Oazu Nantoi, Oleksandr Sushko, Op.cit.
- <sup>13</sup> Eric Stern, *Designing Crisis Management Training and Exercises for Strategic Leaders*, National Defense College, Stockholm, 2014, ISBN 978-91-86137-39-7, 112 p.
- <sup>14</sup> ISBN 978-1-472-48212-9, 278 p.; Chifu Iulian, Nantoi Oazu, *Război informațional: tipizarea agresiunii informaționale a Federației Ruse*, Editura ISPRI, București, 2016.
- <sup>15</sup> Fukuyama Francis, *Identity: Contemporary Identity Politics and the Struggle for Recognition*, Profile Books Ltd, Londra, 2019, 240p.
- <sup>16</sup> Iulian Chifu, *Decizia în Criză*, Editura RAO, București, 2019, ISBN 978-606-006-349-0, 335 p.; Iulian Chifu, Britta Ramberg, *Crisis management in Transitional Societies*, Editura CRISMART SNDC, Stokholm, 2007, ISBN 978-91-85401-64-2, 387 p.; Iulian Chifu, Britta Ramberg, *Managementul crizelor în societățile în tranziție. Cazul României*, Editura RAO, București, 2008, ISBN 978-973-103-687-8, 352 p.
- <sup>17</sup> Zygmunt Bauman, *Globalizarea și efectele ei sociale*, Editura Antet, 2005, ISBN: 973-8203-57-0, 128 p.; Umberto Eco, *Cronicle unei societăți lichide*, Editura Polirom, Iași, 2016, ISBN 978-973-46-6063-6, 363 p.
- <sup>18</sup> Iulian Chifu, „Lecțiile conflictului din Ucraina și perspectiva rezilienței societale”, *Infosfera*, vol. 14, nr. 2, 2022.
- <sup>19</sup> Nassim Nicolas Taleb, *Antifragil - ce avem de câștigat de pe urma dezordinii*, Editura Curtea Veche, 2014.
- <sup>20</sup> Michael J. Mazarr, Jonathan Blake, Abigail Casey, Tim McDonald, Stephanie Pezard, Michael Spirtas, ”Understanding the Emerging Era of International Competition Theoretical and Historical Perspectives”, RAND Corporation, Research Report, 2018, [https://www.rand.org/pubs/research\\_reports/RR2726.html](https://www.rand.org/pubs/research_reports/RR2726.html).
- <sup>21</sup> White House, *National Security Strategy of the United States*, decembrie 2017, <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>.
- <sup>22</sup> Iulian Chifu, *Reconfigurarea securității și a relațiilor internaționale în secolul 21*, Editura ISPRI (în curs de pregătire).
- <sup>23</sup> James Roger, ”Audit of Geopolitical Capability. An assessment of 20 major powers”, Henry Jackson Society, January 2019, ISBN: 978-1-909035-50-8, 64 p., la <https://henryjacksonsociety.org/wp-content/uploads/2019/01/HJS-2019-Audit-of-Geopolitical-Capability-Report-web.pdf>.
- <sup>24</sup> Idem.
- <sup>25</sup> Michael J. Mazarr, *The Societal Foundation of National Competitiveness*, RAND Corporation, 2022, ISBN: 978-1-9774-0939-3.
- <sup>26</sup> Iulian Chifu, „Securitatea tehnologică. Un nou domeniu de strictă actualitate a securității viitorului”, *Infosfera*, vol. 13, nr. 2, 2021, ISSN 2065-3395, p.13-23.
- <sup>27</sup> Athanassios G. Platias, Constantinos Koliopoulos, *Thucydides on Strategy. Grand Strategies in the Peloponnesian War and their Relevance Today*, Columbia University Press, 2010, ISBN978-0-231-70133-4, 197 p.
- <sup>28</sup> Joseph S., Nye, Jr., *Viitorul puterii*, Editura Polirom, Iași, 2011, p. 43.
- <sup>29</sup> Jason Lyall, ”How Inequality Hobbles Military Power. Divided Armies Struggle to Win”, *Foreign Affairs*, July 22, 2022, at <https://www.foreignaffairs.com/ukraine/how-inequality-hobbles-military-power>.
- <sup>30</sup> Michael J. Mazarr, *The Societal Foundation of National Competitiveness*.
- <sup>31</sup> Kevin Rudd, ”Rivals Within Reason? U.S.-Chinese Competition Is Getting Sharper—but Doesn’t Necessarily Have to Get More Dangerous”, *Foreign Affairs*, July 20, 2022, at <https://www.foreignaffairs.com/china/rivals-within-reason>.
- <sup>32</sup> Francis Fukuyama, Op.cit.
- <sup>33</sup> Iulian Chifu, Războiul hibrid și reziliența societală. Planificarea apărării hibride.
- <sup>34</sup> Daron Acemoglu, James A. Robinson, *Why Nations Fail. The Origins of Power, Prosperity and Poverty*, Profile Books, London, 2013, ISBN 978-1-84668-430-2, 529 p.
- <sup>35</sup> Iulian Chifu, *Studii prospective și metodologii alternative. Eșafodajul de securitate în secolul 21*, Editura RAO (în curs de apariție).
- <sup>36</sup> Ian Bremmer, *Every Nation for Itself. Winners and Losers in a G0 World*, Portfolio Penguin, 2012, ISBN 978-1-59184-468-6, 229 p.

# NATO POST-MADRID ȘI CONCEPTUL STRATEGIC 2022: ÎN TRE CONTINUITATE ȘI SCHIMBARE

Vasile CREȚU\*

## Abstract:

*NATO has come a long way to adopt the 2022 Strategic Concept at the Madrid Summit (June 2022), a document which is the expression of the member states' vision regarding the Alliance's place and role in the new security context. The Strategic Concepts usually receive great scholarly attention, due to their position as the second most important document after the Washington Treaty. This article provides a preliminary assessment of the 2022 Strategic Concept by examining the elements of continuity and change, using qualitative research methods, such as document and content analysis. Thus, this issue is addressed based on an analysis of the concepts and terminology used in the 2022 Strategic Concept, considering them relevant for the direction in which the Alliance will evolve. From a structural point of view, this paper contains a section dedicated to the importance of Strategic Concepts, followed by a comparative analysis of the provisions of the concepts developed in the post-Cold War era and, finally, a section dedicated to 2022 Strategic Concept.*

**Keywords:** NATO; alliance; strategic concept; adaptation; deterrence and defence.

## INTRODUCERE

Adoptarea unui nou Concept Strategic cu prilejul Summit-ului de la Madrid (28-30 iunie 2022) consfințește o nouă etapă în evoluția NATO, fiind expresia viziunii statelor membre asupra locului și rolului Alianței în noul context de securitate.

De la înființare, la nivelul NATO au fost adoptate opt Concepte Strategice, acestea ocupând locul secund, ca importanță, după Tratatul Alianței Nord-Atlantice (Washington, 4 aprilie 1949). În general, Conceptul Strategic oferă dinamism și operaționalizează prevederile Tratatului<sup>1</sup>, prin stabilirea priorităților și a provocărilor la care Alianța va răspunde, motiv pentru care primește o atenție deosebită în literatura de specialitate.

În acest context, prezentul articol va analiza prevederile noului Concept Strategic al Alianței prin raportare la elementele de continuitate și de schimbare. Având în vedere tipul studiului, perspectiva metodologică este de tip calitativ, prin utilizarea analizei de document și de conținut ca metode principale, printr-o analiză a conceptelor și terminologiei utilizate, considerate relevante pentru direcția în care evoluează NATO. Din punct de vedere structural, articolul conține o secțiune dedicată importanței Conceptelor Strategice, urmată de o analiză comparativă a prevederilor documentelor strategice elaborate în perioada post-Război Rece și, în cele din urmă, de o secțiune dedicată Conceptului adoptat în vara acestui an.

\* Expert în cadrul Ministerului Apărării Naționale.



## CONCEPTELE STRATEGICE ALE NATO – SCURT ISTORIC, ROL ȘI IMPORTANȚĂ ÎN LITERATURA DE SPECIALITATE

Tratatul Alianței Nord-Atlantice (1949), prin cele 14 articole ale sale, consacră principiile pe care este construită organizația (art. 1 și art. 2 – rezolvarea pașnică a disputelor, abținere de la utilizarea forței, colaborarea economică), bazele pentru funcționarea Alianței (art. 3 – reziliență națională și colectivă; art. 4 – consultare; art. 5 – apărare colectivă; art. 10 – „politica ușilor deschise”), modalitatea de implementare a prevederilor (art. 9 – înființarea Consiliului Nord-Atlantic și a organismelor subsidiare), precum și aspecte ce țin de teritorialitate (art. 6), aplicabilitate (art. 7-8) și de valabilitate (art. 11-14)<sup>2</sup>.

Actul fondator al NATO stabilește, așadar, obiectivele și liniile generale („unirea eforturilor în scopul apărării colective și al menținerii păcii și securității” – Preambul<sup>3</sup>), însă oferă puține detalii despre cum să fie implementate aceste deziderate<sup>4</sup>. Totodată, Tratatul poate fi caracterizat drept vag, întrucât nu stabilește o listă a priorităților și a amenințărilor, fapt care este explicat de faptul că amenințarea sovietică era considerată implicită, nefiind nevoie de o menționare expresă. Pe de altă parte, caracterul Tratatului a fost dat și de negocierile îndelungate și complicate din anii 1948-1949<sup>5</sup>. Cu toate acestea, Tratatul nu a fost niciodată revizuit sau modificat.

În conformitate cu art. 9, pentru implementarea Tratatului a fost înființat Consiliul Nord-Atlantic, în care era reprezentat fiecare stat membru, precum și un Comitet al Apărării (Defence Committee/DC)<sup>6</sup> pentru stabilirea măsurilor specifice aplicării art. 3 și art. 5. În această calitate, la prima reuniune a Comitetului Apărării (5 octombrie 1949), în Directiva către Comitetul Militar, a fost stabilită sarcina dezvoltării strategiei prin elaborarea unui „concept cuprinzător” (*broad*

*concept*), care să fie formulat ținând cont de „amenințările probabile față de fiecare regiune”, să stabilească obiectivele inițiale și să servească drept ghid pentru planificarea apărării<sup>7</sup>.

În acest context, la 6 ianuarie 1950, Consilul Nord-Atlantic a aprobat primul Concept Strategic al Alianței (*DC 6/1 The Strategic Concept for the Defense of the North Atlantic Area*), ca „pas inițial pentru inițierea unei planificări a apărării [...] care vizează asigurarea păcii și reducerea posibilității de agresiune”<sup>8</sup>.

Prin urmare, Conceptul Strategic a devenit principalul document operațional al Alianței, care trasează liniile directoare și orientează planificarea subsecventă. De-a lungul timpului, au fost adoptate opt astfel de documente: patru pe timpul Războiului Rece (1950, 1952, 1957, 1967), respectiv patru începând cu anul 1991 (1991, 1999, 2010 și, cel mai recent, 2022). Această categorisire este motivată, în primul rând, de mediul de securitate bipolar ce a caracterizat prima etapă, precum și de faptul că primele patru concepte au avut o abordare eminent militară<sup>9</sup>, fiind elaborate de Comitetul Militar, într-o variantă clasificată, în timp ce ultimele patru au fost elaborate la nivel politico-diplomatic, devenind publice și fără nivel de clasificare<sup>10</sup>.

Structura Conceptului a evoluat odată cu Alianța, ajungând ca, la sfârșitul Războiului Rece, să joace cel puțin trei roluri: două cu caracter intern (codificarea principalelor decizii și măsuri care sunt deja implementate, precum și stabilirea unei noi direcții strategice) și unul cu caracter extern, prin comunicarea publică a intereselor și a sarcinilor de bază<sup>11</sup>.

Din punct de vedere practic, Conceptul Strategic este un document similar strategiilor de securitate/apărare națională<sup>12</sup>, dar este conceput dintr-o perspectivă supra-statală, ca strategie a unei organizații internaționale. În același timp, Conceptul este expresia viziunii

statelor membre, fiind aprobat într-o manieră interguvernamentală, pe bază de consens, în Consiliul Nord-Atlantic<sup>13</sup>. Documentul reflectă mai degrabă compromisul statelor membre, procesul de elaborare fiind unul laborios (ce include etapele de consultare, implicare, redactare și negociere<sup>14</sup>) în absența unei culturi strategice comune, statele reținând suveranitatea și libertatea de acțiune în plan internațional. Astfel, există autori care consideră întocmai acesta fiind scopul Conceptului Strategic: obținerea unui acord asupra strategiei, indiferent de predispozițiile politice ale statelor membre<sup>15</sup>.

Totodată, Conceptul Strategic funcționează ca o *mare strategie* (*grand strategy*) a comunității euro-atlantice, o parte dintre prevederile acestuia necesitând acțiunile comune ale statelor, care depășesc sfera NATO ca organizație. În plus, unii experți (de exemplu, prof. Marian Zulean de la Universitatea București) argumentează că NATO, prin Conceptul Strategic și Procesul NATO de Planificare a Apărării (NDPP), are un impact major asupra formulării strategiilor de securitate națională în spațiul euro-atlantic<sup>16</sup>, influența fiind astfel bidirecțională.

Din aceste considerente, Conceptele Strategice beneficiază de o atenție deosebită în literatura de specialitate a relațiilor internaționale, cel mai adesea fiind menționate în relație cu sarcinile de bază ale Alianței sau atunci când sunt analizate dosare-cheie din activitatea NATO. În acest sens, o foarte mare parte dintre lucrările referitoare la NATO citează sau fac trimitere, într-o formă sau alta, la Conceptul Strategic valabil la momentul redactării.

O altă categorie este reprezentată de acele studii care pledează pentru adoptarea unui nou Concept, în momentele în care precedentul este considerat învechit sau depășit de evoluțiile mediului de securitate. Suplimentar, se remarcă alte două tipologii: studiile de tip *policy paper*,

orientate către recomandarea unor direcții de acțiune în contextul dezbaterilor pentru un nou document strategic, precum și lucrările care prezintă noile Concepte după ce acestea au fost aprobate. Materialele publicate în ultimii ani se încadrează cu precădere în categoriile menționate în prezentul paragraf.

O zonă mai puțin explorată este reprezentată de studiul Conceptelor în sine, pornind de la relevanță, rol și evoluție. Pe portalul NATO dedicat subiectului, care conține o prezentare succintă a celor opt documente strategice adoptate până în prezent, rolul Conceptelor este definit de următoarele coordonate: (1) setarea strategiei; (2) sublinierea scopului și caracterului durabil al NATO; (3) definirea sarcinilor de bază; (4) stabilirea provocărilor și oportunităților din mediul de securitate; (5) conferirea liniilor directe pentru adaptarea politică și militară<sup>17</sup>. De asemenea, Benedetta Berti, șefa Diviziei de Planificare Politică a NATO, definește Conceptul Strategic ca o „oportunitate unică [...] de promovare a coeziunii, unității și înțelegerii comune” în rândul aliaților<sup>18</sup>.

## EVOLUȚIA ALIANȚEI ȘI CONCEPTELE STRATEGICE POST-RĂZBOI RECE

După 1989, Alianța Nord-Atlantică a parcurs un amplu proces de adaptare atât la nivel organizațional, cât și din prisma activităților în care a fost implicată, prin concentrarea, în principal, pe misiuni de gestionare a crizelor și de menținere a păcii, operațiuni în afara zonei de responsabilitate (*out-of-area*) și diferite forme de cooperare sau parteneriat, inclusiv cu Federația Rusă. De departe, cea mai profundă schimbare a fost generată de dublarea numărului de state membre, de la 16 (în 1991) la 32 (după ce Suedia și Finlanda vor adera la Alianță).

Conceptele Strategice/CS au reflectat toate aceste transformări, scopul prezentei secțiuni fiind analiza comparativă a principalelor prevederi, sintetizate în Tabelul nr. 1.

Conceptul Strategic	Descrierea mediului de securitate	Sarcini de bază
CS 1991	„Amenințarea unui atac simultan la scară largă pe toate fronturile europene ale NATO a fost înlăturată efectiv”. [7] „Riscurile la adresa securității Alianței sunt mai puțin probabil să rezulte din agresiunea calculată împotriva teritoriului Alianței, ci mai degrabă din consecințele negative ale instabilităților care pot apărea din dificultățile economice, sociale și politice grave, inclusiv rivalitățile etnice și disputele teritoriale, cu care se confruntă mai multe țări din Europa Centrală și de Est.” [9]	(1) Fundament pentru un mediu de securitate stabil în Europa, bazat pe dezvoltarea instituțiilor democratice și rezolvarea pașnică a disputelor; (2) Forum transatlantic pentru consultări ale aliaților; (3) Descurajare și apărare; (4) Menținerea echilibrului strategic în Europa.
CS 1999	„În ciuda evoluțiilor pozitive din mediul strategic și a faptului că o agresiune convențională la scară largă împotriva Alianței este foarte puțin probabilă, există posibilitatea ca o astfel de amenințare să apară pe termen lung. Securitatea Alianței rămâne supusă unei game largi de riscuri militare și non-militare.” [20]	(1) Securitate: Fundament indispensabil pentru un mediu de securitate stabil, bazat pe dezvoltarea instituțiilor democratice și rezolvarea pașnică a disputelor; (2) Consultare: Forum transatlantic pentru consultări ale aliaților; (3) Descurajare și apărare; (4) Consolidarea securității și stabilității zonei euro-atlantice, prin (a) managementul crizelor și (b) parteneriate.
CS 2010	„Zona euro-atlantică este în pace și amenințarea unui atac convențional împotriva teritoriului NATO este scăzută”. [12]	(1) Apărare colectivă; (2) Managementul crizelor; (3) Securitate prin cooperare.
CS 2022	„Zona euro-atlantică nu este în pace. [...] Concurența strategică, instabilitatea generalizată și șocurile recurente definesc mediul nostru de securitate mai larg. Amenințările cu care ne confruntăm sunt globale și interconectate.” [6]	(1) Descurajare și apărare; (2) Prevenirea și managementul crizelor; (3) Securitate prin cooperare.

**Tabel 1: Analiza comparativă a principalelor prevederi ale Conceptelor Strategice (CS) post-Război Rece (CS 1991<sup>19</sup>, CS 1999<sup>20</sup>, CS 2010<sup>21</sup> și CS 2022<sup>22</sup> - numărul paragrafului fiind marcat între [...])**

Dacă pe timpul Războiului Rece valabilitatea Conceptelor a fost variabilă (2, 5, 10, respectiv aproape 25 de ani), după 1991 s-a instalat practica elaborării documentului cu o perspectivă de aproximativ o decadă (8, 11, respectiv 12 ani), cu toate că aceasta nu este prevăzută și definită ca atare în corpul documentelor.

Elaborarea unui nou Concept este o sarcină dificilă pentru Alianță, mai ales pentru că prezintă o dilemă în ceea ce privește nivelul de noutate: în situația reafirmării *statu-quo*-ului, procesul poate fi considerat pierdere de timp și efort; la extrema cealaltă, dacă produce prea multe schimbări, devine dificilă armonizarea pozițiilor membrilor

sau relevanța organizației poate fi pusă la îndoială. Astfel, Jamie Shea, fost asistent pentru provocări emergente al Secretarului General al NATO, argumentează că cele mai de succes strategii tind să fie cele care găsesc un echilibru între continuitate și schimbare<sup>23</sup>.

Din această perspectivă, analiza comparativă a Conceptelor ilustrează o continuitate în abordarea extinsă a securității, prin recunoașterea importanței factorilor politici, economici, sociali și de mediu, specifică perioadei de acalmie strategică și proliferării riscurilor neconvenționale, în timp ce principalele schimbări sunt reflectate la nivelul sarcinilor de

bază, derivate din înțelegerea mediului strategic.

Cele două Concepte (1991 și 1999) din prima decadă post-Război Rece prezintă multe similitudini, inclusiv în ceea ce privește perspectiva asupra sistemului internațional, documentul din 1999 fiind mai degrabă o actualizare, în acord cu evoluțiile din anii '90, precum implicarea Alianței în operațiile de menținere a păcii și demersurile statelor central-est europene de aderare la organizație. Primele trei sarcini fundamentale ale NATO sunt menținute, fiind doar sintetizate în cuvinte-cheie (securitate; consultare; descurajare și apărare), în timp ce a patra sarcină este revizuită și transformată din „menținerea echilibrului strategic” în două elemente considerate interconectate – managementul crizelor și parteneriatele.

Conceptul Strategic din 2010 („Angajament Activ, Apărare Modernă”) a marcat o schimbare fundamentală de filosofie atât în ceea ce privește redactarea, printr-un proces de consultare ce a durat aproape doi ani<sup>24</sup>, cât și prin forma și conținutul acestuia, documentul fiind mult mai suplu decât precedentele (38 de paragrafe, comparativ cu 59, respectiv 65). Așa cum rezultă din titlu, documentul din 2010 prevede un rol mai crescut al Alianței în gestionarea crizelor, ca o consecință directă a atacurilor teroriste de la 11 septembrie 2001. Sarcinile de bază sunt stabilite pe următoarele coordonate: (1) apărare colectivă; (2) managementul crizelor; (3) securitate prin cooperare (controlul armamentelor, dezarmare și neproliferare; politica „ușilor deschise”; parteneriate). Practic, Conceptul din 2010 prelua cele două noi atribuții introduse în documentul strategic din 1999, oferindu-le aceeași importanță ca misiunile specifice art. 5.

În general, descrierea mediului de securitate reflectă cu acuratețe viziunea comună a statelor membre privind riscurile și provocările la momentul aprobării Conceptelor, dar capacitatea de previziune poate fi deseori pusă sub semnul întrebării.

De regulă, Conceptul Strategic, în sine, nu aduce transformări revoluționare, ci mai degrabă înglobează practica ultimilor ani. Astfel, de multe ori, schimbarea în NATO este generată de jos în

sus (*bottom-up*), în funcție de evenimente-cheie și nu de documente strategice<sup>25</sup>, exemplele notabile fiind implicarea în operațiile *out-of-area*, respectiv reconcentrarea asupra apărării teritoriale după anexarea Peninsulei Crimeea de către F.Rusă în 2014. O critică adusă Conceptelor ține, așadar, de perisabilitatea acestora, întrucât sunt depășite rapid de evenimente, care impun, la rândul lor, noi adaptări și transformări. De pildă, acțiunile F.Ruse începând cu anul 2014 au schimbat fundamental mediul de securitate, NATO adaptându-se rapid pe dimensiunea militară, prin reasigurarea aliaților de pe flancul estic și stabilirea unei prezențe înaintate pe acest flanc, moment care a generat numeroase apeluri pentru actualizarea Conceptului Strategic. Suplimentar, la nivel militar au fost adoptate Strategia Militară (2019), Conceptul de descurajare și apărare (2020) și Conceptul de ducere a războiului (2021).

În acest context, dar și având în vedere o serie de divergențe interne, NATO a lansat un Proces de Reflecție privind modalitatea în care trebuie să se adapteze în perspectiva anilor 2030, din care a rezultat necesitatea unui nou Concept Strategic<sup>26</sup>, adoptat în cele din urmă la Summit-ul de la Madrid (2022).

## CONCEPTUL STRATEGIC 2022 – ÎNTRE CONTINUITATE ȘI SCHIMBARE

Summit-ul recent de la Madrid a fost descris drept „transformator” de către Secretarul General al Alianței, respectiv „istoric” de către președintele SUA, Joe Biden<sup>27</sup>, mai ales prin prisma adoptării noului Concept Strategic și a deciziilor referitoare la implementarea Agendei NATO 2030, agreată la summit-ul anterior (iunie 2021, Bruxelles). Aprobarea unui document de o asemenea importanță în contextul crizei de securitate generate de invazia rusă în Ucraina, eveniment care a testat soliditatea relației transatlantice, este considerată un simbol de coeziune în sine, indiferent de conținut.

Din punct de vedere structural, actualul Concept cuprinde patru părți de dimensiuni diferite (Misiune și Principii – cinci paragrafe; Mediul Strategic – 14 paragrafe; Sarcini de bază

– 27 de paragrafe; Asigurarea succesului continuu al Alianței – trei paragrafe). Documentul conține atât elemente de continuitate doctrinară, cât și elemente de noutate pe ambele dimensiuni (la descrierea mediului de securitate, respectiv pe dimensiunea operațională), principalele prevederi fiind sintetizate în Tabelul nr. 2.

Conceptul Strategic 2022 reafirmă misiunile și principiile în baza cărora funcționează Alianța, precum și angajamentul ferm pentru apărarea aliaților. Suplimentar, documentul întărește poziția centrală a NATO în cadrul relației transatlantice, nu doar prin consultare, în linie cu art. 4 din Tratat sau cu mențiunile din Conceptele

Capitol	Idei principale
<b>Misiune și Principii [1-6]</b>	<ul style="list-style-type: none"> <li>• Angajamentul ferm pentru apărarea aliaților [1];</li> <li>• Valorile comune [2];</li> <li>• NATO – forum transatlantic unic, esențial și indispensabil pentru consultare, coordonare și acțiune [3];</li> <li>• Întărirea rezilienței naționale și colective, precum și consolidarea avantajului tehnologic [5].</li> </ul>
<b>Mediul Strategic [7-19]</b>	<ul style="list-style-type: none"> <li>• Zona euro-atlantică nu este în pace, fiind marcată de competiție strategică, instabilitate permanentă și șocuri recurente [6];</li> <li>• Rusia – „cea mai semnificativă și directă amenințare” [8-9];</li> <li>• Terorismul – „cea mai directă amenințare asimetrică” [10];</li> <li>• Conflictele, fragilitatea și instabilitatea din Africa și Orientul Mijlociu [11-12];</li> <li>• China – „provocare” la adresa intereselor, securității și valorilor Alianței [13-14];</li> <li>• Spațiul cibernetic – „disputat în orice moment” [15];</li> <li>• Impactul tehnologiilor emergente și disruptive [16-17];</li> <li>• Erodarea sistemului de control al armamentelor, dezarmării și neproliferării nucleare [18];</li> <li>• Schimbările climatice – „impact profund asupra securității Alianței” [19].</li> </ul>
<b>Sarcini de bază [20-46]</b>	<p><i>1. Apărare și descurajare [20-34]:</i></p> <ul style="list-style-type: none"> <li>• Adaptarea și reformarea posturii [20-22];</li> <li>• Posibilitatea invocării art. 5 pentru acțiuni ostile în mediul cibernetic și spațial [25], precum și pentru amenințări hibride [27];</li> <li>• Contracararea terorismului – integrată în „abordarea 360°” [34].</li> </ul> <p><i>2. Prevenirea și managementul crizelor [35-39]:</i></p> <ul style="list-style-type: none"> <li>• Menținerea capacităților de implicare în gestionarea crizelor și integrare cu eforturile civile [35-36];</li> <li>• Creșterea eforturilor de anticipare [38];</li> <li>• Necesitatea parteneriatelor [37, 39].</li> </ul> <p><i>3. Securitate prin cooperare [40-46]:</i></p> <ul style="list-style-type: none"> <li>• Reafirmarea „politicii ușilor deschise” [40-41];</li> <li>• Parteneriatele bazate pe dialog politic și cooperare practică [42, 44];</li> <li>• UE – „partener esențial” [43];</li> <li>• M.Neagră și Balcanii de Vest – zone de „importanță strategică pentru Alianță” [45].</li> </ul>
<b>Asigurarea succesului [47-49]</b>	<ul style="list-style-type: none"> <li>• Investiții continue pentru asigurarea resurselor necesare.</li> </ul>

Tabel 2: Sinteza principalelor prevederi din Conceptul Strategic 2022 al NATO



post-1991, ci și în domeniile de coordonare și acțiune pe toate subiectele care pot afecta securitatea aliaților<sup>28</sup>.

În urma aprobării noului Concept, atenția principală s-a concentrat asupra viziunii Alianței în ceea ce privește mediul strategic, influențată și de actuala criză de securitate, elocventă în acest sens fiind fraza „zona euro-atlantică nu este în pace”<sup>29</sup>. Pe această linie, strategia consemnează trei elemente din care derivă amenințări globale și interconectate: competiția strategică, instabilitatea generalizată și șocurile recurente. În acest tip de document, ordinea cuvintelor nu este una întâmplătoare, ci oglindește percepția statelor membre asupra amenințărilor.

După descrierea generală a mediului de securitate, Conceptul Strategic 2022 menționează „actorii autoritari”<sup>30</sup>, stabilind rolul politic al Alianței și impregnând astfel o dimensiune ideologică (sisteme democratice vs. sisteme autoritare) competiției dintre marile puteri, în care NATO se autodefineste drept apărător al ordinii internaționale bazate pe reguli.

De departe, cea mai radicală schimbare este reprezentată de percepția față de Federația Rusă – considerată drept „cea mai semnificativă și directă amenințare”, marcând o tranziție fundamentală de la logica cooperării (în calitate de parteneri) care a dominat anteriorul Concept Strategic (2010). Prin raportare la F.Rusă, actualul Concept stipulează întărirea posturii de descurajare și apărare, consolidarea rezilienței aliaților și sprijinul acordat partenerilor pentru contracararea influenței maligne și a agresiunii. Ca limbaj, acesta este considerat „specific Războiului Rece”<sup>31</sup>, dar, în același timp, mult mai realist față de optimismul precedentului concept<sup>32</sup>.

Pe fondul intenției declarate a liderilor de la Moscova de modificare a arhitecturii europene de securitate, statele membre agreează că primordială este contracararea intențiilor ostile ale F.Ruse, problema fiind prioritățile secundare, care diferă între capitalele aliate<sup>33</sup>. În această situație, noul Concept Strategic poate fi revelator, întrucât, în continuare, documentul prezintă amenințarea asimetrică generată de

terorism, aflată în strânsă legătură cu conflictele, fragilitatea și instabilitatea specifice Africii și Orientului Mijlociu. Ca urmare, acest Concept acomodează interesele divergente ale statelor aliate pe acest subiect, conferind un loc prioritar problemelor din vecinătatea sudică.

Stabilirea unei strategii de abordare a relațiilor cu R.P. Chineză este, de câțiva ani, o prioritate a agendei transatlantice, inclusiv la nivelul NATO. După ce China a fost menționată, în premieră, în Declarația finală a Summit-ului aniversar de la Londra (3-4 decembrie 2019), ca generând „oportunități și provocări”<sup>34</sup>, noul Concept Strategic se axează mai mult pe a doua dimensiune, prin trimitere la instrumentele politice, economice și militare utilizate de Beijing pentru extinderea influenței la nivel global, precum și controlul asupra sectoarelor cheie<sup>35</sup>. În fapt, Conceptul preia aproape *integral* cele două paragrafe referitoare la R.P. Chineză din Comunicatul Summit-ului de la Bruxelles din 14 iunie 2021<sup>36</sup>, neaducând o schimbare de optică, ci doar o formalizare suplimentară a poziției deja adoptate. Din această perspectivă, Alianța se declară deschisă pentru o „relație constructivă” cu autoritățile de la Beijing, dar nu este clar formatul acesteia, de-a lungul timpului fiind vehiculată inclusiv crearea unui Consiliu NATO-China<sup>37</sup>, după modelul celui cu F.Rusă. Având în vedere lipsa rezultatelor acestuia din urmă sau chiar a eșecului, precum și lipsa disponibilității Beijingului pentru un dialog cu NATO, ca actor de sine stătător, perspectivele pentru formarea unui astfel de organism sunt reduse.

La descrierea mediului de securitate mai sunt incluse, de asemenea, și provocările specifice spațiului cibernetic, riscurile generate/facilitate de tehnologiile emergente și disruptive, precum și schimbările climatice, ca „multiplicator al crizelor și amenințărilor”, toate acestea cu impact transversal asupra sarcinilor de bază ale Alianței<sup>38</sup>.

Chiar dacă atenția, pe termen scurt, a fost acordată secțiunii dedicate evaluării mediului strategic, cheia de boltă a noului Concept Strategic este reprezentată de menționarea apărării colective drept „scopul cheie și cea

mai mare responsabilitate”<sup>39</sup>. Astfel, apărarea colectivă a primit un rol de tip umbrelă, care înglobează cele trei sarcini de bază care sunt, în mare parte, menținute din anteriorul Concept (2010), dar, în același timp, reformulate și nuanțate: (1) descurajare și apărare; (2) prevenirea și managementul crizelor; (3) securitate prin cooperare.

Deși în Conceptul Strategic 2010 apărarea colectivă, pe de o parte, și descurajarea și apărarea, pe de altă parte, erau tratate împreună și interșanjabil, noul Concept le separă, dar fără să definească diferența dintre acestea. Totuși, din punct de vedere conceptual, granița dintre ambele noțiuni este una fină, descurajarea și apărarea putând fi înțelese, în noua viziune, drept coloana vertebrală a apărării colective, celelalte două sarcini fiind complementare și nu izolate una de cealaltă.

Prevalența primei sarcini în Conceptul Strategic 2022 este confirmată, din punct de vedere cantitativ, de întinderea de care beneficiază mini-sectiunea dedicată, acoperind aproximativ o treime din întregul document și fiind de trei ori mai mare decât spațiul alocat celorlalte sarcini de bază. Însă această nuanță intră mai degrabă în logica continuității, ca parte a procesului de revenire la misiunea de bază, după anexarea Pen. Crimeea de către F.Rusă în 2014, reconcentrare asupra apărării teritoriale<sup>40</sup> și întărire a posturii de descurajare și apărare, nefiind astfel strict generată de războiul ruso-ucrainean din ultimele luni.

În ceea ce privește postura de descurajare și apărare, actualul Concept aduce, într-adevăr, și o serie de modificări. În primul rând, este schimbată compoziția acesteia, fiind adăugate capacitățile cibernetice și spațiale la sintagma deja consacrată, prezentă în aproape toate documentele din ultimii 10 ani: „combinație adecvată de capacități nucleare, convenționale și de apărare antirachetă”<sup>41</sup>. În al doilea rând, documentul consacră posibilitatea invocării art. 5 pentru acțiunile ostile din aceste două medii operaționale, precum și pentru acțiunile de tip hibrid<sup>42</sup>.

Cel mai important, Conceptul Strategic 2022 pune bazele pentru conceptul de „apărare înaintată” (*forward defence*), cu forțe dislocate și echipamente pre-poziționate pe flancul estic, într-o manieră mult mai consolidată decât prezența înaintată. Măsurile pe această linie trebuie citite în paralel cu Declarația Summit-ului de la Madrid, textul Conceptului rezumându-se la stabilirea unei noi filozofii pentru întreaga postură. Ca atare, Declarația Summit-ului prezintă noile standarde pentru descurajare și apărare, precum ridicarea grupurilor de luptă la nivel de brigadă, respectiv transformarea Forței de Răspuns a NATO într-un nou Model de Forțe al NATO (*NATO Force Model*)<sup>43</sup>.

În privința noului Model de Forțe, acesta va fi dezvoltat până în anul 2023, se va baza pe forțe specifice pentru apărarea unor aliați și va avea trei niveluri de reacție: (1) 100.000 de militari în maximum 10 zile; (2) 200.000 în 10-30 de zile; (3) cel puțin 500.000 în maximum 180 de zile<sup>44</sup>. În consecință, schimbarea este una fundamentală, prin trecerea de la prezența înaintată, care servea drept garanție pentru un eventual răspuns aliat (*tripwire*), la o forță solidă, capabilă de asigurare a descurajării prin apărare. Cu toate acestea, denumirea de „apărare înaintată” continuă să caracterizeze o viziune vest-eurocentristă, fiind impropriu denumirea „înaintată” atunci când se face referire la propriul teritoriu (al Alianței în sine).

Dificultățile pe care NATO le va întâmpina pe acest palier nu țin neapărat de numărul forțelor, dislocarea lor pe flancul estic fiind considerată chiar partea ușoară a problemei<sup>45</sup>. În schimb, adaptarea planurilor de apărare pentru concentrarea asupra „războiului de intensitate mare, multi-domeniu, împotriva competitorilor nucleari”<sup>46</sup>, cu mai puțină atenție acordată managementului crizelor, contra-insurgenței și operațiilor de stabilizare, aspect care ar trebui să influențeze dezvoltarea și achiziția de capacități, reprezintă adevărata parte spinoasă a implementării noilor prevederi<sup>47</sup>. Totodată, rămâne de văzut în ce măsură noul Concept Strategic și „lecțiile învățate” ale războiului din Ucraina vor genera o revizuire a documentelor operaționale<sup>48</sup>.



În ceea ce privește cea de-a doua sarcină – crizele ce pot afecta securitatea euro-atlantică, textul Conceptului reflectă schimbările din ultimii ani (ex.: retragerea din Afganistan), accentul fiind pus în principal pe componenta de prevenire, în paralel cu menținerea capacităților ce ar putea fi dislocate la nevoie. Față de Conceptul Strategic din 2010, care stabilea clar că această sarcină se referă la acțiunile din afara teritoriului Alianței, actualul Concept face inclusiv trimitere la o dimensiune internă a managementului crizelor, prin integrarea cu sistemele civile de răspuns la crize<sup>49</sup>, probabil după lecțiile pandemiei de COVID-19. Suplimentar, secțiunea dedicată crizelor se întrepătrunde cu cea a parteneriatelor, întrucât documentul pune accent pe dezvoltarea capacităților partenerilor de a gestiona crizele.

Pe latura securității prin cooperare, Conceptul Strategic 2022 aduce, de asemenea, transformări. După ce în 2010 controlul armamentelor, dezarmarea și neproliferarea ocupau un loc central pentru această sarcină de bază, în textul documentului din acest an prevederile pe acest palier sunt diluate și tratate fugitiv la primul pilon, concentrându-se pe reducerea riscurilor și creșterea măsurilor de consolidare a încrederii, în relațiile cu F.Rusă și R.P. Chineză.<sup>50</sup>

Cu privire la politica „ușilor deschise”, actualul Concept reafirmă principiul neimplicării unui stat terț în decizia lărgirii NATO, precum și interdependența dintre securitatea aliaților și a statelor aspirante, context în care Alianța va continua sprijinul acestora în vederea întăririi rezilienței, în această direcție fiind nominalizate Ucraina, Georgia și Bosnia și Herțegovina<sup>51</sup>.

Totodată, parteneriatele, cea de-a doua componentă a securității prin cooperare din Concept, reprezintă una dintre cele mai ambițioase părți din tot documentul, fiind prevăzută sporirea dialogului și a cooperării practice cu UE și cu state din zona Mării Negre, Balcanilor de Vest, Orientului Mijlociului, Sahel, Nordului Africii și, nu în cele din urmă, zonei Indo-Pacific. Relevantă în acest sens este chiar prezența liderilor Japoniei, Coreii de Sud, Australiei și Noii Zeelande la lucrările Summit-ului. Pe acest palier trebuie ținut cont că, la debutul procesului de „reflecție

strategică”, Secretarul General al NATO, Jens Stoltenberg, a insistat asupra dezvoltării unei abordări globale a NATO, aceasta fiind adesea vehiculată în relație cu parteneriatele. Însă, în Conceptul Strategic 2022 această dimensiune globală a NATO este menționată o singură dată, în Prefață, ca „perspectivă globală”, parte care nu este neapărat inclusă în document.

În plus, în relația cu UE, considerat partenerul special și esențial al Alianței, se menționează ariile de cooperare, o absență notabilă fiind securitatea maritimă, care se afla în topul agendei în anul 2016. Noul Concept stabilește, de asemenea, și perspectiva NATO asupra duplicării eforturilor de apărare, subliniind necesitatea implicării statelor non-UE în eforturile europene destinate apărării<sup>52</sup>.

Un alt domeniu care este tratat *in extenso* în document este reziliența, față de care unii autori au pledat inclusiv pentru desemnarea sa drept a patra sarcină de bază a Alianței<sup>53</sup>. Cu toate că ar fi existat argumente pentru un astfel de curs de acțiune, art. 3 al Tratatului fiind fundamentul acestei susțineri, statele membre au optat pentru abordarea rezilienței ca o „responsabilitate națională și un angajament asumat la nivel aliat”<sup>54</sup>, condiție necesară pentru acțiunile subsumate celor trei sarcini de bază, fiind prevăzute atât măsuri interne, proprii organizației și sistemelor de securitate aliate, cât și în relație cu partenerii.

## CONCLUZII: NATO POST-MADRID

Conceptul Strategic 2022 încheie un ciclu de reflecție strategică la nivelul NATO și marchează începutul unei noi etape, de care depinde chiar credibilitatea Alianței: implementarea prevederilor noului document programatic. Chiar dacă mare parte din textul Conceptului este scris la timpul viitor, traducerea cuvintelor în acțiune ar trebui să fie relativ ușoară, întrucât, așa cum a arătat acest articol, multe dintre noile prevederi sunt, de fapt, formalizarea măsurilor deja implementate în ultimii câțiva ani sau chiar revitalizarea unor idei puse în practică în trecut.

În această logică, dilema continuitate *versus* schimbare pare să încline în prima direcție, însă această afirmație este parțial adevărată.

Noul Concept Strategic este, într-adevăr, inovator în multe privințe, cum ar fi descrierea mediului de securitate, unde schimbarea fundamentală față de conceptele post-1991 se resimte în tonalitate, ceea ce indică și ar impune, deopotrivă, asumarea unui rol mult mai asertiv al Alianței. În plus, documentul rupe echilibrul clasic dintre sarcini, solidificând ideea revenirii NATO la misiunea de bază (*back to the basics*) – apărare colectivă și, în subsidiar, descurajare și apărare – și diminuând,

chiar semnificativ, atenția acordată prevenirii și managementului crizelor, respectiv a securității prin cooperare.

Dintr-o perspectivă a terminologiei utilizate, Conceptul Strategic 2022 este, în sine, un amalgam de concepte, în care este inclus câte puțin din toate. Pe alocuri, sunt prevăzute măsuri concrete, în timp ce alte subiecte sunt menționate sumar. În ambele cazuri, există spațiu de manevră în privința implementării.

