Anul XIV nr. 2/2022

INFOSFERA

Revistă de studii de securitate şi informaţii pentru apărare

Publicaţie indexată în bazele de date internaţionale EBSCO şi CEEOL

Revistă cu prestigiu ştiinţific recunoscut de Consiliul Naţional de Atestare a Titlurilor, Diplomelor şi Certificatelor Universitare (CNATDCU)

Direcţia Generală de Informaţii a Apărării

INFORMAȚII

CUPRINS

RĂZBOAIELE SECOLULUI XXI

PERSPECTIVE GEOPOLITICE ȘI GEOSTRATEGICE

AMENINȚĂRI HIBRIDE

INTELLIGENCE STRATEGIC

ISTORIA SERVICIILOR DE INFORMAȚII

RECENZII ȘI SEMNALĂRI

LECȚIILE CONFLICTULUI DIN UCRAINA ȘI PERSPECTIVA REZILIENȚEI SOCIETALE

Iulian CHIFU*

Abstract

Russia's invasion in Ukraine has proved to be an important challenge for a lot of countries and revealed the level of resilience one people could have or find inside its own ranks. But societal resilience is not a given fact and does not have a constant value in time. It could drop dramatically if there are no incentives to maintain the same reasoning and cohesion that led originally to the level of resilience able to do miracles.

Ukraine's lessons in front of the unprovoked, illegal and unjustified Russian aggression are tremendously important to be considered when estimating the resilience of the European countries in front of the costs and risks accepted already by their population. It is crucial for the defense of the collective West in front of Russia's attempt to change the strategic landscape of the world with the war launched in Ukraine.

Keywords*: resilience; societal resilience; service continuity; liquid society; anti-fragile.*

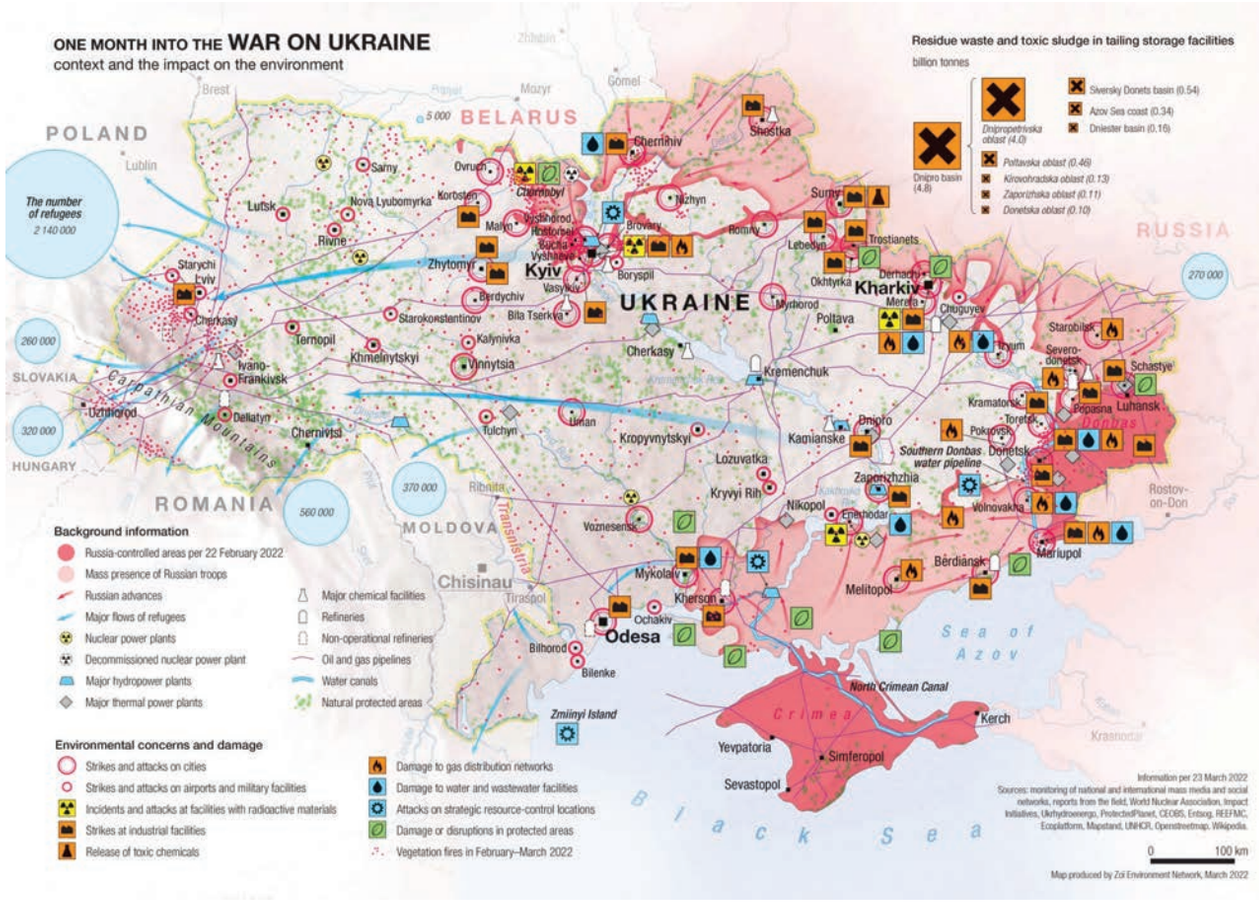
CONCEPTELE DE „REZILIENȚĂ" ȘI „REZILIENȚĂ SOCIETALĂ". APLICABILITATEA LOR ÎN CADRUL NATO ȘI UE

Reziliența are nenumărate definiții și este conceptul cel mai la modă în domeniul securității, dacă ar fi să analizăm doar documentele din ultimii ani adoptate la nivelul UE, NATO și al statelor membre. 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 are multiple domenii în care se manifestă și nenumărate aspecte care țin de reacția potrivită la amenințări și riscuri, precum și de compensarea sau limitarea vulnerabilităților.

Reziliența societală este componenta care se referă la societate. La nivelul securității societale, elementele de securitizat sunt *coeziunea societală* și *identitatea*[1]. Însă, acestora li se adaugă și alte elemente care țin de leadership, încrederea în autoritate, calitatea democrației și a statului de drept, patriotismul, dorința de a-și apăra statul, modul de viață și proprietatea și accesul egal la oportunități.

NATO își are propriile definiții și referințe la reziliență și reziliență societală. Astfel, ideea îmbunătățirii rezilienței apare în Raportul Secretarului General al NATO pe anul 2021[2] și se referă la faptul că societățile puternice sunt prima linie a apărării NATO. Conținutul rezilienței în cazul NATO vizează *protecția infrastructurii critice* pe teritoriul aliat 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.***



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[3], pe de o parte, și salvgardarea societăților, populațiilor și valorilor comune[4], pe de altă parte. Reziliența e asumată drept obiectiv și premisă a apărării și descurajării credibile și conține componenta de pregătire civilă în gestionarea crizelor.

În esență, reziliența este o responsabilitate națională, dar rezultat al unui angajament colectiv. Iar fundamentele rezilienței rezidă exact în angajamentul de prezervare a principiilor libertăților individuale, democrației, drepturilor omului și statului de drept. Prin urmare, reziliența, în lectura NATO, se referă la modul de a reacționa la crize, în fața amenințărilor, la capacitatea de limitare a vulnerabilităților și la prezervarea principiilor și valorilor. Aceasta presupune apărarea primordială a modului de viață al societății democratice.

Reziliența a fost principalul subiect al Summit-ului NATO de la Varșovia[5] (2016) și a cuprins modul de definire, evaluarea rezilienței și întărirea ei. Totodată, aceasta este privită drept corolar sau chiar condiție (sunt auto-influențabile și se susțin reciproc) a descurajării și apărării aliate și a măsurilor de reasigurare în domeniul apărării clasice și hibride. Există șapte cerințe de bază:

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 (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[6].

Ele se circumscriu la cinci arii de amenințări și acțiuni: cyber defence, amenințări hibride, pregătire civil-militară, cooperarea cu UE, cooperarea cu statele partenere.

Dacă NATO are o istorie mai îndelungată în legătură cu reziliența, iar termenul a fost prezent și în forma interimară a noului Concept Strategic al Alianței Nord-Atlantice, și Uniunea Europeană și-a pregătit documentul strategic, Busola Strategică, care are prevederi referitoare la modul în care privesc cei 30 de membri reziliența[7]. Și temele explicite se referă la schimbările climatice, dezastre și urgențe civile. Pe dimensiunea rezilienței economice, temele sunt lanțurile de aprovizionare, rutele de transport, libertatea navigației, securitatea furniturilor.

Temele se extind la construirea rezilienței în fața amenințărilor de securitate la nivelul comunităților și merg până la reziliența instituțională a Uniunii. Reziliența cibernetică în fața atacurilor hibride, mobilitatea militară și reziliența societală se regăsesc în document. UE a adoptat și *European Cyber Resilience Act* – care se referă la infrastructura cibernetică și la standarde, dar regăsim preocupări relative la infrastructura spațială, reziliența maritimă, infrastructura critică și reziliența în fața crizelor.

La capitolul *reziliență societală*, accentul este pus pe asigurarea 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.

REZILIENȚA SOCIETALĂ ÎN DILEMA CONTINUITATEA SERVICIILOR VERSUS CONTINUITATEA INSTITUȚIILOR

În studiile efectuate despre reziliență, am adăugat acestor teme și elementele ce țin de dimensiunea reacției în **construirea rezilienței**, respectiv formula interguvernamentală ***whole of the government*** sau ***whole of the society***. Dar am propus, pe model elvețian, varianta ***whole of the people***, acolo unde *statul* și instituțiile sale cooperează cu *societatea civilă*, cu organizații neguvernamentale și cu structurile asociative formale și informale, dar și cu fiecare cetățean în parte care participă la apărarea propriei securități, în special pe dimensiunea terorismului și a amenințărilor hibride, acolo unde rolul statului nu este suficient[8].

Firește, această perspectivă vine și cu obligativitatea de a asigura încrederea populației și a cetățenilor în autoritate[9], într-o structură care pune cetățeanul în mijlocul acțiunilor legate de dimensiunea securitară și întărește *leadership-ul credibil, bazat pe meritocrație* și așezarea fiecăruia la locul potrivit[10]. El se combină, în mod armonios și obligatoriu, cu securitatea politică[11] ce conține, totodată, opțiunile și diversitatea ofertei politice (calitatea și revalorificarea elitei naturale și profesionale a societății)[12].

Tot la capitolul reziliență, rămâne deschisă discuția vizând *primatul continuității instituționale*, ca efect al rezilienței și forței de a recupera valorile societale și bunurile după criză sau continuitatea serviciilor, ca atribut și obiectiv al instituțiilor. Aici apare problema diferenței dintre anti-fragil și robust[13]: 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 destinate populației?

Dezbaterea nu este deloc trivială. Pentru prima variantă pledează *componenta simbolică* și *experiența istorică.* Astfel, succesiunea statului trebuie menținută în ceea ce înseamnă definiția și condițiile apartenenței la comunitatea internațională și a ONU – teritoriu, populație autoritate. Dacă mâine un stat insular se scufundă și populația e mutată pe continent, într-un spațiu închiriat sau cumpărat pe teritoriul altui stat (Maldive, de exemplu în India)[14], înseamnă acest lucru reziliență? A supraviețuit acel stat? Sau guvernul Svetlanei Tsikhanouskaya are vocație de continuitate a statului Belarus dacă acesta ar

fi înglobat în Rusia? (eterna temă a legitimității guvernului în exil).

Pe de altă parte, există și argumentele contrare care spun că robustețea poate fi risipitoare de resurse în criză. De altfel, pandemia pe care am traversat-o ne dovedește acest lucru, când am putut să desfășurăm mare parte a serviciilor fără a beneficia pe deplin (sau beneficiind în mică măsură) de componenta fizică a instituțiilor: sunt de ajuns câteva laptopuri, ierarhia cunoscută, funcționalitatea Internetului și serviciile pot fi asigurate, în mare măsură, în continuare. Sigur, în domeniul apărării și securității este nevoie de hardware, de componenta fizică a rachetelor, tancurilor sau măcar a UAV-urilor și militarilor antrenați în conflict. Subiectul rămâne deschis.

Lecțiile de reziliență ale Ucrainei se decantează în multiple direcții, pentru diferiți actori. Astfel, pentru ***F.Rusă,*** lecția fundamentală e cea a credulității și a autocrației care ignoră aspectele profesionale în favoarea voinței liderului, care domină sistemul creat de „verticala puterii”[15] și de economia condusă de *siloviki,* prin gestionarea marilor companii energetice în beneficiul regimului. Nu știm dacă reziliența populară în fața lipsurilor și a sancțiunilor sau cea a instituțiilor/ a sistemului în timp de război poate fi menținută. Sau măcar reziliența în privința obiectivelor (nedeclarate) ale războiului din Ucraina.

Pentru ***Ucraina***, *forța de constituire a națiunii după 2014* este punctul de referință în războiul său de independență pe care-l duce acum cu Rusia. S-a vădit relevanța dorinței de apărare a teritoriului și a identității ucrainene, extinse la nivelul întregii populații, indiferent de etnie – în est majoritari erau rușii, la fel și în sudul ocupat, la Kherson și Zaporoje, acolo unde cetățenii ruși cu steaguri ucrainene în mâini au protestat cerând forțelor ruse să plece acasă; tot astfel cum Harkivul, oraș cu 90% etnici ruși, s-a opus armatei ruse. Patriotismul renăscut și coeziunea societală după anexarea Crimeii și agresiunea militară din estul Ucrainei, în 2014, au fost determinante. *Dorința și voința de a lupta* au fost exemplare. Iar cooperarea instituțiilor statului cu societatea civilă și cetățenii obișnuiți a dat măsura rezistenței care a schimbat și planurile actorilor externi și i-a determinat să parieze, din nou, pe Ucraina.

Pentru ***România, Polonia,*** dar și multe alte state, a fost *o revelație dimensiunea rezilienței societale în gestionarea refugiaților*. La efort au participat statul și instituțiile sale, însă, cu precădere, în primă fază, societatea civilă autohtonă și organizațiile internaționale, dar și simplii cetățeni - generoși, ospitalieri și profund umani, veniți să ia câte o familie-două năpăstuite acasă sau să le ajute în orice fel. Și aceasta este o dovadă de reziliență societală de cea mai bună calitate și nu întâmplător s-au revărsat în aceste state atâtea misiuni succesive de prim-plan ale oficialilor aliați și parteneri, din „Occidentul colectiv“[16], pentru a vedea cum s-a putut întâmpla minunea.