## BIBLIOGRAFIE

1. ALBERQUE William, "The new NATO Strategic Concept and the end of arms control", The International Institute for Strategic Studies, 30.06.2022. Disponibil online la <https://www.iiss.org/blogs/analysis/2022/06/the-new-nato-strategic-concept-and-the-end-of-arms-control> și accesat la data de 21.07.2022.
2. ARNOLD Ed., "New Concepts but Old Problems: NATO's New Strategic Concept", Royal United Services Institute, 01.07.2022. Disponibil online la <https://rusi.org/explore-our-research/publications/commentary/new-concepts-old-problems-natos-new-strategic-concept> și accesat la data de 09.07.2022.
3. BECKER Jordan, Michael Duda și Douglas Lute, "From context to concept: history and strategic environment for NATO's 2022 strategic concept", *Defence Studies*, 2022, p. 2.
4. DUȚĂ Adrian-Ion și Vasile Crețu, "Quo Vadis NATO? Procesul de Reflecție NATO 2030 și drumul către un nou Concept Strategic", *Infosfera*, Vol. XII, No. 1, 2021, pp. 13-24.
5. ETERSEN Nikolaj, "Bargaining Power among Potential Allies: Negotiating the North Atlantic Treaty, 1948-49", *Review of International Studies*, vol. 12, nr. 3, 1986, pp. 187-203.
6. FORSTER Anthony și William Wallace, "What is NATO for?", *Survival*, vol. 43, nr. 4, 2001, pp. 107-122.
7. HAMILTON Daniel S., "One Plus Four: What NATO's New Strategic Concept Should Say and How to Achieve It", *Orbis*, Vol. 66, Issue 1, 2022, p. 26-34.
8. KAMP Karl-Heinz, *Why NATO Needs a New Strategic Concept*, NATO Defense College, 2016.
9. KUPCHAN Charles A., "NATO's Hard Road Ahead", *Foreign Affairs*. 29.06.2022. Disponibil online la <https://www.foreignaffairs.com/articles/ukraine/2022-06-29/natos-hard-road-ahead> și accesat la data de 13.07.2022.
10. MARRONE Alessandro, "NATO's New Strategic Concept: Novelties and Priorities", Istituto Affari Internazionali, July 2022. Disponibil online la <https://www.iai.it/en/pubblicazioni/natos-new-strategic-concept-novelties-and-priorities> și accesat la data de 15.07.2022.
11. NATO Archives, "Defence Committee". Disponibil online la <https://archives.nato.int/defence-committee-2> și accesat la data de 17.07.2022.
12. NATO Multimedia, "NATO Experts – What is NATO's Strategic Concept?", 14.06.2022. Disponibil online la <https://www.natomultimedia.tv/app/asset/666020> și accesat la data de 21.07.2022.
13. NATO, "Active Engagement, Modern Defence. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation adopted by Heads of State and Government in Lisbon". Disponibil la [https://www.nato.int/cps/en/natohq/official\\_texts\\_68580.htm](https://www.nato.int/cps/en/natohq/official_texts_68580.htm) și accesat la data de 07.07.2022.
14. NATO, "Brussels Summit Communiqué. Issued by the Heads of State and Government

- participating in the meeting of the North Atlantic Council in Brussels 14 June 2021". Disponibil online la [https://www.nato.int/cps/en/natohq/news\\_185000.htm](https://www.nato.int/cps/en/natohq/news_185000.htm) și accesat la data de 20.07.2022.
15. NATO, "London Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in London 3-4 December 2019". Disponibil online la [https://www.nato.int/cps/en/natohq/official\\_texts\\_171584.htm?selectedLocale=en](https://www.nato.int/cps/en/natohq/official_texts_171584.htm?selectedLocale=en) și accesat la data de 20.07.2022.
16. NATO, "Madrid Summit Declaration. Issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Madrid 29 June 2022". Disponibil online la [https://www.nato.int/cps/en/natohq/official\\_texts\\_196951.htm](https://www.nato.int/cps/en/natohq/official_texts_196951.htm) și accesat la data de 24.07.2022.
17. NATO, "NATO 2022 Strategic Concept". Disponibil online la [https://www.nato.int/nato\\_static\\_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf](https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf) și accesat la data de 01.07.2022.
18. NATO, "New NATO Force Model", 29.06.2022. Disponibil online la [https://www.nato.int/nato\\_static\\_fl2014/assets/pdf/2022/6/pdf/220629-infographic-new-nato-force-model.pdf](https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/220629-infographic-new-nato-force-model.pdf) și accesat la data de 17.07.2022.
19. NATO, "Remarks by NATO Secretary General Jens Stoltenberg and US President Joe Biden at the start of the 2022 NATO Summit", 29.06.2022. Disponibil la [https://www.nato.int/cps/en/natohq/opinions\\_197374.htm](https://www.nato.int/cps/en/natohq/opinions_197374.htm) și accesat la data de 15.07.2022.
20. NATO, "Strategic Concepts", 18.07.2022 (ultima actualizare). Disponibil la [https://www.nato.int/cps/en/natohq/topics\\_56626.htm](https://www.nato.int/cps/en/natohq/topics_56626.htm) și accesat la data de 20.07.2022.
21. NATO, "The Alliance's New Strategic Concept (1991)". Disponibil online la [https://www.nato.int/cps/en/natohq/official\\_texts\\_23847.htm](https://www.nato.int/cps/en/natohq/official_texts_23847.htm) și accesat la data de 04.07.2022.
22. NATO, "The Alliance's Strategic Concept (1999)". Disponibil la [https://www.nato.int/cps/en/natohq/official\\_texts\\_27433.htm](https://www.nato.int/cps/en/natohq/official_texts_27433.htm) și accesat la data de 04.07.2022.
23. North Atlantic Defense Committee, "Directive to the Military Committee", D.C.1/2, 25 October 1949. Disponibil online la [https://archives.nato.int/uploads/r/null/9/9/99044/DC\\_001\\_2\\_ENG\\_PDP.pdf](https://archives.nato.int/uploads/r/null/9/9/99044/DC_001_2_ENG_PDP.pdf) și accesat la data de 21.07.2022.
24. North Atlantic Defense Committee, "The Strategic Concept for the Defense of the North Atlantic Area", D.C.6/1, 1 December 1991. Disponibil online la <https://www.nato.int/docu/stratdoc/eng/a491201a.pdf> și accesat la data de 12.07.2022.
25. PAVEL Barry și Ian Brzezinski, "It's Time for a NATO-China Council", *DefenseOne*, 21.08.2019. Disponibil online la <https://www.defenseone.com/ideas/2019/08/its-time-nato-china-council/159326/> și accesat la data de 20.07.2022.
26. RINGSMOSE Jens și Sten Rynning, *Come Home, NATO? The Atlantic Alliance's New Strategic Concept*, Danish Institute for International Studies/DIIS, Report, 2009.
27. RINGSMOSE Jens și Sten Rynning, "Now for the Hard Part: NATO's Strategic Adaptation to Russia", *Survival*, vol. 59, nr. 3, 2017, pp. 129-146.
28. RINGSMOSE Jens și Sten Rynning, *NATO's New Strategic Concept: A Comprehensive Assessment*, DIIS Report, 2011.
29. SHEA Jamie, "Why does NATO's new Strategic Concept matter?", *Atlantisch Perspectief*, Vol. 34, Nr. 8, 2010, p. 8-13.
30. SLOAN Stanley R., "Negotiating Article 5", *NATO Review*, 01.06.2006. Disponibil online la <https://www.nato.int/docu/review/articles/2006/06/01/negotiating-article-5/index.html> și accesat la data de 24.07.2022.
31. SOCOR Vladimir, "NATO Summit: New Strategic Concept Brings New Realism About Russia", Jamestown Foundation, 06.07.2022. Disponibil online la <https://jamestown.org/program/nato-summit-new-strategic-concept-brings-new-realism-about-russia-part-one/> și accesat la data 17.07.2022.
32. "The North Atlantic Treaty", Washington D.C., 4 April 1949. Disponibil online la <https://www.nato.int/docu/treaty/treaty.htm> și accesat la data de 20.07.2022.

nato.int/cps/en/natolive/official_texts_17120.htm și accesat la data de 07.07.2022.	34. WEBBER Mark, Lawrence Chalmer, Martayn Van de Wall și Hazumu Yano, "The Strategic Concept and strategic coherence", <i>Defence Studies</i> , 2022.
33. TOWNSEND Jim și Anca Agachi, "Build resilience for an era of shocks", Atlantic Council, 14.10.2020. Disponibil online la <a href="https://www.atlanticcouncil.org/content-series/nato20-2020/build-resilience-for-an-era-of-shocks/">https://www.atlanticcouncil.org/content-series/nato20-2020/build-resilience-for-an-era-of-shocks/</a> și accesat la data de 04.07.2022.	35. WIEBES Cees și Bert Zeeman, "The Pentagon Negotiations March 1948: The Launching of the North Atlantic Treaty", <i>International Affairs</i> , vol. 59, nr. 3, 1983, p. 351–63.
	36. ZULEAN Marian (coord.), <i>Strategiile de securitate națională</i> , București, Ed. Tritonic, 2017.

- <sup>1</sup> Jens Ringsmose și Sten Rynning, *Come Home, NATO? The Atlantic Alliance's New Strategic Concept*, Danish Institute for International Studies/DIIS, Report, 2009, p. 6.
- <sup>2</sup> "The North Atlantic Treaty", Washington D.C., 4 April 1949. Disponibil online la [https://www.nato.int/cps/en/natolive/official\\_texts\\_17120.htm](https://www.nato.int/cps/en/natolive/official_texts_17120.htm) și accesat la data de 07.07.2022.
- <sup>3</sup> Idem.
- <sup>4</sup> Anthony Forster și William Wallace, "What is NATO for?", *Survival*, vol. 43, nr. 4, 2001, p. 108.
- <sup>5</sup> Pentru detalii suplimentare despre procesul de negociere a Tratatului Nord-Atlantic, vezi Wiebes Cees și Bert Zeeman, "The Pentagon Negotiations March 1948: The Launching of the North Atlantic Treaty", *International Affairs*, vol. 59, nr. 3, 1983, p. 351–363, și Nikolaj Etersen, "Bargaining Power among Potential Allies: Negotiating the North Atlantic Treaty, 1948-49", *Review of International Studies*, vol. 12, nr. 3, 1986, p. 187-203. Pentru o sinteză a negocierilor privind art. 5, vezi Stanley R. Sloan, "Negotiating Article 5", *NATO Review*, 01.06.2006. Disponibil online la <https://www.nato.int/docu/review/articles/2006/06/01/negotiating-article-5/index.html> și accesat la data de 24.07.2022.
- <sup>6</sup> Comitetul Apărării a funcționat între anii 1949-1952, fiind desființat la prima reorganizare a Consiliului Nord-Atlantic. (NATO Archives, "Defence Committee". Disponibil online la <https://archives.nato.int/defence-committee-2> și accesat la data de 17.07.2022).
- <sup>7</sup> North Atlantic Defense Committee, "Directive to the Military Committee", D.C.1/2, 25 October 1949, p. 28. Disponibil online la [https://archives.nato.int/uploads/r/null/9/9/99044/DC\\_001\\_2\\_ENG\\_PDP.pdf](https://archives.nato.int/uploads/r/null/9/9/99044/DC_001_2_ENG_PDP.pdf) și accesat la data de 21.07.2022.
- <sup>8</sup> North Atlantic Defense Committee, "The Strategic Concept for the Defense of the North Atlantic Area", D.C.6/1, 1 December 1991, para. 4, p. 3. Disponibil online la <https://www.nato.int/docu/stratdoc/eng/a491201a.pdf> și accesat la data de 12.07.2022.
- <sup>9</sup> Karl-Heinz Kamp, *Why NATO Needs a New Strategic Concept*, NATO Defense College, 2016, p. 1.
- <sup>10</sup> NATO, "Strategic Concepts", 18.07.2022 (ultima actualizare). Disponibil la [https://www.nato.int/cps/en/natohq/topics\\_56626.htm](https://www.nato.int/cps/en/natohq/topics_56626.htm) și accesat la data de 20.07.2022.
- <sup>11</sup> Jens Ringsmose și Sten Rynning. *Op. cit.*, p. 7-8.
- <sup>12</sup> Jordan Becker, Michael Duda și Douglas Lute, "From context to concept: history and strategic environment for NATO's 2022 strategic concept", *Defence Studies*, 2022, p. 2.
- <sup>13</sup> Conceptul Strategic din 1967 este singurul care nu a fost aprobat în Consiliul Nord-Atlantic (NAC), fiind adoptat la nivelul Comitetului de Planificare a Apărării, care deținea aceeași autoritate ca NAC. Cu toate acestea, statele membre rămân factorii decizionali, chiar și la acest nivel.
- <sup>14</sup> NATO, "Strategic Concepts", 18.07.2022 (ultima actualizare). Disponibil la [https://www.nato.int/cps/en/natohq/topics\\_56626.htm](https://www.nato.int/cps/en/natohq/topics_56626.htm) și accesat la data de 20.07.2022.
- <sup>15</sup> Mark Webber, Lawrence Chalmer, Martayn van de Wall și Hazumu Yano, "The Strategic Concept and strategic coherence", *Defence Studies*, 2022, p. 2.
- <sup>16</sup> Marian Zulean, „Elaborarea strategiilor de securitate națională: concepte, metode și tehnici de formulare”, în Marian Zulean (coord.), *Strategiile de securitate națională*, București, Editura Tritonic, 2017, p. 26.



- <sup>17</sup> NATO, "Strategic Concepts", 18.07.2022 (ultima actualizare).
- <sup>18</sup> NATO Multimedia, "NATO Experts – What is NATO's Strategic Concept?", 14.06.2022. Disponibil online la <https://www.natomultimedia.tv/app/asset/666020> și accesat la data de 21.07.2022.
- <sup>19</sup> NATO, "The Alliance's New Strategic Concept (1991)". Disponibil online la [https://www.nato.int/cps/en/natohq/official\\_texts\\_23847.htm](https://www.nato.int/cps/en/natohq/official_texts_23847.htm) și accesat la data de 04.07.2022.
- <sup>20</sup> NATO, "The Alliance's Strategic Concept (1999)". Disponibil la [https://www.nato.int/cps/en/natohq/official\\_texts\\_27433.htm](https://www.nato.int/cps/en/natohq/official_texts_27433.htm) și accesat la data de 04.07.2022.
- <sup>21</sup> NATO, "Active Engagement, Modern Defence. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation adopted by Heads of State and Government in Lisbon". Disponibil la [https://www.nato.int/cps/en/natohq/official\\_texts\\_68580.htm](https://www.nato.int/cps/en/natohq/official_texts_68580.htm) și accesat la data de 07.07.2022.
- <sup>22</sup> NATO, "NATO 2022 Strategic Concept". Disponibil online la [https://www.nato.int/nato\\_static\\_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf](https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf) și accesat la data de 01.07.2022.
- <sup>23</sup> Jamie Shea, "What does a New Strategic Concept do for NATO", p. 25, în Jens Ringsmose și Sten Rynning, *NATO's New Strategic Concept: A Comprehensive Assessment*, DIIS Report, 2011.
- <sup>24</sup> Klaus Wittman, "An Alliance for the 21st Century? Reviewing NATO's New Strategic Concept", p. 31, în Jens Ringsmose și Sten Rynning, *NATO's New Strategic Concept: A Comprehensive Assessment*, DIIS Report, 2011.
- <sup>25</sup> Jamie Shea, "Why does NATO's new Strategic Concept matter?", *Atlantisch Perspectief*, Vol. 34, Nr. 8, 2010, p. 8.
- <sup>26</sup> Pentru mai multe detalii privind Procesul de Reflecție NATO 2030, vezi Adrian-Ion Duță și Vasile Crețu, "Quo Vadis NATO? Procesul de Reflecție NATO 2030 și drumul către un nou Concept Strategic", *Infosfera*, Vol. XII, Nr. 1, 2021, pp. 13-24.
- <sup>27</sup> NATO, "Remarks by NATO Secretary General Jens Stoltenberg and US President Joe Biden at the start of the 2022 NATO Summit", 29.06.2022. Disponibil la [https://www.nato.int/cps/en/natohq/opinions\\_197374.htm](https://www.nato.int/cps/en/natohq/opinions_197374.htm) și accesat la data de 15.07.2022.
- <sup>28</sup> NATO, "NATO 2022 Strategic Concept", para. 1-4.
- <sup>29</sup> Idem, para. 6.
- <sup>30</sup> Idem, para. 7.
- <sup>31</sup> William Alberque, "The new NATO Strategic Concept and the end of arms control", The International Institute for Strategic Studies, 30.06.2022. Disponibil online la <https://www.iiss.org/blogs/analysis/2022/06/the-new-nato-strategic-concept-and-the-end-of-arms-control> și accesat la data de 21.07.2022.
- <sup>32</sup> Vladimir Socor, "NATO Summit: New Strategic Concept Brings New Realism About Russia", Jamestown Foundation, 06.07.2022. Disponibil online la <https://jamestown.org/program/nato-summit-new-strategic-concept-brings-new-realism-about-russia-part-one/> și accesat la data 17.07.2022.
- <sup>33</sup> Mark Webber, Lawrence Chalmer, Martayn van de Wall și Hazumu Yano, "The Strategic Concept and strategic coherence", *Defence Studies*, 2022, p. 1.
- <sup>34</sup> NATO, "London Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in London 3-4 December 2019", para. 6. Disponibil online la [https://www.nato.int/cps/en/natohq/official\\_texts\\_171584.htm?selectedLocale=en](https://www.nato.int/cps/en/natohq/official_texts_171584.htm?selectedLocale=en) și accesat la data de 20.07.2022;
- <sup>35</sup> NATO, "NATO 2022 Strategic Concept", para. 13-14.
- <sup>36</sup> NATO, "Brussels Summit Communiqué. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 14 June 2021", para 55-56. Disponibil online la [https://www.nato.int/cps/en/natohq/news\\_185000.htm](https://www.nato.int/cps/en/natohq/news_185000.htm) și accesat la data de 20.07.2022.
- <sup>37</sup> Vezi, spre exemplu, Barry Pavel și Ian Brzezinski, "It's Time for a NATO-China Council", *DefenseOne*, 21.08.2019. Disponibil online la <https://www.defenseone.com/ideas/2019/08/its-time-nato-china-council/159326/> și accesat la data de 20.07.2022.
- <sup>38</sup> NATO, "NATO 2022 Strategic Concept", para. 15-19.
- <sup>39</sup> Idem, para. 1.
- <sup>40</sup> Vezi, spre exemplu, Jens Ringsmose și Sten Rynning, "Now for the Hard Part: NATO's Strategic Adaptation to Russia", *Survival*, vol. 59, nr. 3, 2017, p. 129-146, care analizează dificultatea adaptării posturii de apărare și descurajare față de provocările generate de F.Rusă (valabil la nivelul anului 2017).
- <sup>41</sup> NATO, "NATO 2022 Strategic Concept", para. 20.
- <sup>42</sup> Idem, para. 25, 27.

- <sup>43</sup> NATO, "Madrid Summit Declaration. Issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Madrid 29 June 2022", para. 9. Disponibil online la [https://www.nato.int/cps/en/natohq/official\\_texts\\_196951.htm](https://www.nato.int/cps/en/natohq/official_texts_196951.htm) și accesat la data de 24.07.2022.
- <sup>44</sup> NATO, "New NATO Force Model", 29.06.2022. Disponibil online la [https://www.nato.int/nato\\_static\\_fl2014/assets/pdf/2022/6/pdf/220629-infographic-new-nato-force-model.pdf](https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/220629-infographic-new-nato-force-model.pdf) și accesat la data de 17.07.2022.
- <sup>45</sup> Charles A. Kupchan, "NATO's Hard Road Ahead", *Foreign Affairs*, 29.06.2022. Disponibil online la <https://www.foreignaffairs.com/articles/ukraine/2022-06-29/natos-hard-road-ahead> și accesat la data de 13.07.2022.
- <sup>46</sup> NATO, "NATO 2022 Strategic Concept", para. 22.
- <sup>47</sup> Alessandro Marrone, "NATO's New Strategic Concept: Novelties and Priorities", Istituto Affari Internazionali, July 2022, p. 2. Disponibil online la <https://www.iai.it/en/publicazioni/natos-new-strategic-concept-novelties-and-priorities> și accesat la data de 15.07.2022.
- <sup>48</sup> Arnold Ed, "New Concepts but Old Problems: NATO's New Strategic Concept", Royal United Services Institute, 01.07.2022. Disponibil online la <https://rusi.org/explore-our-research/publications/commentary/new-concepts-old-problems-natos-new-strategic-concept> și accesat la data de 09.07.2022.
- <sup>49</sup> NATO, "NATO 2022 Strategic Concept", para. 36.
- <sup>50</sup> William Alberque, *Art.cit.*
- <sup>51</sup> NATO, "NATO 2022 Strategic Concept", para. 40-41.
- <sup>52</sup> Idem, p. 43.
- <sup>53</sup> Vezi, de pildă, Daniel S. Hamilton, "One Plus Four: What NATO's New Strategic Concept Should Say and How to Achieve It", *Orbis*, Vol. 66, Issue 1, 2022, p. 26-34; Jim Townsend și Anca Agachi, "Build resilience for an era of shocks", *Atlantic Council*, 14.10.2020. Disponibil online la <https://www.atlanticcouncil.org/content-series/nato20-2020/build-resilience-for-an-era-of-shocks/> și accesat la data de 04.07.2022.
- <sup>54</sup> NATO, "NATO 2022 Strategic Concept", para. 26.

# FEDERAȚIA RUSĂ: VECTORI AI POLITICII EXTERNE PE DIRECȚIILE STRATEGICE VEST ȘI SUD-VEST

Gheorghe MATEI\*

## Abstract:

*The fall of the USSR gave birth to new geopolitical realities in Eastern and South-Eastern Europe and the intervention by force and military power was no longer a solution. After years of reform, the Russian Federation was forced to apply coercion to its former political satellites. In this context, the Russian leaders initiated the reconstruction of the old sphere of economic and political influence by using identity conflicts, energy blackmail and hybrid warfare.*

**Keywords:** *Falin-Kvitsinsky doctrine; Crimea; putinism; identity war.*

## INTRODUCERE

Transformarea mediului global de securitate are ca rezultate apariția tendințelor de reafirmare ale unor actori globali/regionali și înlocuirea cooperării cu competiția. Deceniile de tensiuni și confruntări politice și ideologice întreținute de la finalul celui de-al Doilea Război Mondial până la revoluțiile din 1989, cunoscute sub sintagma de „Război Rece”, au fost marcate, în plan politico-ideologic, de confruntarea între democrațiile liberale occidentale și regimurile comuniste totalitare, autodefinite ca „lumea liberă” sau „societatea deschisă” și, respectiv, „lumea anti-imperialistă” sau „democrațiile populare”.

După încheierea Războiului Rece, pârghia militară, folosită de liderii de la Moscova ca ultimă metodă de aducere „pe calea cea dreaptă” a celor ce încercau „să evadeze din pluton” sau să nu mai răspundă comenzii puterii centrale recunoscute anterior, rămânea



Sursa: IREN MOROZ/FOTOLIA

o opțiune necesară, dar nu mai era suficientă și ușor de aplicat în noua configurație geopolitică. Realitatea geopolitică și geostrategică neo-sovietică, de după implozia URSS din anii '90, a necesitat folosirea instrumentelor *soft power* în politica externă rusă, mult mai diverse decât cea în care brațul armat rezolva eventualele „derapaje” ale statelor-satelit. În plan ideologic, ideea inamicului nazist, păstrată și reactivată constant în mentalul colectiv rus, a fost cu ușurință acceptată de către populația F.Ruse și,

\* Autorul este expert în cadrul Ministerului Apărării Naționale.



după aproape opt decenii de la finalizarea celui de-al Doilea Război Mondial, pentru justificarea intervenției militare în Ucraina.

## DOCTRINA FALIN-KVITSINSKY

După sfârșitul Războiului Rece, relațiile F.Ruse cu statele central-est europene au fost marcate de profunde transformări, care au necesitat o adaptare a abordării proiecției doctrinare. Pentru a suplini imposibilitatea aplicării intervenției militare, determinată de noul context geopolitic european, la Moscova a fost elaborată *doctrina Falin-Kvitsinsky*. Aceasta a prevăzut, ca obiectiv de bază, menținerea statelor „foste sovietice” într-o stare de neutralitate față de NATO, controlată de Moscova, prin presiune economică (*cotația preferențială a gazului și promovarea ideii unor crize ale gazului*). De altfel, la începutul anilor '90, statele europene foste componente ale „imperiului exterior” al Moscovei manifestau o orientare tot mai accentuată către Occident. În felul acesta, devenise evidentă necesitatea unor noi metode de intervenție mascată a Kremlinului în problemele interne ale statelor din Europa Centrală, de Est și de Sud-Est, iar cel mai facil instrument era reprezentat de resursele energetice.

Anterior, politica exportului resurselor energetice ale URSS către Occident dăduse naștere doctrinei Falin-Kvitsinsky (apărută în a doua jumătate a anilor 1980, în epoca Gorbaciov), aceasta purtând numele a doi diplomați ruși – Valentin M. Falin<sup>1</sup> și Yuli A. Kvitsinsky<sup>2</sup>. Probabil, pregătită încă de la începuturile dezvoltării infrastructurii de transport al hidrocarburilor (perioada anilor '60-'70), presiunea economică asupra statelor foste socialiste/sovietice a servit drept *componentă coercitivă non-militară* de reșezare la masa discuțiilor și pentru obținerea de beneficii geopolitice, după regulile furnizorului (Federația Rusă).

În afara obiectivelor economice, realizate prin exportul de petrol și gaze, se intenționa, conform acestei doctrine, substituirea intervenției militare cu presiunea economică. Astfel, „*bonusul de ascultare*” și „*gestionarea prin crize*” deveneau

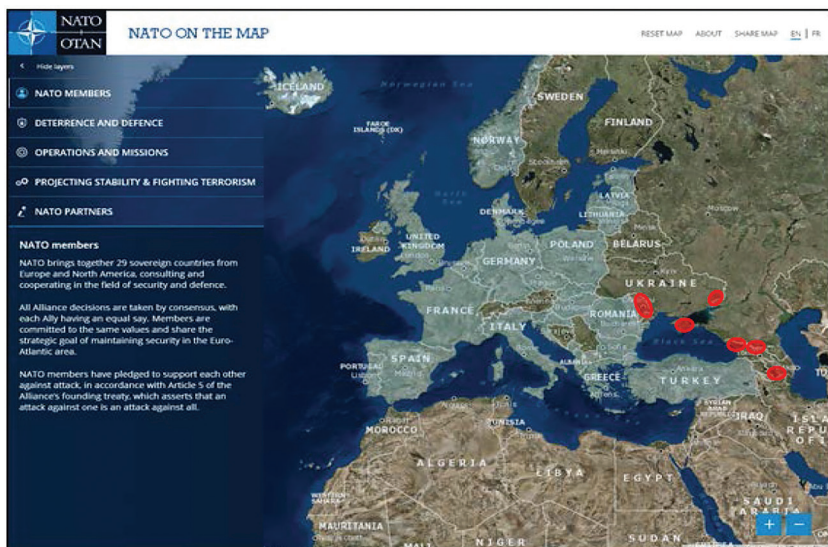
elemente importante ale politicii externe a Federației Ruse în relațiile cu statele din Europa Centrală, de Est și Sud-Est. *Cotația preferențială a gazului*, stabilită în funcție de cursul/răspunsul politic al beneficiarului (stat importator de gaz rusec), și *promovarea ideii unor crize ale gazului* (amenințarea cu oprirea gazului spre un stat sau altul, pe o rută sau alta) au fost menite să creeze oportunități noi de negociere asimetrică pentru decidenții de la Kremlin cu statele europene, în funcție de evoluția contextului geopolitic.

Pentru a crește puterea de proiecție a doctrinei Falin-Kvitsinsky eforturile rusești s-au concentrat atât pe dezvoltarea infrastructurii de transport a gazului spre Europa, cât și pe alte două strategii de acțiune: (a) achiziționarea/concesionarea/participarea în acționariat/preluarea mascată a unor companii/facilități importante ale infrastructurii gazului în diverse state; (b) cumpărarea bunăvoinței autorităților statelor vizate pentru aplicarea ulterioară a prevederilor doctrinei.

În ultimii 20 de ani, prin operaționalizarea noilor gazoducte prin Marea Baltică și Marea Neagră și o intensă campanie de lobby, Moscova a încercat erodarea treptată a coeziunii UE și reducerea dependenței exportului de gaz rusec de principalii actori europeni de tranzit, Polonia și Ucraina. În același timp, capacitatea în exces a gazoductelor de alimentare cu gaz rusec a Europei arată, în primul rând, *dimensiunea geopolitică* a doctrinei Falin-Kvitsinsky și apoi „speranța” furnizorului (Federația Rusă) de creștere a consumului intracomunitar în sprijinul obiectivelor și ambițiilor ruse.

## CONFLICTE ÎNGHEȚATE ÎN REGIUNEA EXTINSĂ A MĂRII NEGRE

Abordarea liderilor de la Moscova, în ultimul deceniu al secolului XX, ca reacție la pierderea controlului pe direcțiile strategice Vest și Sud-Vest și pentru menținerea unei minime zone tampon între foștii poli de putere globală (F. Rusă vs. SUA/NATO), a presupus întreținerea și/sau crearea unor *conflicte identitare*, în faze



În fapt, soluționarea acestor conflicte, indiferent de formă, nu este dorită de liderii de la Moscova. Rezolvarea conflictului, chiar și în varianta independenței sau a alipirii la Federația Rusă, ar oferi posibilitatea statului „mamă” amputat să-și stabilească necondiționat obiectivele de politică externă, eventual independent de voința Kremlinului.

## DOCTRINA PUTIN

diverse (activă sau înghețată) în funcție de evoluția geopoliticii momentului. Beneficiară a politicii de „maximă complicație etnică”<sup>3</sup>, susținută de Iosif Vissarionovici Stalin după cel de-al Doilea Război Mondial, Federația Rusă a alimentat speranțele secesioniste ale unor grupuri etnice din spațiul post-sovietic (Transnistria - Republica Moldova, Abhazia și Osetia de Sud - Georgia, Nagorno-Karabakh – Armenia/Azerbaidjan). În toate cazurile, acțiunea Kremlinului presupunea menținerea pe teritoriul acestora a prezenței militare sub forma unor „trupe de menținere a păcii”, necesare pentru a fi folosite, la nevoie, ca pârghie suplimentară de presiune.

Interesul Moscovei pentru a genera și menține astfel de focare de tensiune latentă este acela de a controla „întregul” (state suverane sau zone de interes strategic) prin instaurarea controlului asupra unei părți (zona de conflict). Menținerea acestor focare permite Federației Ruse să țină captive „statele-mamă” (statele pe teritoriul cărora există un astfel de conflict, mai mult sau mai puțin „înghețat”) și să le modeleze intențiile și obiectivele de politică externă.

Tentativele de soluționare a acestor conflicte au avut la bază următoarele soluții:

- federalizare și regionalizare;
- revenirea pașnică la *statu-quo ante*;
- războiul de recuperare (soluția radicală);
- independența;
- alipirea la Federația Rusă;
- înghețarea pe termen lung a conflictelor (lipsa soluției).

Sucesiunea doctrinară, de la cea marxist-leninistă (începutul sec. al XX-lea) până la cea „putinistă” (în prezent), a presupus, în funcție de cine s-a aflat la conducerea URSS/Federației Ruse, mai multe etape de transformare conjuncturală, astfel:

- de la doctrina **stalinistă**, de recentralizare a puterii spre liderul suprem și implementarea politicilor interne de dezrădăcinare etnică și deportare a celor potrivnici, la doctrina **Brejnev** - de intervenție externă în politicile interne ale statelor socialiste, ca datorie de impunere de către URSS a supremației asupra sateliților;

- de la doctrina **Sinatra** (în „epoca” Mihail Gorbaciov, pe fondul „glasnostului”/ „transparenței”, al perestroikăi/„reconstrucției” și al „uskoreniei”/„accelerării dezvoltării economice”) la doctrina **Falin-Kvitsinsky** și, mai apoi, la doctrina **Putin**.

Politica leninistă „3P” (pace, pământ, pâine) aplicată conaționalilor și/sau adepților socialismului la începutul secolului al XX-lea a fost transformată, în prezent, în doctrina putinistă „3P+1” de politică externă (*pace* - limitează, dar nu se reține de la intervenția militară, *pământ* - respectarea granițelor statelor care răspund comenzii de la Kremlin, *pâine* - Federația Rusă este unul dintre cei mai mari producători de grâu la nivel global și *petrol/gaze* - componenta soft prin doctrina Falin-Kvitsinsky). Mai mult decât

orice, ideologia putinistă ar trebui înțeleasă, în viziunea Kremlinului, ca fiind superioară oricăreia anterioare.

Relaxarea „mâinii de fier” a politicii sovietice (intervenția militară) și plasarea responsabilităților rezolvării problemelor interne către autoritățile statelor „semi-suverane” din Europa Centrală, de Est și de Sud-Est, la începutul anilor '90, ar fi trebuit să determine o reșezare a politicilor de securitate în zona nou creată (zonă tampon între URSS și NATO), spre o *suveranitate amputată* (controlată de la Moscova) sau măcar o *neutralitate față de NATO*.

Interesantă pentru adepți atât din perspectiva aplicării interne (impune „verticala puterii” și suprimarea oponentilor), cât mai ales din perspectiva politicii externe (aplicarea metodelor de manipulare a mentalului colectiv în state țintă), noua ideologie putinistă a încercat să combine unele trăsături ale *neoliberalismului de tip suveran* cu *autoritarismul* și *conservatorismul rusesc*.

Cuprinsă de expansionism și imperialism „în scop nobil”, pentru „binele poporului”, pentru satisfacerea mentalului imperialist rusesc și reunirea tuturor teritoriilor locuite de „ruși, rusofoni și compatrioți”, Federația Rusă ignoră prevederile dreptului internațional, angajamentele sau reglementările asumate, eventual respectându-le doar în punctele și momentele care convin pentru atingerea propriilor obiective, utilizând, acolo unde nu a fost înțeles mesajul, chiar și forța armată pentru a modifica frontierele în spațiul post-sovietic. Totodată, eșuarea/distrugerea statelor/organizațiilor-țintă prin război informațional, cu sprijinul și implicarea activă a lui Igor Ashmanov<sup>4</sup> și prin executarea atacurilor cyber de tip preemptiv pentru subminarea și/sau schimbarea direcției guvernelor și regimurilor democratice, este folosită eficient pentru reconfigurarea politicilor la nivel regional/global.

Combinația de suveranism și autoritarism renăscut sub mantia unei „democrații suverane”, populismul radical, sprijinirea structurilor radical-naționaliste din Europa și nu numai (pentru readucerea la conducerea statelor a regimurilor autoritare, ca primă condiție a

aplicării principiului „divide et impera”), precum și ingerințe în politicile energetice ale unor state sunt folosite ca instrumente de erodare în Europa a valorilor democratice.

Forța de export a modelului putinist (propus ca model rezilient-câștigător), concretizată prin strategii de manipulare, prin panegirice false la adresa unor lideri și prin mascarea/alterarea realizărilor societăților democratice liberale (utilizând metode hibride) determină reorganizări geopolitice cu implicații strategice deosebite și eludarea eforturilor de evoluție democratică, chiar și acolo unde părea că parcursul spre democrație este de nediscutat. Combinația între nivel educațional scăzut (manifestat în statele-țintă prin ignoranță, reziliență scăzută la manipulare și dependență de putere), investiții rusești (prin avanposturi economico-culturale) de acaparare a unor componente strategice în diverse state-țintă și capete de pod militare rusești (în spații din zona proxy și/sau aflate pe direcțiile strategice de acțiune) alimentează tentativele de erodare a încrederii în valorile liberale, arătând, în același timp, celor interesați „modelul-succesului”.

Ideologia „putinistă” exportată în state de „nișă” (chiar dacă unele sunt membre ale unor organizații politico-economice sau politico-militare regionale sau internaționale) vizează reconfigurarea identitară și religioasă a statelor, într-un context în care mondializarea este din ce în ce mai mult promovată ca fiind împotriva „statelor-națiune” și percepută drept un instrument de îmbogățire și de consolidare a instrumentelor și pârghiilor de putere doar de către cei care participă la „masa bogaților”. În felul acesta, **adhocrații** (care, potrivit politologului Mark Galeotti, „se definesc prin loialitate, relația cu șeful și ce pot face pentru el”) trebuie să fie impuși în puncte cheie ale statelor vizate, iar **adhocrația** („instituțiile concurează unele cu altele, legăturile oficiale sunt mai puțin importante decât relațiile personale, favoriții pot cădea în dizgrație, statutul și puterea sunt date mai degrabă de serviciile prestate Kremlinului la nevoie decât de vreo identitate internațională sau socială”) necesită a fi injectată în mentalul colectiv ca unică șansă a reușitei.



În acest context, se poate aprecia că direcția vizată în exportarea „putinismului” este influențarea mentalului colectiv prin utilizarea mijloacelor de propagandă specifice războiului informațional, în sensul construirii unei imagini favorabile „democrației suverane”, ca nouă paradigmă și alternativă față de democrația liberală existentă și cultivată în ultimul secol în societățile occidentale.

## AVANPOSTUL CRIMEEA

Pentru reafirmarea ca actor global de necontestat, Federația Rusă aspiră la „noi orizonturi”, în care ideologia „putinistă” să poată fi adoptată cu ușurință de către elite autoritar-dictatoriale, și mută centrul de greutate al efortului pentru proiectarea doctrinei dinspre Europa spre Africa și Orientul Mijlociu, precum și spre Asia-Pacific.



Ca reacție la extinderea NATO și UE în estul și sud-estul Europei, Federația Rusă adoptă acțiuni de tip „defensiv-expansioniste” de politică externă,

cu invocarea dreptului „de a proteja viața și demnitatea cetățenilor noștri, indiferent unde s-ar afla” și a dreptului „la regiuni unde are interese privilegiate”, unde „se află țări cu care am avut tradițional relații cordiale și prietenești, legături istorice speciale”.

Aceste acțiuni urmăresc o serie de obiective, precum:

- testarea rezilienței statelor pe direcția strategică Vest (consolidarea apărării - regiunile militare Vest și Sud; hărțuire în domeniul aeronaual - Marea Neagră, Marea Baltică, Marea Norvegiei și Mare Nordului; absorbție – Belarus; ofensivă - Ucraina și promovarea intereselor prin interpuși);

- preluarea inițiativei/ofensive pe direcția strategică Sud-Vest (Marea Mediterană, Orientul Mijlociu, nordul Africii și, mai departe, pe continentul african).

Avanpostul nou-creat și consolidat după anexarea din 2014 (Peninsula Crimeea) a fost rapid transformat dintr-un teritoriu „cucerit, cedat, concesionat și revendicat” într-o **redută pe direcția strategică Sud-Vest** și folosit ca o continuare firească a politicii externe expansioniste teritoriale a Federației Ruse.

Revendicarea Peninsulei Crimeea de către „patria-mamă” (Federația Rusă) a fost urmată de ample programe de „conexare facilă” a peninsulei cu zona continentală a Federației Ruse din punct de vedere economic, infrastructură de transporturi și, mai ales, militar, prin supra-aglomerarea cu tehnică și personal pentru atingerea următoarelor obiective:

- controlul militar al regiunii Mării Negre/ al Regiunii Extinse a Mării Negre;
- descurajarea, întârzierea, limitarea și interzicerea prezenței militare NATO în Marea Neagră;
- susținerea efortului militar naval din estul Mării Mediterane, cu nave preponderent din organica Flotei ruse din Marea Neagră (navele din înzestrarea celorlalte flote, urmând să fie angajate în misiuni în alte zone de operații);
- intensificarea cooperării militare prin executarea de activități de instrucție pentru luptă în comun cu state din Orientul Mijlociu și nordul Africii.

## CONCLUZII

Politica externă actuală a Federației Ruse nu diferă foarte mult de cea a Imperiului Țarist din perioada de domnie a dinastiilor Rurik și Romanov. Metodele aplicate pentru îndeplinirea obiectivelor expansioniste au variat în funcție de realitățile momentului și au fost construite în timp pentru a fi folosite atunci când urgența o va cere. Conectarea Europei la resursele energetice ruse și realizarea dependenței europene de acestea au fost atent implementate, cu implicarea unor factori de decizie europeni și cu campanii de

lobby abile derulate pentru a influența politicile statelor vizate.

Promovarea insecurității în vecinătatea Federației Ruse prin conflicte identitare, menținute mai mult sau mai puțin înghețate, are rolul de a opri extinderea NATO și UE spre Est, până când Federația Rusă va trece la etapa militară de readucere la „patria-mamă” a celor ce au părăsit intempestiv „familia sovietică” în anii '90.

Readucerea Peninsulei Crimeea în componența Federației Ruse a fost doar un pas în această direcție și, probabil, modelul de supraaglomerare cu forțe militare va fi utilizat și în teritoriile nou vizate, după anexare.

Acțiunile hibride ale Federației Ruse, de modelare a mentalului colectiv în societățile țintă, coroborate cu inacțiunile statelor vizate pentru implementarea unor politici de creștere a rezilienței instituțiilor statului și dezvoltarea culturii de securitate a populației, pot avea efecte disruptive la nivel societal, benefice impunerii *adhocrației* și *adhocrațiilor*. Nivelul de *adhocrație* din statul vizat și puterea *adhocrațiilor* impuși în funcții importante ale statului sunt semne ale funcționării deficitare ale noilor democrații din Europa de Est și Sud-Est și arată nivelul implementării politicilor neo-imperialiste ale Moscovei în aceste state.

## BIBLIOGRAFIE

1. CHIFU Iulian, ”Conflictele înghețate și responsabilitatea Rusiei: de la „maxima complicație etnică” alui Stalin la „apărarea rușilor de pretutindeni” a lui Putin”, [https://adevarul.ro/international/rusia/conflictele-inghetate-responsabilitatea-rusiei-maxima-complicatie-etnica-stalin-apararea-rusilor-pretutindeni-putin-1\\_569f587f37115986c6b5a99f/index.html](https://adevarul.ro/international/rusia/conflictele-inghetate-responsabilitatea-rusiei-maxima-complicatie-etnica-stalin-apararea-rusilor-pretutindeni-putin-1_569f587f37115986c6b5a99f/index.html), accesat la 16.05.2022.
2. DULEBA Alexander, ”From Domination to Partnership: The Perspectives of Russian-Central-East European Relations”, Final Report, NATO Research Fellowship Program 1996-1998; disponibil la <https://www.nato.int/acad/fellow/96-98/duleba.pdf>, accesat la 12.05.2022.
3. GALEOTTI Mark, *Hai să vorbim despre PUTIN! Ce nu înțelege Occidentul*, Editura Humanitas, București, 2021, 144 p.
4. GONCHAR Mikhailo, Horbach Volodymyr, Pinchuk Anatolii (eds.), *Russian Octopus in action - case “Ukraine”*, Centre for Global Studies “Strategy XXI”, Kiev, 2020, 104 p.
5. GRANT Thomas D., „Frozen Conflicts and International Law”, *Cornell International Law Journal*, vol. 50, nr. 3, 2017, p. 361-413.
6. GRIGORYAN Vardan, Grigoryan Suren, „Russia and the Post-Soviet Space”, *Per Concordiam*, vol. 1, nr. 2, George C. Marshall European Center for Security Studies, 2010, p. 38-43.
7. HILL William H., ”More than a Frozen Conflict: Russian Foreign Policy Toward Moldova”, <https://AtlanticCouncil.org/August2018>, accesat la 17.05.2022.
8. KAPITONENKO Mykola, „Resolving Post-Soviet ‘Frozen Conflicts’”. Is Regional Integration Helpful?”, *Per Concordiam*, vol. 1, nr. 2, George C. Marshall European Center for Security Studies, 2010, p. 33-37.
9. MORAR Filon, „The Myth of ‘Frozen Conflicts’. Transcending Illusive Dilemmas”, *Per Concordiam*, vol. 1, nr. 2, George C. Marshall European Center for Security Studies, 2010, p. 10-17.
10. SIPRI, *Trends in international arms transfers 2019*, March 2020; accesat la 17.05.2022.
11. STÜRMER Michael, *Putin și noua Rusie*, edițiile I și II, Editura Litera, București, 2009 și 2014.
12. ZAGORSKI Andrei, *Russia and East Central Europe after the Cold War, A Fundamentally Transformed Relationship*,

Institute of World Economy and International Relations (IMEMO), Russian Academy of Sciences and Friedrich-Ebert-Stiftung, Prague, 2015; disponibil la [https://www.library.fes.de/pdf\\_files/id-moe/11384.pdf](https://www.library.fes.de/pdf_files/id-moe/11384.pdf), accesat la 12.05.2022.

13. ZANIEWICZ Maciej, "New gas pipeline geopolitics in central and eastern Europe", Warsaw Institute, 21.12.2019; disponibil la [https://warsawinstitute.org/new-gas-pipeline-](https://warsawinstitute.org/new-gas-pipeline-geopolitics-in-central-and-eastern-europe/)

[geopolitics-in-central-and-eastern-europe/](https://warsawinstitute.org/new-gas-pipeline-geopolitics-in-central-and-eastern-europe/), accesat la 12.05.2022.

14. \*\*\*, Centre for Global Studies "Strategy XXI", *Black Sea Security. Analytical Journal*, vol. 2 (38), 2020, 98 p.; <https://geostrategy.org.ua/en/black-sea-security/chornomorska-bezpeka-2-38-2020/zavantazhiti-pdf-ukr>, accesat la 17.05.2022.
15. \*\*\*, UN, *Conflict Analysis Practice Note/ Version: 13 May 2016*, 12 p.

<sup>1</sup> Diplomat al Ministerului de Externe al URSS în Republica Federală Germania (1951-1958), ambasador al URSS în Republica Federală Germania (1971-1978), prim-adjunct al șefului Departamentului Internațional al Comitetului Central al Partidului Comunist al Uniunii Sovietice (1978-1983 / 1988-1991).

<sup>2</sup> Diplomat al Ministerului de Externe al URSS în Republica Federală Germania (1959-1965), șef al Dep.3 European al Ministerului de Externe (1965-1978), ambasador al URSS în Republica Federală Germania (1981-1986), adjunctul ministrului afacerilor externe al URSS și șef al delegațiilor sovietice în negocierile privind tratatele bilaterale cu statele din Europa Centrală (la finalul anilor '80-începutul anilor '90).

<sup>3</sup> Politica migraționistă a lui Stalin a modificat fața Europei postbelice și a devenit un teren fertil pentru conflictele etnice de mai târziu. Politica urmărită a întrunit două scopuri – etnicii din Europa de Est, Caucaz și statele baltice să fie strămutați forțat în Siberia și Asia Centrală, și în etapa subsecventă, să fie indus un flux de populație rusă în republicile non-ruse. Reîntorcerea în țara-mamă în timpul anilor '80 sau după 1990 a fost un proces dificil pentru victimele politicii lui Stalin sau a succesorilor săi, din cauza obstacolelor economice și administrative întâmpinate atât de statul-gazdă, cât și de cel de origine.

<sup>4</sup> Igor Ashmanov - conducătorul RUNET (comunitatea de limbă rusă de pe Internet) și soțul Nataliei Kaspersky (co-fondator și fost președinte al companiei Kaspersky Lab), omul de încredere al lui Putin în campania prezidențială.

# IMPACTUL CONFLICTULUI RUȘO-UCRAINEAN ASUPRA REGIUNII BALCANILOR DE VEST

*Florin-Vasile GROZA\**

## **Abstract**

*The war in Ukraine is fiercely fought for over 6 months and there are no signs that it will lose tempo in the near future. At the beginning of the invasion it seemed that Moscow will succeed in imposing its military and political agenda in a short period and in an easy manner. After half a year, through the determination of the Ukrainian people and with the strong support of the democratic countries the faith of the conflict in the eastern side of the European continent is on the verge of change.*

*The same trends can be noticed in the dynamic of the “geopolitical resonance box” that is the Balkans. At the beginning of the invasion, Russia seemed to have a lot of support from the Balkan area, mainly in the countries that have developed through the history political, economic and cultural ties with Moscow. But this situation is changing with small steps: it started from the political condemnation of the aggression made by United Nations Organization where all 5 Western Balkan countries (that are members of the above mentioned international infrastructure) supported the stance, and months later it continues with military materials delivered by the NATO members from Balkans to Ukrainian forces that are fighting the invaders.*

*From this point of view, the war in Ukraine has a big impact in the Balkans: it determines/pressures all countries from the area to clarify their geopolitical options – in favor of Russia or on the side of Western democracies. But there are signs that this process is not simple and it is not going to be short.*

**Keywords:** Ukraine; Russian Federation; war; NATO; EU; Western Balkans; regional risks; geopolitical opportunities.

## **CONSIDERAȚII PRELIMINARE**

Atacarea de către F.Rusă a Ucrainei (24.02.2022) a generat o veritabilă undă de șoc geopolitic la nivel global. La aproape opt decenii de la încheierea celei mai sângeroase conflagrații mondiale, declanșată tot pe continentul european, prognozele de ordin geopolitic indicau un procent extrem de scăzut în ceea ce privește posibilitatea

ca un nou conflict să zguduie din temelii arhitectura securitară, diplomatică, politică și economică a Europei.

Evident, repere ale unei posibile confruntări între Moscova și Kiev au fost identificate și semnalate anterior inițierii invaziei, însă majoritatea evaluărilor au mizat fie pe un conflict de scurtă durată și cu o intensitate limitată, generat și gestionat de forțele separatiste susținute de Rusia (*worst case scenario*), fie pe

\* *Expert în cadrul Ministerului Apărării Naționale.*



accentuarea presiunilor economice (*componenta energetică*) ale Moscovei la adresa beneficiarilor europeni, astfel încât obiectivele autonomiste ale regiunilor din estul Ucrainei să fie realizate fără implicarea directă a infrastructurii militare. Evaluarea retrospectivă a unor materiale analitice circumscrise dinamicii regionale a relevat o capacitate redusă de anticipare a anvergurii, intensității și violenței acestui război, soldat până în prezent cu zeci de mii de victime și masive distrugerii.