În 2015, un milion de migranți zgâlțâiau Europa din țâțâni, amenințând să o facă bucăți, pentru ca în 2022, Polonia și România, în special, să gestioneze șase milioane de refugiați (numai în țara noastră intrând peste un milion de refugiați, cifra fatidică a anului 2015). Sigur, cârcotașii vorbesc despre componența și structura migrației – tineri, bărbați, musulmani în majoritate, în 2015, versus femei și copii, creștini albi, în 2022. Dar acestea rămân doar un element de diferență specifică în tratarea valurilor de migranți și anclanșarea resorturilor interne de omenie ale populației care sprijină găzduirea refugiaților. Sigur, este vorba despre România și Polonia, state cu 5-7 milioane de cetățeni plecați în lumea largă. Pe de altă parte, relația cu Kievul oficial și percepția Ucrainei în România, mai ales în zonele de frontieră, nu era neapărat cea mai favorabilă înainte de război, știute fiind rănile istorice. Totuși, nu a contat acest aspect.

CE-ȘI DOREȘTE F.RUSĂ ÎN UCRAINA: ÎNFRÂNGEREA OCCIDENTULUI, ALTERAREA LUMII AȘA CUM O ȘTIM

Dar poate cele mai importante ***provocări la adresa reziliență*** vin tocmai din obiectivele Moscovei în legătură cu Occidentul și cu lumea bazată pe reguli[17] și din perspectivele de reziliență necesare Occidentului colectiv pentru a putea

gestiona voința, încrederea și resursele necesare continuării sprijinirii Ucrainei, în ciuda costurilor și a nivelului de risc asumat de societățile occidentale. ***Unanimitatea și unitatea Occidentului în sprijinirea Ucrainei*** *a fost unul dintre pariurile pierdute de Putin.* Dar transformarea conflictului într-un război de uzură, pe termen lung, ridică noi categorii de probleme: costuri, sancțiuni, riscuri crescute, nevoia de reziliență societală a Vestului și capacitatea de a mobiliza cetățenii, în continuare, pe tema Ucrainei.

Pe de altă parte, ***F.Rusă e departe de a fi slabă.*** Moscova nu a pierdut încă războiul, chiar dacă va fi obligată, cel mai probabil, să-și modifice *obiectivul operațional* – câștigarea Donbasului și distrugerea trupelor ucrainene fixate la fosta linie de contact – și pe cel *strategic* - ocuparea completă a litoralului Mării Negre, până la strâmtori, inclusiv provocând NATO în România și, probabil, în Bulgaria.

2014 nu a fost niciodată despre Crimeea sau Donbas, ci despre Ucraina, despre întreaga Ucrainã. Rusia lui Putin a vrut să o forțeze să renunțe la ambițiile sale euro-atlantice și să o readucă în imperiul nou construit. Acum, *Occidentul a fost mai rapid ca în 2014*, mai pregătit, mai decis, și multe state au livrat ce trebuia Ucrainei: arme anti-tanc, anti-aeriene, Stinger etc. Oricum, rușii nu se vor opri și va conta obiectivul strategic, care e Ucraina.

Obiectivul operațional e acum Donbasul, încercuirea și înfrângerea forțelor armate cele mai bune ale Ucrainei, acolo în est, cu speranța că, eventual, ar putea să cadă întreaga Ucrainã, sub efectul de domino. Dacă Rusia are succes acum, în obiectivul ei strategic, ***obiectivul complet constă în controlul/dominarea întregii coaste a Mării Negre***, inclusiv a celei deținute de România[18]. După cum spunea asistentul Secretarului Pentagonului, Celeste Wallander, apărarea de coastă și livrările de arme pentru apărarea aeriană și anti-aeriană vor pregăti **viitoarea luptă a Ucrainei și a întregului Occident cu Rusia lui V.Putin**, ca să nu ajungem să luptăm pe teritoriul NATO. Aceasta este, la orizont, viitoarea luptă.

Definiția victoriei pentru Ucraina și Occident implică un eșec strategic pentru F.Rusă. Sigur, e nevoie, în final, de *o soluție negociată, nu una impusă de F.Rusă.* În termenii cu care suntem cu toții de acord, nu în condițiile Moscovei. V.Putin a vrut un *remake* după marea victorie din al Doilea Război Mondial, ca să se asocieze la ziua de 9 Mai și să salveze imaginea lipsei unei motivații realiste a atacului în Ucraina, măcar față de ruși. Nu a ieșit nicio alăturare. Rusia lui Putin nu a realizat nici astăzi de ce ucrainenii i se opun, de ce nu salută cu flori eliberarea, ca-n 1945, de ce nu s-a întâmplat la fel ca-n Crimeea, să cadă iute, simplu și mai ales fără victime. Nu s-a așteptat să i se opună Ucraina, să nu-l vrea, ci să-și dorească cu adevărat independența. Iar suveranitatea limitată[19] pe care o dorea impusă să nu se poată realiza vreodată.

REZILIENȚA OCCIDENTULUI COLECTIV

Occidentul a avut ***partea sa de eșec***, odată ce s-a declanșat războiul, pentru că nu a oprit de la început caruselul încălcărilor de acorduri, de tratate, de control al armamentelor, de notificare a mișcărilor de trupe și echipamente din partea F.Ruse. Toate aceste încălcări tolerate sau avertizările formale au condus la război. Moscova a crezut că i se permite și poate să meargă mai departe. Că Occidentul „putred" este în declin, divizat, incapabil să reacționeze. Că poate să meargă înainte și să scape și de data asta.

Dacă la nivelul relaționării cu statele din Parteneriatul Estic – dar și cu cele din Balcanii de Vest – „Occidentul Colectiv" a folosit în prim-plan abordarea normativistă pentru a-și acoperi lipsa de voință politică sau chiar de curaj, perspectiva a devenit și mai complicată astăzi. E vorba despre decantarea, încet-încet, în interiorul fiecărui stat al Occidentului, a două componente. Prima este așa-numita ***„partidă a păcii"***, cea care solicită *terminarea conflictului* și *acomodarea rapidă a unei poziții cu Rusia*, cu prețul sacrificării unor bucăți teritoriale ale Ucrainei sau chiar a unor interese ale sale – vezi integrarea în NATO.

Cealaltă este ***„partida justiției"***, care subliniază clar faptul că „nu te mai poți întoarce la *business as usual* cu Rusia", că nu se poate reveni la pozițiile din 2007 sau la cele dinainte de 2014, și că deja am depășit această paradigmă. Sigur,

nu poate exista pace cu F.Rusă: chiar dacă închei un acord, peste niște ani va reveni mai puternică și agresivă să renegocieze de pe pozițiile sale. În fapt, *Moscova a ieșit din joc, din reguli, din cărți.* E pe această poziție, iar drumul înapoi nu mai poate fi făcut.

O Rusie post-Putin va putea negocia rațional o soluție de interes comun, în care nu se impune nimic de către Moscova și se acceptă cu bună credință un acord. Pentru că deja nu mai suntem în lumea dinaintea lui 24 februarie: Rusia nu mai e credibilă, Putin i-a mințit în față pe liderii lumii și a declanșat un război inexplicabil militar și fără nici o rațiune; Occidentul colectiv a ajuns la capătul răbdării cu Rusia și nu mai poate deconta în fața publicului său nevoia de înțelegere cu V.Putin, cu prețul de a risca mai mult și de a plăti mai mult pentru petrolul și gazele rusești; Germania a crescut bugetul militar și transferă arme Ucrainei, rupând și tradiția dependenței energetice de Rusia, prin Nord Stream; iar Finlanda și Suedia au solicitat intrarea în NATO. Statele membre ale Alianței au recunoscut eroarea strategică din 2008, ca început al toleranței și ambiguității față de agresiunile Moscovei în multiple războaie. E, deja, altă lume!

Sigur, reziliența înseamnă a menține publicul angajat în susținerea Ucrainei. Înseamnă a asuma, în continuare, pe termen lung, ***costuri și riscuri mai mari*** – altfel, un coșmar pentru liderii democratici. Înseamnă să arăți în mod credibil F.Ruse că ești gata să-ți asumi costurile și suferințele pentru a-ți apăra principiile și a rezista puternic în promovarea modului tău de viață, liber, democratic, suveran, bazat pe reguli. Iar pe această înălțime morală, relevată de către Ucraina și Zelenski, să recreezi *soft power*-ul și să construiești baza sustenabilității opoziției la lumea plăsmuită de V.Putin.

Iar *extinderea NATO* este exact acest fapt: afirmarea politică a susținerii principiilor comune. Asigurarea condițiilor pentru democrație și libertate (sunt interdependente cele două). Securitatea e legată de democrație și libertate în Europa. De aceea sunt importante. Apoi, *apartenența la UE nu e un substitut pentru NATO.* Modelul finlandez e un model foarte bun, care ar trebui să sublinieze cât de serioase sunt lucrurile. E echivalent cu **dreptul de a exista al națiunilor** și cu suveranitatea lor egală[20]. De ce ar trebui, atunci, Ucraina să sacrifice ceva din teritoriul său, să dea ceva de la ea pentru războiul lui Putin sau limitele rezilienței occidentale? Unde se va mai situa înălțimea morală a societăților europene și occidentale atunci?

Contracararea autocrațiilor, în frunte cu Rusia și China, depinde de gradul de antrenare al partenerilor democratici globali. India și Africa de Sud, de exemplu, nu recunosc războiul colonial al Rusiei, pentru că pentru ei UE/ SUA e colonizatorul. Pe fond, Rusia e un actor neo-imperial, colonial, o metropolă care încearcă să-și recucerească coloniile. Pe această înțelegere, e mai lesne de atras sprijinul lumii întregi pentru sancțiuni și sancționări la vot în Adunarea Generală a ONU.

În materie de ***război informațional*** s-au văzut multiplele vulnerabilități ale Occidentului. De exemplu, impactul ideii de „denazificare" este mai mare în Occident decât în F.Rusă. De altfel, în materia aceasta, tehnica rusă e să găsească precedente legate de SUA și Occident – Kosovo, Irak – pentru a justifica de ce face aceste acțiuni. Și se joacă cu emoțiile pe teme problematice.

Un alt subiect sensibil este această ***dorință excesivă de angajare a lui Putin***, care ascunde și un nivel ridicat de orgoliu referitor la cine e liderul care va obține negocierea reală cu Putin. Politicienii sună la Putin de pe pozițiile slabe, ale solicitanților de avantaje, care vor ceva și sunt gata să sacrifice ceva. E o poziție de negociere ciudată. De jos. Din zona perdanților, a celor care au ceva de pierdut, nu din poziția învingătorilor, reali sau morali, a celor care au dreptate. Asta când Putin este trecutul, nu viitorul.

În fine, dacă avem de-a face cu un război lung, contează ***reziliența susținerii publice pentru Ucraina***. Cum menținem interesată opinia publică în Ucraina? Mâine vine altă criză și atenția fuge. Sau cum depășim costurile pe care sancțiunile și modul convenit de gestionare a situației Rusiei le-au provocat în viața de zi cu zi. Iar asta e un coșmar al liderilor într-o democrație. Totuși, aici se joacă viitorul lumii și al democrației și libertății: dacă Ucraina rezistă și se apără, **cum ar putea Occidentul colectiv să abandoneze și să capituleze doar de dragul păcii?**

BIBLIOGRAFIE

1. BUZAN Barry, Ole Waever, Jaap de Wilde, *Securitatea. Un nou cadru de analiză*, 2010, C.A Publishing, ISBN 978-606-92737-3-9, 330 p.
2. 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*, ediţie bilingvă, Editura Curtea Veche, Bucureşti, 2008, 320 p, ISBN 978-973-1983-00-4, 320 p.
3. CHIFU Iulian, „Războiul hibrid și reziliența societală. Planificarea apărării hibride", *Infosfera*, 1/2018, pp.23-30, ISSN: 2065-3395.
4. CHIFU Iulian, „Renașterea dreptei. Reconectarea la elite", *Adevărul*, 3 iulie 2020, la https://adevarul.ro/news/politica/renasterea-dreptei-reconectarea-elite-1_5eff2ddb5163ec427198fe41/index.html.
5. CHIFU Iulian, „Reziliență strategică: de la stabilitate și prevenție la acțiune pro-activă și adaptabilitate dinamică", *Gândirea Militară*, 1/2021, pp. 10-21.
6. European Union, *A strategic compass for security and defense. For a 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.
7. FAUCONNIER Clémentine, "The power vertical, strength and weakness of Putin's Russia", *Revue internationale et stratégique*, vol. 118, Issue 2, April 2020, pp. 154-162.
8. SHEA Jamie, *Resilience, a core element of collective defense*, document al NATO, https://www.nato.int/docu/Review/2016/Also-in-2016/nato-defence-cyber-resilience/EN/index.htm.
9. JONES A. Robert, *The Soviet Concept of 'Limited Sovereignty' from Lenin to Gorbachev: The Brezhnev Doctrine*, St. Martin's, 1990, 337 p.
10. NATO documents, *Strengthen Resilience Commitment*, 15 June, 2021, https://www.nato.int/cps/en/natohq/official_texts_185340.htm.
11. 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.
12. NATO, *Secretary General Annual Report 2021*, https://www.nato.int/cps/en/natohq/opinions_ 193590.htm?selectedLocale=en.
13. PASKAL Cleo, *Global Warring. How Environmental Economic and Political Crises Will Redraw the World Map*, Key Porter Books, 2010, Toronto, ISBN 978-1-55263-830-9, 288 p.
14. România, Administrația Prezidențială, *Strategia Națională de Apărare a Țării pentru perioada 2020-2024*, la https://www.presidency.ro/files/userfiles/Documente/Strategia_Nationala_de_Aparare_a_Tarii_2020_2024.pdf.
15. SCOTT Ben, "But what rules based order means?", Law Institute, The Interpreter, 2 Novermber 2020, at https://www.lowyinstitute.org/the-interpreter/what-does-rules-based-order-mean.
16. SHERR James, *The Collective Putin and the Collective West*, International Center for Defense and Security, Estonia, at https://icds.ee/en/the-collective-putin-and-the-collective-west/.
17. TALEB Nassim Nicolas, *Antifragil - ce avem de câștigat de pe urma dezordinii*, Editura Curtea Veche, 2014.
18. UN Charter, https://treaties.un.org/doc/publication/ctc/uncharter.pdf.
19. WALLANDER Celleste, *Наша Славна Україна: Rise Up, Ukraine*, Lennart Meri conference, Tallinn, 13-15 mai 2022 at https://youtu.be/NQx41DrB1sY.
20. Warsaw Summit Communiqué, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016, at https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

[1] 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*, ediţie bilingvă, Editura Curtea Veche, Bucureşti, 2008, 320 p., ISBN 978-973-1983-00-4.

[2] NATO, *Secretary General Annual Report 2021*, https://www.nato.int/cps/en/natohq/opinions_193590.htm?selectedLocale=en.

[3] 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.

[4] NATO documents, *Strengthen Resilience Commitment*, 15 June, 2021, https://www.nato.int/cps/en/natohq/official_texts_185340.htm.

[5] *Warsaw Summit Communiqué, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016*, https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

[6] 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.

[7] European Union, *A strategic compass for security and defense. For a 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.

[8] Iulian Chifu, „Războiul hibrid și reziliența societală. Planificarea apărării hibride”*, Infosfera*, 1/2018, pp.23-30, ISSN: 2065-3395.

[9] Iulian Chifu, „Reziliență strategică: de la stabilitate și prevenție la acțiune pro-activă și adaptabilitate dinamică”, *Gândirea Militară*, 1/2021, p. 10-21.

[10] România, Administrația Prezidențială, *Strategia Națională de Apărare a Țării pentru perioada 2020-2024*, la https://www.presidency.ro/files/userfiles/Documente/Strategia_Nationala_de_Aparare_a_Tarii_2020_2024.pdf.

[11] Barry Buzan, Waever Ole, de Wilde Jaap, *Securitatea. Un nou cadru de analiză*, 2010, C.A Publishing, ISBN 978-606-92737-3-9, 330 p.

[12] Iulian Chifu, *Renașterea dreptei. Reconectarea la elite*, Adevărul, 3 iulie 2020, la https://adevarul.ro/news/politica/renasterea-dreptei-reconectarea-elite-1_5eff2ddb5163ec427198fe41/index.html.

[13] Nassim Nicolas Taleb, *Antifragil - ce avem de câștigat de pe urma dezordinii*, Editura Curtea Veche, 2014.

[14] Cleo Paskal, *Global Warring. How Environmental Economic and Political Crises Will Redraw the World Map*, Key Porter Books, 2010, Toronto, ISBN 978-1-55263-830-9, 288 p.

[15] Clémentine Fauconnier, ”The power vertical, strength and weakness of Putin’s Russia”, *Revue internationale et stratégique*, Volume 118, Issue 2, April 2020, pp. 154-162.

[16] James Sherr, *The Collective Putin and the Collective West,* International Center for Defense and Security, Estonia, https://icds.ee/en/the-collective-putin-and-the-collective-west/.

[17] Ben Scott, *But what rules based order means?,* Law Institute, The Interpreter, 2 Novermber 2020, at https://www.lowyinstitute.org/the-interpreter/what-does-rules-based-order-mean.

[18] Celleste Wallander, *Наша Славна Україна: Rise Up, Ukraine*, Lennart Meri conference, Tallinn, 13-15 mai 2022 at https://youtu.be/NQx41DrB1sY.

[19] Robert A. Jones, *The Soviet Concept of ‘Limited Sovereignty’ From Lenin to Gorbachev: The Brezhnev Doctrine.* St. Martin’s, 1990, 337 p.

[20] *UN Charter*, https://treaties.un.org/doc/publication/ctc/uncharter.pdf.

CONSIDERAȚII PRIVIND INVAZIA FEDERAȚIEI RUSE ÎN UCRAINA

*Adrian IVAN**

Abstract

The large-scale invasion of the Armed Forces of the Russian Federation in Ukraine has marked the beginning of the deadliest conflict in Europe within the past decades.

The Russian Armed Forces who attacked Ukraine benefitted from the whole range of their capabilities, including land artillery, AA rockets, long range precision fires (LRPF), short-range ballistic missile (SRBM), electronic warfare units and logistic and fight support structures.

However, the russian forces have generally performed poorly due to the rigid chain of command and control, lack of tactical vision and professionalism of troops, inefficient communications, low accuracy of weapons systems and inadequate logistical support, to which is added the unexpected resistance of the Ukrainian armed forces.

Keywords: *Russian Armed Forces – RuAF; Ukrainian Armed Forces; war; invasion; special military operation; denazification; failed blitzkrieg; drawbacks; planning of operation; command and control; logistic support; infrastructure; objectives.*

ASPECTE PRIVIND PREGĂTIREA INVAZIEI

Invazia pe scară largă a Forțelor Armate ale Federației Ruse (Russian Armed Forces - RuAF) în Ucraina, începând cu februarie 2022, a marcat începutul celui mai sângeros conflict armat din Europa din ultimele decenii. După anul 2014, F.Rusă a creat două noi Armate de Arme Întrunite/ A.A.Î. (Combined Arms Armies - CAA), una în Districtul Militar de Vest (a 20-a A.A.Î., cu cartierul general la Voronezh) și una în Districtul Militar de Sud (a 8-a A.A.Î., cu comandamente la Rostov-pe-Don și Novocherkassk), la granița cu Ucraina. Moscova a creat aceste armate pentru a supraveghea, coordona și exercita comanda și controlul unităților dislocate la graniță. De asemenea, Armata a 8-a A.Î. coordonează structurile militarizate din regiunile din estul Ucrainei controlate de F.Rusă, așa-numitele Republici Populare Donețk și Lugansk (The Donetsk People's Republic - DNR și the Luhansk People's Republic - LNR).

Începând cu mijlocul lunii octombrie 2021 şi până la invazia din luna februarie 2022, F.Rusă mobilizase între 150.000 și 190.000 de militari, constituind 120 de grupuri tactice de nivel batalion întărit (Battalion Tactical Group/Batalonnaya Takticheskaya Gruppa - BTG)[1], la granița sa cu Ucraina, în Belarus și în regiunea Crimeea.

Pe timpul acestei mobilizări s-a putut observa dislocarea forţelor armate din toată F.Rusă către Ucraina, astfel: armatele a 41-a și a 2-a A.Î. s-au dislocat din Districtul Militar Central în Belarus și la granița de nord-est a Ucrainei cu F.Rusă; Armatele 1 tancuri de gardă și a 6-a A.Î. s-au

* *Autorul este expert în cadrul Ministerului Apărării Naţionale.*

repoziţionat din Districtul Militar de Vest la granița de est a Ucrainei cu F.Rusă; armatele a 49-a și a 58-a A.Î. s-au dislocat din Districtul Militar de Sud în Crimeea ocupată și la granița de sud-est a Ucrainei cu F.Rusă; iar armatele a 35-a și a 36-a A.Î. (plus elemente din armatele a 29-a și a 5-a A.Î.) au fost redislocate din Districtul Militar de Est în Belarus. Adiţional, F.Rusă a dislocat unități considerate de elită, cum ar fi cele aeropurtate (The Russian Airborne Troops/Vozdushno-Desantnye Voyska - VDV[2]), infanterie marină și Spetsnaz (unități destinate să execute misiuni speciale, de regulă în teritoriul inamicului), în apropierea granițelor Ucrainei.

Structurile militare dislocate au beneficiat de întreaga gamă de capabilități de care dispun forțele ruse, inclusiv artilerie terestră şi artilerie şi rachete antiaeriene. Forțele terestre au fost întărite şi cu sisteme de rachete de precizie cu rază lungă de acțiune, sisteme de rachete balistice cu rază scurtă de acțiune (tip Iskander-M), unități de război electronic, precum şi structuri de sprijin de luptă şi de sprijin logistic[3]. De asemenea, până în februarie 2022, F.Rusă mobilizase un număr mare de escadrile de luptă, bombardiere și elicoptere ale Forțelor Aerospațiale (The Russian Aerospace Forces/Vozdushno-Kosmicheskiye Sily - VKS), despre care unii analiști credeau că vor juca un rol cheie în invazia inițială[4].

În plan politic, pe 21 februarie 2022, președintele rus, Vladimir Putin, a anunțat că țara sa va recunoaște independența DNR/LNR. Apoi, la scurt timp, preşedintele a anunțat că F.Rusă va trimite „acționari ai păcii" în DNR/LNR, susținând că trebuie să se apere împotriva planurilor ucrainene de invazie și tentative de sabotaj.

„OPERAȚIA MILITARĂ SPECIALĂ" A F.RUSE ÎN UCRAINA

La 24 februarie a.c., forţele armate ale F.Ruse au invadat Ucraina sub pretextul desfășurării unei *„operații militare speciale"*, executată cu scopul de a proteja populația civilă și de a *„demilitariza și denazifica"* Ucraina.

Invazia a debutat cu un atac aerian și cu rachete, folosind muniții ghidate de precizie (precision-guided munition - PGM) împotriva țintelor-cheie. Țintele vizate inițial au inclus centre logistice, instalații navale, centre de comandă și control, sisteme de apărare aeriană și antiaeriană și infrastructură critică[5]. În fazele de început ale atacului, forţele armate ale F.Ruse au utilizat peste 100 de rachete balistice cu rază scurtă (SRBM), inclusiv Iskander-M SRBM, și rachete de croazieră lansate de pe mare.

Strategia inițială a forțelor ruse a constat în obținerea superiorităţii aeriene prin distrugerea apărării antiaeriene a forțelor armate ucrainene și subminarea capacităţii acestora de a coordona apărarea și de a executa contraatacuri (distrugerea sistemului de comandă și control – C2). Eșecul acestei strategii a permis forțelor armate ucrainene să răspundă cu mai mult succes la invazia F.Ruse decât se așteptau majoritatea analiștilor, atât în faza de început a războiului, cât și ulterior[6].

După atacul aerian, forțele terestre ale F.Ruse au atacat din mai multe direcții: la nord de Crimeea ocupată, în direcția Herson; incursiuni limitate spre vest din DNR/LNR; dinspre Belgorod și Kursk din F.Rusă, către orașele Ucrainei, Harkiv și Sumi; o forță puternică pe două direcții dinspre Belarus către capitala Kiev.

Kievul a reprezentat, inițial, o țintă militară cheie a forțelor ruse. Conduse de unități aeropurtate (VDV) și Spetsnaz, aceste forțe au avansat de-a lungul părții de vest a Kievului și au ajuns la periferia orașului în câteva zile. La începutul invaziei, unități rusești din forțele aeropurtate au efectuat un atac aerian riscant pentru a ocupa Aeroportul Internațional Antonov din Hostomel, situat la periferia Kievului. Analiștii au susținut că atacul executat de VDV pentru a ocupa aeroportul a fost menit să permită crearea unui cap de pod, însă forțele militare ucrainene au respins atacul, cauzând pierderi grele acestor unități aeropurtate și doborând mai multe elicoptere[7].

Inițial, forțele ruse au obținut victorii pe toate direcțiile de ofensivă, cele mai însemnate progrese înregistrându-se la nord de Crimeea, provocând

Fig. 1: Dispunerea inițială a forțelor armate în Ucraina

pierderi semnificative forțelor armate ucrainene. Victoriile înregistrate s-au datorat faptului că aici au luptat cele mai moderne și profesioniste mari unități din Districtul Militar de Sud, ele beneficiind de un sprijin logistic consistent. În alte regiuni, forțele ruse au înregistrat progrese lente, dar constante, încercând mai degrabă să ocolească, decât să cucerească, centrele urbane majore, cum ar fi Sumi, Harkiv și Cernihiv[8].

Pe de altă parte, forțele ruse s-au confruntat cu o rezistență ucraineană efectivă încă de la începutul invaziei. În ciuda faptului că nu au anunțat o mobilizare generală până pe 25 februarie, după ce a început invazia, forțele armate ucrainene au exploatat numeroasele deficiențe tactice și operaționale ale forțelor ruse, au contraatacat, au executat ambuscade și acțiuni subversive care au produs pierderi acestora în personal și echipament. Trebuie subliniat faptul că un rol semnificativ în îmbunătățirea capacității armatei ucrainene de a se apăra împotriva forțelor ruse l-au deținut informațiile, sistemele de armament și echipamentele defensive și ofensive, activitățile de consiliere și instruire militară furnizate de către țările occidentale.

SCURTĂ ANALIZĂ A OPERAȚIILOR EXECUTATE DE CĂTRE FORȚELE ARMATE ALE F.RUSE. CAUZE ALE UNUI „BLITZKRIEG" EȘUAT

De ce F.Rusă nu a reușit să obțină o victorie rapidă în Ucraina? Forțele armate ruse au înregistrat rezultate slabe, în general, din cauza unui lanț de comandă și control rigid, a lipsei de viziune tactică și de profesionalism a trupelor, comunicațiilor ineficiente, preciziei reduse a sistemelor de armament și sprijinului logistic deficitar, la toate acestea adăugându-se rezistența neașteptată a forțelor armate ucrainene. Occidentul, și nu numai, se aștepta ca forțele ruse să utilizeze echipamente de înaltă tehnologie, trupe profesioniste și linii de aprovizionare eficiente. Însă, examinarea vehiculelor de luptă ruse capturate a scos la iveală dispozitive de comunicații învechite și rații de alimente expirate. Pe de altă parte, forțele armate ucrainene, deși se află într-un dezavantaj cantitativ și calitativ în ceea ce privește personalul, echipamentul și resursele, s-au dovedit mai rezistente și adaptabile,

inclusiv prin utilizarea eficientă a tacticilor de gherilă.

Este posibil ca sistemul de conducere de la Moscova să nu fie conștient de deficiențele forțelor sale armate? Ca și alte state autoritare, F.Rusă nu are o supraveghere guvernamentală independentă asupra forțelor sale armate, acestea raportând direct președintelui. Disfuncționalitatea unui astfel de sistem a dus, în mod clar, la deteriorarea capacităților militare, chiar dacă forțele armate ruse dispun de unul dintre cele mai mari bugete din lume.

O greșeală strategică a F.Ruse a constat în supraestimarea propriilor capacități și subestimarea celor ucrainene. Întregul plan privind Ucraina s-a bazat pe un scenariu principal, care a implicat suprimarea apărării aeriene ucrainene, cucerirea orașelor-cheie și un atac fulger de succes asupra capitalei Kiev. Conducerea militară a forțelor ruse nu a reușit să anticipeze cât de multă rezistență vor întâmpina din partea forțelor armate ale Ucrainei şi a populaţiei locale. În mod similar, F.Rusă a subestimat răspunsul Occidentului: sancțiunile, izolarea economică și proviziile de armament au ajutat Ucraina.