Dacă șocul inițial a fost relativ ușor absorbit de către statele din infrastructura UE și NATO, efectele acestuia într-un spațiu precum cel balcanic, trecut recent prin tragedia unor conflicte de mai mică anvergură, dar la fel de sângeroase, sunt încă puțin vizibile și, în consecință, dificil de cartografiat. Evident că invazia rusă în Ucraina a impus direcționarea majorității resurselor comunității internaționale spre susținerea statului agresat, însă cunoașterea capacităților de acțiune de tip hibrid, respectiv anticiparea unor posibile strategii de tip „maskirovka\*\*”, aplicate tot mai frecvent de Moscova, a determinat actorii geopolitici relevanți (ONU, SUA, UE, NATO) să identifice și, ulterior, să încerce aplicarea unor măsuri „preventive” în zone vulnerabile, segment în care Balcanii de Vest ocupă o poziție privilegiată.

Astfel, una dintre primele decizii luate în cursul aceleiași zile cu declanșarea invaziei, la nivelul celor două organisme prezente în spațiul balcanic (UE și NATO) a fost cea a sporirii cu 500 de militari a contingentului de menținere a păcii dislocat în Bosnia și Herțegovina. Motivarea acestei decizii a fost cât se poate de clară: deteriorarea situației de securitate internațională. În subsidiar, oficialii europeni și NATO au invocat și influența puternică pe care F.Rusă o exercită în Balcani, inclusiv în Bosnia și Herțegovina, respectiv la nivelul entității administrative a sârbilor bosniaci – Republika Srpska. Poziția reprezentantului sârb, în cadrul președinției tripartite de la Sarajevo, Milorad Dodik, prin care acesta preciza că Bosnia și Herțegovina nu va adera la sancțiunile internaționale impuse Rusiei, a fost de natură a confirma necesitatea consolidării contingentului militar internațional.

O altă confirmare a ipotezei privind influența Rusiei în Balcani a fost furnizată la câteva zile de la declanșarea agresiunii (28.02.2022) și în Muntenegru (stat membru NATO din 2017), unde grupuri de simpatizanți locali ai regimului de la Kremlin au generat adunări spontane în care au afișat bannere cu mesaje de tipul: „Rusia în Ucraina/Serbia în Muntenegru”, „Sperăm că vei (Putin) aduce Kosovo din nou în brațele noastre”,



(28.02.2022/Reuters/Stevo Vasilijevic)

\*\* Substantiv (limba rusă) sinonim cu mascare, camuflare, deghizare; acțiuni de înșelare/inducere în eroare derulate de structuri militare/speciale ale F.Ruse care viza/vizează infrastructura de intelligence occidentală (lexico.uk);

„Pentru frații ruși” etc. Deși aceste manifestări au fost de anvergură redusă, au reușit să demonstreze că strategia Moscovei de „minare” a Balcanilor, respectiv de trasare a unei falii geopolitice între statele pro-Rusia și cele pro-occidentale a fost eficientă.

Acceași falie a fost evidențiată și în procesul de condamnare și sancționare a Rusiei la nivelul unor organisme/organizații internaționale. Astfel, în data de 25.02.2022, Albania (membru nepermanent al Consiliului de Securitate al ONU în perioada 2022-2023) a inițiat o rezoluție prin care a fost condamnată invazia F.Ruse în Ucraina. Documentul nu a fost adoptat pe fondul opoziției evidente a Moscovei, exprimată printr-un veto în Consiliul de Securitate al ONU, respectiv prin abținerea R.P. Chineze. Ulterior, în cadrul unei sesiuni speciale a Adunării Generale a ONU, un număr de 141 de state membre - inclusiv Serbia, Macedonia de Nord, Kosovo, Bosnia și Herțegovina - au votat o rezoluție de condamnare a intervenției militare ruse în Ucraina.

Aparent, acest gest, asumat la unison de statele din Balcanii de Vest, ar fi trebuit să transmită un semnal de unitate și coerență strategică, parte a procesului de integrare euroatlantică; însă, la momentul impunerii de către UE a unor seturi de sancțiuni politico-economice, falia balcanică a fost reliefată din nou: Albania, Kosovo, Macedonia de Nord au dat curs solicitărilor UE, în timp ce Serbia și Bosnia și Herțegovina au refuzat să se ralieze acestor demersuri. Belgradul, prin vocea președintelui Aleksandar Vucic, a justificat opoziția aplicării de sancțiuni la adresa Moscovei prin relația specială (istorică și culturală) pe care cele două națiuni, sârbă și rusă, o au de secole. În fapt, motivele reale au putut fi identificate în plan intern, pe două componente majore: alegerile generale din aprilie a.c., respectiv poziția de forță pe care Moscova o deține în domenii strategice ale economiei Serbiei (energie, bancar, industrie metalurgică). Referitor la primul reper, sondajele realizate de actorii politici de pe scena sârbă au relevat faptul că un procent semnificativ (peste 70%) este favorabil unei relații prioritare cu F.Rusă, în detrimentul celei cu spațiul occidental. Din

perspectivă economică, Serbia are o dependență de aproape 100% de gazul rusesc. În plus, unul dintre marii jucători ruși în domeniul petrolier/energetic – Gazprom – deține 51% din operatorul național sârb în domeniul gazelor și petrolului – NIS (Nafta Industrije Srbije). În decembrie 2021, Moscova a mai realizat o „asigurare strategică suplimentară” - NIS a devenit acționar majoritar la HIP Petrohemija, cel mai mare producător de produse petrochimice din Serbia.

În ceea ce privește Bosnia și Herțegovina, factorul principal care a împiedicat asumarea și implementarea de către Sarajevo a sancțiunilor la adresa Moscovei poartă un singur nume: Milorad Dodik. Reprezentantul sârb al președinției tripartite din Bosnia și Herțegovina și-a asumat, într-o manieră fără echivoc, blocarea oricărei proceduri la nivel național de sancționare a F.Ruse. Opțiunile geopolitice ale liderului sârb bosniac au practicat o motivație duală, similară cu cele ale omologului său de la Belgrad: etnicii sârbi din Bosnia și Herțegovina sunt majoritar favorabili F.Ruse, iar din punct de vedere economic, operatorul rus Zarubezhneft deține rafinăriile din Bosanski Brod și Modrica – principalele platforme de prelucrare a produselor petroliere din Bosnia și Herțegovina.

Poziționările celor doi actori regionali au determinat reacții ale vecinilor. Astfel, la începutul lunii martie, executivul de la Priștina a constituit „Fondul pentru securitate”, demers care viza colectarea de fonduri extrabugetare pentru dotarea Forței de Securitate a Kosovo. Totodată, ministrul apărării, Armend Mehaj, a solicitat accelerarea procesului de obținere a statutului de membru al Alianței Nord-Atlantice de către Kosovo, concomitent cu amplasarea de către Statele Unite a unei baze militare permanente. Totodată, Priștina a transmis un semnal puternic de atașament la valorile europene: a pus în practică seturile de sancțiuni la adresa F.Ruse decise și asumate de către UE.

O poziție similară au adoptat și Albania, Muntenegru și Macedonia de Nord. Statutul de membru al NATO obținut de cele trei state balcanice a facilitat procesul de asumare și implementare a regimului sancționator

occidental care vizează Moscova. Suplimentar, într-o manieră oficială, acestea și-au asumat inclusiv sprijinirea cu echipamente militare a eforturilor Ucrainei. Pe de altă parte, dislocarea unor structuri de forțe speciale aparținând SUA în Albania a generat un plus de confort strategic pentru statele sus-menționate.

## PERSPECTIVE

În contextul în care majoritatea statelor din Balcanii de Vest și-au demonstrat intenția continuării procesului de integrare euroatlantică într-o manieră lipsită de echivoc, este sarcina organismelor europene și nord-atlantice să răspundă într-o manieră similară. Și acest aspect trebuie să se concretizeze în proceduri și etape concrete, care să contureze clar intervalul și parcursul de urmat, astfel încât aceste state să obțină statutul de membri cu drepturi depline în aceste organizații.

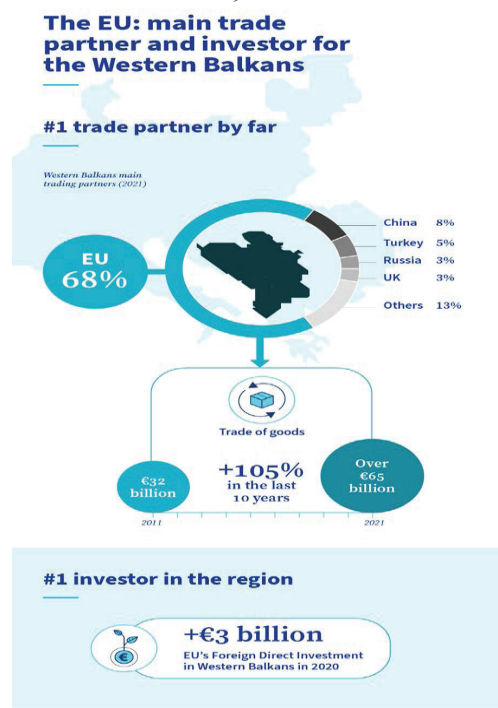
Evaluarea dinamicii geopolitice a celor doi actori internaționali, NATO și UE, demonstrează coerența și perseverența în implementarea unei strategii integratoare de către infrastructura nord-atlantică. Astfel, cu excepția Serbiei, Bosniei și Herțegovinei și Kosovo, celelalte state din Balcanii de Vest sunt deja membre ale NATO. Din această perspectivă, se impune ca și UE să își reconfigureze lista de priorități pe relația cu Balcanii de Vest. Presiunea pusă de acțiunile agresive ale F.Ruse pe infrastructura occidentală se va accentua în contextul în care, cu sprijinul statelor membre UE și NATO, Ucraina începe să configureze o strategie tot mai consistentă în contracararea operațiunilor militare ruse. Această nouă dinamică conflictuală va determina o reconsiderare a strategiei F.Ruse de confruntare a Occidentului, respectiv activarea graduală a problematicei balcanice.

Evaluarea contextului geopolitic regional și internațional relevă un set limitat de opțiuni pe care Moscova le are la dispoziție pentru detonarea „butoiului cu pulbere” al Europei. Din punct de vedere militar, F.Rusă are o prezență modestă în Balcanii de Vest. Singurul reper cu specific, neasumat oficial însă, respectiv Centrul

ruso-sârb pentru acțiuni umanitare, amplasat strategic în localitatea Niș (în centrul Serbiei, pe un coridor strategic și în imediata proximitate a Kosovo, Macedoniei de Nord și Bulgariei), are preponderent capacități de tip *intelligence* și nu de tip militar/combat. În contrapartidă, NATO are o infrastructură net superioară în regiunea Balcanilor: state membre - Macedonia de Nord, Bulgaria, Albania și Muntenegru; infrastructură tip baze militare - în Kosovo și Bosnia și Herțegovina.

Din punct de vedere economic balanța schimburilor comerciale, respectiv a investițiilor directe este net favorabilă UE, comparativ cu ceilalți doi competitori strategici, F.Rusă și R.P. Chineză. Evaluarea reperelor de ordin financiar (prezentate în graficul de mai jos) indică faptul că partenerii occidentali dețin o cotă de 68% din volumul investițiilor/comerțului derulat de statele din Balcanii de Vest.

Coroborarea datelor tehnice cu percepția majorității populației din regiune relevă însă o contradicție flagrantă: lipsa unor proiecte de marketing instituțional la nivelul UE a facilitat sedimentarea, la nivel social, a ideii potrivit căreia principalii parteneri comerciali ai statelor balcanice sunt F.Rusă și R.P. Chineză.



Source: Council of the European Union, General Secretariat

Source: Council of the European Union, Directorate-General for Economic and Financial Affairs

([www.consilium.europa.eu](http://www.consilium.europa.eu))



Moscova este conștientă de faptul că realitățile geopolitice din spațiul balcanic, cel puțin pe componentele militar și economic, îi sunt defavorabile. În consecință, a alocat resurse pentru derularea unui război informațional bine elaborat și ale cărui rezultate sunt vizibile din perspectiva implementării acestuia într-o manieră extrem de eficientă, concomitent cu dezvoltarea unei infrastructuri umane de tip intelligence care este capabilă să execute operațiuni disruptive pe componentele politic, social și economic.

Un ultim exemplu în acest sens l-a constituit instrumentalizarea deciziei autorităților de la Priștina pentru interzicerea elementelor de identificare auto ale Serbiei, utilizate de etnicii sârbi din nordul Kosovo. Revolta etnicilor sârbi a fost transformată într-o veritabilă furtună mediatică, care a operat cu informații false, dar susținute de la cele mai înalte niveluri ale statului rus. Vehicularea variantei potrivit căreia Belgradul ar fi intenționat să intervină militar în sprijinul etnicilor sârbi din Kosovo a determinat reacția ministrului sârb al apărării, care a infirmat aceste zvonuri. Ulterior, autoritățile de la Priștina au anunțat că au reținut pentru câteva ore o jurnalistă din F.Rusă, Daria Aslamova, la

granița dintre Kosovo și Serbia, sub acuzația de apartenență la serviciile de informații rusești.

Pentru a înțelege determinarea Moscovei de a forța aplicarea unui scenariu conflictual în Balcanii de Vest trebuie doar enumerate oficialitățile ruse care s-au implicat în operațiunea prezentată mai sus: purtătorul de cuvânt al Kremlinului – Maria Zaharova; ambasadorul rus la Belgrad, Alexander Botsan Kharchenko, precum și liderul cecen Ramzan Kadyrov.

## CONCLUZII

UE, în special, și NATO, în subsidiar, trebuie să-și adapteze strategiile integratoare față de Balcanii de Vest. Declarațiile politice și scrisorile de intenție nu țin loc de o foaie clară de parcurs. Această abordare, dublată de criza economică și cea alimentară care se profilează tot mai puternic la orizont, vor facilita acțiunile Moscovei, rezultatul cel mai probabil fiind revenirea Balcanilor la postura de „pântecele moale al Europei”, în cel mai fericit caz. În „worst case scenario” ar putea fi luat în considerare un conflict generalizat, într-un spațiu care a acumulat extrem de multe tensiuni și frustrări geopolitice.

## BIBLIOGRAFIE

1. BROWN W. Garrett, Iain McLean, and Alistair McMillan, *A Concise Oxford Dictionary of Politics and International Relations* (4 ed.), Oxford University Press, 2018.
2. CAPLAN Richard, ”International Authority and State Building: The Case of Bosnia and Herzegovina”, *Global Governance: A Review of Multilateralism and International Organizations*, vol. 10, nr. 1, 2004, p. 53–65.
3. <https://www.consilium.europa.eu/en/infographics/eu-economic-and-investment-plan-unprecedented-support-for-the-western-balkans/>
4. <https://www.euractiv.com/section/europe-s-east/opinion/russia-is-seeking-new-wars-and-kosovo-could-be-the-next-one/>
5. <https://www.reuters.com/world/europe/serb-nationalists-montenegro-rally-support-russia-2022-02-28/>

# EFECTELE RĂZBOIULUI DIN UCRAINA ASUPRA REGIUNII ARCTICE

*Iohana-Georgia BURCEA\**

## **Abstract**

*The war in Ukraine deteriorated the security context in Europe, as well as the ties between the West and the East. The new security context in Europe has reverberations on multiple sectors, among which energy, food and migration, as well as on the whole international system.*

*In this new context, the implications of the war in Ukraine are also echoed in the Arctic region, considering Russia's presence and role in the High North. Characterized through its exceptionalism, the High North is currently confronting with new tensions due to Russia assertiveness and the other seven arctic states' reluctance to continue their cooperation with Russia, in the light of its aggression in Ukraine. China's ambitions and interests in the High North and its partnership with Russia will further debilitate the security context in the region. At the same time, the Arctic region is still confronting with issues such as climate change, environmental protection, oil pollution, sustainability and underdevelopment, issues that until recently were addressed through cooperation and dialogue among all arctic states.*

*The present paper explores the different changes and challenges that the region is currently confronting with, in the context of the war in Ukraine, and how the future will look like in the near future. The partial freeze of the Arctic Council activity was the first sign of the relationship deterioration between Russia and the Western countries.*

**Keywords:** Russia; Ukraine; Arctic region; Arctic exceptionalism; regional security; militarization.

## **CONTEXT**

După recunoașterea independenței regiunilor separatiste Donețk și Lugansk de către președintele Vladimir Putin, pe data de 24 februarie 2022 F.Rusă a început invadarea Ucrainei. Regimul de la Moscova a catalogat războiul drept o operațiune specială de „denazificare și demilitarizare” a Ucrainei<sup>1</sup>, în încercarea de a manipula opinia publică și de a-și justifica agresiunea.

Războiul din Ucraina a schimbat dinamica de securitate la nivel internațional, determinând

noi provocări pe mai multe planuri și în mai multe regiuni, în special acolo unde Moscova este implicată activ. Printre acestea se numără și regiunea arctică, ultima frontieră a lumii, zonă ce a fost caracterizată în ultimii treizeci de ani prin pace și cooperare<sup>2</sup>. Cu toate acestea, mediul de securitate arctic traversează, în prezent, vremuri incerte.

Atitudinea F.Ruse, din postura statului cu cea mai mare deschidere la Oceanul Arctic, ridică semne de întrebare cu privire la strategia sa pentru regiune, în contextul izolării sale pe plan internațional. Totodată, interesul din ce în

\* Doctorand în Relații Internaționale în cadrul Școlii Naționale de Studii Politice și Administrative și Junior Researcher la Centrul de Prevenire a Conflictelor și Early Warning (CPC-EW).



ce mai crescut al R.P. Chineze față de „Marele Nord” și parteneriatul sino-rus complică și mai mult contextul actual. La toate acestea se adaugă prezența NATO în regiune, dar și preconizata aderare a Finlandei și a Suediei la Alianță, ceea ce va duce la împărțirea „Marelui Nord” în două zone - la est F.Rusă, iar la vest statele membre NATO.

Pe de altă parte, celelalte șapte state arctice se arată reticente față de continuarea cooperării cu F.Rusă în regiunea arctică. Astfel, la scurt timp după începerea războiului în Ucraina, acestea transmiteau, printr-o scrisoare comună, decizia de a suspenda pentru o perioadă activitatea Consiliului Arctic, urmând să se decidă asupra formei în care cooperarea va putea fi reluată.<sup>3</sup> Între timp, activitatea a fost reluată parțial, fiind excluse acele proiecte și inițiative în care Moscova era implicată.

Consiliul Arctic, înființat în 1996, prin Declarația de la Ottawa, reprezintă principalul for în cadrul căruia problemele regiunii sunt discutate și analizate în vederea găsirii unor soluții potrivite, iar activitatea acestuia atestă diversitatea problemelor cu care „Marele Nord” se confruntă. Consiliul Arctic are un rol important în consolidarea cooperării trans-frontaliere în regiune, reunind toate statele arctice și comunitățile indigene prezente în zonă.<sup>4</sup> Rezultatele Consiliului Arctic s-au făcut remarcate în mai multe sectoare. Semnarea a trei acorduri cu caracter juridic obligatoriu între cele opt state arctice, în cadrul Consiliului, reprezintă un astfel de exemplu. Aceste acorduri se referă la operațiuni de căutare și salvare maritimă și aeronautică, la pregătire și răspuns în cazul deversărilor de petrol, dar și la cooperarea în domeniul cercetării științifice în regiune.<sup>5</sup>

Pe de altă parte, „Marele Nord” se confruntă cu o multitudine de provocări legate de schimbările climatice și vulnerabilitatea mediului, ce necesită cooperare între statele membre. Astfel, gestionarea acestora în lipsa celui mai mare stat riveran de la Cercul Arctic va fi dificilă.

## REGIUNEA ARCTICĂ

În ciuda competiției pentru resurse și rute maritime, după încetarea Războiului Rece regiunea a fost caracterizată de pace, facilitată prin inițierea mai multor formate de cooperare, printre acestea cel mai important fiind Consiliul Arctic. În acest sens, discursul Secretarului General al PC al URSS, Mihail Gorbaciov, din 1987, din Murmansk<sup>6</sup>, rămâne emblematic pentru normalizarea relațiilor dintre statele arctice. În discursul său, acesta cerea ca regiunea arctică să devină o „zonă de pace” și ca nivelul de confruntare militară să fie redus.<sup>7</sup>

Faptul că regiunea se confruntă cu o multitudine de probleme, ce pot fi rezolvate doar prin dialog și deschidere între statele arctice, a facilitat și consolidat cooperarea între acestea. Printre aceste probleme se numără schimbările climatice, protejarea mediului și a speciilor de animale pe cale de dispariție, riscurile asociate eventualelor deversări de petrol, dezvoltarea sustenabilă sau protejarea populațiilor indigene<sup>8</sup>.

Îndelung considerată *terra nullius*, din cauza statutului legal ambiguu, derivat în principal din suprapunerea unor revendicări teritoriale, dar și a temperaturilor ostile, în ultimii ani regiunea arctică a atras atenția mai multor actori internaționali. Creșterea rapidă a temperaturilor în „Marele Nord” a creat premisele necesare pentru explorarea mai amănunțită a regiunii. Topirea accelerată a gheții a deschis accesul la bogate rezerve de resurse naturale, în principal petrol și gaze naturale. Estimările arată că aproximativ 30% din rezervele de gaze naturale ale planetei și 13% din cele de petrol se regăsesc în regiune<sup>9</sup>. De asemenea, retragerea calotei glaciare vine cu promisiunea unor noi rute de transport comercial, care ar conecta continentul european de cel asiatic într-un timp mult mai scurt în comparație cu itinerarele tradiționale.

Interesele statelor arctice se suprapun pe anumite zone, ceea ce a sporit retorica cu

privire la apariția unor tensiuni în regiune și la deschiderea competiției pentru oportunitățile pe care „Marele Nord” le are de oferit. Totodată, suprapunerea revendicărilor teritoriale reprezintă un alt punct de răscruce pentru politica arctică. Modul în care teritoriul va fi împărțit va decide cine va avea cea mai bună poziționare în ceea ce privește potențialul de exploatare a resurselor și a căilor maritime.

Noile oportunități au atras atenția mai multor actori internaționali. Dacă pentru cele opt state arctice (Danemarca, Canada, Norvegia, F.Rusă, Statele Unite, Suedia, Finlanda și Islanda) „Marele Nord” reprezintă o parte importantă din identitatea națională a acestora, în prezent se observă un interes crescut și din partea unor actori care nu au o legătură tradițională cu

regiunea. De departe, R.P. Chineză este actorul non-arctic care își exprimă cel mai pregnant interesul în regiune, cu precădere prin avantajul economic pe care îl deține. Pentru a-și sublinia interesele în zonă, autoritățile de la Beijing au adoptat chiar și o strategie arctică, în anul 2018, prin care au căutat și să-și legitimeze prezența în regiune, declarându-se un stat „aproape arctic”<sup>10</sup>. De asemenea, R.P. Chineză și-a justificat implicarea în zonă prin istoria lungă pe care o deține în ceea ce privește cercetarea arctică, dar și prin schimbările climatice cu care regiunea arctică se confruntă, situație care creează atât oportunități, cât și provocări. Totodată, din 2014, R.P. Chineză are statutul de observator în cadrul Consiliului Arctic.



Figura 1 - Cercul Arctic (sursa: quora.com)

Lansarea ofensivei rusești în Ucraina a separat, însă, restul celor șapte state arctice de F.Rusă, astfel încât „Marele Nord” începe să reflecte situația de pe plan internațional și anume izolarea Rusiei de către Occident. Astfel, pentru prima oară în istorie, șapte din cele opt state arctice au decis, de comun acord, să ia o pauză de la participarea în cadrul Consiliului Arctic, drept răspuns față de războiul pornit de Moscova împotriva Ucrainei<sup>11</sup>. Luând această pauză, cele șapte state vor să își acorde timp de gândire pentru a se decide asupra a ce vor face mai departe și în ce mod mai poate continua cooperarea regională, conform declarației comune semnate de acestea.<sup>12</sup> Circumstanțele agresiunii rusești au determinat cele șapte state să ia această decizie, fără a elimina, însă, varianta în care cooperarea va putea fi reluată la un moment dat, conștiente fiind de consecințele negative pe care această întrerupere le va avea în buna administrare a problemelor regionale.

## **SFÂRȘITUL EXCEPȚIONALISMULUI ARCTIC?**

Excepționalismul arctic este definit prin cooperarea celor opt state arctice, în ciuda diferențelor de viziune și ideologie și a competiției dintre acestea<sup>13</sup>. Ultimele luni au ridicat semne de întrebare cu privire la durabilitatea excepționalismului arctic, în condițiile în care, la momentul actual, pârghiile de legătură dintre F.Rusă și Occident sunt sever deteriorate. Oprirea, pentru moment, a activității Consiliului Arctic reprezintă cea mai importantă dovadă a acestei deteriorări a relațiilor dintre statele arctice. Chiar și în contextul anexării Crimeii, din 2014, activitatea forului multilateral de cooperare a continuat. Singura excepție, la acel moment, a fost boicotarea de către Statele Unite și Canada a unei întâlniri a Consiliului Arctic, ce urma să aibă loc la Moscova<sup>14</sup>.

Cu toate acestea, anexarea Crimeii a reprezentat un prim semnal de alarmă atât pentru statele arctice, cât și pe plan internațional, în general, în ceea ce privește asertivitatea și intențiile F.Ruse.<sup>15</sup> De altfel, începând cu 2014

s-a putut observa și o schimbare în percepția statelor arctice față de provocările din regiune. Astfel, strategiile arctice ale acestora încep deja să indice F.Rusă ca fiind o potențială amenințare. De asemenea, militarizarea masivă a părții de nord a teritoriului rus, exercițiile militare și redeschiderea unor baze militare ex-sovietice din regiune au contribuit la schimbarea percepțiilor față de intențiile Moscovei.

Interesele F.Ruse în regiunea arctică sunt variate, printre acestea numărându-se resursele naturale, rutele maritime, industria piscicolă și infrastructura, proiecte ce necesită investiții masive și politici care să faciliteze creșterea economică și dezvoltarea<sup>16</sup>. De altfel, în noua doctrină navală rusă, anunțată pe 31 iulie 2022, se discută despre importanța regiunii și despre ambițiile Moscovei în „Marele Nord”. Doctrina face referire la planul de extindere a exploatarei resurselor naturale și la creșterea potențialului flotei nordice și al celei din Oceanul Pacific<sup>17</sup>. Totodată, Oceanul Arctic și Marea Bering sunt considerate puncte de interes național, conform noii doctrine<sup>18</sup>.

În acest moment, F.Rusă se găsește izolată pe plan internațional, inclusiv la nivelul regiunii arctice. Totuși, parteneriatul dintre Moscova și Beijing nu trebuie neglijat. În ceea ce privește Arctica, parteneriatul sino-rus este foarte concentrat pe dezvoltarea Rutei Maritime de Nord, drum ce va deveni o alternativă fezabilă pentru conectarea Europei cu Asia, în contextul în care temperaturile vor continua să crească în următorii ani<sup>19</sup>. F.Rusă a depus deja documentația necesară pentru a-i fi recunoscute drepturile de suveranitate asupra rutei. Însă, este nevoie de investiții masive în infrastructură și echipamente pentru a face această rută accesibilă, iar Moscova nu dispune de aceste resurse financiare.<sup>20</sup> Astfel, urmărindu-și propriul interes, autoritățile chineze s-au arătat dispuse să investească în această rută.

Pe de altă parte, parteneriatul sino-rus nu este atât de puternic pe cât pare. În primul rând, vorbim despre un parteneriat bazat pe interese comune, nu de o alianță bazată pe valori comune<sup>21</sup>. Totodată, avantajul financiar pe care R.P. Chineză îl deține în relația bilaterală face ca F.Rusă să joace doar

rolul partenerului junior în cadrul acestui binom<sup>22</sup>. Interesele există de ambele părți, însă China este cea care, la momentul actual, se remarcă drept o putere la nivel global. Izolarea Moscovei și sancțiunile economice impuse de Occident, precum și o viitoare rupere a dependenței Europei de gazul din F.Rusă, vor adânci și mai mult diferența de poziție dintre Moscova și Beijing și vor face F.Rusă să fie și mai dependentă de R.P. Chineză.

Un alt aspect important este legat de renunțarea Suediei și Finlandei la statutul de neutralitate și aderarea celor două la Alianța Nord-Atlantică, ceea ce pune o distanță și mai mare între F.Rusă și celelalte state arctice. Aderarea Finlandei, în special, înseamnă o nouă extindere a granițelor NATO și o frontieră foarte mare între F.Rusă și NATO, ceea ce este greu de acceptat pentru Moscova. Astfel, în acest nou context, devine îndoielnic faptul că F.Rusă va mai dori să colaboreze în formatul Consiliului Arctic. Totodată, este dificil de imaginat modul în care Consiliul Arctic ar mai putea să funcționeze fără participarea celui mai mare stat din „Marele Nord”.

---

## **EVOLUȚII**

---

În ceea ce privește ambițiile Moscovei în regiunea arctică, războiul împotriva Ucrainei o izolează pe aceasta definitiv și îi îngreunează șansele de a-și atinge obiectivele. Parteneriatul cu R.P. Chineză s-ar putea dovedi o plasă de salvare pentru F.Rusă, atunci când vine vorba de dezvoltarea părții de nord a țării, dar și de Ruta Maritimă de Nord sau exploatarea resurselor naturale de care Rusia dispune.

În acest nou context, cooperarea în „Marele Nord” se află sub semnul întrebării. Sancțiunile impuse de Occident și deciziile Finlandei și Suediei de a adera la NATO fac puțin probabilă varianta în care F.Rusă să își mai dorească cooperarea cu celelalte șapte state arctice. Totodată, o eventuală eliminare a Rusiei din Consiliul Arctic nu poate fi decât una voluntară, membrii permanenți neputând fi eliminați în funcție de dorința celorlalți.

O variantă pe care Danemarca, Canada, Norvegia, Statele Unite, Suedia, Finlanda și Islanda o pot urma este aceea de a pune bazele unui nou parteneriat multilateral din care F.Rusă să nu facă parte. Această variantă, însă, nu ar garanta un succes în ceea ce privește gestionarea provocărilor cu care regiunea se confruntă. Fiind cel mai mare stat riveran din regiune, participarea Rusiei în abordarea anumitor problematici importante pentru regiune reprezintă un element cheie pentru soluționarea acestora.

Cele șapte state se află în fața unei dileme de amploare. Continuarea cooperării cu Moscova ar putea fi considerată drept o lipsă de acțiune din partea acestora față de agresiunea împotriva Ucrainei, ceea ce ar putea fi riscant chiar și pentru securitatea regională. Pe de altă parte, refuzul definitiv de a coopera cu F.Rusă în Arctica pune regiunea în pericol, mai ales în contextul provocărilor legate de încălzirea globală, topirea rapidă a gheții și creșterea nivelului apelor.

Pentru bunăstarea regiunii, statele arctice trebuie să găsească o cale de comunicare, astfel încât problemele comune să poată fi gestionate în continuare. De altfel, problemele climatice cu care regiunea se confruntă vor avea reverberații și în alte regiuni ale lumii, dacă nu sunt gestionate corespunzător, astfel că participarea F.Ruse este necesară. Totodată, pentru a avea o garanție în plus legată de securitatea militară a regiunii, statele arctice ar trebui să discute și despre aceste aspecte. Tradițional, sfera militară a fost exclusă din activitatea Consiliului Arctic, însă, în lumina evenimentelor recente, includerea acesteia printre preocupările organizației ar putea preveni militarizarea excesivă a regiunii.

---

## **CONCLUZII**

---

Agresiunea F.Ruse față de Ucraina a dus la o fracturare a cooperării în regiunea Arctică, ceea ce pune excepționalismul arctic sub semnul incertitudinii. Acțiunile forțelor ruse în Ucraina au creat o falie imensă între Occident și Moscova, ceea ce lasă celelalte șapte state arctice într-o postură reticentă față de reluarea cooperării cu F.Rusă.



În ceea ce privește o eventuală extindere sau replicare a acestui conflict în „Marele Nord”, șansele sunt minime. Statele arctice, inclusiv F.Rusă, sunt conștiente de fragilitatea mediului și de impactul devastator pe care un război l-ar avea asupra regiunii, existând șansa ca efectele să fie ulterior resimțite și la sud de Cercul Arctic.

În acest context, regiunea arctică pare să se fi întors la stadiul din timpul Războiului Rece și la

jocul de mare putere. Există șanse semnificative ca, în anii ce urmează, să vedem o militarizare și mai extinsă a regiunii, un interes și mai crescut față de aceasta și mize mai mari. Cu toate acestea, binele comun al regiunii trebuie să prevaleze. Reluarea cooperării pe o arie comună limitată s-ar putea dovedi benefică pentru viitorul regiunii și menținerea stabilității strategice între principalii actori implicați.

## BIBLIOGRAFIE

1. Arctic Council, *International Cooperation in the Arctic*. Disponibil la <https://www.arctic-council.org/explore/work/cooperation/> și accesat la 01.07.2022.
2. BROWN Kerry, “Will Russia be happy as China’s junior partner?”, *Engelsberg Ideas*, 18 martie 2022. Disponibil la <https://engelsbergideas.com/notebook/will-russia-be-happy-as-chinas-junior-partner/> și accesat la data de 03.07.2022.
3. BUCHANAN Elizabeth, “There Is No Arctic Axis”, *Foreign Policy*, 21 iulie 2020. Disponibil la <https://foreignpolicy.com/2020/07/21/no-arctic-axis-china-russia-relationship-resources-natural-gas-northern-sea-route/> și accesat la data de 04.07.2022.
4. BURCEA Iohana-Georgia, „Regiunea Arctică - între cooperare, competiție și militarizare”, *Infosfera*, Anul XIV, nr. 4, 2020.
5. Comisia Europeană, *EU sanctions against Russia following the invasion of Ukraine*, 2022. Disponibil la [https://ec.europa.eu/info/strategy/priorities-2019-2024/stronger-europe-world/eu-solidarity-ukraine/eu-sanctions-against-russia-following-invasion-ukraine\\_en](https://ec.europa.eu/info/strategy/priorities-2019-2024/stronger-europe-world/eu-solidarity-ukraine/eu-sanctions-against-russia-following-invasion-ukraine_en) și accesat la 01.07.2022.
6. EDVARSEN Astri, “Arctic Council Paused: The Search for A Future for Arctic Cooperation Continues”, *The High North News*, 27 aprilie 2022. Disponibil la <https://www.highnorthnews.com/en/arctic-council-paused-search-future-arcticcooperationcontinues#:~:text=The%20pause%20was%20introduced%20by,well%20as%20it%20sub%2Dbodies> și accesat la data de 13.07.2022.
7. EXNER-PIROT Heather, “Between militarization and disarmament: Constructing peace in the Arctic”, *Arctic Yearbook 2019*. Disponibil la <https://arcticyearbook.com/arctic-yearbook/2019/2019-commentaries/324-between-militarization-and-disarmament-constructing-peace-in-the-arctic>. și accesat la data de 14.07.2022.
8. Foreign, Commonwealth & Development Office, *UK sanctions relating to Russia*, 2022. Disponibil la <https://www.gov.uk/government/collections/uk-sanctions-on-russia> și accesat la 01.07.2022.
9. KLIMENKO Ekaterina, “The geopolitics of a changing Arctic”, *SIPRI Background Paper*, decembrie 2019.
10. LACKENBAUER P. Whitney, Ryan DEAN, “Arctic Exceptionalism”, în *The Arctic and World Order* (Kristina Spohr and Daniel S. Hamilton eds), Brookings Institution Press. 2020. Disponibil la <https://transatlanticrelations.org/wp-content/uploads/2020/12/The-Arctic-and-World-Order-ch14.pdf> și accesat la data de 02.07.2022.
11. President of Russia, *Decree on the Fundamentals of State Policy of the Russian Federation in the Arctic for the Period Until 2035*, 2020.
12. Radio Free Europe, “Russia Adopts Updated Maritime Doctrine; Lists U.S., NATO As Primary Threats”. Disponibil la <https://www.rferl.org/a/russia-maritime-doctrine-threats-nato-us/31967675.html> și accesat la 02.08.2022.
13. RUMER Eugene, Richard SOKOLSKY, Paul STRONSKI, “Russia in the Arctic. A Critical



- Examination”, *Carnegie Endowment for International Peace*, 29 martie 2021. Disponibil la <https://carnegieendowment.org/2021/03/29/russia-in-arctic-critical-examination-pub-84181> și accesat la data de 03.07.2022.
14. The State Council Information Office of the People’s Republic of China, *China’s Arctic Policy*, 2018. Disponibil la [http://english.www.gov.cn/archive/white\\_paper/2018/01/26/content\\_281476026660336.htm](http://english.www.gov.cn/archive/white_paper/2018/01/26/content_281476026660336.htm) și accesat la 01.07.2022.
15. TROIANOVSKI Anton, “Putin announces a ‘military operation’ in Ukraine as the U.N. Security Council pleads with him to pull back”, *The New York Times*, 23 februarie 2022, disponibil la <https://www.nytimes.com/2022/02/23/world/europe/putin-announces-a-military-operation-in-ukraine-as-the-un-security-council-pleads-with-him-to-pull-back.html> și accesat la data de 04.07.2022.
16. U.S. Department of the Treasury, “Ukraine-/Russia-related Sanctions”, 2022. Disponibil la <https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information/ukraine-russia-related-sanctions> și accesat la 01.07.2022.
17. U.S. Geological Survey, “Circum-Arctic Resource Appraisal: Estimates of Undiscovered Oil and Gas North of the Arctic Circle”, 2008. Disponibil la <https://pubs.usgs.gov/fs/2008/3049/fs2008-3049.pdf> și accesat la 01.11.2020.
18. U.S. State Department, “Joint Statement on Arctic Council Cooperation Following Russia’s Invasion of Ukraine”. Disponibil online la <https://www.state.gov/joint-statement-on-arctic-council-cooperation-following-russias-invasion-of-ukraine/> și accesat la 01.07.2022.
19. United Nation News, *Russian attacks on civilian targets in Ukraine could be a war crime*, UN Rights Office, 2022. Disponibil la <https://news.un.org/en/story/2022/03/1113782> și accesat la 01.07.2022.
20. WATLING Jack, “Crisis, settlement, or containment - what is to be done on Russia?”, *Engelsberg Ideas*, 19 martie 2022. Disponibil la <https://engelsbergideas.com/essays/crisis-settlement-or-containment-what-is-to-be-done-on-russia/> și accesat la data de 03.07.2022.
21. ZELLEN Barry Scott, “Why a freeze on the Arctic Council is short-sighted”, *The Globe and Mail*, 27 aprilie 2022. Disponibil la <https://www.theglobeandmail.com/opinion/article-why-a-freeze-on-the-arctic-council-is-short-sighted-and-wrong/> și accesat la data de 03.07.2022.

<sup>1</sup> Anton Troianovski, “Putin announces a ‘military operation’ in Ukraine as the U.N. Security Council pleads with him to pull back”, *The New York Times*, 23 februarie 2022. Disponibil la <https://www.nytimes.com/2022/02/23/world/europe/putin-announces-a-military-operation-in-ukraine-as-the-un-security-council-pleads-with-him-to-pull-back.html> și accesat la data de 04.07.2022.

<sup>2</sup> Iohana-Georgia Burcea, „Regiunea Arctică - între cooperare, competiție și militarizare”, în *Infosfera*, Anul XIV, nr. 4, 2020.

<sup>3</sup> U.S. State Department, “Joint Statement on Arctic Council Cooperation Following Russia’s Invasion of Ukraine”. Disponibil online la <https://www.state.gov/joint-statement-on-arctic-council-cooperation-following-russias-invasion-of-ukraine/> și accesat la 01.07.2022.

<sup>4</sup> Arctic Council, “International Cooperation in the Arctic”. Disponibil la <https://www.arctic-council.org/explore/work-cooperation/> și accesat la 01.07.2022.

<sup>5</sup> Idem.

<sup>6</sup> Heather Exner-Pirot, “Between militarization and disarmament: Constructing peace in the Arctic”, *Arctic Yearbook 2019*. Disponibil la <https://arcticyearbook.com/arctic-yearbook/2019/2019-commentaries/324-between-militarization-and-disarmament-constructing-peace-in-the-arctic> și accesat la data de 14.07.2022.

<sup>7</sup> Idem.

<sup>8</sup> Ekaterina Klimenko, “The geopolitics of a changing Arctic”, *SIPRI Background Paper*, decembrie 2019.

<sup>9</sup> U.S. Geological Survey, “Circum-Arctic Resource Appraisal: Estimates of Undiscovered Oil and Gas North of the Arctic Circle”, 2008. Disponibil la <https://pubs.usgs.gov/fs/2008/3049/fs2008-3049.pdf> și accesat la 01.11.2020.

- <sup>10</sup> The State Council Information Office of the People's Republic of China, *China's Arctic Policy*, 2018. Disponibil la [http://english.www.gov.cn/archive/white\\_paper/2018/01/26/content\\_281476026660336.htm](http://english.www.gov.cn/archive/white_paper/2018/01/26/content_281476026660336.htm) și accesat la 01.07.2022.
- <sup>11</sup> Astri Edvarsen, „Arctic Council Paused: The Search for A Future for Arctic Cooperation Continues”, *The High North News*, 27 aprilie 2022. Disponibil la <https://www.highnorthnews.com/en/arctic-council-paused-search-future-arcticcooperationcontinues#:~:text=The%20pause%20was%20introduced%20by,well%20as%20it%20sub%2Dbodies> și accesat la data de 13.07.2022.
- <sup>12</sup> U.S. State Department, ”Joint Statement on Arctic Council Cooperation Following Russia's Invasion of Ukraine”, Disponibil online la <https://www.state.gov/joint-statement-on-arctic-council-cooperation-following-russias-invasion-of-ukraine/> și accesat la 01.07.2022.
- <sup>13</sup> Whitney Lackenbauer P., Dean Ryan, “Arctic Exceptionalism”, în *The Arctic and World Order*, (Kristina Spohr and Daniel S. Hamilton eds.), Brookings Institution Press, 2020. Dispnil la <https://transatlanticrelations.org/wp-content/uploads/2020/12/The-Arctic-and-World-Order-ch14.pdf> și accesat la data de 02.07.2022.
- <sup>14</sup> Barry Scott Zellen, “Why a freeze on the Arctic Council is short-sighted”, *The Globe and Mail*, 27 aprilie 2022. Disponibil la <https://www.theglobeandmail.com/opinion/article-why-a-freeze-on-the-arctic-council-is-short-sighted-and-wrong/> și accesat la data de 03.07.2022.
- <sup>15</sup> Jack Watling, “Crisis, settlement, or containment - what is to be done on Russia?”, *Engelsberg Ideas*, 19 martie 2022. Disponibil la <https://engelsbergideas.com/essays/crisis-settlement-or-containment-what-is-to-be-done-on-russia/> și accesat la data de 03.07.2022.
- <sup>16</sup> President of Russia, *Decree on the Fundamentals of State Policy of the Russian Federation in the Arctic for the Period Until 2035*, 2020.
- <sup>17</sup> Radio Free Europe, ”Russia Adopts Updated Maritime Doctrine; Lists U.S., NATO As Primary Threats”. Disponibil la <https://www.rferl.org/a/russia-maritime-doctrine-threats-nato-us/31967675.html> și accesat la 02.08.2022.
- <sup>18</sup> Idem.
- <sup>19</sup> Eugene Rumer, Richard Sokolsky, Paul Stronski, *Russia in the Arctic. A Critical Examination*, Carnegie Endowment for International Peace, 29 martie 2021. Disponibil la <https://carnegieendowment.org/2021/03/29/russia-in-arctic-critical-examination-pub-84181> și accesat la data de 03.07.2022.
- <sup>20</sup> Idem.
- <sup>21</sup> Elizabeth Buchanan, “There Is No Arctic Axis”, *Foreign Policy*, 21 iulie 2020. Disponibil la <https://foreignpolicy.com/2020/07/21/no-arctic-axis-china-russia-relationship-resources-natural-gas-northern-sea-route/> și accesat la data de 04.07.2022.
- <sup>22</sup> Kerry Brown, “Will Russia be happy as China's junior partner?”, *Engelsberg Ideas*, 18 martie 2022. Disponibil la <https://engelsbergideas.com/notebook/will-russia-be-happy-as-chinas-junior-partner/> și accesat la data de 03.07.2022.

# MILITARIZAREA PENINSULEI CRIMEEA – CAPABILITĂȚI DE RĂZBOI ELECTRONIC ALE FEDERAȚIEI RUSE

*Simion-Călin GHEORGHÎĂ\**

## **Abstract**

*The article will give an argumentative response to an interesting question which travels nowadays. How many aircraft carriers does Russian Federation have, none, one or two? There are three possible answers to this question. The 1<sup>st</sup> answer and most common is one, because everyone knows that Russian Federation poses “Admiral Kuznetsov” aircraft carrier, an old ship which is undergoing a long repair and modernization process. The 2<sup>nd</sup> answer can be none because there are rumors which say that after finishing its repairment process, aircraft carrier “Admiral Kuznetsov” will be transformed in a museum and it won’t sail again. The 3<sup>rd</sup> answer, a more realistic one, may be two, if we take into consideration the fact that Crimean Peninsula can act as an aircraft carrier.*

*We all know that aircraft carriers never sail alone, they always have a group of ships/vessels near them in order to provide logistic support, assure force protection on sea, from land or from underwater threats and sometimes it can be a deterrence force in the region. Within the article I will argue that the third answer is right and Crimean Peninsula can be considered a plane carrier by showing its military capabilities, insisting on contribution of electronic warfare assets to A2/AD (Anti-Access/Area-Denial) environment.*

**Keywords:** *Electronic Warfare; Anti-Access/Area-Denial; electronic surveillance; electronic attack; electronic protection.*

## **INTRODUCERE**

Indiferent de statutul avut (*hanat tătar, stăpânire țaristă, republică autonomă sau parte integrantă a Ucrainei*), Peninsula Crimeea a reprezentat o miză geostrategică de-a lungul timpului pentru statele puternice, riverane Mării Negre și nu numai. Fiind stăpânită succesiv de tătari, ruși, ucraineni și, în prezent, iar de ruși, peninsula a constituit și constituie un motiv de dispută datorită poziției sale strategice în

centrul Mării Negre, fapt care permite statului ce o stăpânește să câștige și să dețină supremația militară în regiune.