1. Deficienţe privind comanda şi controlul

F.Rusă a susținut în mass-media că a realizat îmbunătățiri în cadrul sistemului de comandă și control al forțelor sale armate și că și-a modernizat securitatea sistemelor de comunicații. Astfel, a fost creat un nou sistem de districte militare cu scopul de a muta centrul de greutate de la nivel de divizie la nivel de brigadă, după exemplul SUA de a utiliza brigada drept principală unitate tactică de manevră. Totodată, au fost reorganizate și brigăzile pentru a putea înființa grupuri tactice de luptă (BTG-uri), unde primul batalion din fiecare brigadă este încadrat cu militari profesioniști, ceea ce îi permite să se desfășoare rapid și, teoretic, să lupte cu profesionalism.

Pe timpul desfășurării războiului, s-a putut, însă, observa că forțele ruse par să aibă probleme cu sistemul de comandă - control (C2) atât la nivel tactic, cât și la nivel operativ. Comandanții structurilor din cadrul forțelor ruse au părut nepregătiți pentru multe aspecte ale războiului, fapt dovedit de lipsa de coordonare între comandamente (cum ar fi VKS și Garda Națională) și mari unități și unități. Comanda și controlul au fost îngreunate de problemele cu sistemele de comunicații, acestea conducând în final la scurtarea normelor tactice și, implicit, la apropierea ofițerilor de rang superior de linia frontului, prin nerespectarea normelor tactice în ceea ce priveşte dispunerea punctelor de comandă. Se pare că această expunere a contribuit la un număr semnificativ de victime în rândul ofițerilor de rang superior şi mediu, ofiţeri care sunt cruciali pentru acțiunile duse la nivel tactic[9].

Un alt aspect demn de luat în considerare este reprezentat de *planificarea dezastruoasă a operaţiei* de invadare a Ucrainei. Planul forțelor armate ruse prevedea atacarea Ucrainei pe șase direcții diferite, ceea ce a condus la împărțirea acestor forțe și, implicit, la diminuarea puterii de lovire. Potrivit analiștilor, forţele ruse au executat operații fără o planificare tactică coerentă și fără să execute operații întrunite[10]. Spre exemplu, unități de elită, dar echipate cu armament ușor de infanterie, cum ar fi VDV și Spetsnaz, au condus operații pentru care nu erau instruite sau echipate, cum ar fi lupta în zonele urbane, unde au suferit pierderi majore, în principal din cauza lipsei de armament și mijloace blindate grele. În plus, în numeroase cazuri, unitățile de blindate au avansat fără sprijin de infanterie[11].

În fazele inițiale ale războiului, forțele ruse păreau că nu introduc în luptă multe dintre sistemele de armamente și structuri tactice pe care le concentraseră înainte de invazie. Analiștii au observat puține dovezi că aceste forțe au utilizat sistemele de război electronic sau sisteme avansate de informații, supraveghere și recunoaștere, cum ar fi sistemele/avioanele de cercetare fără pilot[12].

2. Lipsa superiorității aeriene

Unul dintre cele mai semnificative eșecuri ale F.Ruse a fost incapacitatea de a obține superioritatea aeriană. În termeni militari, acest lucru se referă la situația de a avea un grad de dominație suficient pentru a derula operațiuni aeriene (precum susținerea unităților de la sol sau

lovituri aeriene) fără interferențe semnificative din partea adversarilor și a sistemelor lor de apărare antiaeriană.

Înainte de declanșarea invaziei, exista așteptarea ca forţele ruse să obțină rapid superioritatea aeriană. Acest lucru se datora faptului că, cel puţin pe hârtie, Forțele Aeriene ale F.Ruse erau net superioare celor ucrainene. Înainte de invazie Ucraina avea a șaptea forță aeriană, ca mărime, din Europa, numărul total al aeronavelor ucrainene de toate tipurile (de luptă, sprijin aerian, elicoptere, transport și altele) ridicându-se la 200. Spre comparație, forţele armate ale F.Ruse dispuneau de aproximativ 1.500 de avioane doar din categoria celor de luptă. În plus, majoritatea aeronavelor din componența forțelor armate ucrainene sunt mai vechi, din perioada sovietică, Kievul deținând 50 de avioane MiG-29 și 32 de Su-27. Forțele ruse operează versiuni moderne ale aeronavelor sovietice, precum Su-30, Su-33 și Su-35 (variante modernizate ale Su-27, folosite de Ucraina). Aceste forțe sunt înzestrate, de asemenea, cu avioane de atac la sol moderne, precum Su-34 (o altă variantă a Su-27, optimizat pentru operațiuni de atac la sol) și bombardiere strategice cu rază lungă, precum Tu-22, Tu-95 și Tu-160.

Mass-media occidentale anticipau, cu puțin timp înainte de izbucnirea războiului, că o invazie va începe cu un asalt devastator al forțelor ruse asupra capabilităților aeriene ale Ucrainei. Însă, după trei săptămâni de la izbucnirea conflictului, Ucraina încă dispunea de majoritatea sistemelor sale de apărare aeriană. Acest fapt a ridicat semne de întrebare cu privire la motivul pentru care F.Rusă nu se folosește pe deplin de puterea sa aeriană.

Indiferent care ar fi motivul, lipsa superiorității aeriene a forţelor armate ale F.Ruse în primele stadii ale conflictului ar putea fi una dintre cele mai importante erori strategice care a ajutat forțele armate ucrainene. Avioanele rusești au probleme în a se desfășura în sprijinul necesar forțelor terestre, oferindu-le forțelor ucrainene o cale de a contracara înaintarea F.Ruse.

3. Randamentul discutabil al armamentului forțelor armate ruse

Capabilitățile ofensive de „ultimă generație” ale forțelor ruse au probat un randament dezamăgitor. Fazele inițiale ale invaziei au inclus bombardamente strategice ale unor ținte ucrainene cu rachete de croazieră și rachete balistice cu rază scurtă, de tip Iskander.

Mulți analiști au fost surprinși, în special, de rolul aparent limitat pe care forțele aerospațiale (VKS) l-au jucat la începutul invaziei, dincolo de bombardamentul inițial[13]. Forțele terestre ruse

Fig. 2: Sistemul de rachete balistice Iskander-M

păreau să aibă un sprijin aerian limitat, acțiunile VKS bazându-se, în primul rând, pe SRBM-uri Iskander-M. Forțele ruse au lansat rachete de croazieră mai ales pentru a viza infrastructura ucraineană și ţinte din vestul Ucrainei.

Rapoartele sugerează că, până pe 1 martie, acestea au lansat până la 320 de rachete asupra Ucrainei, majoritatea fiind rachete balistice cu rază scurtă, de tip Iskander. Se estimează că rachetele Iskander au o rază de până la 500 de kilometri și o precizie de 2-5 metri. Înainte de invazie era așteptat ca sistemul de rachete Iskander să se dovedească unul eficace și devastator. Însă, în mod curios, randamentul său a lăsat de dorit. De exemplu, rachetele Iskander au fost folosite pentru atacarea bazelor aeriene ucrainene, distrugerea pistelor de aterizare și împiedicarea Forțelor Aeriene ale Ucrainei să opereze eficace.

Pe măsură ce conflictul a avansat, F.Rusă a început să folosească, tot mai des, sisteme de armament mai puțin performate, precum bombe neghidate și bombe cu dispersie. Acest lucru ar putea arăta fie că forțele armate ruse dispun de un număr limitat de arme de ultimă generație, fie că oficialii militari de la Moscova au decis să le țină în rezervă pentru situația în care conflictul ar escalada.

4. Eșecul trupelor aeropurtate ale F.Ruse

Planul forțelor ruse s-a concentrat pe o acțiune militară surpriză, executată în viteză și cu lovituri precise. Liderii militari de la Moscova și-au imaginat un război care să fie finalizat în 48-72 de ore, după capturarea principalelor centre urbane și administrative ale Ucrainei, iar forțele aeropurtate sunt ideale pentru astfel de misiuni, antrenate și echipate pentru acțiuni în viteză, caracterizate de surpriză și agresivitate. Din această perspectivă, comandanții militari ruși au apelat, în mod firesc, la forțele aeropurtate (VDV) pentru a juca un rol cheie în invazia Ucrainei.

Astfel, unitățile de parașutiști, care se mândresc cu un statut de elită, au fost implicate în invazia din Ucraina încă din prima zi. Regimentul 331 al Gărzilor Aeropurtate a avut misiunea de a captura Aeroportul Internaţional Antonov, din apropierea localității Hostomel, în dimineața zilei de 24 februarie. Cucerirea aeroportului din Hostomel ar fi trebuit să fie unul dintre elementele cheie ale unei operații militare, finalitatea dorită fiind realizarea unui *„cap de pod”* prin care alte trupe ale forțelor ruse să fie desantate imediat și să pornească ofensiva către capitala Kiev.

Misiunea principală a unei forțe aeropurtate ce execută un atac asupra unui aeroport este ca, imediat după ce a preluat controlul asupra acestuia, să extindă perimetrul capului de pod astfel încât forțele de apărare să nu aibă timp să contraatace sau să direcționeze un bombardament al artileriei. Asaltul asupra Aeroportului Internaţional Antonov a început încă de la primele ore ale invaziei, după ce nu mai puțin de 30 de elicoptere au desantat câteva sute de parașutiști pentru a cuceri și menține controlul asupra acestui obiectiv strategic.

Însă, după cum se știe, lucrurile nu au funcționat deloc în conformitate cu planul comandanților militari ruși pentru că forțele armate ucrainene au întreprins repede un contraatac, purtat de trupe speciale și convenționale, care au reușit în doar câteva ore să recucerească aeroportul. Cum forțele armate ucrainene se așteptau la un atac asupra Aeroportului din Hostomel, anterior se pare că blocaseră pistele de aterizare cu echipament greu, mașini și obstacole, prin care au reușit să împiedice aterizarea de avioane de transport cu întăriri.

5. Profesionalismul şi moralul militarilor

În anul 2008, F.Rusă a anunțat cu mândrie trecerea de la o forță bazată pe recruţi la forțe armate profesioniste, cu un corp competent de subofițeri (ceea ce le permite celor mai eficiente armate din lume să funcționeze optim la nivel tactic). Centrul de sociologie al forțelor armate ruse a evidențiat (2014) că mai mult de un sfert din personalul chestionat a raportat că sunt probleme cu echipamentul de infanterie. Un articol din anul 2020, apărut într-o publicație a forțelor ruse, evidenţia un decalaj între implementarea sistemelor militare avansate tehnologic și capacitatea militarilor de a le opera eficient. De asemenea, în același an, comandantul Districtului

Militar de Est, generalul Gennady Valeryevich Zhidko, a deplâns lipsa de ofițeri la nivel de batalion și regiment.

Din relatările mass-media, s-a putut observa că un număr semnificativ de trupe care au invadat Ucraina era format din recruți fără experiență de luptă și educație militară sau din rezerviști (şi nu o forță profesionistă, voluntară, condusă de militari de carieră). Au existat exemple anecdotice de militari ruși care nu erau literalmente conștienți de importanța misiunii lor – unii fiind surprinși să descopere că nu se aflau într-un exercițiu în F.Rusă atunci când au fost capturați de ucraineni. Mediul online este presărat de rapoarte despre militarii ruși aparent blocați în convoaie, părăsindu-şi unitățile, tehnica şi echipamentele. De la începutul invaziei, au existat tensiuni între militarii ruși și comandanții lor. Indisciplina și nerespectarea ordinelor au fost frecvente. Soldații, în conversațiile cu părinții lor, interceptate de serviciile de informații ale Ucrainei, se plâng de lipsa hranei, de sistemele de armament învechite şi de echipamentul de slabă calitate, care nu le asigură protecţie.

La toate acestea se adaugă şi un moral foarte scăzut în rândul militarilor ruși. Pierderea unui general în luptă este un lucru incredibil de rar, însă uciderea mai multor generali poate vorbi despre necesitatea ca ofițerii de top să conducă personal activitățile din teren, un semn potențial al lipsei de încredere în lanțul de comandă.

6. Comunicaţiile şi sistemele de război electronic

Forțele armate ruse au arărat că sunt nepregătite pentru multe alte aspecte critice ale războiului modern, unul dintre acestea fiind reprezentat de faptul că structurile militare angajate în război operează fără comunicații criptate, folosind în schimb, adesea, echipamente civile. Lipsa comunicațiilor criptate a afectat capacitatea forțelor ruse de a-și coordona operațiunile și a permis forţelor armate ucrainene să asculte și să exploateze informațiile interceptate[14].

Informațiile din surse deschise și postările online ale forţelor armate ucrainene sugerează că transmisiile radio între forțele armate ale F.Ruse sunt slabe, ceea ce duce la soluții improvizate, inclusiv utilizarea radioului necriptat de înaltă frecvență pentru comunicații pe distanță lungă și a echipamentelor mobile civile. Există unele dovezi că forțele ruse dislocate au în dotare radiourile tactice R-187P1 Azart[15] și R-168-5UN-2. Bombardiere rusești care au transmis pe frecvențe radio înalte au fost interceptate de amatori pasionați de radio. Operațiile actuale din Ucraina sugerează că F.Rusă nu are în serviciu atât de multe mijloace de comunicaţii moderne, pe cât a susținut, și că este posibil să nu fi apreciat în mod adecvat nevoile sale de comunicare pentru gama și amploarea operațiunilor.

Mijloacele de comunicaţii utilizate de forțele ruse sugerează potențiale slăbiciuni grave. Mijloacele radio tip BaoFeng UV-82HP sunt relativ ușor de exploatat de către structurile de război electronic. În primul rând, lipsa de criptare a comunicaţiilor militare înseamnă că mijloacele radio ar trebui să fie relativ sensibile la bruiaj direct. În al doilea rând, această lipsă a criptării facilitează alimentarea traficului fals în rețele. În același timp, transmisiile de la aceste radiouri ar putea fi relativ ușor de detectat folosind echipamente rudimentare.

Sistemele de război electronic (EW) pe care forțele ruse le au în dotare pot bruia comunicațiile civile V/UHF, inclusiv radiourile bidirecționale și rețelele de telefonie mobilă. Sistemul RB-314V Leer-3 EW desfășurat la nivel operațional/tactic poate viza transmisiile de telefonie mobilă. Transmisiile V/UHF pot fi vizate și de sistemele RP-377U/UA EW pe care forțele ruse le desfășoară la nivel tactic. Slaba lor utilizare pe câmpul de luptă demonstrează, pe de o parte, că un număr insuficient de sisteme de EW au fost dislocate, multe dintre acestea fiind într-o stare precară de funcţionare, iar pe de altă parte, că există temerea că, odată utilizate, locaţia sistemelor va fi descoperită şi, astfel, vor deveni ţinte prioritare pentru forţele armate ucrainene.

Forţele armate ucrainene au ucis (până la jumătatea lunii mai a.c.) doisprezece generali ruși și un număr ridicat de ofiţeri superiori, deoarece

forțele ruse utilizează telefoane mobile civile în încercarea de a asigura C2 la linia frontului. Acest eșec indică faptul că nu au investit suficient în asigurarea de comunicații sigure. Mai mult, forţelor armate ale F.Ruse le-a lipsit capacitatea de coordonare între diferite unități: BTG cu BTG, forțele din prima linie cu forțele de sprijin și de rachete, acestea reprezentând doar câteva dintre zonele în care rușii au avut probleme semnificative.

Starea dificilă a comunicațiilor forțelor ruse reprezintă o oportunitate pentru forțele armate ucrainene. Disciplina slabă în utilizarea mijloacelor de comunicații și lipsa criptării acestora pot fi exploatate de structurile EW ucrainene. În timp ce forțele armate ucrainene pot fi inferioare numeric pe câmpul de luptă, ele au ocazia să fie superioare în spectrul electromagnetic. Prin detectarea și localizarea surselor de transmisii radio, forțele ucrainene pot identifica și angaja inamicul cinetic și/ sau electronic. În același timp, prin utilizarea echipamentelor COMINT, forțele armate ucrainene pot exploata rețelele forțelor ruse pentru culegere de informații și diversiune pe câmpul de luptă.

7. Planificarea deficitară a sprijinului logistic

Unul dintre domeniile majore pe care forțele armate ale F.Ruse trebuiau să le îmbunătăţească, începând cu anul 2008, a fost sprijinul logistic. Evoluția conflictului din Ucraina a evidențiat că acestea întâmpină dificultăți cu reaprovizionarea, astfel încât multe unități mecanizate au rămas pe câmpul de luptă fără combustibil. Lipsa combustibilului duce la lipsa hranei, armamentului şi muniției pentru unitățile din prima linie.

Deși liderii politici și militari de la Moscova au alocat resurse pentru dotarea forţelor armate (*programul de stat 2010-2020, investiții de aproximativ 626 de miliarde de dolari*), o mare parte din acești bani a ajuns, în principal, la oligarhi și siloviki sau la foști oameni din aparatul de securitate rus[16].

F.Rusă a avut la dispoziție o perioadă semnificativă de timp să își pregătească invazia și să asigure sprijinul logistic necesar, masând trupe la granița cu Ucraina timp de luni de zile. Însă scenele de după începerea conflictului, cu convoaie enorme împotmolite, incapabile să înainteze, sugerează o gestionare uluitor de incompetentă din partea comandanților forțelor ruse. Aceste eșecuri ale sprijinului logistic sunt la fel de rușinoase pentru F.Rusă, pe cât sunt de benefice pentru Ucraina.

Generalul Robert Barrow afirma, adesea, că *„amatorii vorbesc despre tactică, profesioniștii studiază logistica”*. A face să ajungă muniția, combustibilul, hrana, căldura, electricitatea și echipamentele de comunicații la trupe este crucial. Imaginea convoiului de tancuri, transportoare blindate și alte mijloace de transport militare, blocat pe o distanță de 64 kilometri în afara Kievului, este un bun exemplu de incompetență – orice armată occidentală modernă ar fi elaborat planuri detaliate pentru a se asigura că o astfel de armată, aflată în ofensivă, nu va staționa zile întregi, în coloană, expusă atacurilor terestre şi aeriene.

Problemele sprijinului logistic al forțelor ruse, sprijin prea limitat pentru a susține ofensive simultane pe mai multe direcţii, au determinat împotmolirea ofensivei ruse. Mai mult, forţele armate ucrainene au atacat cu precădere şi au limitat aprovizionarea forțelor invadatoare din adâncime către linia frontului, organizând atacuri rapide şi ambuscade atât terestru, cât şi aerian (cu drone Bayraktar)[17].

Mediul online abundă în relatări despre tancuri și vehicule blindate ale forțelor ruse care au rămas fără combustibil, punându-i pe soldați în ipostaza de a cere, rechiziționa sau fura carburanți pentru a putea să-și continue înaintarea. O parte dintre militarii ruși a fost nevoită să își procure în mod independent hrana, existând relatări despre unii dintre aceştia care au furat găinile populației ucrainene, iar militari ai forțelor speciale ruse au spart magazine pentru a-și face rezerve de mâncare. De asemenea, au apărut informații potrivit cărora rațiile oferite trupelor rusești ar fi fost suficiente pentru doar câteva zile și au existat imagini online cu rații expirate de ani de zile.

8. Infrastructura deficitară a F.Ruse

F.Rusă și-a redus obiectivele de război în Ucraina, redistribuindu-și forțele pentru a

se concentra asupra regiunii de est – Donbas. O întrebare centrală acum este dacă această schimbare de strategie va ajuta la rezolvarea numeroaselor probleme ale forțelor ruse legate de sprijinul logistic în timp de război.

Având un teritoriu vast, F.Rusă este populată slab și inegal, majoritatea oamenilor fiind concentrată în partea europeană a țării. Geografia sa extinsă și terenul dificil – cu stepă, permafrost și inundații sezoniere – forțează structurile forțelor terestre motorizate să se bazeze pe rețelele feroviare și rutiere pentru a transporta trupe, alimente și combustibil în timp de război și de pace.

Spre deosebire de orice altă armată permanentă, F.Rusă dispune de un serviciu auxiliar, cunoscut sub numele de Trupe de cale ferată (*zheleznodorozhniye voiska*), care protejează și întreține serviciile feroviare pentru a fi utilizate în timpul luptei. Aceste trupe, constituite în 10 brigăzi, sunt în organica districtelor militare și au ca misiuni principale repararea căilor de comunicaţie avariate, construcția sau reconstrucția podurilor și mascarea forțelor armate, însă, secundar, pot furniza combustibil, hrană, echipament, armament şi muniţii pe front. Dependența excesivă de transporturile feroviare pentru desfășurarea de trupe la scară largă pare să fi fost una dintre principalele piedici ale F.Ruse în acest război. În nord, forțele ruse nu au reușit niciodată să controleze unul dintre nodurile feroviare din Cernihiv sau din jurul Kievului, iar condițiile meteorologice au făcut ca numeroase vehicule militare să rămână blocate în noroi. Unele vehicule au fost aparent abandonate, fie pentru că nu au putut fi reparate în mijlocul luptei, fie pentru că nu au vrut să le tracteze la mulți kilometri înapoi în F.Rusă pentru reparații.

Forţele armate ucrainene au cunoscut această vulnerabilitate a forțelor ruse și au atacat convoaiele de camioane care transportau alimente și combustibil. Comunicaţia feroviară dintre F.Rusă şi Ucraina a fost, de asemenea, o ţintă timpurie a războiului: armata ucraineană, conștientă de dependența armatei ruse de rețea, a distrus-o la sfârșitul lunii februarie.

ACȚIUNILE FORȚELOR ARMATE ALE UCRAINEI

Mulți analiști au fost surprinși și impresionați de rezistența militară a forţelor armate ale Ucrainei. În ciuda faptului că are o armată mai redusă decât F.Rusă și un dezavantaj cantitativ și calitativ în ceea ce privește echipamentele și resursele, forţele armate ucrainene s-au dovedit rezistente, adaptabile şi flexibile, în măsură să exploateze pașii greșiți și slăbiciunile forțelor ruse[18]. Totodată, forţele armate ucrainene au beneficiat de un nivel ridicat de motivare și recrutare.

În faza inițială a invaziei, forţele armate ucrainene au cedat spaţii largi, cu scopul de a atrage forțele ruse, dar pe măsură ce acestea au avansat nu au mai fost în măsură să asigure sprijin de luptă şi sprijin logistic adecvat. Forţele armate ucrainene au utilizat tactici specifice luptei de gherilă sau ambuscade pentru a ataca liniile de aprovizionare, a izola, obosi și epuiza forțele armate ruse[19].

De asemenea, forţele armate ale Ucrainei au exploatat inteligent şi eficient sistemele de armament cheie (Bayraktar TB2 – furnizate de Turcia) pentru atacul direct asupra tancurilor şi blindatelor și distrugerea sistemelor de artilerie ruse. La acestea s-au adăugat sistemele de armament portabile (FGM-148 Javelin, FIM-92 Stinger şi Brimstone – furnizate în special de SUA şi M.Britanie), care au fost eficiente în lupta împotriva blindatelor, producând pierderi majore de personal și tehnică. Pe parcursul a opt ani de război în Donbas, forţele armate ucrainene au reuşit să îşi perfecţioneze abilităţile de utilizare a sistemelor de artilerie și a sistemelor de avioane fără pilot. Operând în grupuri mici, greu de descoperit din aer, acestea au atacat forțele ruse, simultan, din mai multe direcţii. Totodată, forţele armate ucrainene au blocat înaintarea inamicului prin distrugerea punctelor obligatorii de trecere, luptând direct cu trupele aeriene, țintind sprijinul logistic și rezistând cu curaj în orașele asediate.

Furnizarea de armament şi fluxul de informaţii de la agențiile de informații occidentale le susțin

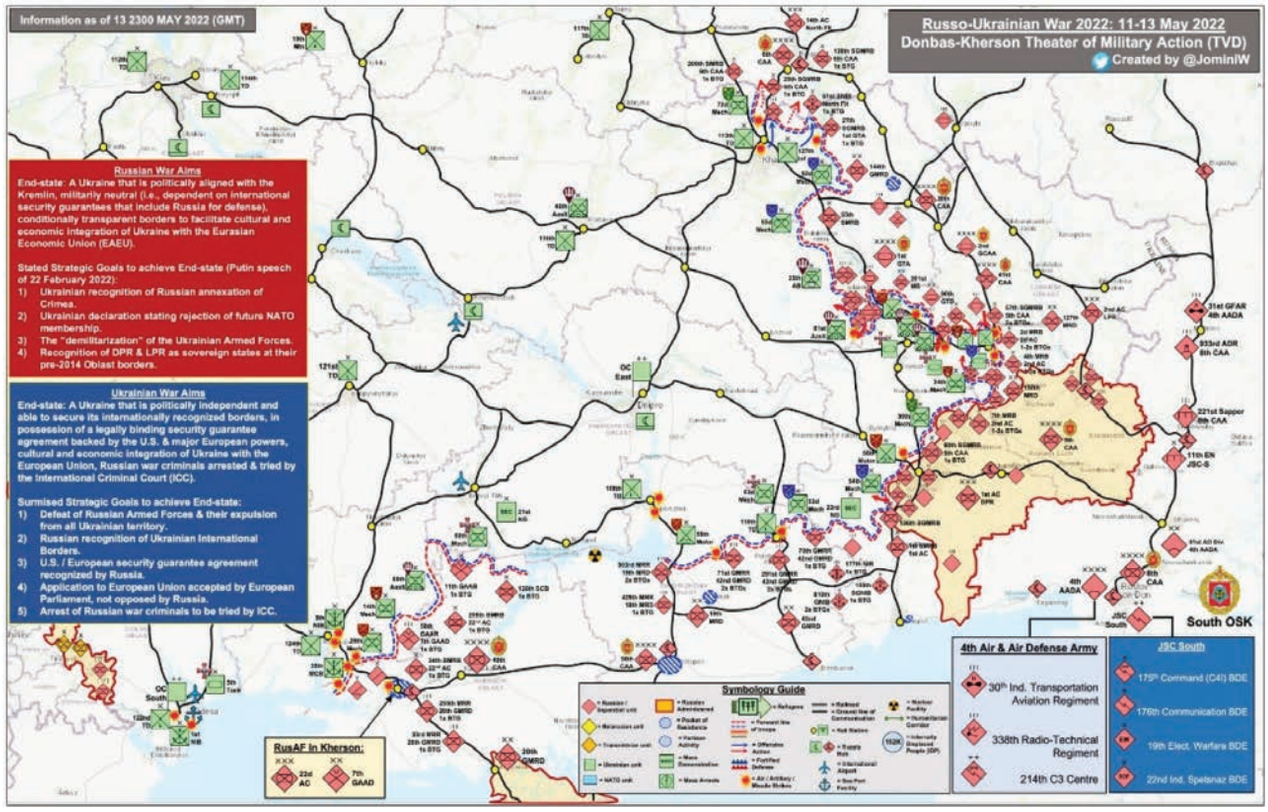


Fig. 3: Dispunerea forţelor armate în Estul şi Sud-Estul Ucrainei (mai 2022)

eforturile. Pe de altă parte, reformele din armata ucraineană, din ultimii ani, își dovedesc acum valoarea. Una dintre cele mai importante schimbări a constat în creșterea rolului subofițerilor, în maniera armatelor NATO. Acest lucru permite/ facilitează transmiterea cunoștințelor și abilităților soldaților. În același timp, armata ucraineană pare să fi adoptat o comandă descentralizată, permițând fiecărei comenzi operaționale să coordoneze și să inițieze operațiunile conform condiţiilor locale. Principiul occidental al *„comenzii misiunii”* a fost adoptat de forțele ucrainene, permițându-le astfel ofițerilor responsabili de unitățile mici să adopte decizii în funcție de dinamica evenimentelor.

Ucraina a fost în măsură să exploateze și potențialul populației civile. În ultimii ani, și-a reformat sistemul de apărare teritorială, încurajând civilii să formeze unități locale de rezistență. Conduse de patriotism și cunoscând câmpul de luptă, unitățile au provocat trupele rusești la fiecare colț, atacând vehicule blindate și liniile de aprovizionare logistică. Un număr substanțial de voluntari civili luptă în forțele cibernetice care apără infrastructura critică a Ucrainei.