Imediat după anexarea Crimeii, în urma referendumului din 16 martie 2014, liderii de la Moscova au acordat peninsulei și orașului Sevastopol statutul de *subiecte federale* ale Federației Ruse, în acest mod putându-se alocă fonduri de la bugetul de stat. Astfel, începând cu anul 2014, investițiile ruse în infrastructură au crescut semnificativ, acestea culminând cu

*\*Expert în cadrul Ministerului Apărării Naționale*

inaugurarea podului peste Strâmtoarea Kerci, la 15 mai 2018, care asigură, în momentul de față, o legătură terestră între peninsula și Federația Rusă<sup>1</sup>.

Investițiile ruse nu s-au limitat doar la domeniul economic, consolidarea din punct de vedere militar a peninsulei constituind o prioritate pentru autoritățile ruse. Realizând importanța strategică a peninsulei, începând cu 2014 Moscova și-a arătat adevăratele intenții și anume transformarea regiunii într-un avanpost care să reprezinte o amenințare reală pentru NATO și Uniunea Europeană.

Conform „Acordului Harkov” (semnat la 21 aprilie 2010, între președinții Dimitri Medvedev și Viktor Ianukovici)<sup>2</sup>, care prelungea până în anul 2042 termenul până la care capacitățile militare ruse puteau staționa în Peninsula Crimeea, numărul structurilor militare ruse și, implicit, al personalului aflat în peninsulă era limitat, acesta putând fi mărit, în situații de criză, cu acordul autorităților de la Kiev și în baza unei notificări prealabile din partea Federației Ruse.

În ianuarie 2014, înainte de anexare, Federația Rusă deținea în Peninsula Crimeea 12.500 de militari, 116 vehicule blindate, 24 piese artilerie, 22 de avioane de vânătoare, 37 de elicoptere și 26 de nave de luptă<sup>3</sup>. Ulterior, după anexare, Federația Rusă și-a consolidat prezența militară în peninsulă, implementând un mediu A2/AD (*Anti-Access/Aria-Denial*),<sup>4</sup> care să-i permită să controleze, limiteze și, la nevoie, să blocheze accesul forțelor altor state în regiunea Mării Negre<sup>5</sup>. Alături de suplimentarea personalului militar, care în anul 2020 ajungea la 32.500 militari<sup>6</sup>, Federația Rusă a dislocat în regiune și tehnică militară modernă: avioane de vânătoare și bombardament, tehnică navală cu capacități de lansare a rachetelor de tipul „Kalibr”, sisteme de apărare antiaeriană de tipul „S-400 Triumf” și „Panțir”, mijloace de apărare de coastă de tipul „Bal” și „Bastion”, mijloace de comunicații și război electronic<sup>7</sup>, care să-i asigure o apărare

multistratificată, interconectată și posibilități multiple de control a Mării Negre.

Conform specialiștilor ruși, „războiul electronic (*Radioelektronnaia borba* – lupta radioelectronică) este un ansamblu de acțiuni și activități specifice care constau în atacul electronic asupra mijloacelor electronice ale adversarului, protecția mijloacelor electronice proprii, contracararea acțiunilor de cercetare tehnică ale inamicului și sprijinul electronic al forțelor proprii”<sup>8</sup>. Așadar, războiul electronic reprezintă o formă a luptei armate care utilizează mijloace electronice împotriva sistemelor C4ISR<sup>9</sup> inamice, în scopul alterării calității informației vehiculate prin acestea și asigurării protecției trupelor proprii.

## FORȚELE ARMATE RUSE DIN PENINSULA CRIMEEA

În Peninsula Crimeea există cel puțin 100 de unități militare, de diferite arme și specialități, aparținând tuturor categoriilor de forțe armate, care pot fi grupate în patru componente: terestră, navală, aeriană și de apărare antiaeriană, subordonate operațional Comandamentului Operativ Strategic Întrunit Sud – Rostov pe Don<sup>10</sup>. Structurile militare din Peninsula Crimeea au o dublă subordonare. Din punct de vedere administrativ, componentele terestră și navală sunt subordonate ierarhic Comandamentului Forțelor Navale Ruse – Moscova, iar componentele aeriană și de apărare antiaeriană

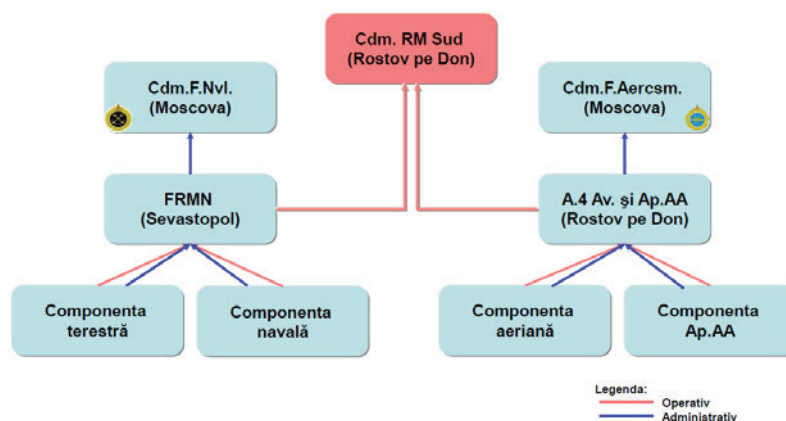


Fig.1 – Relațiile de subordonare a structurilor militare din Peninsula Crimeea



sunt subordonate Comandamentului Forțelor Aerospaciale – Moscova. Din punct de vedere operativ, cele patru componente se subordonează, prin intermediul comandamentelor Flotei Ruse a Mării Negre și Armatei a 4-a Aviație și Apărare Antiaeriană, Comandamentului Operativ Strategic Întrunit Sud – Rostov pe Don, structură care asigură comanda și controlul capacităților militare din Regiunea Militară Sud (figura 1).

Din multitudinea de unități aflate pe teritoriul Peninsulei Crimeea, cele mai importante și care pot constitui amenințări la adresa României sau a statelor membre NATO sunt cele prezentate în tabelul nr.1<sup>11</sup>.

Nr. crt.	Denumire unitate	Localizare	Apartenență
1.	Comandamentul Flotei Ruse a Mării Negre	Sevastopol	Forțele Navale
2.	Baza navală Crimeea	Sevastopol	Forțele Navale
3.	Corpul 22 Armată	Simferopol	Forțele Navale
4.	Divizia 27 Aviație	Belbek	Forțele Aerospaciale
5.	Divizia 31 Apărare Antiaeriană	Belbek	Forțele Aerospaciale
6.	Centrul 475 Război Electronic	Sevastopol	Forțele Navale

Tabelul nr. 1: Principalele structuri militare ruse din Peninsula Crimeea

Structurile prezentate au în organică unități de diferite arme și specialități, înzestrate cu tehnică modernă, o parte din personalul acestora participând activ la ocuparea peninsulei în anul 2014 și, ulterior, la acțiuni militare în teatrul de operații din Siria.

### a) Componenta terestră

Componenta terestră este reprezentată, în principal, de structurile de infanterie marină, artilerie, apărare de coastă și război electronic, subordonate Corpului 22 Armată – Simferopol<sup>12</sup>, înființat în anul 2016. Dintre structurile amintite se remarcă Brigada 810 Infanterie Marină – Sevastopol, cu un rol major în anexarea peninsulei și Brigada 127 Cercetare – Sevastopol. Structurile au în dotare tehnică modernă, printre care transportoare blindate de tipul „BTR-82AM” și vedete rapide de tipul „Raptor” sau bărci anti-sabotaj de tipul „Graniciok”. Alte structuri importante sunt Brigăzile 15 și 126 de Apărare de Coastă – Perevalnoe, care au în înzestrare

sisteme de rachete de tipul „Bastion”, „Bal” și „Utes”, instalate în poziții fixe sau mobile de-a lungul coastelor Crimeii.

Tot din cadrul componentei terestre face parte și Centrul 475 Război Electronic – Sevastopol, structură de nivel batalion care are în înzestrare atât capacități de ordin tactic, cât și operativ-strategic. Dintre capacitățile de nivel tactic, aflate în înzestrarea centrului, cele mai importante sunt sistemele de război electronic de tipul „Diabazol”, „Krasuha 2”/„Krasuha 4” și „Leer 2”/„Leer 3”, acestea operând atât în gama undelor scurte (HF), cât și în gama undelor ultracurte (VHF). Sistemele dispun de puteri de

emisie mari, capabile să neutralizeze prin bruiaj diferite mijloace de comunicații ale adversarului. Toate aceste sisteme au fost testate și în condiții de luptă reală în Donbas sau Siria, având un factor multiplicator asupra acțiunilor de luptă.

Sistemul automatizat de război electronic de tipul „Diabazol”<sup>13</sup> (figura 2), varianta pe roți a sistemului șenilat de tipul



Fig. 2 – Sisteme de RE aparținând componentei terestre (sursa: Jonas Kjellén, Russian Electronic Warfare – The Role of Electronic Warfare in the Russian Armed Forces, pag. 44, 48, 52)



„Borisoglebsk”, este destinat executării acțiunilor de supraveghere în banda de frecvențe 100-2000 MHz și bruiaj electronic în benzile de frecvențe 100-965, 1500-1700 și 1700-1900 MHz, fiind compus din cinci autospeciale de tipul „R-330KMA”, „R-330J (Jitel)”, „R-934UM (Sinița)”, „R-378UM” și „Altaeș-AM”<sup>14</sup>. Autospeciile din compunere pot acționa asupra comunicațiilor radio din benzile V/UHF, comunicațiilor GSM, terminalelor de comunicații prin satelit „INMARSAT” și „IRIDIUM”, precum și a echipamentelor de navigație GPS.

Sistemele de război electronic de tipul „Leer 2” (figura 2) și „Leer 3”<sup>15</sup> sunt destinate căutării, interceptării, identificării și localizării emisiilor electromagnetice de comunicații în banda VHF și executării bruiajului electronic asupra acestora. Sistemul de tipul „Leer 3” este varianta modernă, care dispune și de trei UAV-uri de tipul „Orlan 10”<sup>16</sup>, pe care este instalat elementul de bruiaj activ.

Sistemul de război electronic de tipul „Krasuha 2” (figura 2) este destinat executării bruiajului electronic de non-comunicații, în banda 2,9-3,2 GHz, în scopul protecției obiectivelor terestre împotriva atacurilor aeriene<sup>17</sup>. La rândul său, sistemul de război electronic de tipul „Krasuha 4” (figura 2) este destinat executării bruiajului electronic de non-comunicații, fiind utilizat în special pentru prevenirea și contracararea supravegherii electronice executate de către inamic prin intermediul sateliților de cercetare, sistemelor radar terestre, dronelor de supraveghere și sistemelor aeropurtate de avertizare timpurie (aeronave de cercetare de tipul „E-8C”, UAV-urile de tip „Predator”, „Global Hawk”, sateliții de cercetare „Lacrosse”). Complexul poate asigura protecția unor obiective terestre de nivel operativ-strategic<sup>18</sup>.

## b) Componenta aeriană

Componenta aeriană deține un rol decisiv în executarea acțiunilor de luptă. Ultimele conflicte au arătat că fără a deține supremația aeriană este foarte greu să fie introduse în luptă forțele terestre. Federația Rusă a realizat importanța mijloacelor aeriene, investind masiv în infrastructura militară din Peninsula Crimeea. Componenta aeriană este

foarte bine reprezentată în peninsulă, structurile cele mai importante fiind cele ale Diviziei 27 Aviație – Belbek (*Sevastopol*), care are în organică două regimente de aviație și un regiment de elicoptere, identificate ca fiind:

- Regimentul 37 Aviație – Belbek, înzestrat cu avioane de luptă de tipul „Suhoi 27”, „Suhoi 27SM” și „Suhoi 30M2”<sup>19</sup>;

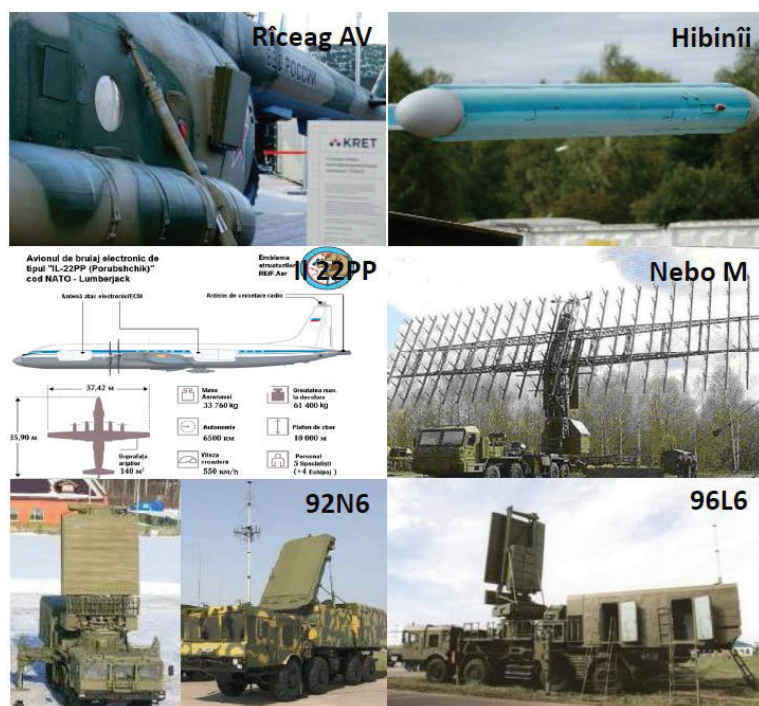
- Regimentul 38 Aviație – Gvardeisk, înzestrat cu avioane de luptă de tipul „Suhoi 24M”, „Suhoi 24MR” și „Suhoi 25SM”<sup>20</sup>;

- Regimentul 39 Aviație – Djankoi (*estul peninsulei*), înzestrat cu elicoptere de tipul „Mi-28N”, „Ka-52”, „Mi-35” și „Mi-8AMTSH”<sup>21</sup>.

Cea de-a doua structură este Divizia 31 Apărare Antiaeriană – Belbek, care are în organică două regimente de apărare antiaeriană și un regiment de trupe radiotehnice. Regimentele de apărare antiaeriană au în dotare mijloace moderne, printre care complexe de apărare antiaeriană de tipul „S-400 Triumph”. Astfel, în peninsulă sunt instalate în poziții de apărare cinci complexe de apărare antiaeriană de tipul „S-400 Triumph”, în zona localităților Evpatoria, Sevastopol, Feodosia, Djankoi și Kerçi<sup>22</sup>. Ultimul complex, instalat la începutul anului 2019 la Kerçi, are misiunea de a asigura apărarea podului de peste Strâmtoarea Kerçi.

Din perspectiva războiului electronic, la nivelul componentei aeriene regăsim mijloace de autoprotecție a platformei, care pot asigura protecția individuală sau a unui grup de aeronave și echipamente specifice. Sistemele de autoprotecție sunt reprezentate de sistemul de război electronic de tipul „Rîceag-AV”, care echipează elicopterele de tipul „Mi-8MTPR-1”, și sistemul aeropurtat de tipul „Hibinî”, instalat pe avioanele de vânătoare de tipul „Su-34”, „Su-35S” și „Su-30SM” (figura 3).

Sistemul de tipul „Rîceag-AV” asigură protecția unei grupări aeriene împotriva rachetelor dirijate prin radar, infraroșu și laser, pe o rază de aproximativ 300 de km, precum și față de bruiajul comunicațiilor aferente UAV-urilor inamice.<sup>23</sup> Sistemul aeropurtat de tipul „Hibinî”, cunoscut în urma incidentului cu distrugătorul american USS „Donald Cook” (aprilie 2014, *Marea Neagră*)<sup>24</sup>, funcționează în banda de



**Fig. 3 – Sisteme radar și RE aparținând componentei aeriene**  
(sursa: Jonas Kjellén, Russian Electronic Warfare – The Role of Electronic Warfare in the Russian Armed Forces, pag. 56, 58, respectiv [www.topwar.ru](http://www.topwar.ru))

frecvență de 1,2-40 GHz, cu o putere de 250 W, și este destinat să înlocuiască toate sistemele de război electronic de autoprotecție individuale și de grup instalate pe aeronavele de vânătoare ale Federației Ruse.

Alături de mijloacele de autoprotecție, componenta aeriană dispune și de platforme aeriene de război electronic, precum avionul de tipul „*IL-22 Porubshchik PP*” (figura 3)<sup>25</sup>, varianta superioară a aeronavei „*AN-12 PP*”, și avioanele de cercetare de tipul „*Su-24MR*”. Dintre platformele amintite, o aeronavă de tipul „*AN-12 PP*” se află în înzestrarea Regimentului 318 Aviație Mixtă – Kacia<sup>26</sup>, iar șase avioane de tipul „*Su-24MR*” în înzestrarea Regimentului 43 Aviație Asalt – Saki<sup>27</sup>.

Alături de mijloacele specifice de război electronic, la nivelul componentei aeriene există numeroase echipamente radar care sunt utilizate pentru culegerea de date și informații din mediul electromagnetic și pentru avertizare timpurie. Radarul de tipul „*NEBO-M*” (figura 3) este un sistem de supraveghere și avertizare multibandă destinat descoperirii și urmăririi țintelor aeriene, inclusiv a aeronavelor cu

tehnologie „*Stealth*” care evoluează la viteze supersonice, a rachetelor balistice și de croazieră, în condițiile unui bruiaj electronic puternic<sup>28</sup>. Sistemul, care acționează în gama de frecvență 150-200 MHz, este compus dintr-un centru de comandă și trei stații radar instalate pe vehicule 8x8 de 24 de tone. În mod circular, radarul de tipul „*NEBO-M*” are o rază de acțiune de 600 km, iar în sector de 1800 km, și poate detecta până la 200 de ținte simultan<sup>29</sup>.

De asemenea, radarele de identificare și de angajare a țintelor din cadrul sistemelor de apărare antiaeriană de tipul „*S-400 Triumph*”, „*92N6*”, respectiv „*96L6*”, pot fi considerate mijloace de război electronic deoarece furnizează coordonatele țintelor care urmează a fi angajate kinetic sau non-kinetic.

Radarele descoperă ținte până la distanțe de 300 km, fiind capabile ca, în modul urmărire-scanare, să supravegheze până la 100 de ținte, dintre care 6 în mod simultan<sup>30</sup>.

### c) Componenta navală

De departe cea mai importantă, componenta navală a fost revitalizată cel mai mult. Începând cu anul 2014, Flota Rusă a Mării Negre a fost înzestrată cu peste 60 de nave, submarine, vedete rapide și nave auxiliare care au intrat în organica Divizei 30 Nave de Suprafață și a Brigăzilor 41 Vedete Purtătoare de Rachete, 68 Nave Antisubmarin și 197 Nave Desant din Sevastopol. Alte structuri importante din cadrul componentei navale sunt Divizionul 519 Nave Cercetare Electronică – Sevastopol și Divizia 4 Submarine – Novorossiisk, ale cărei submarine desfășoară, prin rotație, misiuni în Marea Neagră și Marea Mediterană. Începând cu anul 2016, Flota Rusă a Mării Negre a fost dotată cu șase submarine moderne, din clasa Kilo II (*Varșavianka*), cu capacități de lansare a rachetelor de croazieră de tipul „*Kalibr*”: „*Rostov pe Don*”, „*Krasnodar*”, „*Starîi Oskol*”, „*Novorossiisk*”,



„Kolpino” și „Veliki Novgorod”<sup>31</sup>. De regulă, două dintre aceste submarine desfășoară misiuni în Marea Neagră, două în Marea Mediterană, iar celelalte două se află în rezervă sau în diferite operațiuni de întreținere (*verificări periodice, schimbare acumulatori sau reparații*). Alături de cele șase submarine, Flota Rusă a Mării Negre a primit sau urmează să primească în înzestrare câte șase nave din următoarele clase: fregate „Amiral Grigorovici”, nave purtătoare de rachete „Buyan” și „Buyan M”, nave purtătoare de rachete „Karakut” și nave purtătoare de rachete „Vasilii Bikov”<sup>32</sup>, toate cu capabilități de lansare a rachetelor de croazieră de tipul „Kalibr”.



Fig. 4 – Sisteme RE aparținând componentei aeriene  
(sursa: Jonas Kjellén, Russian Electronic Warfare – The Role of Electronic Warfare in the Russian Armed Forces, pag. 59, respectiv [www.topwar.ru](http://www.topwar.ru))

Din punct de vedere al războiului electronic, Forțele Navale dispun de mijloace de protecție a platformei de tipul „TK-25”<sup>33</sup> (figura 4) sau varianta modernă „TK-28”<sup>34</sup>, care lucrează în gama de frecvențe 1 MHz-40 GHz (*bruijaj activ în banda 250 MHz - 18 GHz*) și pot fi instalate pe nave cu un deplasament cuprins între 200 și 10.000 de tone. Sistemele de tipul „TK-25”, respectiv „TK-28”, sunt destinate asigurării protecției navelor din diferite clase împotriva amenințărilor dirijate prin radar, prin utilizarea bruijajului activ. Echipamentele pot funcționa atât în regim automat, cât și cu comandă manuală.

Cu toate că nu pot fi catalogate ca și capabilități de război electronic, navele de cercetare electronică din cadrul Divizionului 519 Nave Cercetare Electronică – Sevastopol sunt destinate pentru culegerea de date și informații din mediul electromagnetic și nu numai. În funcție de clasă, acestea sunt înzestrate

cu diverse sisteme, mai vechi sau modernizate. Navele de cercetare radioelectronică din dotarea Flotei Ruse a Mării Negre sunt în număr de patru: „Ivan Hurs” (clasa *Iuri Ivanov*), cea mai modernă, a fost repartizată în Marea Neagră în anul 2018 (din cauza incidentului din 27.04.2017, când nava de cercetare electronică „Liman” s-a scufundat în Marea Neagră, în urma ciocnirii cu vasul cargo „Youzarshif H”, care naviga sub pavilion togolez)<sup>35</sup>, „Ekvator”, „Kildin” (clasa *MOMA*) și „Priazovie” (clasa *VIȘNIA*).

Toate navele dispun de mijloace active și pasive de protecție, care în funcție de rolul și deplasamentul navei pot avea diferite versiuni pentru un echipament de RE din aceeași clasă.

Alături de sistemele prezentate, în Peninsula Crimeea mai sunt instalate în poziții fixe și mijloace de RE de nivel strategic sau tactic-operativ, capabile să detecteze ținte și să culegă date la distanțe foarte mare.

Sistemul de RE de tipul „Murmansk-BN”<sup>36</sup> (figura 5) este un complex de nivel strategic, destinat să execute acțiuni de război electronic asupra sistemelor de comunicații radio care deservește elemente de comandă-control militare ale SUA și NATO, respectiv asupra sistemelor aerportate de recunoaștere aeriană și de avertizare timpurie. Sistemul este compus din șapte autospeciale pe platformă „KamAZ-6560”, se instalează complet în 72 de ore și funcționează în banda HF



Fig. 5 – Sisteme de RE de nivel strategic  
(sursa: [www.topwar.ru](http://www.topwar.ru))

(1,5-30 MHz). Putera sistemului este de 20 kW, iar înălțimea catargelor antenelor este de 32 metri<sup>37</sup>.

Radarul OTH\* de tip „Podsolnuh” (figura 5)<sup>38</sup> permite în mod automat, în afara orizontului radio, simultan sau secvențial, detectarea, însoțirea și clasificarea a până la 300 de ținte navale și 100 de ținte aeriene. Radarul este capabil să asigure controlul zonei de coastă până la o distanță de 200 de mile marine. De asemenea, determină coordonatele țintelor și le livrează automatizat sistemelor de identificare a țintelor și complexelor de armament de coastă și de la bordul navelor. Radarul funcționează în banda de frecvență 3-15 MHz, iar cele două câmpuri de antene necesită a fi instalate separat, la distanțe de minim 500 și maxim 3.500 m unul de altul<sup>39</sup>.

Radarul de tipul „Voronej-SM”<sup>40</sup> este un sistem radar de avertizare timpurie de nouă generație, capabil să detecteze ținte de dimensiuni reduse de la distanțe foarte mari. Acesta lucrează în unde centimetrice (3-30 GHz), putând urmări ținte până la distanța de aproximativ 6.000 de kilometri.

## ANALIZA AMENINȚĂRILOR DIN MEDIUL ELECTROMAGNETIC

Din punct de vedere al analizei amenințării și a contribuției războiului electronic la consolidarea capabilităților A2/AD din Peninsula Crimeea, Federația Rusă dispune de echipamente speciale care pot executa întreg spectrul de acțiuni de război electronic în mediul electromagnetic și de posibilități radar cu acoperire în spectrul specific, capabile să detecteze tehnologia „Stealth” și platforme aeriene la distanțe mari (figura 6).

În distanță, amenințarea este caracterizată de posibilitățile tehnice ale echipamentelor, acestea permițând executarea de acțiuni de război electronic în tot bazinul Mării Negre (figura 7). După cum se poate observa, capabilitățile de detecție acoperă mult mai mult decât suprafața Mării Negre și sunt orientate în principal pe direcția strategică SV, pentru a acoperi Europa și cea mai mare parte a Mării Mediterane. La nivel global, sistemul RE de tipul „Murmansk BM” poate fi utilizat și asupra legăturilor de comunicații

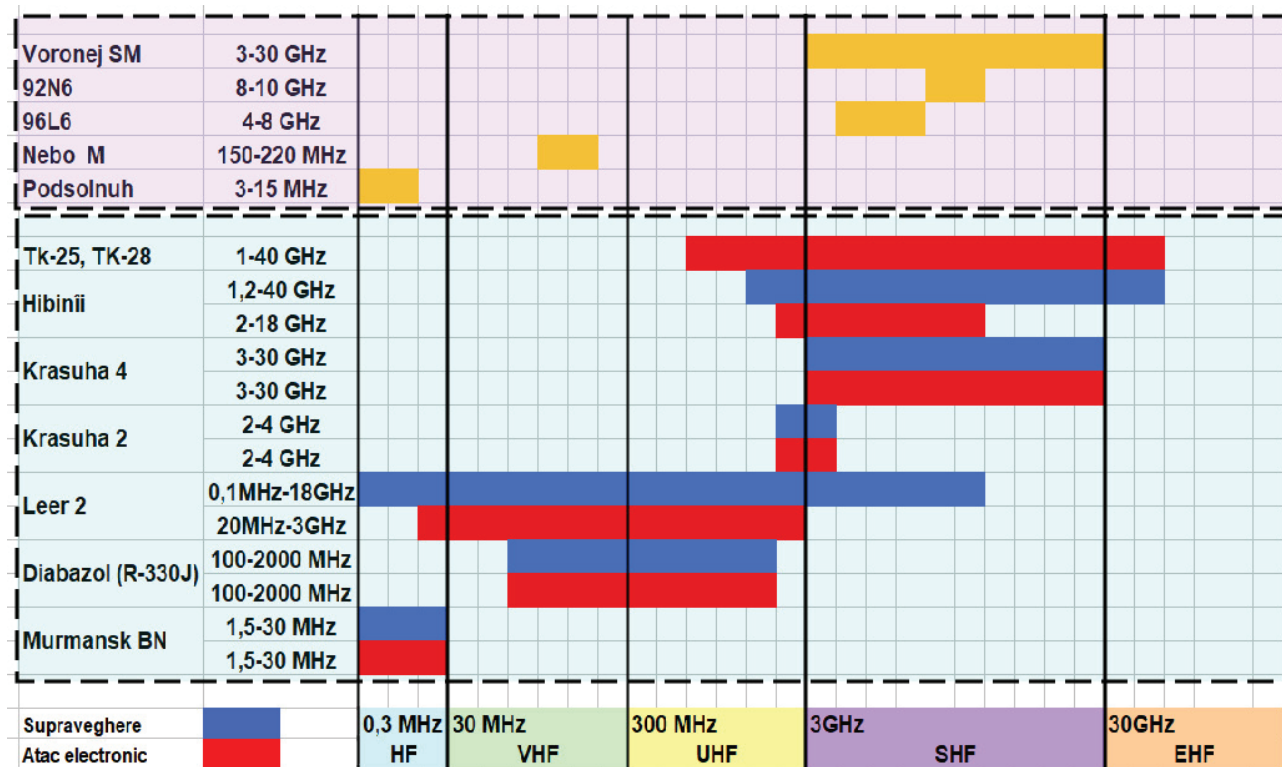
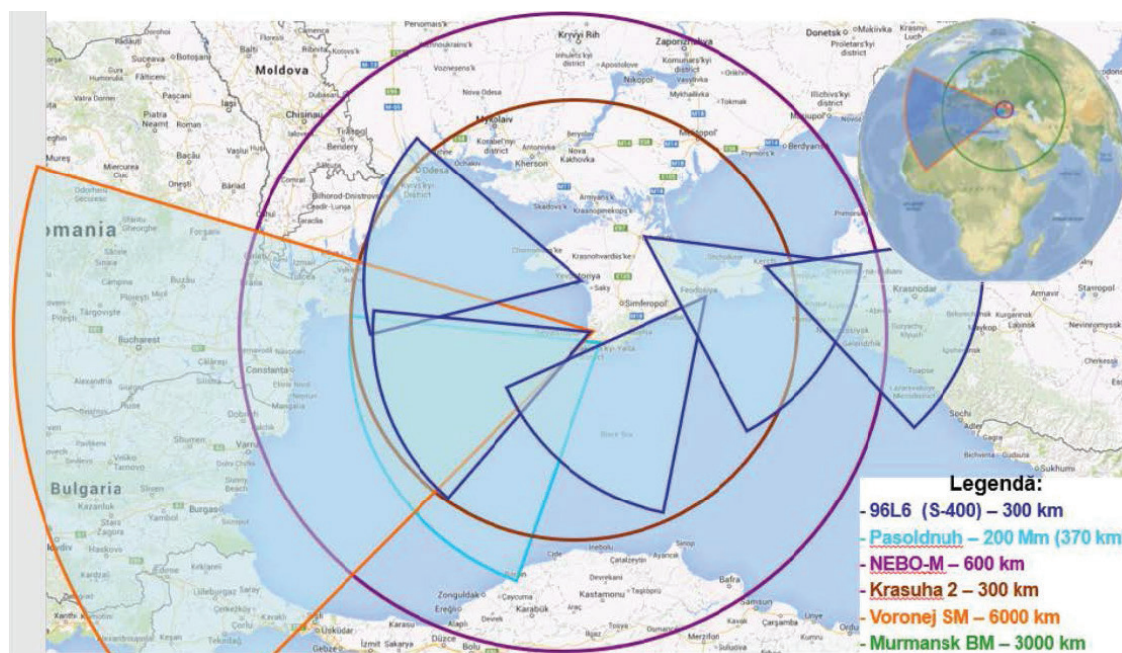


Fig. 6 – Analiza amenințărilor din spectrul electromagnetic

\* Over The Horizon





**Fig. 7 – Acoperirea la nivel regional și global  
cu echipamentele de război electronic din Peninsula Crimeea**

din cadrul comandamentelor regionale NATO; acesta, în anumite condiții, acționează până la o distanță maximă de 3.000 km.

## CONCLUZII

Investițiile ruse în domeniul militar din Peninsula Crimeea au rolul de a consolida capacitățile A2/AD, acest lucru permițându-i Federației Ruse să dețină supremația în Marea Neagră, să limiteze accesul capacităților NATO în regiune, să monitorizeze activitatea acestora în permanență și pe timpul activităților de instruire cu statele riverane și, nu în ultimul rând, să contribuie la proiecția forței în Marea Mediterană sau la susținerea și executarea unor acțiuni terestre din peninsulă pe teritoriul Ucrainei.

Dacă ținem cont de faptul că asemenea „bule”

există și în Kalinigrad, Tartus (Siria) și sunt în curs de dezvoltare în regiunea Arctică, ne putem da seama de importanța pe care forțele armate ale Federației Ruse o acordă războiului electronic și modului de utilizare a acestuia pentru descurajare și apărare regională. Din această perspectivă, forțele ruse au dezvoltat și au instalat în puncte fixe sau mobile, o serie de astfel de capacități care să constituie o amenințare permanentă la adresa membrilor NATO sau a statelor riverane Mării Negre. Având în vedere considerațiile de mai sus, se poate aprecia că Peninsula Crimeea a devenit una dintre cele mai bine apărate regiuni ale Federației Ruse; gruparea de trupe dislocată în peninsulă include tot ceea ce este necesar pentru a respinge un atac sau, cel puțin, pentru a rezista până la sosirea întăririlor.

## BIBLIOGRAFIE

1. BOWEN Andrew S., "Russian Armed Forces: Capabilities", *In Focus*, Congressional Research Service, iunie 2020, 3 p.
2. COSTEA Cătălin Alin, "The Russian Federation and the Implementation of the A2/AD System in the Black Sea: Risks and Threats to Romania", *The Market for Ideas*, 2016, <https://www.themarketforideas.com>, accesat la 08.02.2022.
3. EPISKOPOS Mark, "If Russia's Nebo-M Radar Can "See" the F-35, Is That Enough to Shoot It Down?", <https://nationalinterest.org>, 15 august 2021, accesat la 25.02.2022.

4. FREIER Nathan, "The Emerging Anti-Access/Area-Denial Challenge", *Center for Strategic and International Studies*, mai 2012, accesat la 08.02.2022.
5. HARDING Luke, "Ukraine extents lease for Russia's Black Sea Fleet", *The Guardian*, aprilie 2010, accesat la 03.02.2022.
6. KEIR Giles, BOULEGUE Mathieu, "Russia's A2/AD Capabilities: Real and Imagined", *Parameters: US Army War College Quarterly*, nr. 1-2, vol. 49, martie 2019, pp. 21-36.
7. KJELLÉN Jonas, *Russian Electronic Warfare – The Role of Electronic Warfare in the Russian Armed Forces*, Swedish Defence Research Agency, septembrie 2018, 105 p.
8. LAKIICIUK Pavlo, "Barracks in place of a resort. How Russia is turning occupied Crimea into a military base", martie 2021, disponibil la <https://informnapalm.org/en/crimea-military-base/>.
9. McDERMOTT Roger N., *Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum*, Report, Estonian International Centre for Defence and Security, septembrie 2017, 36 p.
10. MINICH Ruslan, "Russia Shows its Military Might in the Black Sea and Beyond", *Ukrainian World*, <https://ukraineworld.org/>, accesat la 08.02.2022.
11. MIZOKAMI Kyle, "Check Out Russia's, Stealth' Kilo-Class Submarine. Here's What It Can Do", <https://nationalinterest.org.>, accesat la 02.03.2022.
12. OXENSTIERNA Susanne, Westerlund Fredrik (eds.), *Russian Military Capability in a Ten-Year Perspective – 2019*, Swedish Defence Research Agency, septembrie 2019, 146 p.
13. ROTH Andrew, "Putin opens 12-mile bridge between Crimea and Russian mainland", *The Guardian*, accesat la 02.02.2022.
14. SMITH Patrick, *Russian Electronic Warfare A Growing Threat to U.S. Battlefield Supremacy*, American Security Project, aprilie 2020, 11p.
15. THOMAS Timothy L., *Russian Military Thought: Concepts and Elements*, MITRE Corporation, august 2019, 187 p.
16. TUCKER Patrick, "Five S-400 anti-aircraft missile batteries, plus additional troops and fighters, let Moscow better defend the Black Sea and threaten Europe and the Middle East", [www.defenseone.com](http://www.defenseone.com), accesat la 25.02.2022.
17. \*\*\*, Ukraine conflict: Equipment profile, *Janes*, februarie 2022.
18. \*\*\*, *The Military Balance 2021*, The International Institute of Strategic Studies, 2021.

<sup>1</sup> Andrew Roth, "Putin opens 12-mile bridge between Crimea and Russian mainland", *The Guardian*, disponibil la <https://www.theguardian.com/world/2018/may/15/putin-opens-bridge-between-crimea-and-russian-mainland>, accesat la 02.02.2022.

<sup>2</sup> Luke Harding, "Ukraine extents lease for Russia's Black Sea Fleet", *The Guardian*, disponibil la <https://www.theguardian.com/world/2018/apr/21/ukraine-black-sea-fleet-russia>, accesat la 03.02.2022.

<sup>3</sup> Cătălin Alin Costea, "The Russian Federation and the Implementation of the A2/AD System in the Black Sea: Risks and Threats to Romania", *The Market for Ideas*, disponibil la <https://www.themarketforideas.com/the-russian-federation-and-the-implementation-of-the-a2-ad-system-in-the-black-sea-risks-and-threats-to-romania-a176/>, accesat la 08.02.2022.

<sup>4</sup> Nathan Freier, "The Emerging Anti-Access/Area-Denial Challenge", Center for Strategic and International Studies, disponibil la <https://www.csis.org/analysis/emerging-anti-accessarea-denial-challenge>, accesat la 08.02.2022.

<sup>5</sup> Mathieu Boulegue, Keir Giles, *Russia's A2/AD Capabilities: Real and Imagined*, pag.28.

<sup>6</sup> Pavlo Lakiichuk, "Barracks in place of a resort. How Russia is turning occupied Crimea into a military base", *InformNapalm*, disponibil la <https://informnapalm.org/en/crimea-military-base/>, accesat la 08.02.2022.

<sup>7</sup> Ruslan Minich, "Russia Shows its Military Might in the Black Sea and Beyond", *Ukrainian World*, disponibil la <https://ukraineworld.org/articles/russian-aggression/russia-shows-its-military-might-black-sea-and-beyond>, accesat la 08.02.2022.

- <sup>8</sup> Jonas Kjellén, *Russian Electronic Warfare – The Role of Electronic Warfare in the Russian Armed Forces*, pag.21.
- <sup>9</sup> C4ISR – Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance.
- <sup>10</sup> <https://structure.mil.ru/structure/okruga/south>, accesat la 03.02.2022.
- <sup>11</sup> Susanne Oxenstierna, Fredrik Westerlund, *Russian Military Capability in a Ten-Year Perspective*, 2019, pag 49-50.
- <sup>12</sup> Ibid.
- <sup>13</sup> Roger McDermott, "Russia's Electronic Warfare Capabilities as a Threat to GPS", The Jamestown Fundation, disponibil la <https://jemaestown.org/program/russias-electronic-warfare-capabilities-as-a-threat-to-gps/>, accesat la 09.02.2022.
- <sup>14</sup> Jonas Kjellén, *Russian Electronic Warfare – The Role of Electronic Warfare in the Russian Armed Forces*, pag.45.
- <sup>15</sup> <https://topwar.ru/136447-kompleks-rb-341v-leer-3-bombardirovshik-reb-i-prosto-poleznyy.html>, accesat la 09.02.2022.
- <sup>16</sup> Jonas Kjellén, *Russian Electronic Warfare – The Role of Electronic Warfare in the Russian Armed Forces*, pag.49.
- <sup>17</sup> <https://topwar.ru/136221-krasuha-2o-po-nastoyaschemu-tyazhelyy-sluchay.html>, accesat la 09.02.2022.
- <sup>18</sup> <https://www.globalsecurity.org/military/world/russia/krasukha4.htm>, accesat la 09.02.2022.
- <sup>19</sup> <https://www.milkavkaz.org>, accesat la 15.12.2020.
- <sup>20</sup> Ibid.
- <sup>21</sup> Ibid.
- <sup>22</sup> Patrick Tucker, "Five S-400 anti-aircraft missile batteries, plus additional troops and fighters, let Moscow better defend the Black Sea and threaten Europe and the Middle East", disponibil la <https://www.defenseone.com/threats/2019/06/exclusive-satellite-photos-detail-russian-military-buildup-crimea/157642/>, accesat la 25.02.2022.
- <sup>23</sup> Jonas Kjellén, *Russian Electronic Warfare – The Role of Electronic Warfare in the Russian Armed Forces*, pag.58.
- <sup>24</sup> Jonas Kjellén, *Russian Electronic Warfare – The Role of Electronic Warfare in the Russian Armed Forces*, pag.56.
- <sup>25</sup> Jonas Kjellén, *Russian Electronic Warfare – The Role of Electronic Warfare in the Russian Armed Forces*, pag.58.
- <sup>26</sup> <https://www.milkavkaz.org>, accesat la 15.12.2020.
- <sup>27</sup> Ibid.
- <sup>28</sup> Mark Episkopos, "If Russia's Nebo-M Radar Can See the F-35, Is That Enough to Shoot It Down", disponibil la <https://nationalinterest.org/blog/reboot/if-russia%E2%80%99s-nebo-m-radar-can-%E2%80%98see%E2%80%99-f-35-enough-shoot-it-down-191785>, accesat la 25.02.2022.
- <sup>29</sup> Ibid.
- <sup>30</sup> <https://en.topwar.ru/169425-zenitnaja-raketnaja-sistemy-s-400-i-zenitnyj-raketnyj-kompleks-s-350-s-pricelom-v-budushee.html>, accesat la 25.02.2022.
- <sup>31</sup> Kyle Mizokami, "Check Out Russia's 'Stealth' Kilo-Class Submarine. Here's What It Can Do", disponibil la <https://nationalinterest.org/blog/buzz/check-out-russias-stealth-kilo-class-submarine-heres-what-it-can-do-54852>, accesat la 02.03.2022.
- <sup>32</sup> <https://www.maritime-executive.com/editorials/russias-black-sea-fleet-buildup>, accesat la 02.03.2022.
- <sup>33</sup> Catalogul Rosoboronexport, disponibil la <https://roe.ru/eng/catalog/naval-systems/shipborne-electronic-systems/tk-25/>, accesat la 28.02.2022.
- <sup>34</sup> Jonas Kjellén, *Russian Electronic Warfare – The Role of Electronic Warfare in the Russian Armed Forces*, pag.59.
- <sup>35</sup> <https://turkishnavy.net/2017/04/27/russian-intelligence-gathering-ship-liman-sunk-off-the-coast-of-istanbul/>, accesat la 02.03.2022.
- <sup>36</sup> <https://topwar.ru/103795-rossiyskaya-promyshlennost-sozdaet-sistemu-reb-strategicheskogo-naznacheniya.html>, accesat la 28.02.2020.
- <sup>37</sup> Ibid.
- <sup>38</sup> <http://roe.ru/eng/catalog/naval-systems/stationary-electronic-systems/podsolnukh-e/>, accesat la 28.02.2022.
- <sup>39</sup> Ibid.
- <sup>40</sup> <https://www.globalsecurity.org/wmd/world/russia/voronezh-sites.htm>, accesat 02.03.2022.



# VIRTUALIZAREA MEDIULUI OPERAȚIONAL

*Marian ȘTEFAN\**

## **Abstract**

*Cyber operations operated by state actors and non-state entities to recognize and gain presence in relevant networks take place every second and are nowadays a permanent feature of cyberspace. The greatest risk posed by these actions is given by the erroneous attribution of the attacker and the positioning and reaction of the response structures that could give a misinterpretation of the type of cyber attack and therefore could cause a series of retaliation as a result, and escalating the situation could easily get out of hand. A number of other risks involve the acquisition of cyber capabilities by criminal or terrorist organizations and the ease with which they can be turned into highly effective offensive tools in the free market. In conclusion, virtual space has inevitably become a key new segment of the operational environment, risking both the actions of non-state actors and competition between states in the 21st century. The development of information technology has changed the nature of conflicts by creating an additional layer of complexity of traditional battle spaces. Almost global access to the virtual environment has created many opportunities to engage in online battles that affect events both in the physical realm, such as computer systems, and in the cognitive realm of people's attitudes and beliefs.*

**Keywords:** operational environment; virtual environment; technology; hybrid threats.

## **INTRODUCERE**

Actorii statali și non-statali actuali utilizează abordări hibride pentru a-și urmări obiectivele politice și militare, combinând abil operațiunile militare cu atacurile cibernetice, presiunea diplomatică și/sau economică și campaniile de dezinformare (propagandă). În ultimul deceniu, *social media* a devenit rapid unul dintre principalele canale de comunicare utilizate, iar infrastructurile informaționale, rețelele și platformele virtuale de comunicare au fost luate în considerare în elaborarea noilor strategii militare și de securitate. Conflictele din ultimii ani, cum

au fost cele din Libia, Siria, Afganistan, Irak și Ucraina, au demonstrat faptul că *social media* este utilizată pe scară largă pentru a coordona acțiunile, a colecta informații și, cel mai important, pentru a influența credințele și atitudinile publicului țintă, adeseori mobilizându-le pentru acțiune.

Natura complexă și adaptativă a mediului de securitate contemporan și caracterul imprevizibil al acestuia generează dificultăți de analiză a informațiilor și a volumelor de date și aduce în prim-plan ideea că prognozele și scenariile care funcționează într-o situație pot să nu funcționeze în alta asemănătoare, din cauza actorilor implicați, a naturii relațiilor acestora cu entitățile din

\* *Expert în Ministerul Apărării Naționale.*



mediul operațional, precum și din cauza lipsei de comunicare și înțelegere a informațiilor la nivel strategic.

Comunicatul final al Summit-ului NATO din 2018, de la Bruxelles, afirma că statele membre NATO „au fost supuse unei provocări crescânde atât din partea actorilor statali, cât și non-statali, care utilizează amenințări hibride cu scopul de a crea ambiguitate și de a estompa liniile dintre pace, criză și conflict”<sup>1</sup>. Termenul „hibrid” a fost folosit pentru a descrie o gamă largă de măsuri, mijloace și tehnici care includ (dar nu se limitează la): dezinformare, atacuri cibernetice, facilitarea migrației, spionaj, manipularea dreptului internațional, amenințări cu utilizarea forței (atât de către grupurile armate neregulate, cât și de forțele convenționale), subversiune politică, sabotaj, terorism, presiune economică și dependență de resurse energetice.

NATO definește amenințările hibride ca fiind un „tip de amenințare care combină activitățile convenționale, neregulate și asimetrice în timp și spațiu”<sup>2</sup>. Această abordare oferă esența unui produs al sinergiei diferitelor măsuri întreprinse, însă, în aceeași măsură, lasă posibilități de interpretare largă a multor scenarii ce implică utilizarea unui spectru larg al amenințărilor convenționale și neconvenționale. Majoritatea definițiilor actuale ale amenințărilor hibride se bazează puternic pe acțiunile Federației Ruse din Donbas și Crimeea, dar acest lucru riscă să neglijeze unul dintre aspectele cheie ale amenințărilor hibride, cel al adaptabilității. În timp ce abordările referitoare la natura esențială a caracterului hibrid al unei amenințări vor continua să provoace dezbateri, fenomenele care stau la baza termenului rămân reale și produc efecte. Prin urmare, efortul trebuie să se concentreze pe modalitatea în care se pot identifica și utiliza informațiile cu privire la caracteristicile amenințărilor hibride ce afectează mediul operațional.

## ÎNȚELEGEREA VIRTUALIZĂRII MEDIULUI OPERAȚIONAL

Cunoașterea și înțelegerea modului în care acțiunile materializate prin amenințări hibride acționează ca pârgii de influență necesită o

schimbare de perspectivă, de la concentrarea asupra lumii reale/fizice, în care apar evenimente și acțiuni, la domeniul conceptual în care există informațiile și are loc comunicarea.

Mediul informațional este un model de studiu ce trebuie luat în considerare pentru înțelegerea modului în care interacționează actorii și publicul țintă, modul în care oamenii văd lumea din jurul lor și, prin urmare, iau decizii pe baza sensului pe care îl deduc din propria percepție. Acest spațiu conceptual este format din trei dimensiuni interdependente: cognitivă (unde oamenii gândesc, înțeleg și decid), fizică (indivizi, organizații și infrastructură) și informațională (fapte, cunoștințe și date). Analiza mediului informațional poate ajuta la înțelegerea modului în care amenințările hibride exploatează vulnerabilitățile identificate, cum ar fi diviziunile culturale sau stările de nemulțumire de la nivelul societății, generate de aspecte sociale și economice, pentru a submina sau diviza națiunea vizată, beneficiind, în același timp, de interesele strategice ale unui actor responsabil.

Abordarea problemelor interne și construirea rezilienței sociale este o componentă cheie a combaterii amenințărilor hibride. Toate activitățile întreprinse de un actor, ce instrumentează seturi de amenințări hibride, vizează afectarea mediului informațional și influențează luarea deciziilor în dimensiunea cognitivă. Așadar, în timp ce informațiile pot ajuta o entitate națională, capacitatea de a influența audiențele țintă și de a produce efecte provine din sinergia tuturor instrumentelor de putere națională, inclusiv măsuri diplomatice, informaționale, militare și economice. În același timp, sinergia diferitelor măsuri ostile poate exploata vulnerabilitățile în întreaga gamă a variabilelor mediului operațional ale unei națiuni vizate - politică, militară, economică, socială, informațională și de infrastructură (cunoscută sub numele de spectrul PMESII).

În ultimii 20 de ani, capabilitățile cibernetice au devenit un nou instrument formidabil al puterii naționale pentru diferite entități statale și un instrument de intruziune și coerciție

pentru entități non-statale. Pe lângă utilizarea acestor capacități pentru a obține secrete de stat, precum în spionajul tradițional, acest nou instrument este utilizat și pentru o serie de alte scopuri perturbatoare. Acestea includ: susținerea propriei dezvoltări economice prin sustragerea proprietății intelectuale, amenințarea cu perturbarea instituțiilor financiare, a industriilor petroliere, a centralelor nucleare, a rețelilor electrice și a infrastructurii de comunicații a statelor considerate adversare sau competitori, încercarea de a interveni și influența procesele democratice, cum ar fi alegeri sau sondaje, degradarea capacităților militare și, în anumite cazuri, limitarea capacității unui alt stat de a dezvolta arme nucleare.

Exemplele dezvăluite de mass-media privind operațiile cibernetice instrumentate de entități statale împotriva altor state includ pe cele ale Statelor Unite ale Americii și Iranului (unul împotriva celuilalt), ale Israelului și Iranului (unul împotriva celuilalt), ale F.Ruse împotriva Estoniei, Georgiei și Ucrainei, precum și încercările chineze de a fura proprietate intelectuală la scară industrială. Operațiile rusești îndreptate împotriva proceselor democratice din SUA și Regatul Unit al Marii Britanii au primit, de asemenea, o atenție considerabilă din partea instituțiilor media internaționale, la fel ca și acțiunile de răspuns ale SUA împotriva grupului IRA din Sankt Petersburg, considerat a fi parțial responsabil de aceste intruziuni. O evidentă acțiune cibernetică rusă împotriva SUA instrumentată și identificată la sfârșitul anului 2020, denumită „SolarWinds”, a reprezentat, de asemenea, o experiență ce a testat sistemele informatice ale instituțiilor civile și departamentale ale SUA.

Au existat, în istoria recentă, o serie de alte operații și acțiuni cibernetice instrumentate de entități statale și non-statale îndreptate asupra unor structuri internaționale de banking, servicii medicale și elemente de infrastructură critică ale căror efecte au fost resimțite la nivelul societății și al publicului larg, dar care au fost lipsite de acoperire mediatică largă deoarece procesul de reconstrucție și măsurile de reziliență au căutat să limiteze elementele de detaliu acțional, în special

la nivelul structurilor statale. Astfel, operațiuni ale Iranului împotriva Arabiei Saudite, ale Coreei de Nord împotriva Sony Pictures și a sistemului bancar global sau acțiunile SUA, Regatului Unit și Australiei îndreptate asupra organizației Statul Islamic au produs efectele unei confruntări clasice, cinetice. Unele operațiuni, atacuri cibernetice sau acțiuni direcționate s-au desfășurat fără restricții, rezultând o serie de victime colaterale; de exemplu, malware-ul NotPetya, pe care rușii l-au folosit împotriva Ucrainei, a deteriorat grav linia de transport Maersk, iar malware-ul WannaCry, pe care nord-coreenii l-au folosit împotriva sistemului bancar global, a afectat Serviciul Național de Sănătate al Regatului Unit.

Varietatea amenințărilor la adresa oricărui stat și a cetățenilor săi, în spațiul cibernetic, reprezintă principala preocupare a structurilor abilitate, care încearcă să creeze instrumente viabile și politici clare, cu scopul de a atenua riscurile pe care amenințările cibernetice le prezintă economiilor digitalizate, infrastructurilor naționale critice și cetățenilor, prin investiții considerabile în capacitățile de protecție a securității cibernetice. Acestea alimentează creșterea unui sector ciber-industrial globalizat, structurile statale și alianțele politico-militare încercând să încorporeze capacitățile cibernetice în strategiile naționale, în politicile de investiții și în doctrinele și planurile militare. Statele care și-au construit astfel de politici în domeniul cibernetic și-au dat seama de gradul în care prosperitatea economică, precum și securitatea națională și influența geostrategică, depind de gestionarea riscurilor cibernetice. Acest lucru devine cu atât mai critic pe măsură ce viața de zi cu zi, afacerile și problemele societății, devin din ce în ce mai dependente de Internet, generând o abordare inedită sub forma „*Internetul tuturor lucrurilor*”, concept ce face referire la interconectarea activităților umane cu acțiunile obiectelor utilizate în mod curent: case inteligente, traiul în orașe inteligente, cu vehicule inteligente. Unele state, precum Rusia și China, pledează de mulți ani în cadrul Națiunilor Unite pentru un nou model de guvernare a Internetului, care ar aduce un control mai mare din partea statului, față de echilibrul între guverne și sectorul

privat susținut de celelalte mari puteri mondiale și denumit în mod obișnuit „libertatea Internetului”.

În centrul strategiilor naționale ale SUA și Chinei, ca urmare a războiului comercial dintre cele două mari puteri, se află competiția pentru controlul asupra tehnologiilor care stau la baza dezvoltării viitorului spațiu cibernetic - cum ar fi producția de microcipuri, asamblarea computerelor, Internetul mobil (5G), arhitecturile cloud, sistemele de cabluri și routere. Măsurile adoptate de SUA în anul 2020, de a interzice aplicațiile software chineze TikTok și WeChat, în cadrul programului Clean Network<sup>3</sup>, au adăugat o dimensiune suplimentară, în paralel cu interzicerea de lungă durată a participării firmelor chineze la crearea și utilizarea aplicațiilor software din SUA, ca parte a politicii „Marele Firewall”.

Având în vedere avantajele geostrategice, economice și de securitate pe care le-ar aduce o poziție de lider în tehnologiile informaționale avansate, statele recunosc că pot fi considerate superputeri doar dacă dețin și gestionează infrastructuri digitale de ultimă generație. Creșterea masivă a numărului de persoane care utilizează modul de lucru digital, la birou sau de acasă, ca urmare a COVID-19, a avut implicații evidente pentru securitatea cibernetică, cu o creștere a activității ciberneticе maligنے. Aceste tendințe nu reprezintă o surpriză absolută, deoarece în condițiile existenței restricțiilor asupra mobilității umane, s-au constatat scăderi evidente ale oportunităților de criminalitate organizată și de spionaj în lumea fizică, în același timp înregistrându-se creșteri proporționale în sfera digitală. Însă, și înainte de apariția problemelor pandemice generate de COVID-19 lumea se confrunta deja cu un alt tip de pandemie virală – în spațiul cibernetic. În fiecare zi, securitatea națională și prosperitatea globală sunt afectate semnificativ de intruziuni ciberneticе. Desigur, amenințarea la adresa sănătății și vieții umane este mai puțin gravă decât cea a virusurilor biologici, dar rămâne de analizat dacă operațiunile ciberneticе, neidentificate la timpul oportun, necontrolate și negestionate corespunzător, pot provoca distrugerі mai mari și chiar decese, fie

prin accidente, fie prin proiecția tipului de agent intruziv sau perturbator.

Lecțiile învățate din modul în care statele au colaborat pentru a lupta împotriva COVID-19 – de exemplu, cu privire la restricțiile de mișcare și furnizarea de echipamente de protecție personală și încercarea de a dezvolta remedii terapeutice și vaccinuri viabile – ar putea, prin extrapolare, să fie aplicabile pentru a face față acestei pandemii ciberneticе. Astfel, abordarea internațională de stabilire a unor norme semnificative de comportament pentru spațiul cibernetic ar putea fi intensificată. Statele ar putea să-și intensifice eforturile de a lucra împreună pentru a combate criminalitatea cibernetică la nivel global, poate cu o anumită formă de partajare între state a „ADN-ului” tehnic al amenințărilor criminale ciberneticе, în același mod în care a fost împărtășit ADN-ul COVID-19. În plus, unele dintre lecțiile post-COVID-19 despre importanța creșterii rezilienței naționale și globale la șocuri strategice vor fi aplicabile, în egală măsură, și planurilor de abordare a unei catastrofe ciberneticе. Pe măsură ce prosperitatea națională, securitatea și educația guvernamentală au devenit din ce în ce mai dependente de spațiul cibernetic, înțelegerea dezvoltării și utilizării puterii ciberneticе de către state s-a transformat într-o necesitate.

O serie de organizații au dezvoltat metodologii pentru măsurarea puterii ciberneticе, majoritatea acestora concentrându-se, în principal, pe securitatea cibernetică. Într-o abordare metodologică holistică, Institutul Internațional pentru Studii Strategice (*International Institute for Strategic Studies/IISS*) din Londra propune o analiză comparativă a mai multor elemente considerate esențiale pentru capacitățile ciberneticе ale diferitelor entități statale, după cum urmează:

- *strategii și doctrine* – analizează cele mai importante documente guvernamentale, indiferent de titlurile formale care le sunt atribuite, care stabilesc prioritățile și bugetele, descriu politica de management sau schimbarea organizațională sau urmăresc creșterea gradului de conștientizare a publicului cu privire la strategia națională;

- *politici de guvernare, comandă și control* – categorie ce se referă la evoluția și eficiența structurilor guvernamentale și militare de nivel superior, precum și a celor de nivel operațional;

- *capacitatea cibernetică de bază* – capacitatea identificării și gestionării amenințărilor și exploatării oportunităților din spațiul cibernetic;

- *nivelul de dependență cibernetică* – indicator care reflectă vitalitatea și amploarea economiei digitale a unui stat, inclusiv relațiile sale internaționale în acest domeniu din perspectiva adoptată de G20 în anul 2016, care tratează ansamblul efectelor economice ale tehnologiei informației și comunicațiilor moderne (TIC) în toate sectoarele, nelimitându-se doar la valoarea estimată a producției companiilor TIC de bunuri și servicii;

- *securitate și reziliență cibernetică* – reprezintă un indicator care acoperă capacitatea de bază în domeniul securității cibernetice a unui stat, inclusiv capacitatea sa de a răspunde și de a se recupera la un nivel semnificativ de securitate cibernetică în urma unor incidente; acest indicator include, de asemenea, stabilirea standardelor de securitate, inovarea tehnică, managementul riscurilor specifice sectorului, eficacitatea industriei autohtone de securitate cibernetică și gradul în care statul a reușit să dezvolte și să extindă o forță de muncă specializată în domeniul cibernetic;

- *statutul de lider global în domeniul cibernetic* – în cadrul acestui indicator este luată în considerare măsura în care un stat se angajează, influențează și încearcă să conducă colaborarea internațională în domeniul cibernetic; prin urmare, această categorie include diplomația internațională relevantă, alianțele formale, implicarea în forumuri internaționale și participarea la cooperarea tehnică internațională și aranjamentele de asistență reciprocă;

- *capabilități cibernetice ofensive* – domeniu ce acoperă operațiunile cibernetice care sunt destinate, în principal, să producă un efect, mai degrabă decât cele menite să colecteze informații; astfel de operațiuni variază de la cele concepute pentru efecte cognitive până la cele concepute

pentru distrugere fizică – indiferent dacă operațiunile sunt conduse de entități civile sau structuri militare, sau dacă țintele sunt civile sau militare (de asemenea, sunt luați în considerare factorii care dictează utilizarea de către fiecare stat a capacității sale cibernetice ofensive, inclusiv voința politică, regimurile juridice și cadrele etice).

Statele analizate în studiul IISS, SUA și China, s-au luptat să modeleze cadre normative de politici durabile pentru spațiul cibernetic, fie în scopul exploatării de noi oportunități, fie în scopul apărării împotriva noilor amenințări. Dinamismul mediului cibernetic a forțat aceste două state, cu statut și ambiții de lider mondial în domeniu, să întreprindă reevaluări și revizuiți ale documentelor strategice cheie în mod constant și continuu.

În moduri care variază de la o țară la alta, structurile tradiționale ale guvernului, managementul corporativ și organizarea socială se străduiesc în mod constant să se adapteze în timp util. Deși „perturbator” este un termen suprautilizat în contextul amenințărilor cibernetice, acesta reprezintă caracteristica predominantă a forțelor aflate în joc. Cercetările în domeniu de până acum, confirmă faptul că nu numai SUA și China, ci și o serie de alte state aflate în această competiție tehnologică sunt încă în fazele incipiente de a gestiona implicațiile strategice ale spațiului cibernetic. Ambițiile și viziunile imaginative sunt abundente și s-au manifestat deja în proiecte de pionierat care includ orașe inteligente, mașini fără șofer, operații la distanță și robotică cu utilizare militară. Cu toate acestea, în majoritatea țărilor, alinierea acestor ambiții la procesele naționale de luare a deciziilor s-a dovedit dificilă. Sectorul privat, condus de nevoile consumatorilor, se situează cu mult înaintea reglementărilor și politicilor guvernamentale. Unele guverne percep spațiul cibernetic ca pe o arenă a competiției existențiale. În pofida încercărilor politice de a pune în aplicare sisteme internaționale de colaborare, pentru a atenua impulsurile competitive, există un sentiment de criză și inadecvare omniprezent în cercurile politice, actorii privați fiind în



postura de a acționa în scopul maximizării profiturilor. Impactul acestor acțiuni concurente asupra formulării diferitelor strategii naționale a produs efecte pozitive, însă puține guverne cred că strategiile lor actuale sunt capabile să atingă obiectivele declarate. Concurența interstatală în spațiul cibernetic a devenit o competiție asupra capacității de a dezvolta strategii eficiente de dezvoltare națională și, apoi, de a le implementa.

În domeniul dezvoltării tehnologice, păstrarea secretului reprezintă una dintre cele mai mari provocări, fapt care împiedică o abordare internațională mai coerentă cu privire la gestionarea riscurilor pe care le implică operațiunile ciberneticе, deoarece capacitățile sensibile de informații și structurile de informații care le gestionează sunt în centrul operațiunilor defensive și ofensive derulate de entitățile statale. De exemplu, capacitățile concepute de țările membre ale „clubului” Five Eyes pentru a detecta activitățile teroriste online, după evenimentele 9/11, s-au dovedit esențiale în detectarea și atribuirea unor atacuri ciberneticе. De asemenea, tehnicile sensibile de hacking, pe care statele le-au dezvoltat pentru a colecta informații despre o serie de adversari, oferă oportunități de instrumentare a unor operații ciberneticе ofensive.

Drept urmare, organizații precum Agenția Națională de Securitate (NSA) din SUA și Cartierul General de Comunicații Guvernamentale (GCHQ) din Marea Britanie au fost generatoarele unor abordări naționale a problemicii ciberneticе. SUA și Marea Britanie se numără printre țările în care a fost recunoscută necesitatea unei mai mari transparențe în ceea ce privește securitatea cibernetică, existând în acest sens o serie de inițiative guvernamentale pentru a îmbunătăți deschiderea, inclusiv o mai mare partajare a datelor cu privire la amenințări și vulnerabilități, față de industria privată de profil și publicul larg.

În acest sens, statele cu capacități ciberneticе solide încearcă să facă eforturi pentru ceea ce ar putea fi descris ca un răspuns pentru „întreaga societate” cu privire la securitatea cibernetică, acțiuni ce implică un parteneriat strâns și schimbul de informații între sectoarele

public, privat și academic, precum și parteneriate strânse la nivelul sectoarelor civil-militare. De asemenea, aceste eforturi includ programe inovatoare de perfecționare și educație, precum și campanii publice care vizează sporirea gradului de conștientizare a publicului larg, supus deopotrivă riscurilor și amenințărilor aduse de utilizarea tehnologiilor conectate sau dependente de mediul cibernetic. Există însă diferențe de abordare a acestor programe și inițiative în funcție de sistemul de guvernare al statelor. În mod previzibil, regimurile autoritare folosesc metode de control și direcționare guvernamentală stricte, fiind mai concentrate pe controlul răspândirii diferitelor conținuturi (idei și opinii) pe Internet, decât pe protecția tehnică a rețelelor critice. În consecință, state precum China, Iran și Rusia încearcă fiecare să își dezvolte propriile rețele de Internet „suverane”, controlate de stat, pentru a le permite să se izoleze, la nevoie, de rețeaua globală de Internet, pe care o percep ca fiind dominată de politicile și interesele SUA. Democrațiile liberale, pe de altă parte, tind spre o abordare mai distribuită, cu inovația națională condusă în mare măsură de sectorul privat și de mediul academic, o preocupare majoră fiind modul în care este protejată confidențialitatea datelor individuale ale cetățenilor. Rezultatul implementării acestor politici democratice este o industrie de securitate cibernetică fluidă, adaptabilă și rezilientă, de miliarde de dolari, precum și investiții mari în securitatea de ultimă generație realizate chiar de către furnizorii de servicii de Internet. Aceste state se străduiesc, de asemenea, să păstreze un Internet global, cu mai multe părți interesate, cu guvernanta echilibrată între guvernele naționale, sectorul privat, organizațiile neguvernamentale și mediul academic.

Este de remarcat faptul că, în Indexul global de securitate cibernetică al ITU, principalele democrații liberale tind să obțină un scor considerabil mai mare în domeniul securității ciberneticе decât statele cu regimuri autoritare. Acest lucru reflectă parțial vitalitatea mai mare a sectoarelor lor industriale de securitate cibernetică. În SUA, acest sector contribuie cu o

parte mult mai mare din PIB-ul național decât în China, deși decalajul a început să se reducă ușor. Pe scurt, ambele metode de creare a unei abordări integratoare a securității cibernetice par să aibă puncte forte și puncte slabe, dar cea folosită de democrațiile liberale poate fi considerată cea mai eficientă, în general, deoarece creează responsabilități și asumări din partea actorilor implicați.

Marile puteri statale în domeniul cibernetic de vârf operează o varietate de abordări pentru dezvoltarea și utilizarea capabilităților cibernetice ofensive. Cei care își permit cele mai mari investiții în termeni de personal și bani, cum ar fi SUA și China, tind să mențină o separare clară între capabilitățile militare și cele civile, chiar și acolo unde cooperarea militar-civilă este puternică. Alte state, cum ar fi Australia, Franța, Israel și Marea Britanie, tind spre o abordare militar-civilă mai sudată, compensând lipsa de resurse printr-o agilitate operațională mai mare. Majoritatea statelor mențin dezvoltarea și utilizarea capabilităților cibernetice ofensive sub control guvernamental strict și în limitele unui regim juridic strict. Cu toate acestea, unele guverne – Rusia și Iran în special – sunt mai tolerante cu „hackerii patrioți” (hackeri privați care promovează interesele statului) și cu grupurile de criminalitate cibernetică care operează de pe teritoriile lor, uneori chiar coordonându-se cu aceștia.

În cazul componentei ofensive a capabilităților cibernetice există, de asemenea, câteva diferențe doctrinare cheie, atât pentru China, cât și pentru Rusia, aceasta reprezentând doar o componentă tehnică a unor capabilități mai largi de operațiuni informaționale, fiind doar un mijloc de a-și controla propriul spațiu informațional și de a-l submina pe cel al adversarilor, în ceea ce aceste state percep ca fiind starea de conflict continuu de idei cu Occidentul. Prin urmare, instrumentul cibernetic ofensiv a fost transformat într-un agregat al mașinilor de propagandă ale acelor state și un mijloc de a crea și de a furniza „știri false”, reprezentând, totodată, un mijloc de a penetra infrastructura critică a adversarului.

În acest sens, maniera de utilizare a acestei capabilități ofensive oferă atât Chinei, cât și Rusiei, avantajul de a avea o abordare mai integrată a modului de utilizare a capabilităților cibernetice ca parte a unei strategii geopolitice mai ample. Încercările Rusiei, în cadrul Organizației Națiunilor Unite, de a scoate în afara legii astfel de capabilități „militare” și utilizarea de către aceasta a unor instrumente relativ clare, cum ar fi NotPetya, împotriva Ucrainei, pot fi indicatori ai acestei asimetrie de acțiune ce presupune o metodă hibridă de utilizare a instrumentelor de putere națională.

Ceea ce diferențiază SUA, în ceea ce privește utilizarea componentei ofensive a capabilităților cibernetice, este precizia chirurgicală sofisticată, adaptată la scara unei arii de operații militare. Beneficiind de avantajul strategic de a fi primul motor global al dezvoltării tehnologice, investind mai devreme și mai mult decât China și Rusia în bazele puterii cibernetice, potențialul cibernetic ofensiv al SUA beneficiază și de alianțele strânse cu alte state cu capabilități cibernetice solide.

Dialogul internațional și acordurile cu privire la utilizarea capabilităților cibernetice ofensive au generat, cel puțin până acum, doar sfaturi și politici de consiliere, având în vedere sensibilitatea acestui domeniu și percepțiile diferite generate de interesele geo-strategice multipolare. Au fost elaborate norme generale de comportament în spațiul cibernetic (neobligatorii și voluntare), sub auspiciile ONU, în anul 2015, încercând să se limiteze vizarea infrastructurii naționale critice de relevanță deosebită<sup>4</sup>. În anul 2019, au început lucrările conduse de Comitetul Internațional al Crucii Roșii concentrate pe încercarea de a defini utilizarea responsabilă de către entitățile statale a capabilităților cibernetice ofensive<sup>5</sup>. În general, pentru a gestiona riscurile proliferării și escaladării necontrolate a utilizării capabilităților cibernetice ofensive, trebuie identificate căi și metode pentru dialogul interstatal. Acest lucru va presupune ca statele să gândească, în mod creativ, la modul în care asigură o mai mare transparență în scopul protejării elementelor de infrastructură națională critică. Lipsurile, neajunsurile și decalajele tehnologice, care se manifestă în cazul

unor state ce nu posedă resursele necesare și expertiza instrumentării mediului cibernetic, pot fi compensate prin alianțe și asocieri internaționale. Alianța cibernetică dominantă este, fără îndoială, cea construită pe baza parteneriatului de informații Five Eyes, ce funcționează de 65 de ani. Toate cele cinci țări sunt în mod individual capabile din punct de vedere cibernetic – SUA reprezentând reperul tehnologic și statul cu cele mai solide capacități și politici – însă fiecare stat are un câștig semnificativ din această alianță.

Conștientizând potențialul militar al utilizării domeniului cibernetic, mai multe state au întreprins o serie de eforturi politice pentru a-și adapta și transforma strategiile, doctrinele și structurile militare pentru a recunoaște atât oportunitățile, cât și amenințările generate de tehnologiile ciberneticе și spațiale. Statele lider, în special SUA și China, preconizează că un viitor război va fi câștigat/pierdut într-un spațiu cibernetic guvernat de inteligența artificială și platformele spațiale. Mai mulți factori au stat la baza modelării și transformării conceptuale a actualelor abordări naționale, printre aceștia numărându-se: amploarea vulnerabilității ciberneticе în sistemele de comandă și control, potențialul național în domeniul cibernetic și industrial-tehnologic, gradul de dependență de capacitățile de informații civile și reticența la schimbare a militarilor conservatori.

Dezvoltarea și utilizarea în creștere a capacităților ciberneticе de către entități statale au fost, într-o oarecare măsură, intensificate de șocuri strategice generate de acțiuni militare. Primul dintre acestea a venit în 1991, în timpul Primului Război din Golf, când SUA s-au dovedit capabile să integreze informații și arme de înaltă precizie, ghidate într-o măsură pe care nicio altă putere militară nu o reușise până la acel moment. Acestui moment istoric i-au urmat o serie de alte evenimente, printre care menționăm operațiunile americane din 1999 împotriva forțelor Republicii Federale Iugoslavia din Kosovo, ce au produs un efect de șoc similar, presupusa utilizare a instrumentelor ciberneticе în operațiunile militare americane în Irak în 2003, ce a atras atenția pe scară largă, la fel ca și rolul inedit al Internetului

în așa-numitele „revoluții colorate” din anii 2000, din Georgia, Kârgâzstan și Ucraina. Ca urmare a vulnerabilităților interne identificate, China și Rusia au început să facă eforturi prin intermediul ONU, încă din 2003, pentru un control mai mare al statului asupra spațiului cibernetic „suveran”. Unda de șoc s-a produs în urma scurgerilor de informații generate de Edward Snowden în 2013, cu dezvăluirile despre amploarea și sofisticarea capacităților ciberneticе ale SUA și ale aliaților, inclusiv rolul jucat de companiile digitale de top din SUA în facilitarea colectării informațiilor. În același timp, China este în măsură să genereze propriile unde de șoc în spațiul cibernetic, cel mai cunoscut aspect referindu-se la furtul constant de proprietate intelectuală occidentală la scară industrială.

---

## **CONCLUZII**

---

Având în vedere aspectele prezentate, putem concluziona că SUA rămân cel mai capabil stat din punct de vedere al gestionării domeniului cibernetic, regăsindu-se, totuși, într-o competiție acerbă cu principalul competitor, China. Avantajul minim față de China se datorează liderilor politici americani care, încă de la mijlocul anilor 1990, au oferit o direcție politică clară pentru consolidarea puterii ciberneticе naționale, susținând în același timp investițiile masive în dezvoltarea capacităților civile și militare, câștigând astfel o vastă experiență operațională, ceea ce a condus la dezvoltarea celei mai puternice baze digital-industriale din lume. Acest lucru este evidențiat de gama de companii americane capabile să detecteze și să atribuie atacuri ciberneticе instrumentate de actori statali și de complexitatea dovedită a capacităților ciberneticе ofensive ale SUA în domeniul militar și civil.

Puterea cibernetică a SUA se bazează, de asemenea, pe o capacitate de inteligență cibernetică de clasă mondială, cu acoperire globală și tehnici criptografice de ultimă generație, și este amplificată de parteneriate extrem de integrate cu alte state care sunt, de asemenea, printre cele mai capabile din lume să gestioneze problemele ciberneticе. SUA au căutat să devină un actor cibernetic ofensiv responsabil, guvernat

de legislația internațională și care se străduiește să limiteze potențialele daune colaterale. De asemenea, au căutat să-și gestioneze gradul de dependență de spațiul cibernetic, nu numai în scopul securității naționale, ci și din motive economice și politice. Această provocare este exacerbată de complexitatea structurilor sale de guvernare cibernetică și de comandă și control, în care numărul mare de agenții implicate

reprezintă un potențial impediment pentru agilitatea luării deciziilor operaționale. Acești factori, ce combină o serie de rigori și reguli stricte, oferă adversarilor SUA un avantaj în utilizarea tehnicilor cibernetiche nesofisticate, care vizează subversiunea, dar sunt instrumentate sub pragul legal pentru a fi considerate acte de agresiune care ar putea justifica un răspuns de natură militară.

## BIBLIOGRAFIE

1. AUSTIN Greg, "US Policy: From Cyber Incidents to National Emergencies", în AUSTIN Greg (ed.), *National Cyber Emergencies: The Return to Civil Defence*, Abingdon, Routledge, 2020, 272 p.
2. BRYNJOLFSSON Erik și COLLIS Avinash, "How Should We Measure the Digital Economy?", *Harvard Business Review*, noiembrie-decembrie 2019, <https://hbr.org/2019/11/how-should-we-measure-the-digital-economy>.
3. ENGSTROM Jeffrey, "Systems Confrontation and Systems Destruction Warfare: How the People's Liberation Army Seeks to Wage Modern Warfare", RAND Corporation, 2018, [https://www.rand.org/content/dam/rand/pubs/research\\_reports/RR1700/RR1708/RAND\\_RR1708.pdf](https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1708/RAND_RR1708.pdf).
4. GREENBERG Andy, "China Tests the Limits of its US Hacking Truce", *Wired*, 31 octombrie 2017, <https://www.wired.com/story/china-tests-limits-of-us-hacking-truce>.
5. HANNAS William C., James Mulvenon and Anna B. Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernization*, Abingdon: Routledge, 2013, 320 p.
6. NAKASHIMA Ellen, "White House authorizes "offensive cyber operations" to deter foreign adversaries", *The Washington Post*, 20 septembrie 2018, [https://www.washingtonpost.com/world/national-security/trump-authorizes-offensive-cyber-operations-to-deter-foreign-adversaries-bolton-says/2018/09/20/b5880578-bd0b-11e8-b7d2-0773aa1e33da\\_story.html](https://www.washingtonpost.com/world/national-security/trump-authorizes-offensive-cyber-operations-to-deter-foreign-adversaries-bolton-says/2018/09/20/b5880578-bd0b-11e8-b7d2-0773aa1e33da_story.html), accesat la 16.11.2021.
7. NIELSEN Jessica R., "New Digital Economy Estimates", *Bureau of Economic Analysis*, August 2020, <https://www.bea.gov/system/files/2020-08/New-Digital-Economy-Estimates-August-2020.pdf>.
8. SEGAL Adam, "An Update on U.S.–China Cybersecurity Relations", *Council on Foreign Relations*, 17 noiembrie 2017, <https://www.cfr.org/blog/update-us-china-cybersecurity-relations>.
9. SCHILLER Dan, *Digital Capitalism: Networking the Global Market System*, Cambridge, MA: MIT Press, 2000, 320 p.
10. \*\*\*, Cyber Resilience Review (CRR), Cybersecurity and Infrastructure Security Agency, <https://www.us-cert.gov/resources/assessments>.
11. \*\*\*, Director of National Intelligence, "Industry Snapshot: Summary of Partner Responses to the FY 2015–2019 IC S&T Investment Landscape", 2015, <http://www.dni.gov/files/documents/atf/In-STeP%20-%20Industry%20Snapshot.pdf>.
12. \*\*\*, Joint Publication 3-12 (JP 3-12), Department of Defense (USA), 8 June, 2018, [https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3\\_12.pdf](https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf).
13. \*\*\*, International Humanitarian Law and Cyber Operations during Armed Conflicts, <https://www.icrc.org/dih>.



[www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts](http://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts).

14. \*\*\*, Office of Management and Budget, "A Budget for America's Future: Analytical Perspectives", Washington DC, 2020, <https://www.govinfo.gov/content/pkg/BUDGET-2021-PER/pdf/BUDGET-2021-PER.pdf>.
15. \*\*\*, US Department of State, "Announcing the Expansion of the Clean Network to Safeguard America's Assets", 5 august 2020, <https://china.usembassy-china.org.cn/announcing-the-expansion-of-the-clean-network-to-safeguard-americas-assets>.
16. \*\*\*, US Department of Defense, "Summary: Department of Defense Cyber Strategy 2018", [https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/Cyber\\_Strategy\\_Summary\\_Final.pdf](https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/Cyber_Strategy_Summary_Final.pdf).
17. \*\*\*, United States Cyber Command, "Beyond the Build: Delivering Outcomes through Cyberspace – The Commander's Vision and Guidance for US Cyber Command", 2015, <https://nsarchive2.gwu.edu/dc.html?doc=2692135-Document-27>.
18. \*\*\*, United States Cyber Command, "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command", 2018, <https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010>.
19. \*\*\*, United States Department of Homeland Security, „Cyber Resilience Review”, Factsheet, <https://www.cisa.gov/sites/default/files/publications/Cyber-Resilience-Review-Fact-Sheet-508.pdf>.
20. \*\*\*, United Nations Conference on Trade and Development, "Digital Economy Report 2019", Geneva, p. 23, [https://unctad.org/system/files/official-document/der2019\\_en.pdf](https://unctad.org/system/files/official-document/der2019_en.pdf), accesat la 15.11.2021.
21. \*\*\*, United Nations General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", A/70/174, 22 iulie 2015, [https://www.un.org/ga/search/view\\_doc.asp?symbol=A/70/174](https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174).
22. \*\*\*, White House, *National Security Strategy of the United States of America*, decembrie 2017, <https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>.
23. \*\*\*, White House, *National Cyber Strategy of the United States of America*, septembrie 2018, <https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>.
24. \*\*\*, White House, "Executive Order on Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities", 19 ianuarie 2021, <https://trumpwhitehouse.archives.gov/presidential-actions/executiveorder-taking-additional-steps-address-national-emergency-respect-significant-malicious-cyber-enabled-activities>.
25. \*\*\*, White House, "Memorandum on Renewing the National Security Council System", 4 februarie 2021, <https://www.whitehouse.gov/briefing-room/statements-releases/2021/02/04/memorandum-renewing-the-national-security-council-system>.

<sup>1</sup> Declarația Summit-ului de la Bruxelles, emisă de șefii de stat și de guvern participanți la reuniunea Consiliului Atlanticului de Nord de la Bruxelles, 11-12 iulie 2018", Organizația Tratatului Atlanticului de Nord, 11 iulie 2018.

<sup>2</sup> NATO Standardization Office (NSO), AAP-6, *NATO Glossary of Terms and Definitions* (2018 edition), p. 62.

<sup>3</sup> Programul Clean Network al guvernului SUA are ca scop protejarea vieții private a cetățenilor americani și a companiilor americane „de intruziunile agresive ale unor actori maligni, cum ar fi Partidul Comunist Chinez”; US Department of State, Announcing the Expansion of the Clean Network to Safeguard America's Assets, 5 August 2020, <https://china.usembassy-china.org.cn/announcing-the-expansion-of-the-clean-network-to-safeguard-americas-assets>.

<sup>4</sup> <https://undocs.org/A/70/174>, accesat la 10.11.2021.

<sup>5</sup> "International Humanitarian Law and Cyber Operations during Armed Conflicts", <https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts>, accesat la 10.11.2021.

# PROVOCĂRI HIBRIDE DE NATURĂ BIOLOGICĂ

Paul MIHAI\*

## Abstract

*Biological threats need to be conceptualized in a new framework and through new governance practices designed to address the challenges posed by the ever-changing boundaries of global health. This turn has turned potential biological threats into the main factors that require rigorous planning of institutional and individual preparedness for an effective approach to pandemic emergencies. Biological threats, as events that transcend the molecular boundaries of viruses, are turning hybrid social networks into the main focus of a global response to infectious diseases. In this article, I will present and analyze some important issues related to the threats posed by biological weapons and bioterrorism, the use of biotechnology to improve biological warfare agents and I will summarize the measures and constraints on countering bioterrorism and the response to biological weapons.*

**Keywords:** *biological threats; biological warfare; biotechnology; bioterrorism; biological weapons; biological attack.*

## INTRODUCERE

Provocarea în combaterea amenințărilor hibride este aceea că tacticile desfășurate sunt de „ardere lentă” și executate sub pragul conflictului armat, făcând dificil și chiar imposibil un răspuns eficient al statelor-țintă. O acțiune hibridă nedetectabilă/ascunsă poate apărea cu întârziere pe „radar”, cât timp evenimentul aparent izolat nu este pus în context, ca parte a activităților unui stat menite să submineze adversarii. Amenințările hibride sunt una dintre principalele provocări cu care se luptă în prezent democrațiile occidentale. Aceste amenințări se regăsesc în știri, în mare parte încadrate sau învăluite în fenomene *hibride* specifice, cum ar fi dezinformarea, amestecul străin în alegeri și *hackurile* cibernetice. Guvernele ne avertizează asupra lor, iar instituții

precum NATO și UE elaborează documente de politică și organizează simpozioane și ateliere de lucru pentru a le analiza, discuta și pentru a trage concluzii. Diferiți furnizori de securitate sunt în proces de definire a strategiilor și de dezvoltare a capacităților pentru a contracara amenințările hibride. Un răspuns final la amenințările hibride nu a fost găsit și, după toate probabilitățile, nu există, în mod imediat și eficient. Combaterea acestor amenințări va rămâne o sarcină foarte dificilă atâta timp cât amenințările hibride vor evolua datorită progreselor tehnologice și a noilor modalități de ducere a campaniilor hibride. Această scanare a orizontului, bazată pe trecerea în revistă a literaturii și mass-media, a sesiunilor de experți și a schimburilor de informații cu institute internaționale, surprinde unele dintre tendințele și evoluțiile actuale și emergente în conflictele și amenințările hibride.

\* Autorul este doctorand în domeniul „Științe militare” în cadrul Universității Naționale de Apărare „Carol I” din București.

## EVOLUȚIA RĂZBOIULUI BIOLOGIC

De-a lungul istoriei, oamenii au conceput modalități noi și inovatoare de a ucide alți oameni. Când tehnologia era primitivă, războinicii foloseau orice le oferea natura. Arderea culturilor a fost probabil cea mai ușoară și mai timpurie formă de război menită să submineze un inamic, la fel ca otrăvirea apei de băut a unei comunități, folosind animale moarte sau putrezite<sup>1</sup>.

**Războiul biologic timpuriu.** Forme puțin mai avansate de război biologic au apărut când soldații au început să scufunde sulitele în fecale și să arunce șerpi otrăvitori în taberele adverse. În timpul epidemiei de „moarte neagră” de la mijlocul anilor 1300, tătarii au catapultat cadavrele pline de ciumă peste ziduri în orașele deținute de inamicii lor europeni (ex.: cetatea genoveză Caffa din Peninsula Crimeea). Deși această acțiune este, uneori, creditată cu răspândirea ciumei, șobolanii și puricii lor au fost mult mai eficienți în răspândirea ciumei bubonice decât contactul cu cadavrele. Având în vedere starea de igienă din majoritatea orașelor sau castelelor medievale, nu era nevoie să se asigure o sursă exterioară de infecție. Cu ciuma tifoidă, variolă, dizenterie și difterie, prezente deja în multe comunități, tot ceea ce era de obicei necesar era să lase natura să-și urmeze cursul. În mod similar, există un mit larg răspândit conform căruia coloniștii europeni i-au infectat intenționat pe nativii de pe continentul american cu variolă. Deși este adevărat că armata britanică a încercat această strategie în timpul războaielor francez și indian de la mijlocul anilor 1700, marea majoritate a deceselor nativilor americani, poate până la 95% din populație, s-a datorat infecției accidentale cu variolă și alte boli<sup>2</sup>.

**Războiul biologic modern** a început în timpul Primului Război Mondial. Deși germanii au refuzat să folosească agenți biologici împotriva oamenilor, i-au folosit împotriva animalelor, infectând caii aliați cu morva (*Burkholderia mallei*) și antrax. De cealaltă parte, francezii au folosit morva împotriva cailor germani<sup>3</sup>. Mai târziu, în timpul celui de-al Doilea Război Mondial, japonezii au infectat experimental

prizonierii de război chinezi cu boli înfiorătoare, cum ar fi holera, febra hemoragică epidemică și boli venerice. De asemenea, au fost responsabili pentru aruncarea *bombelor cu purici infectați cu ciumă* asupra orașelor din China, deși acest lucru probabil a avut un efect redus pentru că ciuma era deja endemică în regiune<sup>4</sup>.

După al Doilea Război Mondial, în special în timpul războiului din Coreea, Statele Unite și-au intensificat programul de arme biologice. Poate cel mai controversat aspect al programului a fost eliberarea intenționată a agenților biologici, precum relativ-inofensiva *Serratia marcescens*, peste câteva orașe americane, cu scopul de a studia modul de dispersare. Armata a infectat neintenționat 11 civili, dintre care unul a murit. Până în anul 1969, SUA a introdus în programele biologice militare antraxul și tularemia. Ulterior, în 1975, SUA a renunțat la toate armele biologice prin semnarea Convenției privind armele biologice (BWC)<sup>5</sup>.

Uniunea Sovietică a semnat, de asemenea, BWC, dar și-a extins eforturile în acest domeniu. Amploarea programului era uluitoare, sovieticii fabricând câteva sute de tone de antrax, iar o eliberare accidentală în 1979 a ucis 66 de oameni. Fosta URSS a fabricat, de asemenea, mii de kilograme de variolă și ciumă, iar în 1989 se presupune că a reușit să armeze virusul *Marburg*, care provoacă o febră hemoragică mortală, asemănătoare cu *Ebola*. Aceste acuzații rămân însă neconfirmate. În cele din urmă, sub președintele Boris Elțin, în 1992, Rusia și-a încheiat programul de arme biologice, dar soarta stocurilor rămâne neclară<sup>6</sup>.

Într-o notă similară, în anii 1990, Irakul a recunoscut în fața inspectorilor Națiunilor Unite că a produs mii de tone de toxină botulinică concentrată și antrax. Deși guvernul irakian și-a abandonat programul de arme biologice după primul război din Irak, nu se cunoaște statutul și locul unde se află cantitățile mari de material infecțios pe care le-a dezvoltat<sup>7</sup>.

Un alt actor de interes pentru experții în biosecuritate l-a reprezentat organizația Al Qaeda, care a derulat un efort pentru realizarea de arme biologice pe scară largă în Afganistan. Acest demers a fost stopat în 2001, atunci când SUA i-a

bombardat facilitățile și taberele de antrenament. Majoritatea experților consideră că încercările ulterioare ale Al Qaeda de a reconstitui aceste arme s-au concentrat mai degrabă pe armele chimice decât pe cele biologice<sup>8</sup>.

**Amenințarea atacurilor biologice recente.** În anul 1984, adepții din Oregon/SUA ai guru-ului indian Bhagwan Shree Rajneesh au organizat un atac care a îmbolnăvit aproape 800 de oameni cu febră tifoidă. Membrii sectei au introdus bacterii în salate și alte recipiente pentru alimente, la un restaurant local, după ce încercările lor de a contamina alimentarea cu apă au eșuat. Ei sperau să influențeze rezultatele alegerilor locale, împiedicând locuitorii să ajungă la secțiile de votare. Deși 43 de persoane au fost internate în spital, nimeni nu a fost ucis, iar infractorii au fost urmăriți penal<sup>9</sup>.

Un atac biologic a avut loc în SUA imediat după acțiunile Al Qaeda asupra World Trade Center și Pentagon, din 11 septembrie 2001. Un autor necunoscut a trimis prin poștă o pulbere care conținea spori infecțioși de antrax, având ca destinatari doi senatori americani și mai multe instituții de presă. Cinci persoane au murit de antrax după ce au fost expuse la materialul din scrisori, iar 17 s-au îmbolnăvit. Personalul medical a oferit vaccinul cu antrax ca profilaxie post-expunere pentru aproximativ 1.700 de persoane potențial expuse care luau și antibiotice pentru a combate antraxul. Dintre acești oameni, aproape 200 au fost de acord cu vaccinul și au primit toate dozele din acesta<sup>10</sup>.

Astăzi, războiul biologic este considerat o amenințare, indiferent de sursă – actori statali, non-statali, implicit teroriști și *lupi singuratici*. Există totuși un dezacord cu privire la nivelul de amenințare reprezentat de acest lucru. Mulți cred că teroriștii ar fi incapabili să efectueze un atac biologic eficient, la scară largă. Așadar, în 1984, cultul Rajneesh a produs toxinfecții alimentare în micul oraș din Oregon în scopuri politice, adăugând Salmonella în recipientele de salate. Aum Shinrikyo, un cult japonez care a comis atacul cu gaz sarin în metroul din Tokyo în 1995, a experimentat, de asemenea, arme biologice, dar fără rezultate răsunătoare<sup>11</sup>. Iar atacul cu antrax

din SUA din 2001 a ucis doar 5 persoane. Scepticii indică incidentele acestea ca fiind dovada că bioteroriștii sunt incapabili să provoace daune pe scară largă. Însă, alți analiști nu sunt de acord cu această minimalizare. Unii agenți biologici, cum ar fi antraxul, necesită puțină experiență pentru a crește sau a se transforma în arme letale. Având în vedere că informațiile microbiologice sunt universal disponibile pe Internet, unii experți apreciază că este doar o chestiune de timp până să aibă loc un mare atac bioterorist. Un mic avion echipat pentru tratarea culturilor agricole și încărcat cu antrax, trimis să survoleze un oraș important ar putea ucide sute de mii, dacă nu chiar milioane de oameni.