REEVALUAREA OBIECTIVELOR FORȚELOR ARMATE ALE F.RUSE

Spre sfârșitul lunii martie a.c., ofensiva forțelor ruse în jurul Kievului a stagnat. Forțele armate ucrainene au lansat multiple contraofensive și au împins forțele invadatoare spre frontiera de nord. Analiștii au remarcat că, după ce nu a reușit să obțină rapid o victorie decisivă, F.Rusă și-a reevaluat obiectivele și strategia pentru obținerea de câștiguri teritoriale în sudul și estul Ucrainei. Astfel, un prim obiectiv reevaluat de către forțele ruse îl reprezintă regenerarea unităților care au suferit pierderi grele de personal și echipamente militare.

Un alt obiectiv probabil îl reprezintă realizarea joncțiunii între forţele ruse care avansează dinspre nord-est (deplasându-se spre sud de la Harkiv) cu unități care se deplasează spre nord dinspre sud şi sud-est. Aici terenul favorizează unităţile de tancuri şi blindate, precum şi mijloacele de artilerie autopropulsată

ale armatei ruse și îngreunează executarea de atacuri de tip gherilă de către forţele armate ucrainene.

În același timp, trebuie remarcat faptul că forțele ruse şi-au intensificat loviturile cu PGM-uri cu rază lungă de acțiune împotriva țintelor din vestul Ucrainei, cu precădere împotriva industriei de apărare ucrainene în încercarea de a o paraliza și de a submina puterea de luptă pe termen lung a armatei ucrainene.

Pe fond, unii analiști[20] s-au întrebat dacă F.Rusă dispune de suficiente efective pentru a-și atinge obiectivele politice și militare, fără o mobilizare națională. Din această perspectivă, în perioada mai-iunie a.c. forțele ruse au continuat să execute bombardamente fără discriminare, utilizând atât aviaţia, cât şi unităţile de rachete.

Pe de altă parte, posibilitatea ca F.Rusă să fie de acord cu o înțelegere politică sau cu încetarea focului este redusă, cu excepția cazului în care consideră că a obținut suficiente câștiguri teritoriale pentru a-și atinge obiectivele revizuite și pentru a prezenta o narațiune victorioasă publicului intern.

BIBLIOGRAFIE

1. BELIAKOVA Polina, ”Russian Military’s Corruption Quagmire”, *Politico.eu*, 8 martie 2022.
2. BORGER Julian, ”The Drone Operators Who Halted Russian Convoy Headed for Kyiv”, *The Guardian*, 28 martie 2022.
3. Congressional Research Service, *Russia’s War in Ukraine: Military and Intelligence Aspects*, 13 aprilie 2022.
4. COOPER Helene, Eric Schmitt, ”Russia’s War Lacks a Battlefield Commander, U.S. Officials Say”, *The New York Times*, 31 martie 2022.
5. GALEOTTI Mark, ”Echoes of Afghanistan in Russian Soldiers’ Poor Discipline in Ukraine”, *Moscow Times*, 1 aprilie 2022.
6. GORDON Michael, Alex Leary, ”Russia, Failing to Achieve Early Victory in Ukraine, Is Seen Shifting to Plan B”, *The Wall Street Journal*, 20 martie 2022.
7. GORDON Michael, Max Rust, ”Russian Buildup near Ukraine Features Potent Weapons Systems, Well-Trained Troops”, *The Wall Street Journal*, 14 februarie 2022.
8. HORTON Alex, Shane Harris, ”Russian Troops’ Tendency to Talk on Unsecured Lines Is Proving Costly”, *The Washington Post*, 27 martie 2022.
9. JUDAH Tim, ”How Kyiv was Saved by Ukrainian Ingenuity as Well as Russian Blunders”, *Financial Times*, 10 aprilie 2022.
10. KOKCHAROV Alex, John Raines, ”Russia Begins „Blitzkrieg” Invasion of Ukraine with Objective of Quick Victory; Intensive Fighting Likely Across Country”, *Janes IHS*, 25 februarie 2022.
11. MARSON James, ”Putin Thought Ukraine Would Fall Quickly”, *The Wall Street Journal*, 3 martie 2022.
12. NEWDICK Thomas, ”A Rundown of Russia’s Arsenal of Artillery That Could Wreak Havoc on Ukraine’s Cities”, *The Drive*, 4 martie 2022.
13. PEREZ-PENA Richard, ”Russia Batters and Encircles Ukrainian Cities, as Diplomacy Falters”, *The New York Times*, 10 martie 2022.
14. RATHBONE John Paul, Roman Olearchyk, Henry Foy, ”Ukraine Uses Guerrilla Counter-Attacks to Take Fight to Russia”, *Financial Times*, 1 aprilie 2022.
15. SCHWARTZ Felicia, Roman Olearchyk, Sam Jones, ”U.S. and Kyiv Warn of New Russian Offensive in Eastern Ukraine”, *Financial Times*, 11 aprilie 2022.
16. STEWART Phil, Idrees Ali, *What Happened to Russia’s Air Force? U.S. Officials, Experts Stumped*, Reuters, 1 martie 2022.

17. STROBEL P.Warren, Michael R. Gordon, ”Biden Administration Altered Rules for Sharing Intelligence with Ukraine”, *The Wall Street Journal*, 8 martie 2022.
18. URBAN Mark, *The Heavy Losses of an Elite Russian Regiment in Ukraine*, BBC, 2 aprilie 2022.
19. US Department of Defense, *Senior Defense Official Holds a Background Briefing*, Press Release, 8 aprilie 2022.
20. WATLING Jack, ”Why the Battle for Donbas Will Be Very Different from the Assault on Kyiv”, *The Guardian*, 9 aprilie 2022.

[1] BTG - reprezintă o unitate de manevră alcătuită, de regulă, dintr-un batalion (2-4 companii de infanterie mecanizată) întărit cu structuri de apărare aeriană, artilerie, geniu și sprijin logistic. De obicei, acestora li se adaugă și o companie de tancuri și una de artilerie și rachete antiaeriene.
[2] Trupele VDV - sunt structuri de elită din cadrul forțelor armate ale F.Ruse, alături de Forțele Strategice de Rachete și Forțele Spațiale Ruse. Acestea includ: parașutiști și forțe de desant aerian.
[3] Michael R. Gordon, Max Rust, ”Russian Buildup near Ukraine Features Potent Weapons Systems, Well-Trained Troops”, *The Wall Street Journal*, 14 februarie 2022.
[4] VKS - s-au înființat la 1 august 2015, prin fuziunea Forțelor Aeriene Ruse (VVS) și a Forțelor Ruse de Apărare Aerospațială (VVKO). Acestea includ forțele aeriene, de apărare aeriană și de apărare spațială.
[5] Alex Kokcharov, John Raines, ”Russia Begins „Blitzkrieg” Invasion of Ukraine with Objective of Quick Victory; Intensive Fighting Likely Across Country”, *Janes IHS*, 25 februarie 2022.
[6] Warren P. Strobel, Michael R. Gordon, ”Biden Administration Altered Rules for Sharing Intelligence with Ukraine”, *The Wall Street Journal*, 8 martie 2022.
[7] James Marson, ”Putin Thought Ukraine Would Fall Quickly. An Airport Battle Proved Him Wrong”, *The Wall Street Journal*, 3 martie 2022.
[8] Richard Perez-Pena, ”Russia Batters and Encircles Ukrainian Cities, as Diplomacy Falters”, *The New York Times*, 10 martie 2022.
[9] Helene Cooper, Eric Schmitt, ”Russia’s War Lacks a Battlefield Commander, U.S. Officials Say”, *The New York Times*, 31 martie 2022.
[10] Mark Galeotti, ”Echoes of Afghanistan in Russian Soldiers’ Poor Discipline in Ukraine”, *Moscow Times*, 1 aprilie 2022.
[11] Mark Urban, The Heavy Losses of an Elite Russian Regiment in Ukraine, BBC, 2 aprilie 2022.
[12] Thomas Newdick, ”A Rundown of Russia’s Arsenal of Artillery That Could Wreak Havoc on Ukraine’s Cities”, *The Drive*, 4 martie 2022.
[13] Phil Stewart, Idrees Ali, What Happened to Russia’s Air Force? U.S. Experts Stumped, Reuters, 1 martie 2022.
[14] Alex Horton, Shane Harris, ”Russian Troops’ Tendency to Talk on Unsecured Lines Is Proving Costly”, *The Washington Post*, 27 martie 2022.
[15] R-187P1 Azart este un SDR tactic digital de a șasea generație, cu criptare încorporată, conceput pentru a oferi forțelor ruse comunicații sigure și rezistente la bruiaj. Funcționează în benzile de frecvență foarte înaltă (VHF)/ultra înaltă frecvență (UHF), are o rază de acțiune de 18 km în comunicații la sol și, în funcție de configurație, poate fi folosit ca stație repetitoare și poate utiliza GLONASS sau GPS pentru a oferi poziționare.
[16] Polina Beliakova, ”Russian Military’s Corruption Quagmire”, *Politico.eu*, 8 martie 2022.
[17] Julian Borger, ”The Drone Operators Who Halted Russian Convoy Headed for Kyiv”, *The Guardian*, 28 martie 2022.
[18] Tim Judah, ”How Kyiv was Saved by Ukr Ingenuity as Well as Russian Blunders”, *Financial Times*, 10 aprilie 2022.
[19] John Paul Rathbone, Roman Olearchyk și Henry Foy, ”Ukraine Uses Guerrilla Counter-Attacks to Take Fight to Russia”, *Financial Times*, 1 aprilie 2022.
[20] US Department of Defense, Senior Defense Official Holds a Background Briefing, Press Release, 8 aprilie 2022.

RĂZBOIUL HIBRID RUS: DE LA ANEXAREA CRIMEII LA CONFLICTUL DIN UCRAINA

*Ștefania-Crina DUMITRESCU**

Abstract

One of the phenomena that marked the first decade of the 21st century is hybrid war. Today we are witnessing a phenomenon that was born, developed and that continues to bring changes to the classic war, without a set of defining characteristics of this new way of fighting, the hybrid war. The phenomenon of war became known with the annexation of Crimea in 2014 by the Russian Federation. After a long period of time in which Russia threatened the international scene in terms of nuclear powers, now it announces a total war and launches a large-scale invasion, the West feeling compelled to react.

Keywords: *hybrid warfare; Russian Federation; Crimea; disinformation; propaganda.*

UNELE CONSIDERAȚII PRIVIND CONCEPTUL DE „RĂZBOI HIBRID”

Agresiunea recentă a Federației Ruse împotriva Ucrainei a reamintit importanța analizei „războiului hibrid”[1]. Cu toate acestea, conceptul de „război hibrid” este pe cât de contestat, pe atât de popular. Când oamenii de știință sau analiștii/practicienii menționează conceptul, aceștia nu afirmă întotdeauna același lucru. Mai mult, definițiile privind „războiul hibrid” adoptate de statele și instituțiile occidentale prezintă diferențe semnificative. Așadar, conceptul de „război hibrid” rămâne încă neînțeles în totalitate.

Pentru a oferi un punct de plecare în căutarea înțelegerii fenomenului, amenințările hibride sunt apreciate ca fiind ,,abilitatea unuia sau mai multor actori de a folosi un amestec de acțiuni (convenționale și neconvenționale) în spațiul de luptă și dincolo de sfera acestuia, cu efecte negative asupra ciclului decizional al adversarului, în scopul atingerii obiectivelor vizate”[2]. Războiul hibrid se referă, în esență, la utilizarea unor metode neconvenționale de război combinate cu mijloacele tradiționale de acțiuni militare.

Simplificând, războiul hibrid implică o interacțiune sau o fuziune a instrumentelor de putere convenționale și neconvenționale, dar și instrumente de subversiune[3]. Aceste instrumente sunt combinate într-o manieră sincronizată pentru a exploata vulnerabilitățile unei ținte/unui adversar și pentru a obține efecte sinergice.

Primele preocupări în legătură cu utilizarea academică a termenului „hibrid” datează din anul 2007, vârful de lance în dezvoltarea conceptului analizat fiind lucrarea publicată de către Frank Hoffman[4], *Conflict în secolul 21. Apariția războaielor hibride*[5]. Studiul expertului american se referea la adaptabilitatea impresionantă a adversarilor SUA, aceștia pregătind și folosind,

* ***Autorul este expert în cadrul Ministerului Apărării Naționale.***

în mod inovator, diferite metode şi capabilităţi asimetrice[6].

Fiind un război modern al secolului 21, războiul hibrid acoperă diverse tipologii care sunt foarte schimbătoare, conform obiectivelor și strategiilor utilizatorilor săi. F.Rusă, ca unul dintre cei mai importanți utilizatori ai formelor de manifestare ale războiului hibrid, promovează propriile sale tipologii hibride. De exemplu, când F.Rusă a inițiat agresiunea împotriva Ucrainei, în 2014, folosind o serie de mijloace non-militare sau clandestine, acoperite de eforturi extinse de dezinformare și însoțite de negare oficială, NATO a început să folosească termenul „hibrid" pentru a descrie ceea ce părea a fi un nou tip de război[7].

Amenințările hibride se pot manifesta sub diverse forme, confruntarea desfășurându-se „în mai multe dimensiuni: 1) politico-diplomatică; 2) economică (prin presiuni economice, restricții comerciale, sancțiuni etc.); 3) informațională (ca război informațional, caracterizat prin recurgerea la propagandă, dezinformare, manipulare, intoxicare etc.); 4) societală, a relațiilor interetnice (prin folosirea unei sau unor minorități dintr-un stat în vederea destabilizării situației; o modalitate vizează crearea de republici autoproclamate, prin încălcarea dreptului internațional, nerecunoscute de comunitatea internațională, cum a fost cazul unor state post-sovietice, unde au fost create și forțe para-militare separatiste); 5) intelligence; 6) informatică (cibernetică – recurgerea la atacuri cibernetice); 7) militară (angajarea forțelor armate)"[8].

ACȚIUNI HIBRIDE ALE FEDERAȚIEI RUSE ÎN CRIMEEA

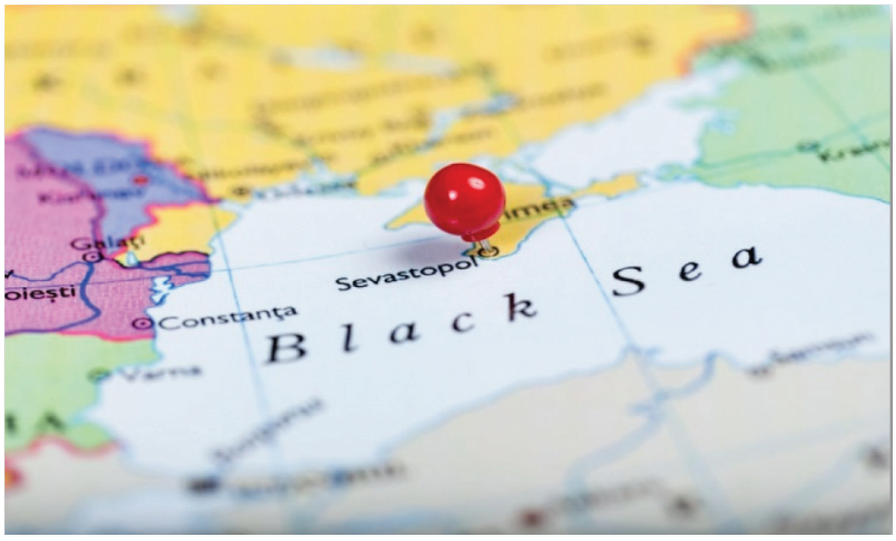
Războiul hibrid include mijloace precum constrângerea economică, dezinformarea și propaganda, utilizarea proxy-urilor sau a războiului cibernetic. Având în vedere numeroasele avantaje pe care le oferă acest tip de război, este de înțeles de ce națiunile aleg astăzi acest curs de acțiune.

„Cea mai serioasă problemă care a stat în faţa Rusiei a constituit-o Ucraina, considerată o lovitură monstruoasă la adresa securităţii Rusiei şi inadmisibilă"[9]. După anexarea Peninsulei Crimeea de către Federația Rusă, în anul 2014, NATO a utilizat termenul de „război hibrid" referindu-se la așa-numita „nouă" formă de conflict derulată de F.Rusă în Ucraina. Fără îndoială, această alegere reprezintă punctul de cotitură în evoluția conceptului de „război hibrid". În primul rând, utilizarea și popularitatea termenului „război hibrid" au crescut dramatic în dezbaterile militare și strategice ale Occidentului. În al doilea rând, deoarece activitățile forțelor ruse în Ucraina nu se potriveau pe deplin conceptualizărilor anterioare ale *războiului hibrid*, sensul acestuia a fost supus din nou unei extinderi conceptuale[10].

Pe scurt, Rusia și-a atins obiectivele politice în Ucraina utilizând un amalgam de instrumente non-cinetice, inclusiv atacuri cibernetice, propagandă, dezinformare, constrângere economică și presiune diplomatică, dar și mijloace militare, cum ar fi desfășurarea de operațiuni clandestine și război proxy. În plus, F.Rusă a negat în mod constant implicarea sa în Ucraina. Așa-numitul „război hibrid" al F.Ruse în Ucraina nu a fost constituit doar dintr-o combinație de elemente regulate și neregulate sau dintr-o combinație de instrumente militare și non-militare, ci a inclus și acțiuni sub acoperire și de inducere în eroare, principalele caracteristici definitorii ale campaniei subversive inițiate de forțele ruse în Ucraina fiind crearea de ambiguitate și a premisei „negării plauzibile"[11].

În acest context, *războiul hibrid* a fost asociat în mare măsură cu așa-numita „doctrină Gherasimov"[12], care subliniază distincțiile dintre război și pace. Ca atare, conceptul de „război hibrid" a fost prezentat, în general, ca fiind caracterizat prin metode cinetice și non-cinetice atât în lucrările academice, cât și în documentele de politică sau de strategie ale instituțiilor occidentale[13].

În cazul invaziei din 2014, nu există nicio îndoială că anexarea Crimeii a fost una dintre cele



mai de succes invazii contemporane. Informațiile ruse au jucat un rol crucial în menținerea discreției realizării planului. Cu soldații amplasați în mod regulat în Crimeea și câțiva voluntari civili sub acoperire, invazia s-a produs pe neobservate. Mai exact, au existat bărbați ruși în uniforme ucrainene care pretindeau a fi polițiști și militari, așa-zișii „omuleți verzi”[14], care aveau rolul de a crea circumstanțele favorabile pentru anexarea Crimeii. După anexare, acești voluntari și „soldați” au ajutat la securizarea bazelor ucrainene. Aceasta a fost o pătrundere secretă, planificată în detaliu, care a accelerat procesul de anexare și a evitat revoltele din partea autorităților ucrainene.

Vladimir Putin, președintele Federației Ruse, a afirmat, în data de 17.04.2014, faptul că „pericolul cel mai mare era acela că populaţia vorbitoare de limbă rusă se simţea ameninţată”, ceea ce i-a determinat pe locuitorii Crimeii să ceară ajutorul Rusiei[15]. Războiul hibrid s-a declanşat după discursul ținut de V.Putin, din data de 21.02.2014, discurs ce privea protejarea compatrioților, surprinzând Ucraina din punct de vedere politic și informațional, inclusiv prin blocarea site-urilor web și a rețelelor ucrainene.

În principal, F.Rusă a vizat Crimeea, Donețk și Luhansk; astfel, după instrucţiunile Kremlinului, au urmat operaţiile stabilite - blocarea unităţilor militare ucrainene sau atacarea acestora, ocuparea infrastructurii Crimeii, controlul clădirilor principale ale regiunii. Nici procedurile legale privind referendumul nu s-au respectat: astfel, în doar două zile, F.Rusă a semnat tratatul de aderare a Crimeii şi a oraşului Sevastopol. După toate acestea, cele două provincii, Luhansk şi Donețk, au fost atacate, în timp ce propaganda rusă a produs o dezinformare totală.

Strategia războiului hibrid a devenit una dintre cele mai folosite tehnici și, în același timp, o formă avansată de ducere a războiului de către F.Rusă, deși aceasta era obișnuită cu războaiele clasice, războaie cu forțe militare, fronturi și o numeroasă tehnică militară.

ACȚIUNI HIBRIDE ALE FEDERAȚIEI RUSE ÎN ACTUALUL CONFLICT DIN UCRAINA

În data de 24 februarie 2022, Federația Rusă a lansat războiul împotriva Ucrainei. Actualul conflict reprezintă o continuare a aceleiași ideologii revanșarde care a condus la evenimentele din 2014, președintele rus încercând să revizuiască ordinea internațională post-Război Rece, dar și să reconfigureze locul F.Ruse în lume. Acesta dorește ca Rusia să fie printre cele mai importante state din punct de vedere geopolitic, însă fiecare pas pe care l-a realizat după 2014 a dus la o izolare accentuată și un declin pe scena internațională. Urmărindu-și orbește obiectivele, regimul lui Putin a trecut de la războiul hibrid, pe care l-a purtat împotriva Ucrainei în perioada 2014-2021, la un război preponderent clasic împotriva vecinului său din vest, începând cu 24 februarie 2022[16].

Moscova a folosit o formă avansată de război hibrid în Ucraina de la începutul anului 2014, care s-a fundamentat, în mare măsură, pe un element de război informațional pe care rușii îl numesc „control reflexiv”[17]. Controlul

Sursa: AP Photo/www.wilsoncenter.org

reflexiv este un concept „unic rusesc" bazat pe *maskirovka*[18], veche noțiune sovietică prin care „se transmit unui oponent informații special pregătite, modelând în mod decisiv percepțiile adversarului asupra situației"[19]. Moscova a folosit această tehnică pentru a convinge SUA și aliații săi europeni să rămână pasivi în fața eforturilor F.Ruse de a perturba Ucraina prin mijloace militare și non-militare.

Războiul informațional al Kremlinului nu reprezintă rezultatul unei inovații teoretice. Toate conceptele de bază și majoritatea tehnicilor au fost dezvoltate de Uniunea Sovietică cu zeci de ani în urmă. Așadar, operațiunile informaționale rusești în Ucraina nu anunță o nouă eră a progreselor teoretice, deși urmăresc să creeze tocmai această impresie. Din această perspectivă, războiul informațional rus reprezintă o provocare semnificativă pentru Occident, dar nu una de neînvins. Obiectivul principal al tehnicilor de control reflexiv pe care Moscova le-a folosit în conflictul din Ucraina a fost acela de a convinge Occidentul să rămână „pe margine", în timp ce forțele ruse s-au desfășurat în Ucraina.

Dezinformarea servește scopului evident de a ascunde obiectivele reale ale Moscovei. Aceasta a permis F.Ruse să nege, de exemplu în 2014, că forțele sale erau prezente în Ucraina, deoarece operațiunile sale de luptă erau ascunse sub o campanie activă de propagandă. De asemenea, creează acoperire diplomatică pentru activitățile militare și de politică externă ale F.Ruse, păstrând astfel libertatea de acțiune a Kremlinului. Campania de dezinformare are rolul de a îngreuna procesul de estimare, de către analiștii militari, a dimensiunii reale a prezenței militare rusești în zona de conflict. Totodată, dezinformarea activă oferă F.Ruse mai multă flexibilitate în alegerea metodelor de exacerbare a conflictului din Ucraina și lărgește spectrul potențialelor soluții diplomatice pe care le poate urmări.

Rezultatele acestor eforturi au fost multiple, Moscova putând să construiască și să extindă propria implicare militară în Ucraina. Pe de altă parte, nu au schimbat fundamental atitudinile occidentale cu privire la acțiunile ruse în Ucraina și nici nu au creat un mediu informațional favorabil Moscovei. Mai presus de toate, F.Rusă nu a reușit până acum să transforme avantajele strategice de război hibrid în succese majore și durabile pe teritoriul Ucrainei.

CONCLUZII

Spre deosebire de războaiele clasice, conflictele armate din era modernă implică actori statali și nestatali care utilizează diverse mijloace de influență și strategii militare. O astfel de situație creează dificultăți în identificarea mijloacelor și strategiilor asociate conflictului. În plus, războiul din secolul XXI este desfășurat cu ajutorul unei abordări hibride. Personalul militar nu reprezintă singura țintă în războiul hibrid, acesta incluzând și civilii, fapt care poate crea instabilitate politică, revolte, dezinformare, influențând rețele sociale și rezultate electorale.

Oricare ar fi motivul, nu există nicio justificare ca o țară să invadeze și să preia o altă țară. Un astfel de act ar trebui să fie condamnat ferm de către toate instituțiile internaționale, iar UE și ONU, precum și alte instituții globale, trebuie să reacționeze decisiv pentru a arăta că lumea internațională nu acceptă un astfel de atac.

---

[1] V. Gherasimov, "The value of Science in the Foresight: New Challanges Demand Rethinking the Forms and Methods of Carrying our Combat Operations", *Vayenno – Pranyshlenyy Kurier*, 2013.

[2] A. Rațiu, *Gestionarea dinamicii conflictelor asimetrice*, Editura Academiei Forțelor Terestre „Nicolae Bălcescu", Sibiu, 2012, p.53.

[3] https://www.ft.com/content/ff95ee3f-a1b8-4a54-9657-6a1aaecc105f, acceast la data de 17.05.2022.

[4] Frank G. Hoffman, *"Conflict in the 21st Century: The Rise of Hybrid Wars"*, Potomac Institute for Policy Studies, Arlington, 2007.

[5] Idem.

[6] https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html, accesat la data de 18.05.2022.

[7] https://cepa.org/west-must-prepare-for-russian-hybrid-warfare/, accesat la data de 18.05.2022.

[8] Frank G. Hoffman, "Hybrid Warfare and Challenges", *Joint Force Quarterly*, 2009, http://ndupress.ndu.edu/,accesat la data de 18.05.2022.

[9] A.Dughin, *Bazele Geopoliticii*, Editura Euroasiatică, București, 2011, p. 235.

[10] https://cepa.org/the-evolution-of-russian-hybrid-warfare-ukraine/, accesat la data de 22.05.2022.

[11] Idem.

[12] https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-25538/, accesat la data de 19.05.2022.

[13] https://www.setav.org/en/report-russias-hybrid-war-in-ukraine-2014-2018/, accesat la data de 19.05.2022.

[14] https://www.bbc.com/news/uk-60745961, accesat la data de 19.05.2022.

[15] https://www.britannica.com/place/Ukraine/The-crisis-in-Crimea-and-eastern-Ukraine, accesat la data de 22.05.2022.

[16] https://www.wilsoncenter.org/blog-post/war-ukraine-beginning-end-putins-russia, accesat la data de 20.05.2022.

[17] M. Mateski, „Russia, Reflexive Control, and the Subtle Art of Red Teaming", *Red Team Journal,* 2016, https://www.redteamjournal.com/, accesat la data de 20.06.2022.

[18] https://georgetownsecuritystudiesreview.org/2017/02/01/disinformation-and-reflexive-control-the-new-cold-war/, accesat la data de 21.05.2022.

[19] M. Mateski, „Russia, Reflexive Control, and the Subtle Art of Red Teaming", *Red Team Journal,* 2016, https://www.redteamjournal.com/, accesat la data de 21.06.2022.

R.MOLDOVA ȘI BOSNIA ȘI HERȚEGOVINA - POSIBILI PIONI DE TIP „PROXY" ÎN STRATEGIA KREMLINULUI DE INTERNAȚIONALIZARE A CONFLICTULUI RUSO-UCRAINEAN?

Florin-Vasile GROZA*

Abstract

After almost three months since the beginning of the so called Russian special military operation in Ukraine, Moscow has started to see its strategical project of conquering Ukraine declining. In February 2022, Kremlin elites assumed that war with Kiev will be more like "a walk in the park" because the Ukrainians would be more than happy to be freed from the "Nazi regime" and will welcome Russian soldiers with "flowers and hugs".

Three months later, the Ukrainians are fighting Russian invaders. Meanwhile, Moscow is facing a huge international pressure that targets financial and energy resources, Putin allies and friends and military leaders involved in atrocities against civilian population from operations areas.

The statements made by the Russian top diplomats leave no doubt about the course Moscow is going to develop in the months to come. But there are questions about how Kremlin is going to act:

- military – generating false flag operations in the south-eastern flank of EU and NATO in order to make the two blocks react? Not very likely. Russian army is barely keeping lines in eastern Ukraine, with soldiers and Wagner mercenaries revolting against unprofessional generals.

- politically – applying disruptive strategies in European countries that are not members of the two alliances EU and NATO in order to destabilize the whole continent? Very likely if the military campaign in Ukraine turns bad for Putin. From the geopolitical point of view, Moldova and Bosnia and Herzegovina are the perfect choices for Kremlin.