## CONTAGIOZITATEA VIRUSURILOR ȘI AGENȚILOR VIRALI

**Variola.** Agentul etiologic viral al variolei este un membru al familiei poxvirusurilor. Poxvirusurile sunt cele mai complexe virusuri animale și sunt atât de mari încât pot fi observate cu un microscop cu lumină. Virusul variolei infectează doar oamenii, ceea ce a permis eradicarea sa de către Organizația Mondială a Sănătății, sarcină finalizată până în anul 1980. Variola este foarte infecțioasă și există în două variante: *Variola major*, cu o rată a mortalității de 30%-40%, și *Variola minor*, cu rată a mortalității de aproximativ 1%.

**Filovirusurile.** Virusurile *Ebola* și *Marburg* formează o familie de virusi ARN monocatenar negativ, cunoscuți sub numele de Filovirusuri. Pacienții afectați vomită și le curge sânge, în special din ochi și urechi. Focarele de *Ebola* din Sudan și Zair au avut o rată de decese între 80% și 90%, dar există tulpini strâns legate, care nu sunt la fel de virulente. Transmiterea necesită, în general, o expunere substanțială la fluidele corporale infectate, astfel încât filovirusurile sunt dificil de dobândit prin expunere ocazională. În practică, acest lucru le face o alegere relativ slabă pentru utilizare ca agent de război biologic<sup>12</sup>.

**Flavivirusurile.** Febra *Dengue* și febra galbenă sunt ambele cauzate de membrii familiei Flavivirus. Febra galbenă este adesea letală, în



timp ce *Dengue* este rareori fatală, dar este foarte dureroasă și determină o incapacitare a victimelor timp de câteva zile. Cu toate acestea, ambele sunt răspândite prin mușcături de insecte, ceea ce ar face dificilă utilizarea lor ca arme biologice.

**Arenavirusurile.** Un arenavirus care a apărut în regiunea râului Lassa din Nigeria, la sfârșitul anilor 1960, provoacă febra hemoragică *Lassa*, care seamănă simptomatic cu o infecție de *Ebola*. Acest virus are o mortalitate extrem de mare și este răspândit de obicei de rozătoare.

**Coronavirusurile.** Fac parte dintr-o familie de virusuri care determină infecții la om și animale, inclusiv la păsări și mamifere. Aceste virusuri pot determina la om de la o răceală comună până la unele mai severe și chiar boli respiratorii fatale, precum Sindromul Respirator din Orientul Mijlociu - MERS-CoV și Sindromul Respirator Acut Sever - SARS. SARS-CoV-2 este un coronavirus nou, identificat pentru prima oară în decembrie 2019 într-un focar de pneumonie din China. Virusul se răspândește în principal prin aer atunci când oamenii sunt aproape unul de celălalt. Părăsește o persoană infectată în timp ce respiră, tușește, strănută sau vorbește și ajunge la altă persoană prin gură, nas sau ochi. De asemenea, se poate răspândi prin suprafețe contaminate. Oamenii rămân infectați timp de până la două săptămâni și pot răspândi virusul chiar dacă nu prezintă simptome<sup>13</sup>.

## AGENȚII DE RĂZBOI BIOLOGIC ȘI BIOTEHNOLOGIA

Se sugerează adesea că ingineria genetică ar putea fi folosită pentru a crea versiuni mai periculoase ale agenților infecțioși. Deși există ceva adevăr în această afirmație, trebuie luate în considerare anumite aspecte. Un bioterorist poate încerca să modifice genetic o bacterie de laborator inofensivă, precum *E.coli* (*Escherichia coli*). Bacteriile ar putea fi proiectate pentru a *călători sub acoperire* atunci când intră în corpul uman, ascunzându-se de sistemul imunitar. În plus, bacteriile ar putea fi programate să respingă celulele imune prin injectarea lor cu toxine, iar alte gene ar putea fi adăugate pentru a smulge

proviziile vitale de fier din celulele sanguine. În cele din urmă, bacteriile ar putea fi modificate pentru a fi foarte infecțioase. Un astfel de agent biologic ar fi o armă înfricoșătoare. Ceea ce este și mai îngrozitor, din păcate, această bacterie există deja. Se numește *Yersinia pestis* și este agentul ciumei bubonice, fiind încă endemic în multe părți ale lumii, inclusiv China, India, Madagascar și Statele Unite. Așadar, în loc să dedice ani de zile pentru a construi genetic o armă biologică letală, un bioterorist ar putea pur și simplu să izoleze unul dintre produsele oferite de natură. Prin urmare, *îmbunătățirea* bolilor infecțioase prin inginerie genetică este probabil o amenințare minoră, dar din ce în ce mai posibilă<sup>14</sup>.

**Creșterea agresivității agenților patogeni.** Se știe că unitatea sovietică de război germinativ a modificat virusul variolei și a generat o varietate de mutanți și hibrizi artificiali. Detaliile sunt în mare parte indisponibile. Cu toate acestea, experimentele recente cu variola șoarecelui - virusul *Ectromelia* - au dat rezultate importante. Variola șoarecilor este legată de variola, dar infectează doar șoarecii. Virulența sa variază foarte mult în funcție de tulpina de șoarece. Șoarecii rezistenți genetic se bazează pe imunitatea mediată de celule, mai degrabă decât pe anticorpi. Cercetătorii au modificat virusul variolei șoarecelui prin inserarea unei gene umane<sup>15</sup>.

Moartea din înțepătura unui melc con se datorează în mare parte  $\alpha$ -conotoxinelor, care provoacă paralizia musculară și declanșează stopul cardio-respirator. Iar alte toxine pot declanșa colapsul cardiovascular. Din punct de vedere simptomatic,  $\alpha$ -conotoxinele seamănă cu toxina botulinică, deși mecanismul de acțiune este diferit. Preocuparea din perspectiva războiului biologic nu este că un guvern sau un grup de teroriști ar recolta venin din melcii con, ci că toxinele ar fi sintetizate chimic.

Rezultate similare au fost observate cu tulpinile de virus *Vaccinia*, care este folosit pentru vaccinarea împotriva variolei. Unul dintre motivele pentru care variola este atât de virulentă poate fi dat de faptul că subminează brusc răspunsul imun mediat de celulele organismului<sup>16</sup>.

**Crearea de viruși camuflați.** Cu ajutorul ingineriei genetice este, de asemenea, posibil să se ascundă un virus potențial periculos în interiorul unei bacterii inofensive. Această strategie este deja folosită în natură atunci când bacteriofagii își introduc genomul în cromozomi sau plasmide bacteriene și, mai târziu, reapar pentru a infecta alte gazde. Teoretic, clonarea întregului genom al unui virus mic într-o plasmidă bacteriană ar putea crea o armă biologică. Virușii mai mari ar putea fi găzduiți cu cromozomi artificiali bacterieni<sup>17</sup>.

## MANIFESTĂRI ALE BIOTERORISMULUI

Un *atac biologic* al teroriștilor poate părea mai degrabă un element de intrigă într-un film de acțiune decât o amenințare realistă. Și, într-adevăr, posibilitatea unui astfel de atac poate fi foarte îndepărtată. Totuși, atacurile biologice au avut loc în trecut, unul chiar în 2001. În consecință, o colecție de instituții și agenții guvernamentale sunt implicate în planificarea răspunsurilor la potențialele atacuri biologice.

**Amenințările cu armele biologice** ar putea include eliberarea deliberată de către atacatori a unui agent care provoacă una sau mai multe dintre o varietate de boli diferite. Autoritățile de sănătate publică au dezvoltat un sistem de priorizare a agenților biologici în funcție de riscul acestora pentru securitatea națională. Astfel, agenții de categoria A au cea mai mare prioritate și aceștia sunt agenți ai bolii care prezintă un risc major pentru securitatea națională, deoarece se pot transmite de la persoană la persoană și pot duce la o mortalitate ridicată, cu potențial crescut în a provoca perturbări sociale. Aceștia sunt antraxul, botulismul, ciuma, variola, tularemia și o colecție de viruși care provoacă febră hemoragică, cum ar fi *Ebola*, *Marburg*, *Lassa* și *Machupo*. Acești agenți de boală există în natură, dar ar putea fi manipulați pentru a le crește periculozitatea. Agenții de categoria B sunt moderați, ușor de diseminat și au ca rezultat o mortalitate scăzută. Aceștia includ bruceloza, morva, febra Q, toxina ricină, febra tifosului și alți agenți. Agenții de

categoria C includ agenți de boală care ar putea fi proiectați pentru diseminarea în masă, în viitor, precum virusul *Nipah*<sup>18</sup>.

Utilizarea vaccinurilor eficiente ar proteja probabil vieți și ar limita răspândirea bolilor într-o urgență legată de armele biologice. Sunt disponibile vaccinuri licențiate pentru câteva amenințări, cum ar fi antraxul și variola, iar cercetările sunt în curs de dezvoltare și producere de vaccinuri pentru alte amenințări, precum tularemia, virusul *Ebola* și virusul *Marburg*. Cu toate acestea, multe amenințări legate de bolile produse de arme biologice nu dispun de un vaccin corespunzător.

**Amenințarea bioteroristă.** *Model State Emergency Health Powers Act* din 2001, care este un document conceput de guvernul federal al SUA pentru a ghida organele legislative în elaborarea legilor privind urgențele de sănătate publică, a definit bioterorismul ca fiind „utilizarea intenționată a oricărui microorganism, virus, substanță infecțioasă sau produs biologic care poate fi proiectat ca rezultat al biotehnologiei sau al oricărei componente naturale sau elaborate prin bioinginerie, a oricărui astfel de microorganism, virus, substanță infecțioasă sau produs biologic, pentru a provoca moartea, boală sau alte deficiențe biologice la un om, un animal, o plantă sau alt organism viu pentru a influența conduita guvernului sau pentru a intimida sau constrânge o populație civilă”<sup>19</sup>. Războiul biologic și bioterorismul sunt adesea folosite în mod interschimbabil, dar bioterorismul se referă, de obicei, la actele comise de un actor non-statal, mai degrabă decât de o țară.

**Iminența atacurilor biologice.** Opiniile experților diferă cu privire la plauzibilitatea unui atac biologic. Reprezentanții structurilor cu responsabilități în domeniul securității naționale din SUA au declarat, în 2008, că *bioterorismul reprezintă o amenințare mai probabilă decât terorismul nuclear*. Alți experți insistă asupra faptului că posibilitatea oricărui atac, în special a unui atac la scară largă, este mică, având în vedere provocările imense determinate de

cultivarea și desfășurarea agenților biologici. De exemplu, dificultățile tehnice de a aerosoliza un agent de boală și de a-l dispersa în mod precis și pe scară largă, menținându-i virulența, sunt enorme. Oricum, majoritatea specialiștilor în biosecuritate recunoaște că potențialul unui atac nu trebuie ignorat. În plus, pregătirile pentru un atac biologic vor beneficia, probabil, de un răspuns adaptat și la alte tipuri de urgențe de sănătate publică<sup>20</sup>.

## CONTRACARAREA BIOTERORISMULUI

**Pregătirea pentru atacuri biologice.** În 2001, înainte de atacurile din 11 septembrie, mai multe agenții și grupuri academice din SUA au derulat un exercițiu pe tema unui atac biologic, cu numele de cod *Dark Winter*, luând în calcul o infectare cu virusul variolei. Scenariul, care a funcționat pe o ipoteză de aproximativ 12 milioane de doze disponibile de vaccin, bazată pe stocurile disponibile atunci de vaccin împotriva variolei, a demonstrat slăbiciuni grave ale sistemului de sănătate publică în asigurarea unui răspuns eficient la bioterorism<sup>21</sup>. O vulnerabilitate cheie, evidențiată de exercițiu, a fost lipsa de vaccinuri. Acest lucru a determinat, cel puțin în cazul variolei, adăugarea a sute de milioane de doze de vaccin împotriva variolei la rezervele de vaccin din SUA. Alte dificultăți expuse au fost conflictele dintre prioritățile federale și de stat în gestionarea resurselor, lipsa infrastructurii medicale pentru a face față victimelor în masă și nevoia crucială ca cetățenii americani să aibă încredere și să coopereze cu liderii. Reacția celor expuși la antrax în atacurile de după 11 septembrie, prin reticența de a lua vaccinul cu antrax, a reflectat teama lor de efectele secundare ale vaccinului și neîncrederea în personalul medical. În orice incident bioterorist la scară largă, această neîncredere poate fi un obstacol major pentru limitarea eficientă a unui agent infecțios<sup>22</sup>.

Autoritățile speră că planificarea în caz de dezastre și elaborarea unor contramăsuri medicale

eficiente pentru atacurile biologice vor minimiza impactul oricărui astfel de atac și vor acționa, de asemenea, ca descurajare pentru cei care ar putea lua în considerare un astfel de atac. Dacă atacul ar putea fi ușor stăpânit și abordat, atunci o națiune teroristă sau neprietenoasă ar putea fi mai puțin motivată să inițieze o astfel de acțiune.

**Răspunsul la armele biologice.** O varietate de instituții și agenții federale, de stat și locale, sunt implicate în SUA în pregătirea și răspunsul la situații de urgență de sănătate publică. Rolul acestora este de a construi și consolida pregătirea națională pentru urgențele de sănătate publică cauzate de evenimente naturale, accidentale sau intenționate. O finanțare corespunzătoare trebuie să sprijine constituirea și gestionarea depozitelor de vaccinuri, medicamente și materiale medicale necesare a fi desfășurate în situații de urgență la nivel național.

De asemenea, sunt responsabilizate și finanțate structuri care efectuează studii și experimente privind amenințările biologice actuale și viitoare, evaluează vulnerabilitățile și elaborează evaluări ale riscurilor/determină efectele potențiale pentru a ghida dezvoltarea de contramăsuri, precum detectoare, medicamente, vaccinuri și tehnologii de decontaminare. Altele sunt responsabile pentru răspunsul și analiza atacurilor cu arme biologice după ce acestea au loc, pentru a ajuta anchetatorii să identifice autorii și să determine originea și metoda atacului. Departamentele de sănătate statale și locale, precum și spitalele publice și private și agențiile locale de aplicare a legii, ar fi, de asemenea, implicate în răspunsul la o urgență de sănătate publică cu arme biologice. Rolurile lor sunt conturate în planurile naționale de răspuns și sunt abordate în detaliu prin planuri specifice fiecărei organizații.

Cerințele de reglementare pentru autorizarea unui vaccin sunt complexe și se aplică unui proces în mai multe etape de testare a siguranței, imunogenității și eficacității și supravegherii post-autorizare. Un vaccin tipic ar putea fi în

dezvoltare și studii clinice timp de 10 până la 20 de ani înainte de licență. O provocare în acordarea de licențe a vaccinurilor pentru răspunsul la amenințările cu armele biologice este absența unora dintre acești agenți ai bolii în lumea naturală. Eficacitatea vaccinului este mai dificil de stabilit atunci când expunerea naturală la un agent patogen este imposibilă și când studiile asupra provocării umane nu sunt fezabile<sup>23</sup>.

#### ***Asigurarea vaccinurilor și anticorpilor.***

Într-o urgență la scară largă, în care un vaccin este disponibil sau potențial disponibil, ar fi necesară o cantitate mare de vaccin și ar fi necesară rapid. Stocurile naționale strategice trebuie să asigure suficiente vaccinuri împotriva variolei pentru a vaccina fiecare persoană din țară în cazul unui atac cu arme biologice. De asemenea, stocul va deține milioane de doze de vaccin cu antrax, alte vaccinuri, medicamente antivirale și alte consumabile medicale. Implementarea rapidă a unui vaccin este esențială pentru succesul acestuia în prevenirea bolilor. Pentru unele boli, vaccinarea după expunere poate să nu aibă niciun efect asupra prevenirii bolii, iar pentru altele vaccinarea trebuie să aibă loc foarte repede după expunere, pentru profilaxie<sup>24</sup>.

Experții în biosecuritate au sugerat că utilizarea agenților pentru imunizarea pasivă ar putea juca un rol ca răspuns la anumite atacuri cu arme biologice. Avantajul utilizării anticorpilor, mai degrabă decât a vaccinurilor, pentru răspunsul la un eveniment bioterorist este că anticorpii oferă protecție imediată, în timp ce un răspuns protector generat de un vaccin nu este imediat și, în unele cazuri, poate depinde de o doză de rapel administrată ulterior. Candiții pentru această potențială aplicare a imunizării pasive includ toxina botulinică, tularemia, antraxul și ciuma. Pentru majoritatea acestor ținte s-au efectuat doar studii pe animale și, prin urmare, utilizarea imunizării pasive în potențiale evenimente cu arme biologice se află încă în stadii experimentale<sup>25</sup>.

## **CONCLUZII**

Un atac biologic, inițiat de o grupare teroristă sau de un stat ostil, pare să fie o posibilitate îndepărtată, dar care necesită o planificare a răspunsului la urgențe de sănătate publică. Mai multe simulări, realizate în câteva țări democratice dezvoltate, precum SUA, Franța, Germania, Marea Britanie, prin implicarea mai multor instituții specializate și agenții, au dezvăluit punctele slabe ale sistemelor concepute pentru a răspunde la urgențe biologice. Aceste exerciții au ajutat la concentrarea eforturilor de planificare organizațională și funcțională și de elaborare a unor planuri de urgență necesare unei coordonări acționale eficiente pentru ca un eveniment de amploare, produs de arme biologice, să nu excedă capacităților medicale disponibile sau să provoace îmbolnăviri și decese pe scară largă și să conducă la perturbări economice și sociale majore.

Așadar, într-un eveniment cu arme biologice, realizarea rapidă și întrebuintarea cu succes a vaccinurilor, precum și asigurarea anticorpilor și a altor medicamente, depind și de o serie de alți factori. Aceste nevoi se referă la personalul specializat în combaterea atacului, stabilitatea sistemului de transport în caz de urgență, disponibilitatea unor capacități medicale viabile, eficiența vaccinului și medicamentelor și capacitatea sistemului de sănătate publică de a comunica cu publicul și de a asigura vaccinurile și medicamentele către persoanele care au nevoie de ele.

Epidemiile și pandemiile sunt tipuri de dezastre care sunt capabile să copleșesc sistemele de sănătate, perturbând comunități și determinând efecte devastatoare asupra societății, în special economice și psihologice. În această perioadă de ordine haotică, în care diferențele de opinii dintre actorii globali, precum SUA, Rusia, China și UE, se accentuează, când terorismul produce o insecuritate continuă în arena internațională, când epidemiile și pandemia de COVID-19 pun la grea încercare sănătatea multor popoare și când utilizarea puterii armate reprezintă soluția adoptată în majoritatea conflictelor regionale, spectrul războiului nerestricționat amenință, în fiecare clipă, pacea fragilă.



## BIBLIOGRAFIE

1. BARRY Kellman, *Bioviolence: Preventing Biological Terror and Crime*, New York, Cambridge University Press, 2007, 392 p.
2. CARUS W. Seth, *Bioterrorism and Biocrimes: The Illicit Use of Biological Agents Since 1900*, Washington DC, Center for Counterproliferation Research, National Defense University, 2001, 220 p.
3. CARUS W. Seth, "A century of biological-weapons programs (1915–2015): reviewing the evidence", *Nonproliferation Review*, vol. 24, nr. 1-2, 2017, pp. 129-153.
4. CAUDLE L.C., "The biological warfare threat", în Sidell FR, Takafuji ET, Franz DR, *Medical Aspects of Chemical and Biological Warfare*, Washington DC, Office of the Surgeon General, Borden Institute, Walter Reed Army Medical Center, 1997, pp. 451–466, [http://www.bordeninstitute.army.mil/cwbw/default\\_index.htm](http://www.bordeninstitute.army.mil/cwbw/default_index.htm).
5. CAVES Jr. John P., Carus W. Seth, *The Future of Weapons of Mass Destruction: Their Nature and Role in 2030*, Occasional Paper 10, Washington DC, National Defense University Press, 2014, 6 p.
6. CHIFU Iulian, Nantoi Oazu, *Război informațional. Tipizarea agresivității informaționale a Federației Ruse*, Editura Institutului de Științe Politice și Relații Internaționale „Ion I.C. Brătianu” al Academiei Române, București, 2016, 542 p.
7. COLEMAN C., Frieman M., „Coronaviruses: important emerging human pathogens”, *Journal of Virology*, vol. 88 (10), 2014, pp. 5209-5212.
8. COX N., Tamblyn S., Tam T., „Influenza pandemic planning”, *Vaccine*, vol. 21 (16), 2003, pp. 1801-1803.
9. DANZIG Richard, *Aum Shinrikyo: Insights into How Terrorists Develop Biological and Chemical Weapons*, 2nd ed., Washington DC, Center for a New American Security, 2012, 65 p.
10. EITZEN E.M. Jr., Takafuji E.T., "Historical overview of biological warfare", în Sidell FR, Takafuji ET, Franz DR, *Medical Aspects of Chemical and Biological Warfare*, Washington DC, Office of the Surgeon General, Borden Institute, Walter Reed Army Medical Center, 1997, [http://www.bordeninstitute.army.mil/cwbw/default\\_index.htm](http://www.bordeninstitute.army.mil/cwbw/default_index.htm).
11. FELDMANN H., Geisbert T., „Ebola haemorrhagic fever”, *The Lancet*, nr. 377 (9768), 2011, pp. 849-862.
12. GEISLER Erhard, Courtland Moon John Ellis (eds.), *Biological and Toxin Weapons: Research, Development and Use from the Middle Ages to 1945*, Stockholm International Peace Research Institute/SIPRI, Oxford University Press, 1999, 277 p.
13. GOSTIN L.O., Lucey D., Phelan A., „The Ebola epidemic: a global health emergency”, *JAMA*, nr. 312 (11), 2014, pp. 1095-1096.
14. GRONVALL G.K., *Synthetic biology: Safety, security, and promise*, Baltimore, CreateSpace Independent Publishing Platform, 2016, 198 p.
15. GUILLEMIN Jeanne, *American Anthrax: Fear, Crime, and the Investigation of the Nation's Deadliest Bioterror Attack*, 1st ed., New York, Times Books, 2011, 336 p; Expert Behavioral Analysis Panel, *The Amerithrax Case: Report of the Expert Behavioral Analysis Panel*, Vienna, VA: Research Strategies Network, 2011.
16. HARRIS Elisa D., "Dual-Use Threats: The Case of Biological Technology", în *Governance of Dual-Use Technologies: Theory and Practice*, ed. Elisa D. Harris, Cambridge, American Academy of Arts and Sciences, 2016, pp 60-111.
17. HARTMAN A., Towner J., Nichol S., „Ebola and marburg hemorrhagic fever”, *Clinics in Laboratory Medicine*, vol. 30 (1), 2010, pp. 161-177.
18. HUANG Y., "The SARS epidemic and its aftermath in China: A political perspective", în: KNOBLER, S., Mahmoud, A., Lemon, S., Mack, A., Sivitz, L., Oberholtzer, K., *Learning from SARS: Preparing for the Next Disease Outbreak*. Workshop Summary, National Academies Press, Washington DC, 2004, pp 116-136.
19. JEFFREY D. Simon, *Terrorists and the Potential Use of Biological Weapons: A Discussion of Possibilities*, RAND Corporation, Santa Monica CA, 1989, 35 p.
20. JONES K., Pate N., Levy M., Storeygard A., Balk D., Gittleman J., Daszak P., „Global trends

- in emerging infectious diseases”, *Nature*, nr. 451 (7181), 2008, pp. 990-993.
21. KATZ R., Fischer J., „The revised international Health Regulations: A framework for global pandemic response”, *Global Health Governance*, vol. 3 (2), 2010, p.
  22. KEIM P., „A novel botulinum neurotoxin and how it tested our scientific institutions”, *Journal of Infectious Diseases*, nr. 213 (3), 2016.
  23. LE GUENNO B., „Haemorrhagic Fevers and Ecological Perturbations”, în O.-R. Kaaden, C.-P. Czerny, W. Eichhorn (eds.), *Viral Zoonoses and Food of Animal Origin. A Re-Evaluation of Possible Hazards for Human Health*, Conference proceedings, Springer-Verlag, Vienna, 1997, pp. 191-199.
  24. LEITENBERG Milton, „Aum Shinrikyo’s Efforts to Produce Biological Weapons: A Case Study in the Serial Propagation of Misinformation”, *Terrorism and Political Violence*, vol. 11, nr. 4, 1999, pp. 149-158.
  25. LEITENBERG Milton, *Assessing the Biological Weapons and Bioterrorism Threat* (Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College), 2005, 117 p.
  26. LIPSITCH M., Riley S., Cauchemez S., Ghani A., Ferguson N., „Managing and Reducing Uncertainty in an Emerging Influenza Pandemic”, *New England Journal of Medicine*, nr. 361 (2), 2009, pp. 112-115.
  27. MAURICE J., „The Zika virus public health emergency: 6 months on”, *The Lancet*, nr. 388, 2016, pp. 449-450.
  28. NATIONAL RESEARCH COUNCIL, Committee on Research Standards and Practices to Prevent the Destructive Application of Biotechnology, *Biotechnology Research in an Age of Terrorism*, National Academies Press, Washington DC, 2004, pp. 107-130.
  29. NGYUEN-VAN-TAM J.S., Penttinen P.M.P., „Preparedness and Response to Pandemics and Other Infectious Disease Emergencies”, în SELLWOOD C., Wapling A., *Health Emergency Preparedness and Response*, CABI, Wallingford, UK, 2016, pp. 152-165.
  30. NOWAK R., „Killer mousepox virus raises bioterror fears”, *New Scientist*, 2001, <https://www.newscientist.com/article/dn311-killer-mousepox-virus-raises-bioterror-fears>.
  31. OUGRHAM-GORMLEY S.R., *Barriers to bioweapons: The Challenges of Expertise and Organisation for Weapons Development*, Ithaca NY, Cornell University Press, 2014, 240 p..
  32. REDDY P., „An overview of Ebola. An emerging virus”, *World Journal of Pharmacy and Pharmaceutical Sciences*, nr. 4 (6), 2015, pp. 370-376.
  33. SEMENZA J.C., Lindgren E., Espinosa L., Balkanyi L., Penttinen P., Rocklöv J., „Determinants and Drivers of Infectious Disease Threats in Europe”, *The European Journal of Public Health*, vol. 25 (3), 2015, pp. 581-589.
  34. TAUBENBERGER J.K., Morens D.M., „1918 Influenza: The mother of all pandemics”, *Emerging Infectious Diseases*, vol. 12 (1), 2006, pp. 15-22.
  35. The Federal Select Agent Program, „Select agents and toxins list”, <https://www.selectagents.gov/selectagentsandtoxinslist.html>.
  36. TOHMATSU Haruo, „The Strategic Correlation between the Sino-Japanese and Pacific Wars”, în PEATTIE Mark, Edward J. Drea, Hans van de Ven, *The Battle for China: Essays on the Military History of the Sino-Japanese War of 1937-1945*, Stanford University Press, 2011, 614 p.
  37. TUCKER Jonathan B. (ed.), *Toxic Terror: Assessing Terrorist Use of Chemical and Biological Weapons*, Cambridge, MIT Press, 2000, 320 p.
  38. U.S. Department of the Army, „Military Biology and Biological Agents”, Washington DC, Government Printing Office, 1964, în SIPRI, *The Problem of Chemical and Biological Warfare*, vol. 2, 311.
  39. US Army Medical Research Institute for Infectious Diseases, *Medical Management of Biological Casualties Handbook*, 4th ed. Frederick MD, Fort Detrick, 2001.
  40. XIAO FANG Li, *Blood-weeping Accusations: Records of Anthrax Victims*, Beijing, Zhong yang wen xian chu ban she, 2005.
  42. SHELDON H. Harris, *Factories of Death: Japanese Biological Warfare, 1932-1945, and the American Cover-up*, New York, Routledge, 2002, 424 p.

43. WHO, 2014, "World Health Organization Statement on the Meeting of the International Health Regulations Emergency Committee Regarding the 2014 Ebola Outbreak in West Africa", <http://www.who.int/mediacentre/news/statements/2014/ebola-20140808/en/>.
43. WHO, 2016a, "Ebola Situation Report. 30 March 2016", World Health Organization, <http://apps.who.int/ebola/current-situation/ebola-situation-report-30-march-2016>.
44. WHO, 2016d, "Fifth Meeting of the Emergency Committee under the International Health Regulations (2005) Regarding Microcephaly, Other Neurological Disorders and Zika Virus", World Health Organization, <http://www.who.int/mediacentre/news/statements/2016/zika-fifth-ec/en/>.
45. WHO Group of Consultants, *Health Aspects of Chemical and Biological Weapons*, Geneva, Switzerland, World Health Organization, 1970.
46. YAKOB L., Walker T., „Zika virus outbreak in the Americas: the need for novel mosquito control method", *The Lancet Global Health*, vol. 4 (3), 2016, pp. 148-149.
47. YU Victor L., „*Serratia marcescens*: historical perspective and clinical review", *The New England Journal of Medicine*, nr. 300, 1979, pp. 887-893.
48. ZILINSKAS Raymond A., „Iraq's biological weapons. The past as future?", *JAMA*, vol. 278, nr. 5, 1997, pp. 418-424.
49. ZILINSKAS Raymond A., *The Soviet Biological Weapons Program and Its Legacy in Today's Russia*, Center for the Study of Weapons of Mass Destruction, Occasional Paper 11, Washington DC, National Defense University Press, 2016, 60 p.

- <sup>1</sup> E.M. Eitzen Jr., E.T. Takafuji, "Historical overview of biological warfare", în Sidell FR, Takafuji ET, Franz DR, eds. *Medical Aspects of Chemical and Biological Warfare*, Washington, DC, Office of the Surgeon General, Borden Institute, Walter Reed Army Medical Center, 1997, pp. 415-423, online [http://www.bordeninstitute.army.mil/cwbw/default\\_index.htm](http://www.bordeninstitute.army.mil/cwbw/default_index.htm), accesat la 28 octombrie 2021.
- <sup>2</sup> W. Seth Carus, *A Short History of Biological Warfare*, pp. 222-223.
- <sup>3</sup> Mark L. Wheelis, "Biological Sabotage in World War I", în *Biological and Toxin Weapons: Research, Development and Use from the Middle Ages to 1945* (Geissler Erhard and John Ellis Courtland Moon eds.), Stockholm International Peace Research Institute/SIPRI, Oxford University Press, 1999, pp. 35-62.
- <sup>4</sup> Haruo Tohmatsu, "The Strategic Correlation between the Sino-Japanese and Pacific Wars", în *The Battle for China: Essays on the Military History of the Sino-Japanese War of 1937-1945*, Mark Peattie, Edward J. Drea, and Hans van de Ven (eds.), Stanford University Press, 2011, accesat la 29 octombrie 2021.
- <sup>5</sup> W. Seth Carus, "A century of biological-weapons programs (1915-2015): reviewing the evidence", *Nonproliferation Review*, vol. 24, nr. 1-2, 2017, pp. 129-153.
- <sup>6</sup> Davis J. Christopher, "Nuclear Blindness: An Overview of the Biological Weapons Programs of the Former Soviet Union and Iraq", *Emerging Infectious Diseases*, vol. 5, nr. 4, 1999, accesat la 31 octombrie 2021.
- <sup>7</sup> RA Zilinskas, "Iraq's biological weapons. The past as future?", *JAMA*, 1997, p. 418-424.
- <sup>8</sup> Milton Leitenberg, *Assessing the Biological Weapons and Bioterrorism Threat*; Rolf Mowatt Larssen, *Al Qaeda Weapons of Mass Destruction Threat: Hype or Reality?*, Belfer Center for Science and International Affairs, Harvard Kennedy School, Cambridge, 2010, accesat la 29 octombrie 2021.
- <sup>9</sup> LC Caudle, "The biological warfare threat", în FR Sidell, ET Takafuji, DR Franz, *Medical Aspects of Chemical and Biological Warfare*, Washington, DC, Office of the Surgeon General, Borden Institute, Walter Reed Army Medical Center, 1997, pp. 451-466. online [http://www.bordeninstitute.army.mil/cwbw/default\\_index.htm](http://www.bordeninstitute.army.mil/cwbw/default_index.htm), accesat la 01 noiembrie 2021.
- <sup>10</sup> Jeanne Guillemin, *American Anthrax: Fear, Crime, and the Investigation of the Nation's Deadliest Bioterror Attack*, Times Books, New York, 2011, accesat la 01 noiembrie 2021.
- <sup>11</sup> Milton Leitenberg, "Aum Shinrikyo's Efforts to Produce Biological Weapons: A Case Study in the Serial Propagation of Misinformation", *Terrorism and Political Violence*, vol. 11, no. 4, 1999, pp. 149-158.
- <sup>12</sup> Hartman A., Towner J., Nichol S., "Ebola and Marburg hemorrhagic fever", *Clinics in Laboratory Medicine*, vol. 30 (1), 2010, pp. 161-177.
- <sup>13</sup> Coleman C., Frieman M., "Coronaviruses: important emerging human pathogens", *Journal of Virology*, vol. 88 (10), 2014, pp. 5209-5212.
- <sup>14</sup> Bramanti B, Stenseth NC, Walløe L, "Plague: a disease which changed the path of human civilization", p. 1-26, în Yang R, Anisimov A, *Yersinia pestis: retrospective and perspective*, Springer, Heidelberg, Germany, 2016, accesat la 04 noiembrie 2021.



- <sup>15</sup> Esteban David J., Buller R. Mark L., "Ectromelia virus: the causative agent of mousepox", *Journal of General Virology*, vol. 86 (10), 2005, pp. 2645-2659.
- <sup>16</sup> Henderson DA, Moss B, "Smallpox and Vaccinia", in Plotkin SA, Orenstein WA, *Vaccines* (3rd ed.). Philadelphia, Pennsylvania, WB Saunders, 1988, accesat 06 noiembrie 2021.
- <sup>17</sup> Ceccarelli M., Colantuoni V., Graziano G., Rampone S., *Bioinformatica. Sfide e prospettive*, Ed. Franco Angeli, Milano, 2006, ISBN-10: 8846482786, ISBN-13: 979-8846482785, pp. 58-72.
- <sup>18</sup> Ougrham-Gormley SR, *Barriers to bioweapons: The challenges of expertise and organisation for weapons development*, Ithaca NY, Cornell University Press, 2014, accesat la 08 noiembrie 2021.
- <sup>19</sup> *Model State Emergency Health Powers Act*, Center for Law and the Public's Health, Georgetown University Law Center, Washington DC, 2001, p. 9.
- <sup>20</sup> W. Seth Carus, *Bioterrorism and Biocrimes: The Illicit Use of Biological Agents Since 1900*, Center for Counterproliferation Research, National Defense University, Washington DC, 2001, pp. 71-73.
- <sup>21</sup> *Dark Winter—About the Exercise*, Center for Health Security, University of Pittsburgh Medical Center, 5 November 2020, accesat la 09 noiembrie 2021.
- <sup>22</sup> Jeanne Guillemin, *op.cit.*
- <sup>23</sup> Jones K., Pate N., Levy M., Storeygard A., Balk D., Gittleman J., Daszak P., "Global trends in emerging infectious diseases", *Nature*, nr. 451 (7181), 2008, pp. 990-993.
- <sup>24</sup> Lipsitch M., Riley S., Cauchemez S., Ghani A., Ferguson N., "Managing and reducing uncertainty in an emerging influenza pandemic", *The New England Journal of Medicine*, nr. 361 (2), 2009, pp. 112-115.
- <sup>25</sup> Katz R., Fischer J., "The revised international Health Regulations: a framework for global pandemic response", *Global Health Governance*, vol. 3 (2), 2010, accesat la 11 noiembrie 2021.



# TEHNOLOGIILE CUANTICE ȘI IMPACTUL LOR ASUPRA SECURITĂȚII INFORMATICE

*Sergiu Beniamin MĂLUȚAN\**

## **Abstract**

*The digital revolution, which began in the second half of the 20th century with the transition from analog to digital electronics and the mass adoption of electronic computers, and the subsequent emergence of the Internet changed the way we organize our activities and whole life. This progress, which marked the beginning of the information age, created a lot of new opportunities, but also of challenges, one of them being security. Computer security has emerged as a natural necessity first among state actors, followed by banking institutions and companies, and finally among all users of digital products or services.*

*In this paper we aim to see the current state of maturity of quantum technologies and to anticipate the opportunities and challenges in the field of information security that will appear as a natural reaction once their large-scale adaptation.*

**Keywords:** information security; cryptography; quantum technology; emerging technologies.

## **INTRODUCERE**

Istoria calculatorului cuantic a început în anul 1980 când fizicianul Paul Benioff a propus primul model arhitectural al unui calculator cuantic, perioadă în care a fost inițiată producția microprocesoarelor pe 8 biți. Doi ani mai târziu, Richard Feynman a afirmat, într-un articol, că pentru a putea face simulări complexe ale sistemelor cuantice este nevoie de un calculator cuantic. Richard Feynman este creditat ca pionier al calculatorului cuantic deoarece a arătat că există probleme care nu pot fi rezolvate eficient nici prin scalarea calculatoarelor clasice, nici prin paralelismul excesiv, ci doar folosind un calculator cuantic. Odată identificată nevoia, s-a deschis drumul spre cercetare și dezvoltare, chiar dacă calculatoarele electronice erau doar la început de drum.

Deși limitat la doar 2 qubiți și era stabil doar pentru 2 secunde, primul calculator cuantic capabil să încarce date, să efectueze operații și să returneze un rezultat a fost creat în anul 1998 de către cercetătorii Isaac Chuang, Neil Gershenfeld și Mark Kubinec. Acest calculator a avut mai degrabă rolul de a demonstra că acest tip de calculator este realizabil decât de a executa un program cu o utilitate reală, cu toate că Peter Shor a publicat algoritmul care îi poartă numele, descriind cum pot fi rezolvate problema logaritmilor discreți și cea a factorizării numerelor mari utilizând un calculator cuantic, ceea ce ar compromite protocoalele criptografice bazate pe aceste probleme matematice și anume RSA și criptografia pe curbe eliptice.

O mare problemă în dezvoltarea de programe pentru acest tip de procesoare o constituie

\* *Expert în Ministerul Apărării Naționale.*

faptul că nu pot fi salvate stări intermediare din procesul de calcul, iar o singură eroare intervenită implică reluarea procesului de la început, o mare provocare fiind dezvoltarea de mecanisme eficiente de detecție a erorilor. Chiar dacă, în prezent, nu este încă o amenințare reală pentru sistemele criptografice cu chei publice standardizate, cercetătorii dezvoltă algoritmi criptografici rezistenți la atacurile care se bazează pe utilizarea unui calculator cuantic, denumiți generic algoritmi criptografici post-cuantici.

Google a anunțat în anul 2019 că a atins supremația cuantică, adică folosind procesorul cuantic propriu Sycamore (54 de qubiți) a reușit să rezolve un calcul în 200 de secunde, în timp ce aceeași problemă ar fi fost rezolvată de un super calculator clasic în mai mult de 10.000 de ani; un anunț similar a fost făcut în anul 2021 de către guvernul chinez. Totuși, trebuie menționat faptul că problemele alese pentru a demonstra supremația cuantică nu sunt unele generale, ci sunt alese special pentru a fi pretabile la un asemenea experiment, calculatoarele cuantice fiind mult mai rapide în rezolvarea anumitor tipuri de probleme, dar mai lente în alte cazuri.

## PRINCIPII ALE FIZICII CUANTICE

**Superpoziția** este un principiu fundamental al fizicii cuantice care stipulează că dacă o particulă se poate afla în una din două sau mai multe stări cuantice, atunci orice combinație lineară între acele stări reprezintă o stare în plus în care se poate afla particula respectivă. În cazul qubiților, care pot fi 0 sau 1, aceștia se pot afla într-o a treia stare fiind 0 și 1 în același timp, dar odată măsurată starea de superpoziție aceasta devine fie 0, fie 1.

**Inseparabilitatea cuantică** (*entanglement*) este un fenomen cuantic care face ca stările cuantice în care se pot afla anumite particule elementare să fie strâns legate între ele, adică funcția de undă care descrie sistemul din care fac parte particulele respective nu poate fi redusă prin factorizare la mai multe funcții elementare. Pe baza acestui fenomen, se pot dezvolta comunicații cuantice, codare super densă și

teleportare cuantică. Teleportarea cuantică este un proces care permite transferul informației codificate în starea cuantică a unei particule, de la sursa care o emite la destinație fără a transfera și particula respectivă, ci doar starea ei. Dat fiind faptul că acest gen de transfer se realizează printr-un canal clasic, viteza de transfer nu va depăși viteza uzuală a canalului de comunicație.

## CRİPTOGRAFIA CUANTICĂ ȘI CRİPTOGRAFIA POST-CUANTICĂ

Criptografia cuantică reprezintă o subramură a criptografiei care se bazează pe fenomene din fizica cuantică, în timp ce criptografia post-cuantică se referă la dezvoltarea de soluții clasice care să asigure nivelul de securitate dorit pornind de la premiza că adversarul beneficiază de avantajele unui procesor cuantic.

În momentul de față, National Institute for Science and Technologies/NIST are deschisă o competiție pentru a stabili standardul pentru algoritmi de criptare și semnătură electronică cu rezistență post-cuantică. Desemnarea algoritmilor câștigători este programată pentru acest an, competiția debutând în anul 2017. Aici trebuie avut în vedere că acest tip de algoritmi, post-cuantici, sunt proiectați să reziste atacurilor cunoscute care s-ar putea realiza, cu condiția de a avea acces la un calculator cuantic, dar există posibilitatea dezvoltării altor tipuri de algoritmi care să slăbească protocoalele criptografice clasice.

Cele mai dezvoltate protocoale criptografice bazate pe fizica cuantică sunt cele utilizate în negocierea sau schimbul de chei criptografice (*QKD*). Ideea unui astfel de protocol a fost propusă pentru prima dată în anul 1970, dar a început să se dezvolte începând cu anii 1990, când tot mai mulți fizicieni au devenit interesați de tehnologiile cuantice. Progresul în acest domeniu a fost remarcabil, existând soluții comerciale bazate pe această tehnologie, fiind cea mai matură dintre toate conceptele bazate pe mecanica cuantică. Distribuția cuantică a cheilor reprezintă o metodă sigură de distribuire și partajare a cheilor utilizate de algoritmi și

protocoalele criptografice, utilă mai ales pentru protejarea de informații pe o perioadă lungă de timp, cum ar fi datele medicale ale unui pacient pe tot timpul vieții acestuia sau secrete de stat clasificate pe o perioadă îndelungată. În situații ca cele descrise anterior, dacă partajarea cheilor se face folosind criptografia clasică există riscul ca o persoană rău intenționată să stocheze datele în formă criptată și cheia protejată până în momentul în care tehnologia evoluează suficient de mult pentru a avea la dispoziție puterea de calcul necesară pentru a decodifica datele sensibile. O problemă esențială a protocoalelor de schimb de chei o constituie necesitatea ca acestea să rămână private pe timpul transferului, iar mecanismul QKD are la bază tocmai principiul conform căruia, odată ce este observată, o particulă își modifică proprietățile cuantice; așadar, dacă cineva încearcă să intercepteze cheia, nu doar că o va modifica și nu va putea fi utilizată (deci nu constituie un avantaj pentru atacator), dar corespondenții vor conștientiza că linia de comunicații este monitorizată.

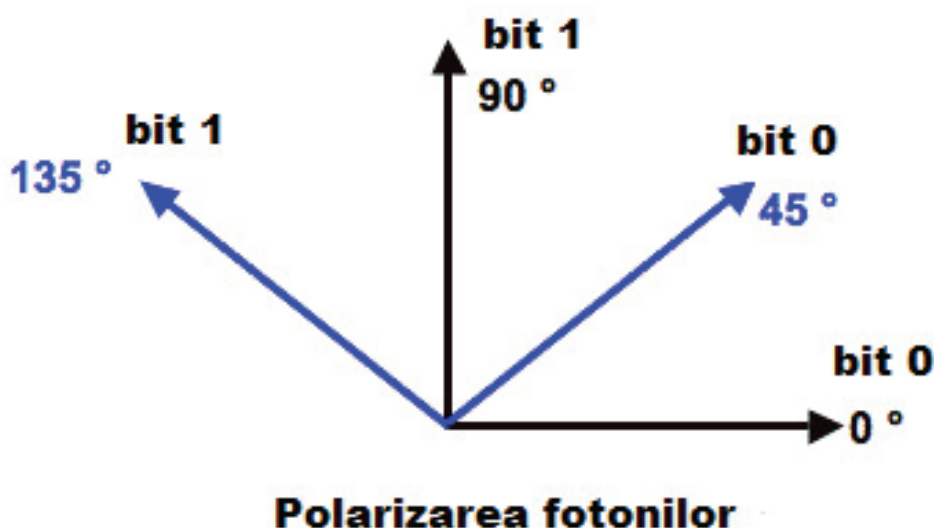
Pentru dezvoltarea unui asemenea sistem este necesară codificarea biților în funcție de polarizarea fotonilor din fluxul de comunicație. De exemplu, în figura de mai jos este reprezentată codificarea fotonilor astfel: un foton rotit cu 45 de grade se codifică în valoarea 0, iar un foton

rotit cu valoarea unui unghi complementar se va codifica în valoarea 1.

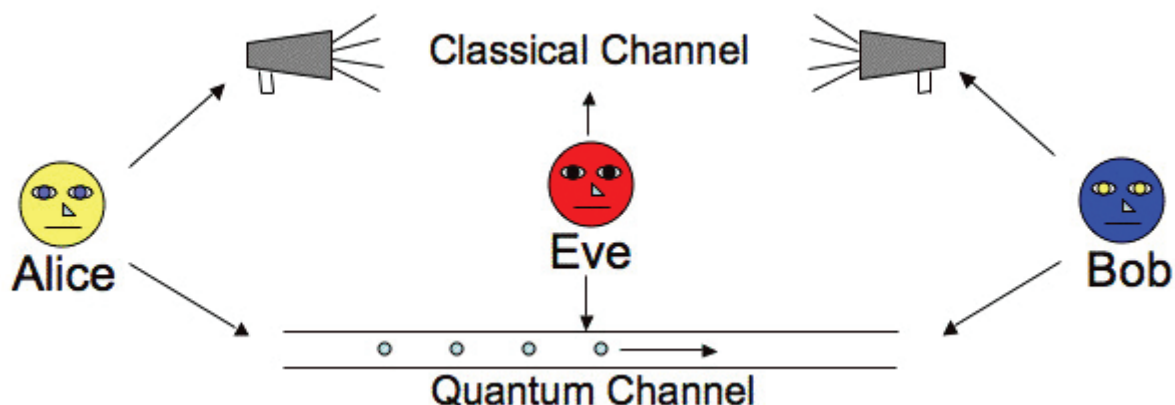
Protocolul BB84, propus în anul 1984, este cel mai cunoscut protocol din familia QKD. Acest protocol prezintă o metodă securizată prin care doi corespondenți, Alice și Bob, negociază o cheie criptografică simetrică, utilizând două canale de comunicații, unul clasic și unul cuantic. Protocolul este sigur din punct de vedere teoretic, fără a fi nevoie să facem presupuneri despre resursele de care dispune, în încercarea de a intercepta cheia, deoarece protocolul nu se bazează pe timpul necesar pentru a rezolva o problemă matematică grea din punct de vedere al numărului de calcule, ci pe imposibilitatea de a încălca legile fizicii.

Totuși, canalul de comunicație cuantic nu oferă autentificare fiind susceptibil la atacuri de tipul *Man-in-the-Middle*, dacă autentificarea nu se realizează pe un canal de comunicație clasic, după modelul prezentat în figura 2.

În această schemă, Alice se autentifică cu Bob pentru a evita interpunerea Atacatorului pe canalul de comunicație cuantic dintre cei doi. Alice îi transmite lui Bob un flux de fotoni polarizați, reprezentând un șir de 0 și 1, iar Bob folosește un șir de filtre aleatoriu pentru a decodifica informația primită de la Alice, după care îi trimite acesteia secvența de filtrare pe care



**Figura 1: Polarizarea fotonilor**  
(conform Mart Haitjema, "A Survey of the Prominent Quantum Key Distribution Protocols", 2007)



**Figura 2: Schimb de chei la nivel cuantic**  
(conform Mart Haitjema, "A Survey of the Prominent Quantum Key Distribution Protocols", 2007)

a folosit-o. Alice verifică filtrele folosite corect și utilizează biții corespunzători pentru a genera cheia.

O categorie de probleme de securitate, de tipul *side-channel*, ar putea fi generată de semnalul de zgomot din cadrul canalului de comunicație și de echipamente imperfecte. În aplicațiile reale, Alice și Bob, în cazul în care măsurătorile lor nu sunt perfect corelate, nu pot să fie siguri dacă discrepanțele dintre măsurătorile lor au fost cauzate de zgomotul introdus pe canalul de comunicație de către echipamentele utilizate sau de către o persoană terță care a perturbat starea fotonilor încercând să măsoare polarizarea acestora.

O altă problemă este dată de calibrarea sursei de fotoni. Dacă aceasta emite fotoni legați între ei (*entangled*), adică au aceleași proprietăți chiar dacă traseul lor este diferit, distincția dintre ei devenind imposibilă, atunci Eve poate capta acest tip de fotoni fără ca cei doi utilizatori reali ai sistemului să fie conștienți că cineva monitorizează canalul prin care realizează schimbul de chei.

## STADIUL ACTUAL

Cea mai lungă rețea de acest gen este operațională în R.P. Chineză, având o lungime de peste 2000 de km, asigurând legătura între orașele Beijing și Shanghai și fiind utilizată de companii și instituții bancare. În Statele Unite ale Americii,

compania Quantum Exchange a construit o rețea similară, conectând centrele de date din Manhattan și New Jersey. În Europa există inițiativa EuroQCI (Infrastructura de comunicații cuantice în Europa), în cadrul strategiei de dezvoltare digitală a UE, unde participă și România, planul de investiții fiind evaluat la peste un miliard de euro. Un alt proiect de dezvoltare a unei infrastructuri de comunicații cuantice în România este cel numit QUANTGRID. De asemenea, în universitățile românești au început să se dezvolte programe de studii postuniversitare axate pe studiul tehnologiilor cuantice, creând astfel un cadru propice pentru pregătirea specialiștilor în domeniu.

În cazul comunicațiilor cuantice, principala problemă o reprezintă necesitatea unui repetitor cuantic, care să permită scalarea acestor rețele într-un mod cât mai eficient. Soluția practică momentan constă în crearea de noduri de rețea securizate și de încredere, unde informația codată în proprietățile cuantice ale particulelor este decodificată și recodificată pentru a fi transmisă mai departe.

## CONCLUZII

Chiar dacă tehnologiile cuantice par încă la început de drum, ele sunt studiate încă de la apariția calculatoarelor digitale clasice, iar adoptarea lor la scară largă pare să se apropie cu pași din ce în ce mai rapizi.



Tehnologiile cuantice sunt utilizate chiar dacă nu pot acoperi eficient nevoile actuale de scalabilitate. Acestea fac parte din categoria tehnologiilor emergente, în continuă dezvoltare și joacă un rol important în securitatea informatică, implicit în războiul cibernetic. Chiar dacă în momentul actual calculatoarele cuantice nu pot periclita securitatea comunicațiilor clasice, trebuie să fim mereu pregătiți și să acordăm o

importanță deosebită datelor sensibile care trebuie protejate o perioadă lungă de timp (secrete de stat, de exemplu) și care ar putea fi interceptate și păstrate de atacator pentru a fi decriptate atunci când va avea la dispoziție un calculator cuantic.

Prin urmare, este esențial să avem mereu informații actualizate legate atât de progresul altor state în acest domeniu, cât și de posibilele probleme care ar putea fi generate de aceste noi tehnologii.

## BIBLIOGRAFIE

1. ARUTE Frank, Arya Kunal și alții, "Quantum supremacy using programmable superconducting processor", *Nature*, vol. 574, nr. 7779, octombrie 2019, pp. 505-510.
2. BENIOFF Paul, "The Computer as a Physical System: A Microscopic Quantum Mechanical Hamiltonian Model of Computers as Represented by Turing Machines", *Journal of Statistical Physics*, vol. 22, nr. 5, 1980, p. 563-591.
3. DIRAC Paul Adrien Maurice, *The Principles of Quantum Mechanics* (third edition), Oxford University Press, 1947, pp. 10-12.
4. FEYNMAN P. Richard, "Simulating physics with computers", *International Journal of Theoretical Physics*, vol. 21, 1982, pp. 467-488.
5. GIBNEY Elizabeth, "Europe plans giant billion-euro quantum technologies project", *Nature*, nr. 532, Aprilie 2016.
6. GILES Martin, "Explainer: What is quantum communications?", *MIT Technology Review*, 14 february 2019, <https://www.technologyreview.com/2019/02/14/103409/what-is-quantum-communications/>.
7. HAITJEMA Mart, "A Survey of the Prominent Quantum Key Distribution Protocols", <https://www.cse.wustl.edu/~jain/cse571-07/ftp/quantum/#entanglement>.
8. KIM Jeong San, Gilad Gour, Barry C. Sanders, "Limitations to sharing entanglement", *Contemporary Physics*, vol. 53, nr. 5, 2012, pp. 417-432.
9. KOK Pieter, "Photonic quantum information processing", *Contemporary Physics*, vol. 57, nr. 4, 2016, pp. 526-544.
10. PFAFF W. și alții, "Unconditional quantum teleportation between distant solid-state quantum bits", *Science*, vol. 345, nr. 6196, May 2014, pp. 532-535.
11. SHOR Peter W., "Algorithms for Quantum Computation: Discrete Logarithms and Factoring", *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 1994, pp. 124-134.
12. SWAYNE Matt, "China's Superconducting Quantum Computer Sets Quantum Supremacy Milestone", <https://thequantuminsider.com/2021/06/30/chinas-superconducting-quantum-computer-sets-quantum-supremacy-milestone/> June 30, 2021.
13. ZEILINGER Anton, *Dance of the Photons: From Einstein to Quantum Teleportation*, Ed. Farrar, Straus and Giroux, 2010, 320 p.
14. ZEILINGER Anton, "Experiment and the foundations of quantum physics", *Review of Modern Physics*, vol. 71, nr. 2, 1999, pp. S288-S297.
15. WISEMAN H. M., "From Einstein's theorem to Bell's theorem: a history of quantum non-locality", *Contemporary Physics*, vol. 47, nr. 2, 2006, pp. 79-88.

# METACOGNIȚII ȘI NIVEL IERARHIC

**Cristian ILIE\***

## **Abstract**

*This study develops differences between metacognition capabilities – type or hierarchic level. Categories of metacognition capabilities (related to cognition knowledge and cognition regulation) were evaluated using Romanian version of Metacognitive Awareness Inventory (MAI).*

*The results indicated major variables of scoring at two of MAI scales. Also, the results indicate that the scoring doesn't change by type.*

**Keywords:** metacognition; ANOVA; type; hierarchic level.

## **INTRODUCERE**

Metacognițiile ocupă un loc important în cadrul teoriilor cognitive privind învățarea. În sens general, acestea se referă atât la cunoștințele pe care un individ le are despre funcționarea propriilor procese mentale, cât și la competențele metacognitive care includ capacitatea persoanei de a-și reprezenta propria activitate cognitivă, capacitatea de monitorizare și evaluare a acesteia, capacitatea de adaptare flexibilă în raport cu cerințele diverselor sarcini, capacitatea de alegere a unor strategii și metode adecvate și înțelegerea relațiilor dintre proceduri și rezultate (Flavell, J. H., 1979). Competențele cognitive sunt acele competențe necesare pentru a efectua o sarcină, iar competențele metacognitive sunt competențele necesare pentru a înțelege modul în care aceasta a fost realizată.

Există o bază de cercetare în creștere în domeniul interdisciplinar al metacogniției care demonstrează efectele de amploare ale

acesteia asupra conducerii diferitelor structuri organizaționale.

Cunoașterea acelor variabile psihologice, care se diferențiază în funcție de nivelurile ierarhice, poate orienta procesul decizional în situațiile de selecție, de aceea evaluarea competențelor metacognitive ocupă un rol important în cadrul procedurilor de selecție pentru pozițiile de conducere (DeRue, D. S., Nahrgang, J. D., Hollenbeck, J. R., & Workman, K., 2012). Totodată, relevarea variabilelor psihologice care au capacitate discriminatorie în raport cu criteriul nivelului ierarhic permite și optimizarea procesului de planificare a succesiunii în cadrul organizațional.

Concomitent, evidențierea constructelor psihologice cu potențial predictiv pentru nivelul ierarhic poate avea un rol important în identificarea talentelor, facilitând astfel procesul de dezvoltare a carierei și implicarea în programe de *training* sau *coaching* adaptate nevoilor persoanelor din organizație (DeRue, D. S., & Wellman, N., 2009).

\* Psiholog doctor, Ministerul Apărării Naționale.

În plus, competențele metacognitive, au fost și sunt motiv al studiilor empirice și teoretice, care folosesc personalul militar și contextul organizațional militar ca subiect (Grome, A., Beth C., Metcalf, K. A., Laufersweiler, D., and Strouse, R., 2015). Aceste cercetări științifice exploatează utilitatea și aplicabilitatea competențelor metacognitive în domeniul conducerii, pentru succesul misiunilor în mediile operaționale viitoare, care sunt din ce în ce mai complexe și mai ambigue (Hannah, Sean T., and Bruce J. Avolio., 2010).

De altfel, în toate organizațiile moderne este cunoscut faptul că soluțiile originale și de calitate superioară ale problemelor complexe și confuze sunt rezultatul utilizării eficiente și adecvate ale competențelor metacognitive. (Hannah, Sean T., Peter L. Jennings, and Orly Ben-Yoav Nobel, 2010).

Abilitatea de „a gândi despre gândire” accelerează dezvoltarea liderilor (Metcalf & Shimamura, 1994), deoarece le permite acestora identificarea atuurilor și a punctelor slabe, înțelegerea a ceea ce știu, dar și ce nu știu, precum și progresul capacității de a-și monitoriza și a-și adapta propriul proces de învățare (Avolio & Hannah, 2008).

Deși abilitățile metacognitive sunt legate de inteligență (Borkowski, 1985), alte cercetări sugerează că acestea acționează independent (Swanson, 1990), întrucât inteligența se raportează la abilități cognitive, iar abilitățile metacognitive se raportează la înțelegerea și reglarea proceselor de gândire, contribuind astfel la învățare și la rezolvarea de probleme. În acest sens, diferite studii au demonstrat că abilitățile metacognitive au legătură cu rezolvarea creativă a problemelor (Marshall - Mies et al., 2000), luarea deciziilor (Batha & Carroll, 2007), gândirea critică (Magno, 2010) și cu performanțele profesionale ale liderului (Mumford, Zaccaro, Harding, Jacobs, & Fleishman, 2000).

Abilitățile specifice unui leadership performant sunt numeroase, complexe și depind de context; tocmai de aceea, abilitățile metacognitive au un rol deosebit în dezvoltarea unui lider (Marshall - Mies et al., 2000). Spre deosebire de

dezvoltarea abilităților tipice diferitelor posturi organizaționale, liderii se întâlnesc cu provocări ce au un grad ridicat de ambiguitate și risc, care solicită pe lângă buna cunoaștere a oamenilor, resurselor, structurii și competențe de rezolvarea creativă a problemelor (Mumford, Zaccaro, Harding, Jacobs, & Fleishman, 2000).

Fără circumstanțe clare și coerente, liderii trebuie să utilizeze competențele metacognitive pentru a se adapta la cerințele situaționale. Efectul acestora poate include conștientizarea de sine, reglarea învățării utilizând experiențele personale sau ale altora, înțelegerea comportamentului celorlalți, precum și influențarea acestora și chiar facilitarea dezvoltării subordonaților (e.g., Gardner, Avolio, Luthans, May, & Walumbwa, 2005).

Abilitățile metacognitive pot îmbunătăți acuratețea convingerilor liderilor despre ei înșiși, permițându-le să-și identifice inconsistențele comportamentale și epistemice și, totodată, să-și ajusteze credințele iraționale, astfel încât să fie reprezentative pentru realitate. În plus aceste abilități ajută la încorporarea noilor experiențe în concepția despre sine, indiferent dacă acestea intră în conflict cu convingerile și perspectivele anterioare, permițând astfel dezvoltarea unei înțelegeri mai rafinate a fenomenelor și proceselor specifice. Lord și Hall (2005) afirmă faptul că abilitățile metacognitive sunt deosebit de importante pentru liderii care au dobândit deja competențe de conducere, deoarece acestea au devenit automate, iar creșterea eficienței profesionale va fi sporită doar prin automonitorizare, evaluare și alegere a unor strategii diferite, adecvate situațional.

Deși nu există un consens în privința definirii constructului și nu este explicată precis utilitatea lui, abilitățile metacognitive sunt un domeniu de interes științific. Sunt numeroase studii, riguroase metodologic, ale căror rezultate relevă conexitatea abilităților metacognitive cu rezolvarea problemelor, gândirea critică, luarea deciziilor și conducerea.

Pentru a reuși în viitor, orice organizație este necesar să identifice, să dezvolte și să promoveze persoanele potrivite cu abilitățile potrivite în

pozițiile ierarhice potrivite. O activitate cheie, în acest sens, implică identificarea abilităților specifice, care sunt necesare pentru a ajuta orice structură organizațională să obțină succesul. Din această perspectivă, rafinarea modului în care își valorifică resursele umane este un proces continuu, dar benefic în încercarea de a anticipa, influența și răspunde eficient la dinamica mediului operațional. Nu în cele din urmă, cercetările în domeniul competențelor metacognitive reprezintă o oportunitate pentru augmentarea eforturilor de creștere a calității capitalului uman, în special în domeniul competențelor cognitive și sociale.

OBIECTIVUL CERCETĂRII

Obiectivul principal al acestui studiu este de a identifica dacă metacognițiile au capacitatea de a discrimina între niveluri ierarhice diferite. Nivelul ierarhic fiind considerat unul dintre indicatorii extrinseci ai succesului profesional. Rezultatele acestui demers științific pot avea un rol important în diferite zone ale psihologiei aplicate, printre care se numără: selecția de personal, dezvoltare personală, *leadership-ul*, recunoașterea și managementul talentelor.

**Ipoteza 1:** Competențele metacognitive se diferențiază în funcție de nivelele ierarhice.

**Ipoteza 2:** Între participanții de gen feminin și masculin din cadrul respondenților nu există diferențe semnificative la nivelul competențelor metacognitive.

METODA

1. Participanți

Înainte de evaluarea propriu-zisă, fiecare participant a primit un formular de consimțământ

informat, care se referea la persoanele care vor avea acces la scorurile pe care le va fi obținut persoana evaluată și cuprindea informații despre participarea voluntară la un proiect de cercetare prin furnizarea datelor rezultate din evaluarea cu chestionare psihometrice. Toate persoanele au fost de acord să participe la acest studiu, în formularul de consimțământ garantându-se confidențialitatea tuturor informațiilor personale. Metoda de eșantionare a fost una de conveniență.

În continuare, vor fi detaliate caracteristicile eșantionului final. Cercetarea s-a desfășurat pe un eșantion de 405 de subiecți, dintre care 360 bărbați și 45 femei, cu vârste cuprinse între 21 și 55 de ani ( $m = 36,60$ ,  $ab. std. = 3,07$ ). Nivelul educațional al persoanelor incluse în eșantion este unul ridicat, 318 (78,8%) dintre participanți având cel puțin studii universitare, iar 86 (21,2%) de persoane având studii doar postliceale.

2. Instrument

Inventarul *Metacognitive Awareness Inventory* – MAI este un instrument de evaluare auto-raportat, ce cuprinde 52 de itemi. Acesta este conceput să măsoare două dimensiuni, respectiv cunoștințe despre cogniții și cunoștințe despre reglarea cognițiilor. Pentru obținerea versiunii românești a MAI, toți itemii au fost supuși unui proces de traducere și adaptare. După traducerea inițială, s-a realizat o serie succesivă de analize de conținut pentru fiecare item, în cadrul colectivului, până am ajuns la un consens cu privire la forma finală a tuturor itemilor.

REZULTATELE

Mediile și abaterile standard calculate pe baza scorurilor brute sunt prezentate în *Tabelul 1*.

Tabelul 1: Mediile și abaterile standard calculate pe baza scorurilor brute

	CD	CC	CP	P	SMI	RS	MÎ	E
Media	32,59	19,86	15,30	27,78	36,93	19,60	23,00	22,06
Abaterea standard	5,059	3,241	2,587	4,459	5,923	3,279	4,407	3,695
Valoarea minimă	8	5	4	7	10	5	7	6
Valoarea maximă	40	25	20	35	48	25	35	30



Pentru a analiza diferențele între dimensiunile evaluate cu *Metacognitive Awareness Inventory* (MAI) pentru cele două grupe de subiecți, organizate în funcție de nivelul ierarhic, a fost utilizată o analiză de varianță de tip ANOVA, caracterizată frecvent ca fiind omnibuz t-test (Marczyk, DeMatteo, Festinger, 2005).

Rezultatele acestei analize sunt prezentate în Tabelul 2.

respectiv reglarea cognițiilor măsurate cu MAI, și anume: *Strategii de management al informațiilor* și *Monitorizarea înțelegerii*. Scala care manifestă potențialul de discriminare cel mai ridicat este *Monitorizarea înțelegerii* ( $F(405)=10,139, p< .05$ ). Aceasta este urmată de scala *Strategii de management al informațiilor* ( $F(405)= 8,976, p < .05$ ).

Pentru a analiza cea de-a doua ipoteză a acestui studiu a fost derulată o comparație între

Tabelul 2: Rezultate ANOVA

Dimensiune	Media (c)	Media (ex)	Df	F	p
Cunoștințe declarative	32,88	31,48	404	5,297	,022
Cunoștințe condiționale	20,01	19,31	404	3,164	,076
Cunoștințe procedurale	15,38	14,98	404	1,668	,197
Planificare	28,02	26,91	404	4,246	,040
Strategii de management al informațiilor	37,38	35,24	404	8,976*	,003
Reglarea strategiilor	19,65	19,41	404	,368	,544
Monitorizarea înțelegerii	23,36	21,67	404	10,139*	,002
Evaluare	22,25	21,36	404	3,962	,047

Notă: Mediile sunt calculate pe baza scorurilor brute; N = 405; \* $p<.05$ .

Din numărul total de opt scale doar două au potențialul de a diferenția semnificativ cele două nivele ierarhice, incluse în această analiză. Scalele care diferențiază semnificativ sunt doar într-o singură categorie a cunoașterii metacognițiilor,

rezultatele obținute, la scalele Inventarul MAI, de către personalul de gen feminin și cel de gen masculin. Tabelul 3 prezintă diferențele de medii între cele două loturi de subiecți, așa cum reies din analiza de varianță de tip ANOVA.

Tabelul 3: Rezultate ANOVA

Dimensiune	Media(b)	Media(f)	Df	F	p
Cunoștințe declarative	32,72	31,53	404	2,195	,139
Cunoștințe condiționale	19,93	19,38	404	1,141	,286
Cunoștințe procedurale	15,39	14,58	404	3,933	,048
Planificare	27,83	27,40	404	,372	,542
Strategii de management al informațiilor	36,95	36,73	404	,053	,817
Reglarea strategiilor	19,57	19,84	404	,287	,593
Monitorizarea înțelegerii	23,03	22,82	404	,084	,771
Evaluare	22,13	21,49	404	1,217	,271

Notă: Mediile sunt calculate pe baza scorurilor brute; N = 405.

O analiză comparativă a diferențelor de medii înregistrate în cadrul eșantionului acestui studiu indică faptul că nu sunt diferențe semnificative între participanții de gen feminin și cel de gen masculin.

## DISCUȚII

Examinarea datelor prezentate relevă faptul că unele competențe metacognitive subiacente dimensiunii *Reglarea cognițiilor*, măsurate cu Inventarul *MAI*, variază semnificativ de la un nivel ierarhic la altul. La un prag de semnificație de .05, competențele metacognitive *Strategii de management al informațiilor* și *Monitorizarea înțelegerii* diferă de la un nivel ierarhic la altul, prezentând valori medii semnificativ mai ridicate cu cât subiecții sunt mai sus pe piramida ierarhiei profesionale.

Pentru celelalte trei competențe metacognitive, cu rol în reglarea cognițiilor, *Planificare*, *Evaluare* și *Reglarea strategiilor*, nu s-au observat diferențe semnificative între medii. De asemenea, nici pentru scalele dimensiunii, ce se referă la cunoștințele pe care un individ le are despre funcționarea propriilor procese mentale și anume *Cunoștințe declarative*, *Cunoștințe condiționale* și *Cunoștințe procedurale*, la nivelul eșantionului utilizat în acest studiu, nu s-au înregistrat diferențe semnificative. Analiza diferențelor de gen în cadrul eșantionului nu a scos în evidență diferențe ale nivelului de elevație al competențelor metacognitive.

Astfel, se poate susține ipoteza că în cadrul populației cu funcții de conducere diferențele de competențe metacognitive manifestă tendința de a se estompa, competențele persoanelor de gen masculin și ale celor de gen feminin fiind relativ similare, probabil acesta fiind un efect cumulativ al proceselor educative, de selecție a resursei umane și de promovare profesională.

Rezultatele care indică faptul că scala *Monitorizarea înțelegerii* manifestă potențialul de discriminare între categoriile de personal, organizate în funcție de nivelul ierarhic, sunt în conformitate cu studiul lui Halpin (1996) care a subliniat importanța automonitorizării, alături

de flexibilitatea cognitivă, intuiție și experiența profesională, în rezolvarea problemelor specifice conducerii. De altfel, în anii care au urmat studiului lui Halpin, numeroși cercetători au inclus competențele metacognitive în diferite studii care aveau ca obiectiv identificarea cerințelor critice pentru succesul liderilor.

Markensini (1996) a obținut, la rândul lui, rezultate asemănătoare cu ale acestui studiu, care susțin că abilitățile cognitive și competențele metacognitive sunt esențiale pentru succesul conducerii. În 1998, Gumbert a subliniat rolul metacognițiilor în rezolvarea problemelor în contextul avansului tehnologiei digitale, iar Morrison și Flencher (2002) au realizat un raport în care au identificat competențele metacognitive, ca fiind una dintre cele opt competențe cheie ale „pregătirii cognitive” ale viitorilor lideri. Într-un mod asemănător, rolul competențelor metacognitive, ca o componentă critică în integrarea diferitelor cunoștințe și experiențe de către lideri, a fost cercetat, cu rezultate semnificative, și de Hannah (2010), care la finalul studiului său concluzionează că abilitățile metacognitive nu sunt, în sine, suficiente pentru adaptarea liderilor la viitoarele riscuri asimetrice, ci mai degrabă ele trebuie „profund integrate” cu experiențe și cunoștințe valoroase.

De altfel, Hannah și Sowden (2012), într-un alt studiu despre conducere, au formulat concluzii asemănătoare, în sensul că studiul competențelor metacognitive este la fel de important precum este și înțelegerea complexității cognitive și a structurilor mai profunde de cunoaștere, care împreună îmbunătățesc capacitatea de adaptare a unui lider la condițiile viitoarelor provocări. Rezultatele acelui studiu sunt congruente cu cele obținute de Marshall - Mies & All (2000), care au investigat relația dintre competențele metacognitive și actul de conducere. În altă ordine de idei, conform lui Zacaaro (2014), includerea evaluării personalității, în cadrul studiului influenței competențelor metacognitive asupra eficienței conducerii, aduce un plus de cunoaștere.

Importanța competențelor metacognitive a fost demonstrată și în studiul lui Grome & All (2015). Aceste constructe psihologice alături de abilitățile de rezolvare a problemelor complexe

și aptitudinile mentale generale au fost utilizate în selecția, organizarea și pregătirea unor echipe de conducere flexibile cognitiv.

## LIMITE

Conform standardelor de cercetare în domeniu, una dintre limitele, cu impact, ale acestui studiu ține de calitatea lotului utilizat. Dimensiunea redusă și structura dezechilibrată din perspectiva de gen a eșantionului este posibil să fi exercitat influențe negative asupra analizelor statistice specifice. Pe lângă volumul eșantionului, o altă limită importantă este legată de faptul că respondenții studiului au fost selectați din categoria persoanelor cu funcții de execuție și din categoria celor cu funcții de conducere, de la baza ierarhiei profesionale. Reprezentativitatea acestui eșantion nu poate fi utilizată pentru a extinde concluziile unui astfel de studiu la nivelul întregii organizații.

Mult mai adecvată ar fi utilizarea unei metode stratificate de eșantionare, aceasta din

urmă putând garanta alocarea proporțională a participanților în funcție de criteriile sau specificațiile reprezentative pentru populația țintă.

## CONCLUZII

În literatura specifică acestui domeniu, părerile sunt destul de nuanțate și trimit către explicații ușor diferite ale rolului competențelor metacognitive în relația cu *leadership*-ul. Totuși, se poate concluziona faptul că pe baza măsurării cu MAI se pot realiza inferențe, la acest moment cu precauție, referitoare la potențialul diferiților indivizi de a accede la felurite niveluri ierarhice în funcție competențele metacognitive.

Pentru inferențe mai robuste ar trebui reluat acest studiu, însă utilizând un design de cercetare longitudinal, în care să se analizeze evoluția profesională, ascensiunea diferitelor persoane în unul sau mai multe niveluri ierarhice și luând în considerare diferențele specializări existente.

## BIBLIOGRAFIE

1. AVOLIO B. J., Hannah S. T., "Developmental readiness: Accelerating leader development", *Consulting Psychology Journal: Practice and Research*, vol. 60, nr. 4, 2008, pp. 331–347.
2. BORKOWSKI J. G., "Signs of intelligence: Strategy generalization and metacognition", în *The Growth of Reflection in Children* (YUSSEN R. Steven ed.), 1985, pp. 105–144.
3. BATHA K. & Carroll M., "Metacognitive training aids decision making", *Australian Journal of Psychology*, vol. 59, nr. 2, 2007, pp. 64–69.
4. DERUE D. S., Nahrgang J. D., Hollenbeck J. R. & Workman, K., "A quasiexperimental study of after-event reviews and leadership development", *Journal of Applied Psychology*, vol. 97, nr. 5, 2012, pp. 997–1015.
5. DERUE D. S., Wellman N., "Developing leaders via experience: The role of developmental challenge, learning orientation, and feedback availability", *Journal of Applied Psychology*, vol. 94, nr. 4, 2009, pp. 859–875.

6. GROME Anna, Beth Crandall, Kimberly A. Metcalf, Dawn Laufersweiler and Robert Strouse, *Best Practices in Military Design Teams*, Technical Report 1349, Alexandria VA, Army Research Institute for the Behavioral and Social Sciences, 2015.
7. GUMBERT Jack, "Leadership in the Digitized Force", *Military Review*, vol. 78, nr. 1 (Jan/Feb 1998), pp. 13–23.
8. HALPIN M. Stanley, *The Human Dimensions of Battle Command: A Behavioral Science Perspective of Battle Command*, Research Report 1696, Alexandria VA, U.S. Army Research Institute for the Behavioral and Social Science, 1996.
9. HANNAH T. Sean, and Bruce J. Avolio, "Ready or not: How do we accelerate the developmental readiness of leaders?", *Journal of Organizational Behavior*, vol. 31, nr. 8, 2010, pp. 1181–1187.
10. HANNAH T. Sean, Walter J. Sowden, "Leadership in the Profession of Arms", *Oxford Handbook of Leadership* (M. Rumsey ed.), New York, Oxford University Press, 2012, pp. 291–310.

11. MARKESSINI Joan, *Executive Leadership in a Changing World Order: Requisite Cognitive Skills*, ARI Contractor Report 96-05, Alexandria, VA, U.S. Army Research Institute for the Behavioral and Social Sciences, June 1996.
13. MARSHALL-MIES C. Joanne, Edwin A. Fleishman, Jennifer A. Martin, Stephen J. Zaccaro, Wayne A. Baughman and Michael L. McGee, "Development and evaluation of cognitive and metacognitive measures for predicting leadership potential", *The Leadership Quarterly*, vol. 11, nr. 1, 2000, pp. 135-153.
14. MORRISON John E., J.D. Fletcher, *Cognitive Readiness*, IDA Paper P-3735, Alexandria, VA, Institute for Defense Analyses, 2002.
15. METCALFE J. E., Shimamura A. P., *Metacognition: Knowing about knowing*, Cambridge, MA, MIT Press, 1994.
17. MUMFORD M. D., Zaccaro S. J., Harding F. D., Jacobs T. O., Fleishman E. A., "Leadership skills for a changing world: Solving complex social problems", *The Leadership Quarterly*, vol. 11, nr. 1, pp. 11–35.
18. MAGNO C., "The role of metacognitive skills in developing critical thinking", *Metacognition and Learning*, vol. 5, nr. 2, 2010, pp. 137–156.
19. ZACCARO J. Stephen, *Senior Leadership: An Annotated Bibliography of Research Supported by the Army Research Institute*, ARI Research Note 98-11, Alexandria, VA, U.S. Army Research Institute for the Behavioral and Social Sciences.



# SERVICIILE DE INFORMAȚII ROMÂNEȘTI ȘI FRANCEZE – PARTENERE ÎN COMBATEREA PERICOLULUI COMUNIST ÎN ANII '20 AI SECOLULUI TRECUȚ

*Ioan-Codruț LUCINESCU\**

## **Abstract:**

*After World War I, maintaining peace on continent was strategic objective for Romania and France, both winners of the global conflagration. Soviet Russia, with its communist ideology on the rise, was considered a real threat for European democracies. In the interwar period, cooperation between Romanian and French intelligence services played a major role in counterring the actions of the soviet secret services.*

**Keywords:** *espionage; intelligence services; intelligence cooperation; secret agents; Romania; France; Soviet Russia.*

## **INTRODUCERE**

Sfârșitul Primului Război Mondial a marcat mutații profunde la nivel global în relațiile internaționale. În Europa, „lumea” din 1919 era total diferită față de cea din 1914, cu un mozaic de noi state ce încercau să-și găsească calea spre dezvoltare. În acest context, România și-a creat, chiar din primii ani postbelici, o complexă rețea de alianțe externe, în primul rând cu țările din arealul său geografic cu care împărtășea interese similare legate de menținerea sistemului de pace Versailles; dar, la fel de insistent, a urmărit consolidarea alianței începute în timpul războiului mondial cu cele două mari puteri

europene învingătoare, Franța și Marea Britanie, „pilonii” arhitecturii de securitate continentale.

Menținerea integrității teritoriale a constituit obiectivul strategic al politicii externe a țării în perioada interbelică, practic toate guvernele, indiferent de coloratura politică, considerându-l sistem de referință. Politica de alianțe consecvent promovată de București sub imperiul regulilor de securitate colectivă ducea, implicit, la acțiuni comune de protecție și apărare în fața unor potențiale agresiuni externe. Aceasta deoarece prevederile sistemului tratatelor de pace de la Versailles – Saint-Germain, Neuilly sur Seine, Trianon și Sevres – au fost aplicate într-un mod necorespunzător de către puterile învingătoare, creând premisele reapariției politicilor

*\*Expert în studii privind istoria serviciilor de informații.*

revizioniste pe continentul european, chiar la scurt timp după încetarea ostilităților militare.

Alianța cu Franța, devenită după 1918 principala putere politică și militară a Europei, va juca un rol special, relațiile în domeniul securității<sup>1</sup> (inclusiv pe palierul serviciilor secrete) având un istoric consacrat încă din perioada constituirii statului român, desfășurată în mai multe etape începând cu ianuarie 1859.

---

### **SERVICIILE DE INFORMAȚII ROMÂNEȘTI ȘI FRANCEZE ÎN PRIMUL DECENIU INTERBELIC**

---

Sistemul național de securitate s-a confruntat, în anii războiului, cu servicii de informații puternice, precum cele german și austro-ungar, iar din această confruntare pe „frontul secret” atât Armata, cât și Ministerul de Interne au căpătat o vastă experiență în domeniul informativ și contrainformativ. Această experiență își va dovedi utilitatea în anii de pace care vor urma, împotriva atacului concertat al serviciilor de spionaj ale statelor revizioniste, în primul rând Uniunea Sovietică și Ungaria horthystă.

Marele Stat Major, instituția superioară de comandă, concepție și control a armatei române, a avut de îndeplinit sarcini complexe, reieșind mai pregnant ca niciodată importanța cunoașterii inamicului sub toate aspectele sale; necesitatea unor fluxuri informative continue și eficiente, care să stea la baza deciziilor militare, a condus la evidenta dezvoltare a serviciilor de informații naționale.

După încheierea ostilităților militare și adaptarea la situația de pace, Marele Stat Major se reorganizează, în 1919, pe 2 diviziuni, în care sunt grupate compartimentele de lucru. Ca și structură specializată, Secția a 5-a Informații și Contrainformații se subordona Diviziunii a II-a și se confrunta cu numeroase probleme care trebuiau cunoscute și eficient gestionate: necesitatea supravegherii informative în noile teritorii unite cu Vechiul Regat, în special în Basarabia, unde aveau loc acțiuni teroriste organizate de sovietici; oprirea propagării ideilor comuniste și anarhiste în societatea românească, odată cu reîntoarcerea miilor de foști prizonieri de război (în special a

celor din armata austro-ungară, care se aflaseră ani de zile în captivitatea rusă); ținerea sub control a tendințelor secesioniste manifestate de o parte din elita maghiară din Transilvania, nemulțumită de pierderea privilegiilor pe care le deținuse anterior etc.

Odată cu demobilizarea Armatei la 1 aprilie 1921, Marele Stat Major (MStM) a emis Ordinul nr. 200/20 septembrie 1922 privind organizarea și funcționarea serviciilor din subordine. Astfel, Biroul 2 Informații „studiază, centralizează și exploatează informațiile asupra inamicului”, pentru prima dată fiind enunțat explicit principiul confirmării și verificării informației obținute - „o informație are valoare de regulă numai dacă este controlată cu alta din altă sursă”<sup>2</sup>.

Marea Unire din 1918 a creat nu numai un stat mult sporit din punct de vedere al teritoriului, populației sau potențialului economic, dar a adus cu sine și vulnerabilități sociale și politice care trebuiau monitorizate și ținute sub control. De aceea, era nevoie ca pe întreg teritoriul României să se structureze o rețea informativă a Armatei, care, în colaborare cu structurile de informații ale Ministerului de Interne (Siguranța Statului), să cunoască starea de spirit a populației și potențialele nemulțumiri cu efect destabilizator pentru securitatea națională și activitatea serviciilor secrete ale statelor revizioniste (Ungaria, Rusia Sovietică sau Bulgaria) ce organizau în țară atentate, sabotaje, greve, racolări de personalități politice și militare etc. În consecință, în aprilie 1920, generalul Constantin Christescu, șeful Marelui Stat Major, semnează documentul „Instrucțiuni relative la formarea în fiecare garnizoană a unui birou de informații”, birou care trebuia creat în cel mai scurt timp posibil în toată țara și care să dea un impuls important activității de informații/contrainformații la nivel național<sup>3</sup>.

În următorii ani, serviciul de informații al Armatei cunoaște noi transformări, din octombrie 1927 Diviziunea a II-a în cadrul Marelui Stat Major având următoarea structură: Biroul 1 Căutare informații; Biroul 2 Contrainformații; Biroul 3 Studiul informativ și atașați militari; Biroul 4 Instrucțiuni informative și tratate; Biroul

5 Cifru și Biroul Interpreți; ulterior, va fi înființat și Biroul Radio, ce va cunoaște o dezvoltare evidentă odată cu declanșarea celei de-a doua conflagrații mondiale<sup>4</sup>.

Instituțiile de securitate ale Franței vor reprezenta un model ce va fi preluat în România în anii '20 pe multiple planuri, de la Consiliul Suprem de Apărare a Țării la Serviciul Secret. În contextul mai larg al reformării instituțiilor cu atribuții în asigurarea securității naționale, în anul 1924 Marele Stat Major hotărăște înființarea „Biroului Secret din Divizia a II-a (Secția a II-a)”, sub conducerea lui Mihail Moruzov. În faza inițială, Consiliul Suprem de Apărare a Țării a stabilit ca noua structură, cunoscută ulterior sub numele de Serviciul Secret de Informații al Armatei Române (SSI), să rămână un organ tehnic civil, subordonat șefului Secției a II-a din Marele Stat Major<sup>5</sup>. Referitor la începuturile SSI, Eugen Cristescu, viitorul șef al Serviciului Special de Informații în perioada guvernării antonesciene, afirma: „Marele Stat Major s-a hotărât în cursul anului 1924 să înființeze un serviciu civil de informații (Serviciul Secret), după modelul Serviciului francez, atașat la Secția a II-a, ca organ auxiliar al acestuia. Pentru aceasta, MStM s-a oprit asupra unui ofițer de siguranță, Mihail Moruzov. Începuturile au fost destul de dificile”<sup>6</sup>.

Trebuie să amintim faptul că însuși Consiliul Suprem de Apărare a Țării din perioada interbelică era o creație având ca model instituția similară din Franța. Acest aspect reiese din raportul din 22 decembrie 1921 al atașatului militar român la Paris, colonel Șuțu, care transmitea către MStM informații referitoare la reorganizarea sistemului de securitate și apărare francez. În document se arată faptul că, datorită noilor realități postbelice, s-a hotărât reorganizarea Consiliului Superior al Apărării Naționale și înființarea, sub autoritatea guvernului, a unui Comitet de Studii necesar mobilizării economice a țării.

Obiectivul general al Consiliului, ajutat de acest organism tehnic (Comitetul) este acela „de a menține echilibrul vital al țării, dând în același timp Armatei puterea militară voită și a-i asigura în permanență materialul de război cel mai bun și toate aprovizionările utile în timp de război.

În componența Consiliului de Apărare Națională intră toți factorii responsabili și competenți ai guvernului, prezidat de Președintele Republicii Franceze. (...) Important este de semnalat faptul că Consiliul poate convoca pentru a asculta „à titre consultatif” orice persoană susceptibilă a aduce concurs lucrărilor sale”<sup>7</sup>.

Acest Consiliu Superior va sta la baza înființării în România, prin Decretul-Lege nr. 999/13 martie 1924, a Consiliului Suprem de Apărare a Țării (CSAT), având sarcina de a studia și a lua deciziile cele mai adecvate în problemele care vizau apărarea națională. În componența CSAT intrau: președintele Consiliului de Miniștri (primul ministru), care era și conducătorul acestui organism, miniștrii principalelor departamente – de Război, Interne, Afaceri Străine, Industrie și Comerț, Agricultură, Sănătate, Lucrărilor Publice și membrii Consiliului Superior al Oștirii (cu vot consultativ)<sup>8</sup>.

Principalele obiective care au stat în atenția acestuia, în perioada sa de existență, se refereau la reorganizarea Armatei, Poliției, Jandarmeriei și a altor structuri din cadrul aparatului național de apărare (justiția militară, legislația specială referitoare la serviciile de informații românești etc.). CSAT se întrunea, de regulă, de două ori pe an, în lunile martie și septembrie; dacă era invitat și Regele, acestuia i se încredința conducerea lucrărilor. La fel ca în Franța, dacă pe ordinea de zi se aflau probleme care necesitau prezența unor specialiști, aceștia erau invitați să-și expună punctul de vedere. Rolul organismului a fost, însă, foarte redus, fiind neglijat pe măsură ce autoritatea regelui Carol al II-lea se consolida, acesta participând doar la câteva întruniri în perioada 1930-1940. CSAT-ul a fost desființat, odată cu prăbușirea regimului carlist în vara anului 1940 și accederea la putere a generalului Ion Antonescu (septembrie 1940).

După încheierea primei conflagrații mondiale, conducerea militară franceză a trecut la o amănunțită analiză a structurilor de informații naționale, din care a reieșit necesitatea creării unor noi servicii de *intelligence*, adaptate contextului postbelic și rolului central jucat de Franța în relațiile internaționale; aceasta după ce

serviciile de informații își dovediseră valoarea în acerbă confruntare „pe frontul secret” în anii războiului (1914-1918).

De altfel, eficiența și profesionalismul serviciilor de informații franceze, începând cu a doua jumătate a secolului al XIX-lea, sunt remarcate și de un profesionist în domeniul *intelligence* și adversar înverșunat al acestora, colonelul Walter Nikolai, șeful serviciului secret al armatei imperiale germane (între 1913 și 1919). În memoriile sale, publicate în anul 1923, Nikolai afirma: „Franța fu creatorea actualului serviciu de informație politic-militar (ca tip de organizație, n.n.). Napoleon al III-lea, în urma ascensiunii Prusiei sub Bismark, dete serviciului de informație militar o formă de dezvoltare solidă. Dânsul creie în anul 1855 poliția specială eminent pregătită și răspândită pe întreg teritoriul Franței, care deveni în războiul franco-german cel mai important factor al spionajului. După războiul republica și-a înființat biroul II din Marele Stat Major, care conducea organizarea serviciului de spionaj contra Germaniei. Astăzi (1923, n.n.) când Franța se află în apogeul situațiunii sale militare este totodată cel mai perfect instructor și dirigitor în acest domeniu”<sup>9</sup>.

Ca urmare a reorganizării sistemului informativ național, pe lângă Biroul 2 (Deuxième Bureau) care exista în Statele Majore ale celor trei arme principale – Armată, Marină și Aviație, se va crea un serviciu francez de informații militare în cadrul Ministerului de Război. Service de Renseignements et de Contre-Espionnage, prescurtat SR-CE, era o structură total acoperită, personalul său acționând numai sub identități false. Având un personal de 120 militari cu pregătire în domeniul informațiilor, repartizați între serviciul central și cele șase posturi frontaliere, serviciul francez de informații militare se compunea din două structuri principale<sup>10</sup>:

- serviciul de informații propriu-zis (Service de Renseignements/SR), însărcinat cu culegerea de informații despre adversari, informații transmise pentru sinteză și exploatare operativă Deuxième Bureau al Marelui Stat Major.

- o secție ce asigura contraspionajul: Service de Contre-Espionage, dar aria sa de acțiune era, în

cea mai mare parte, tot în exteriorul frontierelor franceze – avea ca misiune operativă și protejarea agenților și operațiilor desfășurate de SR în străinătate, iar activitatea sa esențială consta în recrutarea și coordonarea agenților introduși în serviciile secrete adverse; această secție de contraspionaj a fost organizată, în anii '30, în sub-secții geografice (precum SR), focalizate pe principalii potențiali inamici: secțiunea germană, italiană și sovietică – cărora li s-a alăturat o secțiune de arhivă și fișier, precum și o secțiune consacrată propagandei revoluționare comuniste.

În cadrul Ministerului de Interne, principalele inovații în domeniul contraspionajului, în raport cu situația anterioară, au constat în înființarea Comisariatului pentru siguranță națională și a unei brigăzi specializate în cadrul Siguranței generale. Această brigadă, însărcinată cu supravegherea potențialilor spioni care acționau pe teritoriul francez, a rămas totuși cu un efectiv redus – un comisar și 10 inspectori<sup>11</sup>.

La nivelul țării, activitatea de contraspionaj era desfășurată pe timp de pace cu precădere de către Siguranța Generală, care beneficia de infrastructura și sprijinul logistic al celorlalte servicii ale Ministerului de Interne (mult mai dezvoltate decât cele ale Armatei). Funcționarii Siguranței, care desfășurau acest gen de activitate profesională, ocupau funcția de comisari speciali, având în subordine un număr variabil de polițiști<sup>12</sup>.

Totuși, principalul serviciu de informații francez a rămas, așa cum fusese și înainte, Biroul 2 (Deuxième Bureau) al Armatei, prin prisma fondurilor alocate, personalului și fluxului informativ pe care îl genera către conducerea politico-militară a Franței. Acest fapt era posibil deoarece dispunea de o rețea transcontinentală de ofițeri de informații ce o deserveau și anume atașării militare, care furnizau o enormă masă de informații diverse sintetizate – politice, militare, economice etc. Săptămânal, Deuxième Bureau din cele trei arme (infanterie, marină și aviație) primea sute de rapoarte, note, atenționări etc. despre problematicile ce interesau, sub o formă sau alta, nu numai instituția militară, dar și conducerea politică națională<sup>13</sup>.



Între Deuxième Bureau și Ministerul Afacerilor Străine exista o strânsă colaborare, politica externă a Franței beneficiind permanent de sprijinul serviciilor de informații (prin intermediul atașărilor militari aflați la post pe lângă ambasadele și consulatele din diverse părți ale lumii), model care va fi preluat și de alte state, inclusiv de către România.

## **COLABORAREA PENTRU COMBATAREA COMUNISMULUI, ÎN PRIMUL DECENIU INTERBELIC**

Victoria revoluției comuniste în octombrie 1917 în Rusia provoacă un adevărat seism în relațiile internaționale. Apare, astfel, un stat care urmărește să-și exporte ideologia totalitară pe întreg mapamondul, conform devisei „proletari din toate țările, uniți-vă”; Rusia sovietică, din 1922 având titulatura oficială URSS, devine o putere revizionistă, nerecunoscând granițele europene stabilite conform sistemului tratatelor de pace de la Versailles. Deși eșuează în încercarea de schimbare a regimurilor politice europene prin forța armelor (1919 - 1921), Moscova continuă, pe parcursul a aproape două decenii interbelice, să submineze stabilitatea continentală, devenind, alături de Germania lui Adolf Hitler, principalul factor al subminării Ligii Națiunilor.

În aceste condiții, este lesne de înțeles atenția pe care serviciile de informații ale statelor învingătoare în prima conflagrație mondială au acordat-o politicii sovietice de subminare și sabotare a societăților capitaliste, o politică complexă dusă cu variate instrumente politice, economice, ideologice sau militare.

Pentru Franța, pericolul comunist devine o problemă de securitate națională imediat după încheierea Primului Război Mondial; liderii francezi au susținut, pe toate planurile, armatele anticomuniste care au luptat în războiul civil din Rusia (1918 - 1922), fără însă a reuși răsturnarea regimului lui Lenin. Serviciile secrete ale Rusiei Sovietice, în primul rând faimoasa CEKA<sup>14</sup>, a infiltrat agenți în Partidul Comunist Francez (PCF) chiar din momentul înființării acestuia, în anul 1920. Bulgarul Lebedev, având numele

conspirativ „Stepanov”, a fost primul „rezident” trimis în Franța de către Moscova pentru a organiza și a conduce spionajul sovietic. Ajuns la Paris în toamna lui 1920, sub identitatea falsă de Chavaroché, recrutează membri din Comitetul Central al PCF pentru crearea unor rețele de spionaj industrial, în industriile de armament și aeronautică. Reușește să activeze în Franța timp de mai mulți ani, trimițând conducerii sovietice informații prețioase care vor ajuta la modernizarea industriei URSS. De asemenea, asigură agenților CEKA, veniți ulterior, acoperire legală, locuințe conspirative etc.<sup>15</sup> Deznodământul se produce în vara lui 1924, când Service de Contre-Espionage, aflat deja pe urmele sale, încearcă fără succes să-l aresteze; Lebedev scapă și fuge la Moscova, unde activează încă doi ani ca expert pe probleme franceze; este lichidat de succesoarea CEKA, OGPU, deoarece devenise o persoană „care știa prea multe”.

Acest început este continuat în forță de zeci de agenți ai serviciilor sovietice, unii veniți pe diverse canale în Franța, dar mulți dintre ei fiind chiar francezi cu importante conexiuni politice și economice („Rețeaua Cremet” fiind un exemplu de succes). Însă toți, indiferent de origine, urmăreau să transpună în practică ordinele Moscovei de transformare a puternicei mișcări sindicale franceze într-un vector al ideologiei de extremă stângă și factor destabilizator al regimului capitalist.

Stabilirea de relații diplomatice între Franța și URSS, în octombrie 1924, ușurează considerabil munca agenților Moscovei<sup>16</sup>; odată cu instalarea ambasadei și a unor reprezentanțe comerciale sovietice, nu mai este necesar să se recurgă la curieri speciali pentru trimiterea informațiilor în URSS, spionajul sovietic având acum „cadrul legal” pentru a acționa pe teritoriul francez. În fața acestui grav pericol la adresa securității interne, autoritățile politice și militare franceze adoptă, în anii '20, măsuri ferme pe două planuri:

- *pe plan intern*, în februarie 1927, aparatul de securitate arestează aproximativ o sută de persoane, printre care Bernstein și Grodnicki, șefii „antenei” sovietice din Franța; iar rețeaua condusă de Jean Crémét, membru în Biroul

Politic al PCF, care ajunsese să penetreze întregul segment al industriei de apărare și să monitorizeze transportul feroviar și maritim al țării, este destructurată<sup>17</sup>;

- *pe plan extern*, consolidează relațiile cu statele anti-revizioniste, întărindu-le capacitățile militare prin livrări de armament, pregătirea personalului, organizare modernă etc.; de asemenea, se aprofundează colaborarea între serviciile de informații franceze și cele aliate pentru combaterea ideologiei comuniste și a rețelilor de spionaj sovietice.

Atât Franța, cât și România se găsesc în vizorul Moscovei, din postura acestora de apărătoare acerbe a *statu-quo*-ului politic european și a frontierelor stabilite prin sistemul tratatelor de pace. România, considerată de Moscova „stat imperialist” care a „ocupat” Basarabia într-un moment de slăbiciune al statului rus (ianuarie 1918), trebuia cu orice preț destabilizată intern, pentru ca, la momentul oportun, să poată fi invadată și transformată într-un „stat proletar”. Din cauza pericolului iminent pentru securitatea națională, aspectele interne și externe având legătură cu comunismul erau atent monitorizate de serviciile informative ale Armatei și Ministerului de Interne. Mai ales pe plan extern, situația trebuia cunoscută în timp util, o agresiune armată împotriva României fiind considerată, de conducerea militară, foarte posibilă.

Astfel, într-un raport realizat de Biroul 1, Secția a V-a Informații din cadrul Marelui Stat Major, pe baza informațiilor furnizate de agentura Armatei în perioada 01-15 decembrie 1920, este reliefată propaganda anti-românească din Ucraina sovietică și pregătirile de război ale comuniștilor ruși: „În același timp, propaganda de ură contra României continuă cu o și mai mare îndârjire ca până acum, întrunirile de protestare contra alipirei Basarabiei - sub direcția lui Racovschi<sup>18</sup> – intensificându-se peste tot (de la 2 la 3 ori pe săptămână), atât în localitățile din apropierea frontierei, cât și mai în interior. Mai în toate orașele unde se găsesc trupe, autoritățile civile și militare dau serbări și baluri, cu cari ocazii ofițerii bolșevici țin discursuri patriotice,

spunând că << în curând Basarabia va fi smulșă din ghiarele românilor cotorpitori >>. Astfel, într-o conferință ținută în ultimele zile trupelor și populației din Bilinevca (vest Odesa) de către Racovski, arătând spre Basarabia, el își termină cuvântarea cu cuvintele << în curând vei fi a noastră >>”<sup>19</sup>.

Până spre mijlocul anilor '20 ai secolului trecut, pericolul unui război declanșat de Moscova împotriva României a fost unul real, constituind subiect de îngrijorare și pentru statele beneficiare ale păcii, fie că e vorba de Franța și Marea Britanie sau Iugoslavia, Cehoslovacia, Polonia. În această perioadă, necesitatea unui flux informativ continuu și precis despre intențiile reale ale sovieticilor a fost de importanță capitală, comandamentul Armatei române beneficiind de informații de ultimă oră și din surse externe, în principal pe filieră franceză și poloneză. Acest lucru se întâmpla prin intermediul atașărilor militare din capitalele europene, dar nu numai. De exemplu, atașatul militar român de la Paris, colonel Șuțu, raporta Marelui Stat Major, în mai 1921: „Din informațiuni precise, Ministerul de Marină francez știe că actualmente Marina bolșevicilor în Marea Neagră s-a mărit cu un submarin, astfel încât această marină dispune acum în apele noastre de două submarine. Credem că această informație are o deosebită importanță pentru România, fiind dată necesitatea vădită ce o avem a fi stăpâni în Marea Neagră”<sup>20</sup>.

De asemenea, tot în luna mai 1921 (pe data de 18), atașatul militar român la Ankara, colonel Glatz, își informa superiorii din țară despre cele mai noi deplasări de trupe și armament ale sovieticilor spre frontiera Basarabiei, informații provenite de la Deuxième Bureau: „După aprecierile francezilor, totalul trupelor bolșevice de pe frontul român reiese că sunt așezate în regiunile: Gaesin-Iampol-Kamenetz-Podolsk-Proscurov-Bar, care se urcă la 23-24 divizii, dintre care trei de cavalerie. Francezii pretind că transportul trupelor pe frontul nostru nu s-a terminat încă. Bolșevicii au îndreptat din Caucaz spre frontul nostru Divizia letonă reorganizată și Divizia internațională, care a fost completată cu comuniști maghiari recrutați dintre foștii prizonieri de război”<sup>21</sup>.

În continuarea raportului, ofițerul arăta că analiștii serviciilor francez, britanic și polonez considerau probabilă atacarea României de către Rusia Sovietică din motive economice, ideologice și militare evidente. Astfel, prin ocuparea Basarabiei s-ar asigura o aprovizionare constantă a Armatei Roșii cu alimente, furaje și alte furnituri, vitale pentru continuarea operațiunilor militare de anvergură. O victorie sovietică împotriva României ar fi și un semnal politic și ideologic extrem de important pentru avântul mișcării comuniste internaționale, mai ales după înfrângerea categorică în fața Poloniei, în vara anului 1920. Iar din punct de vedere militar, ocuparea Basarabiei ar asigura Sovietelor o bază ideală de operațiuni spre Balcani și ar putea veni în sprijinul comuniștilor bulgari, aflați într-o poziție puternică și beneficiind de un larg sprijin intern<sup>22</sup>. Odată ocupată Bulgaria și instaurat aici un regim comunist, întreaga Europă de Sud ar fi căzut sub controlul Moscovei<sup>23</sup>.

Evoluția evenimentelor internaționale a spulberat, însă, visurile liderilor comuniști sovietici, resursele umane și materiale uriașe alocate declanșării „revoluției proletare” neducând la succesul scontat. De altfel, autoritățile române au contribuit direct la zădărnicierea declanșării „revoluției” în Bulgaria în vara lui 1924, aspect reliefat și de autoritățile din țara vecină. Astfel, ziarul bucureștean „Îndreptarea” (din 9 iulie 1924) prelua materiale apărute în presa de la Sofia. Articolul cu titlul „România sprijină acțiunea guvernului bulgar?”, arată că „un comunicat oficial anunță că guvernul bulgar este ferm hotărât să reprime orice încercare de revoluție, având în acest sens sprijinul Iugoslaviei și României, țări cari sunt ferm hotărâte să împiedice propagarea ideilor comuniste în peninsula Balcanică. Ziarele guvernamentale (bulgare, n.n.) arată că Rusia sovietică nu poate veni în ajutorul comuniștilor bulgari din cauză că România formează o barieră puternică între Rusia și Bulgaria”<sup>24</sup>.

Nereușindu-se organizarea unor ample mișcări comuniste social-politice în Balcani, atenția Cominternului s-a îndreptat asupra României<sup>25</sup>. Dar planurile sovieticilor de declanșare a unei serii de „revolte populare” pe

teritoriul statului român au fost cunoscute de către autorități, datorită atât rețelelor informative ale Siguranței și Armatei, create în interiorul mișcării comuniste românești și balcanice, cât și unei cooperări eficiente în *intelligence* cu serviciile partenere francez, polonez și iugoslav. De altfel, un cunoscut spion sovietic, Boris F. Lagozerov, arestat în anul 1925 la Cernăuți de agenții Siguranței, mărturisea în memoriile sale că la închisoarea Doftana erau deja închise circa 30 de persoane condamnate pentru spionaj în favoarea URSS<sup>26</sup> (în toată țara erau sute de cetățeni români și străini încarcerați pentru că desfășuraseră acțiuni de spionaj în favoarea Rusiei Sovietice).

Dar cooperarea româno-franceză pe palierul informativ nu era doar bilaterală, serviciile de informații militare român, francez și polonez conlucrând strâns, în operațiuni comune antisovietice. Acest fapt reiese pregnant din raportul strict secret adresat, în iunie 1923, de atașatul militar francez în România, locotenent-colonel Alfred Thierry, Ministerului de Război și Marelui Stat Major (Deuxième Bureau), în care sunt prezentate interesante aspecte de ordin informativ în ceea ce privește securizarea frontierei româno-sovietice prin intermediul serviciilor de informații aliante, aspecte pe care le detaliem în rândurile următoare<sup>27</sup>:

„Colonelul Kaspchewski din Statul Major al Armatei Poloneze a fost trimis de Varșovia la București pentru a studia, împreună cu Statul Major al Armatei Române, posibilitățile reale de coordonare a eforturilor militare ale României și Poloniei pe frontiera cu Rusia. De la sosirea sa, Colonelul însoțit de căpitanul Wielogłowski, atașat militar pe lângă Legația Poloneză, a venit să mă vadă și să mă informeze, în linii mari, despre misiunea sa. Am putut să cunosc rezultatele, reîntorcându-i vizita înainte de plecare. Convorbirile lui cu Generalul Grosky, în absența Generalului Cristescu, reținut acasă de gripă, au fost axate pe planurile de operațiuni ale celor două armate (română și poloneză, n.n.) în caz de atac al armatei ruse în zona de frontieră cu cele două țări.

Ele (discuțiile) nu au putut conduce la un rezultat apreciabil din cauza lipsei informațiilor

precise ale Statul Major Român cu privire la posibilitățile de a mobiliza armata. Nu am fost surprins. Prima mea impresie după întâlnirea personală cu generalul Gorsky este că planul de mobilizare al Armatei Române nu a suferit modificări din 16 Mai 1922; se impun clarificări urgente. (...)

Guvernul român, liniștit de promisiunea unui împrumut de 100 de milioane franci și prin atitudinea pacifistă actuală a Armatei Ruse a Ucrainei, întârzie și nu pare să acționeze. El realizează, însă, că deficitul de echipamente și lipsa de forță a diviziunilor sale de la frontiera de est din cauza absenței permanente a unui număr mare de soldați și a reducerii cailor prin măsuri economice impuse de ministrul finanțelor a pus Basarabia într-o situație primejdioasă. O incursiune a cavaleriei ruse ar fi cu atât mai probabil să reușească, deoarece beneficiază de complicitatea populației (basarabene, n.n.), nemulțumită de menținerea stării de asediu.

La frontiera cu Nistru nu sunt instalate posturi radiotelegrafice române. Colonelul Kaspchewski a propus, fără succes, instalarea de posturi poloneze de radiogonometrie pe această graniță. Totuși, Statul Major Român a admis instalarea unui ofițer de informații al atașatului militar polonez, la Akermann (Cetatea Albă, n.n.); acest agent va monitoriza în special țarmul mării până la Odesa. Căpitanul Wielogłowski va asigura legătura cu Serviciul nostru (Deuxième Bureau, n.n.), informându-ne în legătură cu aspecte de interes. Este de dorit ca frontiera rusă să fie permanent vegheată.

Colonelul Kaspchewski s-a reîntors la Varșovia cu speranța că vizita Regelui României în Polonia, la mijlocul verii, va permite Statului Major Polonez să studieze cu mai multă precizie coordonarea planurilor operaționale ale celor două armate<sup>28</sup>.

De altfel, relațiile de prietenie și alianță cu Polonia (încurajate de Franța pentru întărirea frontului antisovietic) au determinat Marele Stat Major român să înceapă o intensă colaborare pentru confruntarea materialului informativ procurat de Statele Majore român și polonez referitor la Rusia Sovietică. În toamna anului 1927

a avut loc prima conferință cu acest caracter, apoi ele s-au repetat în mod periodic, la 17 ianuarie 1929, 3 mai 1930, 22 iunie 1931 etc.<sup>29</sup>

Existența, la începutul anilor '20, a unei colaborări informative româno-franceze „pe teren”, având ca obiectiv Rusia Sovietică, este atestată și printr-un raport al Securității Române din perioada comunistă, în care se arată: „Este știut faptul că după marea Rev. Socialistă din Octombrie țările Antantei au trimis numeroase trupe intervenționiste, care în cele din urmă au fost înfrînte și izgonite de pe teritoriul tînărului stat sovietic. Țările capitaliste însă, au recurs la tot felul de acțiuni contra-revoluționare și de spionaj, astfel Serviciul de Spionaj englez „Intelligence Service” și „Biroul II Francez” și-au trimis în România reprezentanții săi, care să creeze o agentură informativă, prin care să culeagă informații din Uniunea Sovietică.

Fostul gardist alb Bogomolet Victor, fugit din Uniunea Sovietică în anul 1919, a fost numit conducătorul agenturii engleze, iar la agentura franceză niște ofițeri de carieră din Franța. Fiecare agentură lucra separat, avînd sectoare bine definite (de trecere a frontierei româno-sovietice, n.n.). Dat fiind că englezii dispuneau de fonduri mari, au avut un cîmp de activitate mai mare, folosind mai multe subcentre de informații pe malul Nistrului, pe unde îi trecea și pe agenții recrutați<sup>30</sup>.

Menționăm faptul că frontiera româno-sovietică era una dintre cele mai bine păzite granițe de pe continent, așa cum se arată și în raportul din decembrie 1920 al serviciului de informații al Marelui Stat Major, care evidențiază pericolul cu care agenții români și ai serviciilor partenere se confruntau în încercarea de a pătrunde la est de Nistru: „Astfel, ei (sovieticii, n.n.) au intensificat serviciul de patrulare în scop de a împiedica trecerea agenților noștri; au oprit – sub pedeapsa cu moartea – orice comunicație cu malul românesc (populația de pe malul Nistrului a căror case au ferestre spre malul românesc, au ordinul de a le închide cu obloane), iar frontiera română a fost declarată complet închisă<sup>31</sup>.

Importanța creării și menținerii deschise a unor asemenea culoare de acces pe teritoriul



sovietic era vitală pentru serviciile de informații românești și aliate, deoarece numai astfel putea fi asigurat un flux de informații constant, iar agenții trimiși în misiune să știe că au o cale sigură de întoarcere. De aceea, între Marele Stat Major al Armatei române și conducerile militare franceză și britanică au fost stabilite acorduri de colaborare, prin care se asigura și „concesionarea” unor sectoare ale frontierei fluviale cu Uniunea Sovietică către serviciile de informații aliate; în cazul Franței, sectorul de graniță stabilit se afla în zona Soroca<sup>32</sup>.

În luna mai 1923, pe filiera Biroului Militar Francez din România, structurile contrainformative românești dispuneau de informații de mare valoare operativă. Deuxième Bureau urmărise, începând cu primăvara anului 1921, un german pe nume Ganzer, care trezise suspiciuni datorită deselor călătorii pe care le efectua pe ruta Rusia Sovietică – Spania, de fiecare dată evitând cu grijă să tranziteze Franța. Serviciul francez stabilise rolul lui Ganzer și anume cel de curier cu informații de mare importanță pentru acțiunile comuniste în Occident, deoarece germanul era un agent de încredere al lui Gheorghe Cicerin, comisarul sovietic pentru Afaceri Externe și artizanul strânsei colaborări cu Germania pentru revizuirea tratatelor de pace<sup>33</sup>.

Din convorbirile avute la Barcelona de informatorii săi cu Ganzer, Deuxième Bureau aflase detalii importante pentru securitatea continentală, pe care le-a împărtășit și omologilor din statele aliate. Astfel, conducerea militară românească era informată despre anumite clauze secrete ale Tratatului de prietenie germano-sovietic încheiat la Rapallo, în aprilie 1922, document ce își va arăta importanța în deceniul următor, prin accelerarea înarmării celor două puteri revizioniste. Tratatul, în anexele confidențiale, prevedea, din punct de vedere militar, un plan de campanie comun pentru armatele germană și sovietică, având obiectivul „de a strivi” armatele poloneze; următoarea mișcare strategică prevedea ca trupele rusești să atace, cu întreaga forță, România, având

„spatele” asigurat de armata germană, care, în așteptare, trebuia să prevină intervenția militară a Cehoslovaciei și/sau Iugoslaviei în sprijinul armatei române<sup>34</sup>.

În noiembrie 1925, structurile sistemului de securitate națională al Franței beneficiază de informații de mare importanță provenite din sursă românească, așa cum reiese din nota secretariatului Marelui Stat Major francez adresată Ministerului de Externe (Quai d’Orsay). În document se arată că atât Armata, cât și Poliția franceză au fost informate de partea română despre pericolul unei adevărate „invazii” a agenților comuniști în Occident, prin utilizarea unor acte de identitate, atestate etc., perfect falsificate de către serviciile secrete sovietice<sup>35</sup>.

Este foarte posibil ca această informare să fie urmarea vizitei efectuate în octombrie 1924 la Berlin de către un înalt funcționar din Siguranța Statului, al cărui nume nu este prezentat în document (semnătura sa este indescifrabilă), la invitația directorului Secției Politice din cadrul Poliției berlineze, consilierul Oexle. Deplasarea a avut loc ca urmare a descoperirii, într-o mică localitate de lângă Berlin, a celui mai mare atelier clandestin de falsificare descoperit până atunci, aparținând serviciilor secrete sovietice.

Astfel, în raportul din 22 octombrie 1924 adresat atât conducerii Armatei, cât și Siguranței Statului și Ministerului de Externe sunt reliefate aspecte de interes referitoare la procedeele sovietice de falsificare a documentelor oficiale din diverse state: „Un dulap enorm de 7-8 metri lungime care în primele despărțituri este ocupat de cutii de lemn, formatul celor de țigări de foi. În aceste cutii se află mii de ștampile de gumă, organizate pe State, capitale, județe, comune. Altă serie plină cu ștampile de gumă, reprezentând oficiile publice, toate ministerele, polițiile, primăriile, prefecturile, cercuri de recrutare, oficii de stare civilă. Fiecare stat din Europa era în amănunțime reprezentat, pe cât de perfect executate, pe atât de ideal ordonate și clasificate. O altă serie de despărțituri este ocupată de mape groase, în care se află formulare ale tuturor statelor, clasificate într-o ordine perfectă”<sup>36</sup>.

În continuare, comisarul de siguranță arată profesionalismul falsificării semnăturilor multor miniștri, secretari de stat, chiar și a directorului general al Siguranței Statului, Romulus Voinescu. Aceeași situație era valabilă și pentru celelalte state europene, deoarece „mi s-a arătat semnătura lui Shober din Viena și a lui Richter din Berlin (directorii generali ai polițiilor austriacă și germană, n.n.) pe care ei susțin a fi a lor, nu plastografiată; atât de perfect sunt executate. Și astfel sunt reprezentate toate statele din Europa și din America”.

Prin rețelele CEKA și ale Internaționalei Comuniste (Comintern), agenții sovietici procurau prin diverse metode „pașapoarte cu numere exacte, pe care le rețineau în arhivă. La un moment dat se schimba fotografia pentru posesor (...) Astfel, celebra comunistă Ruth Fischer (lider al Partidului Comunist German și agent Comintern, ce avea ca sarcină declanșarea unor acțiuni revoluționare în Occident, inclusiv în Franța prin rețeaua comunistă locală, n.n.) avea pașaport pe numele exact de Anna Bosshardt, pașaport elvețian, cu care era când la Paris și Londra, când la Roma și Varșovia”<sup>37</sup>.

## CONCLUZII

Mediul de securitate instabil din deceniul al treilea al secolului XX a dus la necesitatea vitală a cooperării între aliații dornici să păstreze pacea pe continentul european. România și

Franța își consolidează multiplele relații stabilite începând cu august 1916, componenta militară și de *intelligence* fiind în prim-plan. Interesul Parisului de a crea un veritabil „cordon sanitar” anticomunist la frontiera europeană a Rusiei sovietice s-a tradus printr-o susținere politică, militară și economică specială a Poloniei și României. Datorită faptului că Uniunea Sovietică continua să provoace tulburări și revolte sociale pe teritoriul românesc, cu scopul de a destabiliza țara, schimbul de informații de securitate între serviciile secrete franceze și românești (de multe ori și cu concursul celor poloneze) devine o constantă, ridicată la un nivel superior în ceea ce privește eficacitatea combaterii acțiunilor subversive inițiate de Moscova.

În același timp, trebuie subliniat faptul că Parisul a avut, începând cu anii 1924-1925, odată cu reluarea relațiilor diplomatice cu Moscova, o politică oarecum ambiguă față de noua putere comunistă, deoarece considera că Rusia Sovietică nu este o amenințare față de hegemonia politico-militară franceză în Europa. Acest fapt s-a tradus și prin sincope în ceea ce privește cooperarea în *intelligence* cu aliații săi central-europeni, inclusiv cu România. Totuși, „pericolul comunist” continua să fie o preocupare pentru ambele state, chiar dacă raportarea la acesta diferea substanțial; în cazul României, miza era mult mai mare, fiind în joc asigurarea pe termen lung a suveranității și integrității statului.

## BIBLIOGRAFIE

1. Arhivele Naționale ale României, Fonduri: *Direcția Generală a Poliției, PCM-SSI; Microfilme Franța*.
2. Arhiva Serviciului Român de Informații, Fonduri: *Documentar și Penal*.
3. APARASCHIVEI Sorin, PINTILIE Florin-Badea, *Din istoria oficială a contraspionajului românesc*, Editura ANIMV, București, 2018.
4. BOYCE Robert (editor), *French foreign and defence policy, 1918-1940*, Taylor & Francis e-Library, 2005.
5. Consiliul Securității Statului, Direcția Învățăământ, *Din Memoriile lui Eugen Cristescu*, București, 1968.
6. LUCINESCU Ioan Codruț, „Cristian Racovski în dosarele Siguranței Generale a Statului”, în *Revista Română de Studii de Intelligence*, nr. 9/ iunie 2013.
7. MITROKHIN Vasiliy, „CHEKISM”. *Tales of the CHEKA. A KGB Anthology*, The Yurasov Press, London, 2008.
8. MORARU Pavel, *Serviciile secrete și Basarabia (1918-1991)*, Editura Militară, București, 2008.

9. NICOL Andrei, „Contribuții ale atașărilor militari români la dezvoltarea relațiilor româno-franceze (1930-1936)”, în *Studia Universitatis Moldaviae*, nr. 4 (64), Universitatea de Stat din R.Moldova, Chișinău, 2013.
10. NICOLESCU Andrei, NICOLESCU Lenuța (coord.), *Atașatii militari români în primul deceniu interbelic. Rapoarte*, Mioveni, 2014.
11. NICOLESCU Lenuța, „Secția a 2-a Informații a Marelui Stat Major”, în revista *Document*, nr. 2 (6)/1999.
12. SPÂNU Alin, *Serviciul de informații al României în războiul de întregire națională (1916-1920)*, Editura Militară, București, 2012.
13. WARUSFEL Bertrand, „Histoire de l'organisation du contre-espionnage français entre 1871 et 1945”, în VAISSE Maurice (coord.), *Il n'est point de secrets que le temps ne révèle - Études sur l'histoire du renseignement*, Centre d'Études d'Histoire de la Défense, Éditions Lavauzelle, 1998.
14. WOLTON Thierry, *KGB-ul în Franța*, Editura Humanitas, București, 1992.

- <sup>1</sup> Din cauza schimbărilor care au intervenit pe plan internațional și apariției unor transformări majore în viața statelor, conceptul de „securitate națională” a evoluat semnificativ pe parcursul secolului XX. După sfârșitul Războiului Rece, termenul de „securitate” a fost redefinit în urma unei analize a problematicei la nivel internațional, lucru efectuat, în premieră, la începutul anilor '90, de către teoreticienii Ole Waever și Barry Buzan în cadrul Școlii de la Copenhaga.
- <sup>2</sup> Lenuța Nicolescu, „Secția a 2-a Informații a Marelui Stat Major”, în revista „*Document*”, nr. 2 (6)/1999, p. 58.
- <sup>3</sup> Alin Spânu, *Serviciul de informații al României în războiul de întregire națională (1916-1920)*, Editura Militară, București, 2012, p. 138.
- <sup>4</sup> Lenuța Nicolescu, op. cit., p. 59-60.
- <sup>5</sup> Arhiva Serviciului Român de Informații (în continuare ASRI), Fond documentar, Dosar nr. 2652, fila 45.
- <sup>6</sup> Consiliul Securității Statului, Direcția Învățământ, *Din Memoriile lui Eugen Cristescu*, București, 1968, Biblioteca Centrală ANIMV, p. 17.
- <sup>7</sup> Andrei Nicolescu, Lenuța Nicolescu, *Atașatii militari români în primul deceniu interbelic. Rapoarte*, Mioveni, 2014, pp. 180-181.
- <sup>8</sup> Alin Spânu, *Istoria serviciilor de informații/contrainformații românești în perioada 1919 – 1945*, Casa Editorială Demiurg, Iași, 2010, p. 153.
- <sup>9</sup> Arhivele Naționale ale României (în continuare ANR), Fond Ministerul de Război. Marele Stat Major, Dosar nr. 121, fila 9.
- <sup>10</sup> Bertrand Warusfel, „Histoire de l'organisation du contre-espionnage français entre 1871 et 1945”, în Maurice Vaisse (coord.), *Il n'est point de secrets que le temps ne révèle - Études sur l'histoire du renseignement*, Centre d'Études d'Histoire de la Défense, Éditions Lavauzelle, 1998, p. 99 și urmât.
- <sup>11</sup> Ibidem.
- <sup>12</sup> Ibidem.
- <sup>13</sup> Robert Boyce (editor), *French foreign and defence policy, 1918 – 1940*, Taylor&Francis e-Library, 2005, p. 234.
- <sup>14</sup> Vezi pe larg Vasiliy Mitrokhin, „*CHEKISM*”. *Tales of the CHEKA. A KGB Anthology*, The Yurasov Press, London, 2008.
- <sup>15</sup> Thierry Wolton, *KGB-ul în Franța*, Editura Humanitas, București, 1992, p. 20.
- <sup>16</sup> Ibidem., p. 21.
- <sup>17</sup> Ibidem., p. 22.
- <sup>18</sup> ANR, Fond Direcția Generală a Poliției, Dosar nr.3/1920, file 71-72, apud Ioan Codruț Lucinescu, „Cristian Racovski în dosarele Siguranței Generale a Statului”, în *Revista Română de Studii de Intelligence*, nr. 9, 2013.
- <sup>19</sup> Ibidem.
- <sup>20</sup> Andrei Nicolescu, Lenuța Nicolescu (coord.), *Atașatii militari români în primul deceniu interbelic. Rapoarte*, Mioveni, 2014, p. 125.
- <sup>21</sup> Ibidem., p. 111.
- <sup>22</sup> Amintim faptul că Bulgaria s-a aflat într-o situație extrem de dificilă în perioada 1920-1925, datorită poziției puternice deținute de Partidul Comunist Bulgar (creat în 1919), sprijinului de care ideile comuniste se bucurau într-o bună parte din societate (în special în rândurile tinerilor), dezamăgirilor cauzate de pierderea războiului etc. Eliminarea pericolului comunist s-a datorat atât măsurilor adoptate de guvernului Tsankov (care a desființat Partidul Comunist în anul 1924 și a confiscat numeroasele proprietăți pe care le deținea), cât și sprijinului extern, inclusiv din partea României, care a eliminat „ruta” de transfer de oameni, bani și arme din Uniunea Sovietică spre Balcani.

<sup>23</sup> Andrei Nicolescu, Lenuța Nicolescu (coord.), op. cit., p. 112.

<sup>24</sup> ANR, Fond Direcția Generală a Poliției, Dosar nr. 22/1924, fila 35.

<sup>25</sup> Acțiunile subversive ale Moscovei îndreptate contra României făceau parte dintr-un amplu scenariu strategic cu ramificații continentale, așa cum reiese și din Raportul nr. 7722 din 3 ianuarie 1924 al Corpului IV Armată (ANR, Fond Direcția Generală a Poliției, Dosar nr. 3/1920, fila 207), adresat Ministerului de Război. Documentul prezintă informații importante pentru securitatea națională deoarece „Guvernul din Moscova, prin generalul de divizie Csenafentoff, ar fi delegat pe mai mulți ofițeri superiori, între cari pe generalii de brigadă Incoff, Dobrici, Nozcoff, atașatul militar sovietic din Berlin și Harnitonoff, cu aducerea la îndeplinire a propagandei republicane printre ofițerii Armatei române începând cu provinciile alipite și terminând cu vechiul regat.(...) În acest scop se vor trimite fonduri de la Moscova la Berlin, care a rămas centrala propagandei, cu ramificație la Viena. În ceea ce privește legătura cu România s-a stabilit ca la Budapesta să se centralizeze informațiunile militare din Ardeal, la Odessa cele din Basarabia; la Lemberg cele din Bucovina, la Sofia cele din Moldova și parte din Muntenia (...)”.

<sup>26</sup> Pavel Moraru, *Serviciile secrete și Basarabia (1918 - 1991)*, Editura Militară, București, 2008, p. 151.

<sup>27</sup> ANR, Fond Microfilme Franța, Rola 190.

<sup>28</sup> *ibidem*.

<sup>29</sup> Sorin Aparaschivei, Florin-Badea Pintilie, *Din istoria oficială a contraspionajului românesc*, Editura ANIMV, București, 2018, p. 77.

<sup>30</sup> ASRI, Fond Documentar, Dosar 4702, fila 57.

<sup>31</sup> ANR, Fond Direcția Generală a Poliției, Dosar nr.3/1920, file 71-72.

<sup>32</sup> ASRI, Fond Penal, Dosar 73865, vol. 1, fila 313.

<sup>33</sup> ANR, Fond Direcția Generală a Poliției, Dosar nr.35/1923, fila 1.

<sup>34</sup> *Ibidem*.

<sup>35</sup> ANR, Fond Microfilme Franța, Rola 190.

<sup>36</sup> ANR, Fond Direcția Generală a Poliției, Dosar nr. 23/1924, fila 2.

<sup>37</sup> *Ibidem*, fila 3.



# FOOD FOR THOUGHT

*Secțiunea #foodforthought cuprinde o selecție de resurse bibliografice (documente oficiale, cărți și rapoarte), publicate în ultima perioadă, cu impact semnificativ asupra domeniului studiilor de securitate și informații.*

Vasile CREȚU

## DOCUMENTE OFICIALE

### NATO și Noul concept Strategic

NATO. "NATO 2022 Strategic Concept". 29.06.2022.

[https://www.nato.int/nato\\_static\\_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf](https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf)



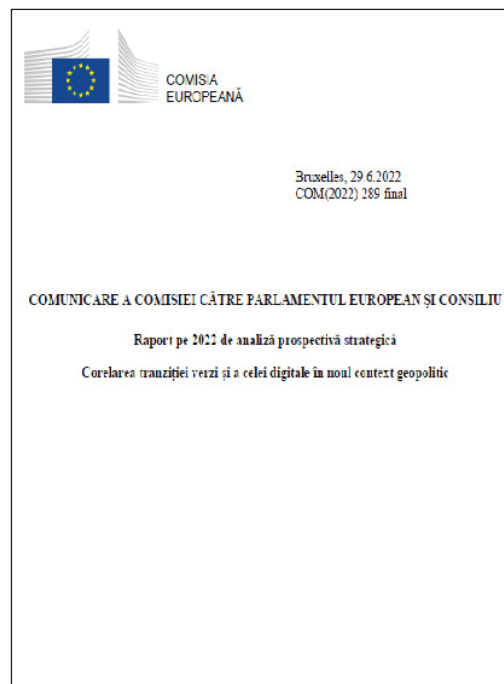
Conceptul Strategic, al doilea document ca importanță la nivelul Alianței după Tratatul Nord-Atlantic, stabilește direcția, prioritățile și sarcinile de bază. Noul Concept, adoptat de șefii de state și de guverne pe timpul Summit-ului de la Madrid (29-30 iunie 2022), marchează încheierea reflecției „NATO 2030”, reafirmă valorile Alianței și apărarea colectivă ca misiunea principală și reformulează sarcinile de bază, astfel: (1) descurajare și apărare; (2) prevenirea și managementul crizei; (3) securitatea prin cooperare. În ceea ce privește mediul de securitate, Conceptul Strategic pornește de la ideea că „în spațiul euro-atlantic nu este pace”, zona fiind caracterizată de competiție strategică, instabilitate generalizată și șocuri recurente. Rusia este definită drept „cea mai semnificativă și directă amenințare la adresa securității aliaților” și, în același timp, își pierde statutul de partener al NATO.

## UE și dubla tranziție: verde și digitală

Comunicare a Comisiei către Parlamentul European și Consiliu. „Raport pe 2022 de analiză prospectivă. Corelarea tranziției verzi și a celei digitale în noul context geopolitic.” Bruxelles, 29.06.2022, COM(2022)289final.

<https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52022DC0289&from=EN>

Cea de-a treia ediție a raportului anual de analiză prospectivă al UE, elaborat sub egida vicepreședintelui Comisiei Europene pentru relații interinstituționale și *foresight*, este dedicată interacțiunilor dintre tranziția verde și digitală, ambele fiind setate ca priorități politice europene cu impact în toate domeniile. Raportul din 2022 se fundamentează pe cele 10 megatendințe identificate în Raportul din 2021, având ca premisă accentuarea acestora în noul context geopolitic („schimbări geopolitice tectonice”), aspect care impune corelarea celor două tranziții. Printre măsurile propuse, consolidarea rezilienței și a autonomiei strategice ocupă un loc central, fiind anticipată o creștere a importanței geopoliticii tehnologiilor critice.



## CĂRȚI



**RĂZBOIUL PENTRU SUPREMAȚIE**

**SUA-CHINA**

**ȘI CELE CINCI FORȚE  
CARE SCHIMBĂ LUMEA**

Consecințe pentru România

Valentin Naumescu

OPUS • ȘTIINȚE POLITICE

POLIROM

### Competiția strategică SUA-China și dinamica politicii internaționale

Valentin Naumescu, *Războiul pentru supremație SUA-China și cele cinci forțe care schimbă lumea: Consecințe pentru România*, Ed. Polirom, 2021

Literatura de specialitate din domeniul relațiilor internaționale acordă o importanță deosebită competiției dintre marile puteri, îndeosebi rivalității sino-americane.

Cartea *Războiul pentru supremație SUA-China și cele cinci forțe care schimbă lumea: Consecințe pentru România*, apărută la finalul anului 2021, este inedită în peisajul bibliografic românesc atât prin subiect, cât și prin abordare, punând în centrul atenției consecințele asupra României. Structurată în două părți, cartea analizează scena internațională, pe de o parte, din perspectiva actorilor (SUA, China, Rusia, UE) și, pe de altă parte, din perspectiva a cinci forțe care schimbă lumea (educația, tehnologia, mediul, comunicarea și ideologia).

## Impactul inteligenței artificiale – evoluție sau revoluție?

Henry A. Kissinger, Eric Schmidt și Daniel Huttenlocker, *The Age of AI: And Our Human Future*. John Murray Press, 2021.

Inteligența artificială (IA) este deja o realitate, impactul acesteia resimțindu-se transversal în aproape toate domeniile. În general, studiile pe acest subiect se împart în două categorii: autorii entuziaști, care susțin că IA va revoluționa lumea, respectiv autorii sceptici, care prezintă IA ca o evoluție, dar în același timp evidențiază implicațiile negative și urmăresc limitarea implementării IA. Cartea, scrisă de trei autori cu experiențe diferite (H.Kissinger – fost secretar de stat și autor prolific în domeniul relațiilor internaționale; E.Schmidt – fost CEO Google; D.Huttenlocker – profesor la MIT), adresează întrebările care vor domina anii următori și oferă o analiză echilibrată asupra impactului IA în domeniile sănătății, economiei, geopoliticii, dreptului și militar.

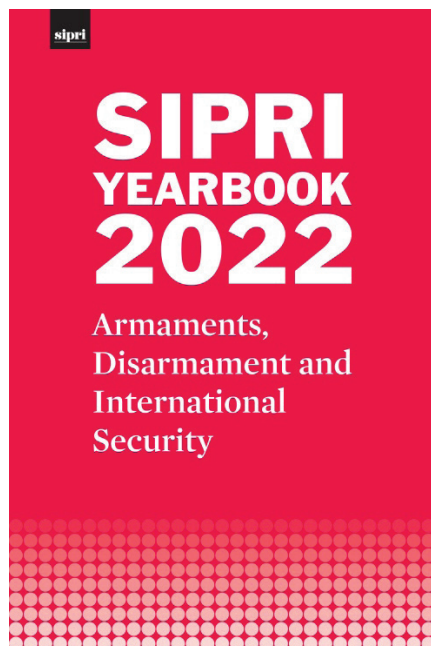


## RAPOARTE, STUDII

### Securitatea internațională, armamentele și dezarmarea

Stockholm International Peace Research Institute. "SIPRI Yearbook 2022: Armaments, Disarmament and International Security". 2022.

[https://www.sipri.org/sites/default/files/2022-06/yb22\\_summary\\_en\\_v3.pdf](https://www.sipri.org/sites/default/files/2022-06/yb22_summary_en_v3.pdf)



SIPRI Yearbook 2022, publicat anual începând cu anul 1968, este un reper în ceea ce privește evoluția securității internaționale, oferind analize și date relevante despre nivelul cheltuielilor militare, producția și comerțul cu tehnică militară, managementul crizelor, precum și eforturile din domeniul controlului armamentelor, dezarmare și neproliferare nucleară. Raportul din 2022 evidențiază continuarea tendinței de creștere a cheltuielilor militare la nivel global (fiind depășit, pentru prima dată, pragul de 2.000 de miliarde de dolari), precum și de accelerare a înarmării atât în plan convențional, cât și nuclear. SUA, Rusia, Franța, China și Germania ocupă primele cinci poziții în exportul de armamente, asigurând 77% din volumul total al exporturilor.

## Percepția populației din statele din Europa Centrală și de Est asupra problemelor de securitate

Dominika Hajdu et al. "Globsec Trends 2022: CEE amid the war in Ukraine". Centre for Democracy&Resiliece, GLOBSEC, Bratislava.

<https://www.globsec.org/wp-content/uploads/2022/05/GLOBSEC-Trends-2022.pdf>

În baza unei cercetări sociologice realizate în martie 2022 în nouă state din Europa Centrală și de Est (Bulgaria, Cehia, Estonia, Letonia, Lituania, Polonia, România, Slovacia și Ungaria), experții GLOBSEC analizează modalitatea în care s-a schimbat percepția populației din aceste țări după izbucnirea conflictului din Ucraina. Printre rezultate se numără următoarele: (1) 80% din populație percepe apartenența la structurile euro-atlantice ca fiind benefică; (2) 75% consideră SUA ca principalul aliat; (3) nivelul de conștientizare al amenințărilor generate de China este redus; (4) se remarcă o preferință pentru utilizarea instrumentului economic ca răspuns la acțiunile Rusiei, în detrimentul celui militar.



## Analiza prospectivă și planificarea apărării în ministerul rus al apărării



CLINT REACH, ALYSSA DEMUS, EUGENIU HAN, BILYANA LILLY, KRYSTYNA MARCINEK, YULIYA SHOKH

## Russian Military Forecasting and Analysis

The Military-Political Situation and Military Potential in Strategic Planning



Clint Reach et al. "Russian Military Forecasting and Analysis: The Political-Military Situation and Military Potential in Strategic Planning", Santa Monica, CA: RAND Corporation, 2022.

[https://www.rand.org/content/dam/rand/pubs/research\\_reports/RRA100/RRA198-4/RAND\\_RRA198-4.pdf](https://www.rand.org/content/dam/rand/pubs/research_reports/RRA100/RRA198-4/RAND_RRA198-4.pdf)

Modalitatea în care ministerul rus al apărării evaluează mediul de securitate și își planifică politicile de apărare reprezintă o întrebare-cheie, în special în contextul războiului din Ucraina. Cercetătorii RAND oferă atât o analiză descriptivă a arhitecturii instituționale implicate, cât și aspecte metodologice privind realizarea analizelor prospective (indicatori și factori evaluați), lucrarea fiind centrată asupra analizelor de tip „situație politico-militară” și „determinare a potențialului militar”. Dincolo de perspectiva teoretică, autorii prezintă o serie de analize practice, din care rezultă principalele concluzii, precum problemele operaționale pentru Rusia derivate din coeziunea NATO.



## Competiția strategică SUA-China în domeniul diplomatic

Graham Allison, Alyssa Resar și Karina Barbesino, "The Great Diplomatic Rivalry: China vs the U.S.", *Belfer Center for Science and International Affairs*, Harvard Kennedy School, Report, August 2022.

<https://www.belfercenter.org/publication/great-diplomatic-rivalry-china-vs-us>

Raportul, elaborat în cadrul Proiectului „Evitarea Războiului între Marile Puteri” al Centrului Belfer pentru Știință și Afaceri Internaționale/Universitatea Harvard, analizează comparativ SUA și China în ceea ce privește activitatea sistemelor diplomatice în perioada 2000-2020, prin raportare la răspunsurile față de principalele provocări. Lucrarea evidențiază performanțele celor două state în diferite aspecte ale diplomației (arta diplomației – *statecraft*; arhitectura diplomatică – norme, regimuri, instituții; „diplomația de zi cu zi” – *gardening*), identificând, de asemenea, tendințe care vor modela, în viitor, evoluția rivalității sino-americane.



## Descurajarea amenințărilor hibride

Sean Monaghan, "Deterring hybrid threats: Towards a fifth wave of deterrence theory and practice". The European Centre of Excellence for Countering Hybrid Threats. 31.03.2022.

<https://www.hybridcoe.fi/wp-content/uploads/2022/03/20220331-Hybrid-CoE-Paper-12-Fifth-wave-of-deterrence-WEB.pdf>



În concepția autorului, proliferarea amenințărilor hibride și a „tacticilor situate sub pragul războiului” este o consecință a descurajării și a reducerii practicii războiului interstatal. În același timp, amenințările hibride alterează fundamentele descurajării (capabilitate, credibilitate și comunicarea intenției), fiind astfel dificilă descurajarea manifestării acestui tip de acțiuni. În acest context, autorul dezvoltă un cadru general de adaptare a teoriei (și, implicit, a practicii) descurajării pentru amenințările hibride, marcând trecerea la cel de-al cincilea val teoretic.