Keywords: *Ukraine; Russian Federation; NATO; EU; Bosnia and Herzegovina; Moldova; hybrid warfare; proxy war; regional risks.*

RĂZBOIUL PRIN PROXY – CONSIDERAȚII TEORETICE ȘI ISTORICE

A doua jumătate a secolului XX a marcat o schimbare de paradigmă strategică pentru marii actori internaționali din perspectiva filozofiei de purtare a războiului. Astfel, de la concepția clasică, sintetizată de dictatorul sovietic Iosif Stalin, potrivit căreia fiecare „își impune sistemul până unde ajunge cu armata", aplicată la finalul celui de-al Doilea Război Mondial (concepție care s-a dovedit extrem de costisitoare din punct de vedere uman, material și financiar), s-a trecut la o nouă paradigmă caracterizată de confruntarea

* ***Autorul este expert în cadrul Ministerului Apărării Naţionale.***

prin interpuși/ războiul prin proxy. Schimbarea a fost generată de mai mulți factori militari și politico-economici:

- dezvoltarea și deținerea de capacități nucleare cu destinație militară de către un număr semnificativ de actori (SUA, URSS/F.Rusă, Israel, Franța, Marea Britanie, China, Pakistan, India etc.), care s-au integrat în alianțe cu o volatilă/fluidă geometrie geopolitică;
- costurile tot mai ridicate ale tehnologiilor militare integrate în platformele de luptă (avioane, tancuri, rachete, sateliți etc.), aspect care a impus o abordare de tip contabil (raport cost-beneficiu) a modului de purtare a războiului;
- consolidarea societăților democratice, în care accentul a pivotat pe drepturile omului, concomitent cu apariția unor mișcări anti-război în statele occidentale, mișcări cu un impact mediatic și social semnificativ.

În contextul acestor transformări, competiția globală pentru delimitarea sferelor de influență și proiectarea intereselor geopolitice ale actorilor relevanți a continuat, însă într-o manieră adaptată, neasumată din punct de vedere militar și, de cele mai multe ori, nici politic, definită generic ca războiul/ conflictul prin proxy. Asumarea acestei noi paradigme conflictuale a necesitat și o conceptualizare ideologică și doctrinară. Astfel, o abordare teoretică extrem de sintetică definește războiul prin proxy ca „un conflict armat dintre două state sau actori non-statali care acționează la instigarea sau în numele altor părți care nu sunt implicate direct în ostilități”[1]. Acest tip de conflict este produsul relației dintre un *binefăcător* (stat sau actor non-statal), care nu este implicat direct în dinamica conflictului (ex. război civil), și partenerul local/ intern, care beneficiază de sprijin în armament, pregătire militară, fonduri etc.

O abordare mai exhaustivă din punct de vedere teoretic menționează că „războaiele prin proxy sunt substitutul prin care statele sau alți actori ne-statali încearcă să își proiecteze/ atingă interesele strategice concomitent cu evitarea implicării directe în conflicte sângeroase. Această abordare se bazează pe o percepție intrinsecă a riscului – intervenția directă în conflict ar fi nejustificată, costisitoare (politic, financiar, material), nelegitimă sau nefezabilă”[2].

În consecință, un război proxy este un conflict armat între două sau mai multe entități (state, alianțe sau actori nestatali) care acționează în numele altor părți, care nu sunt direct implicate în ostilități. În opinia unor experți[3], pentru ca un conflict să fie considerat un război proxy acesta trebuie să îndeplinească, cumulativ, câteva condiții:

- manifestarea unei relații conflictuale/ beligerante între două părți cu o relevanță geopolitică redusă, neafiliate unor alianțe militare majore;
- existența unei relații directe, asumate (politic, economic etc.), între actorii externi și părțile beligerante;
- relația să fie de durată, să se manifeste anterior conflictului;
- existența unor interese convergente (politice, financiare, militare, ideologice etc.) între partea beligerantă și statul „sponsor/binefăcător”.

Conceptul nu este unul cu caracter inedit, specific perioadei contemporane, fiind pus în practică pe tot parcursul istoriei umane, din antichitate și până în prezent. Astfel, prima confruntare de anvergură din Antichitate, care a inclus și războiul prin proxy, a fost conflictul dintre două mari imperii: cel roman și cel part. Început în anul 64 î.H (b.C.), războiul dintre cele două forțe ale Antichității (respectiv, succesorii acestora, Imperiul bizantin și cel sasanid) s-a derulat pe parcursul a aproape 7 secole, până în anul 628 d.H. (a.C.), generând confruntări directe, dar și prin intermediul unor state vasale/ clientelare amplasate geografic pe trei continente – Europa, Asia și Africa. Durata conflictului și amplitudinea geografică au generat costuri imense, care au pus bazele unor crize interne puternice, finalizate cu declinul ambelor imperii. De această oportunitate a profitat o nouă forță, Califatul Rashidun (cunoscut și sub numele de Califatul Bine Călăuzit), care a invadat ambele imperii, cucerind teritorii întinse în Orientul Mijlociu, Caucaz, Europa de Est și nordul Africii.

În perioada medievală și modernă, principalele puteri de pe continentul european s-au confruntat prin războaie de tip proxy pe întreg mapamondul - din Orientul Îndepărtat, prin Orientul Mijlociu, Balcani, Africa și până pe continentul american.

Perioada cea mai relevantă, din perspectiva impactului și intensității utilizării în plan global a războiului de tip proxy, a fost intervalul cuprins între finalul celui de-al Doilea Război Mondial și căderea Zidului Berlinului/începutul procesului de dezintegrare a Uniunii Sovietice, în contextul geopolitic denumit generic Războiul Rece. Intensificarea utilizării acestui tip de conflict a fost generată de rațiuni de ordin securitar – ambele puteri globale aflate în confruntare, SUA și URSS, au dezvoltat rapid capabilități nucleare consistente, amplasate pe tot globul (inclusiv pe submarine nucleare) ca parte a conceptului de „surprindere strategică". În consecință, izbucnirea unei confruntări directe între cei doi actori, respectiv alianțele din care făceau parte – NATO și Tratatul de la Varșovia, ar fi adus omenirea în pragul unui cataclism nuclear.

În acest context, ambele puteri globale au ajuns la concluzia că o confruntare clasică, pe teritoriul unor state terțe, cu utilizarea de armament convențional, de mică amploare, era mult mai eficientă din perspectiva raportului resurse utilizate (umane, logistice, financiare) - beneficii obținute (contracararea proiectelor expansioniste, teritoriale sau ideologice, ale adversarului). Deși, din punct de vedere al relațiilor internaționale, ambele superputeri se aflau în situația de pace, a urmat o perioadă de 45 de ani de competiție ideologică, economică și militară acerbă, translatată în războaie și confruntări sângeroase purtate pe patru continente: Europa, Asia, Africa și America Latină. Scriitorul britanic George Orwell a definit această perioadă ca „pacea care nu este pace"[4].

Primele confruntări de tip proxy dintre cele două puteri au avut loc pe continentele european și asiatic (Orientul Mijlociu), imediat după finalizarea ultimei conflagrații mondiale, și au fost generate de anunțul Marii Britanii cu privire la intenția de a se retrage din Grecia și Turcia, state care, conform înțelegerii de la Yalta, intraseră sub tutelă majoritar occidentală. În contextul în care ambele state se confruntau cu o ascensiune violentă a partidelor comuniste finanțate de Moscova, Washingtonul a dezvoltat rapid o nouă concepție de contracarare a expansiunii sovietice, definită generic sub denumirea de „doctrina Truman" și potrivit căreia SUA avea responsabilitatea sprijinirii națiunilor/statelor amenințate de blocul condus de URSS. Această concepție strategică a fost sintetizată într-un discurs susținut (12.03.1947) de către președintele Harry S. Truman în fața Congresului: „politica Statelor Unite trebuie să fie sprijinirea popoarelor libere care rezistă tentativelor de subjugare a minorităților armate sau a presiunilor externe"[5].

În contrapartidă, Moscova s-a implicat activ în susținerea forțelor comuniste combatante în conflictele din Coreea (1950-1953 și 1966-1969) și Vietnam (1961-1975). În cazul conflictelor de pe teritoriul peninsulei coreene, niciuna dintre forțele beligerante nu a putut revendica o victorie clară, aspect care a generat crearea a două entități statale, fiecare sub influența ideologică, politică și militară a uneia dintre marile puteri-sponsor. Respectivul *statu-quo* este de natură a genera și în prezent o situație extrem de tensionată, în contextul în care rolul URSS a fost preluat de R.P. Chineză – o putere globală în ascensiune care contestă tot mai vehement rolul pre-eminent al SUA la nivel mondial.

Rezultatul indecis al competiției globale dintre cele două blocuri politico-ideologice și militare a determinat o extindere a arealului și amplitudinii conflictelor de tip proxy. Astfel, la începutul anilor '60, confruntarea s-a extins și în America Latină, unde au avut loc revoluții și contrarevoluții sângeroase, care afectează și în prezent dinamica geopolitică din zona sudică și centrală a continentului american.

Efectul ambiguu al primelor confruntări de pe continentul asiatic a determinat declanșarea unei noi confruntări, de această dată pe teritoriul Vietnamului. După aproape 15 ani de lupte, partida comunistă susținută de blocul sovietic a câștigat, aspect care a fost greu digerat de către Occident. Oportunitatea unei revanșe a apărut în momentul declanșării (1979) invaziei

sovietice în Afganistan, pentru susținerea regimului comunist de la Kabul. După un deceniu de confruntări sângeroase, care au solicitat la maxim resursele umane și logistice ale Moscovei, luptătorii islamiști/mujahedinii (puternic sprijiniți de către Occidentul condus de Washington) au reușit să determine retragerea forțelor sovietice din Afganistan. Retragerea, similară unei înfrângeri, a marcat începutul declinului pentru Uniunea Sovietică – fenomen care s-a reverberat în întreaga infrastructură comunistă din estul Europei.

Dezintegrarea blocului comunist condus de Moscova a oferit, la finele secolului XX - începutul secolului XXI, o oportunitate strategică pentru Washington și partenerii occidentali. Această oportunitate s-a materializat în derularea rapidă, succesivă (în valuri), a unui proiect integrator ambivalent care a vizat majoritatea statelor foste membre ale Pactului de la Varșovia, respectiv CAER. Astfel, în decurs de aproape 15 ani, state precum Polonia, Ungaria, România, Cehia și Slovacia au devenit membri cu drepturi depline în cadrul celor două alianțe politice, economice și militare occidentale – Uniunea Europeană și NATO.

Inițial, URSS și, apoi, F.Rusă au avut în anii ’90 reacții punctuale, precaute, prin care au încercat să temporizeze/contracareze procesul de afirmare a independenței statelor ex-sovietice, reacții materializate în conflicte scurte, de mică intensitate: de exemplu, războiul din Transnistria (1992). Ulterior, în contextul preluării puterii de către Vladimir Putin, Moscova a intrat într-un proces de revenire graduală din punct de vedere economic și militar. Semnalul acestei reveniri pe tabla geopolitică globală a fost dat de implicarea forțelor Kremlinului în conflictele din Caucaz, apoi în cele din Orientul Mijlociu și în fosta sa zonă de influență – Ucraina și acvatoriul Mării Negre. Invadarea Georgiei, implicarea în conflictul dintre Armenia și Azerbaidjan, precum și în cel din Siria, au demonstrat, într-o manieră lipsită de echivoc, voința Moscovei de a se așeza din nou la masa marilor puteri. Reacția precaută a Occidentului, doar pe componenta politico-diplomatică, a fost interpretată de liderul de la Kremlin ca o negare a relevanței globale a națiunii ruse. În consecință, Moscova a ridicat miza geopolitică, a invadat Crimeea și a precipitat conflictul din Donbas.

Privite retrospectiv, cele două operațiuni militare de tip hibrid au avut rolul unui tester: identificarea nivelului de disponibilitate al Occidentului de a se confrunta cu F.Rusă pe un teritoriu de maxim interes pentru ambii competitori. Alegerea Ucrainei, în 2014, ca spațiu de confruntare nu a fost una aleatorie, Moscova pregătindu-și meticulos (sau, cel puțin, așa a părut) fiecare pas din strategia de provocare a Washingtonului și Bruxellesului:

- profilul geografic al teritoriului ucrainean era extrem de familiar pentru liderii militari ruși;
- infrastructura militară ucraineană era slăbită de corupție și de diluarea calității profesionale a cadrelor de conducere;
- economia de tranziție era, de asemenea, marcată de corupție și de lipsa competitivității/piața rusă fiind în continuare o destinație prioritară a producătorilor ucraineni;
- mediul politic extrem de volatil și fragilizat de implicarea fățișă a unor oligarhi cu puternice conexiuni la Moscova;
- procentul mare de populație rusofonă și/sau rusofilă, localizată preponderent în zona estică, la frontiera ucraineano-rusă;
- lipsa unui proiect integrator în infrastructura europeană sau nord-atlantică, cu etape clare și bine delimitate temporal și procedural.

Mixarea specificităților ucrainene susmenționate cu ingredientele geopolitice ale unei confruntări tot mai dinamice, respectiv criza energetică globală (care a relevat dependența Occidentului de resursele rusești), au generat, recent, contextul apreciat de Moscova ca o fereastră de oportunitate unică pentru revitalizarea ambițiilor hegemonice pe continentul european. Rezultatul a fost declanșarea (24.02.2022) invaziei Ucrainei, acțiune generic definită ca „operațiune militară specială”.

TRANSNISTRIA – OPȚIUNE MILITARĂ SAU „MASKIROVKA“ STRATEGICĂ PENTRU BALCANII DE VEST

După trei luni (februarie-mai) de confruntări militare, Ucraina a continuat să reziste ofensivei ruse, uneori cu rezultate surprinzătoare (mai ales pe zona de operații Nord, Kiev - Harkiv), urmare a unui sprijin logistic, militar, informațional și financiar consistent din partea Occidentului. În aceste condiții, mesajele Kremlinului de natură a justifica războiul împotriva celor pe care anterior lansării invaziei îi numea „frați” (de sânge și întru credință) tind să-și diminueze atractivitatea, inclusiv pe plan intern. De asemenea, sancțiunile economice vor începe treptat să producă efecte economice și sociale negative. Astfel, în perioada aprilie-mai a.c., Vladimir Putin a simțit nevoia identificării unei „supape“ care să îi ofere timp pentru găsirea unor soluții și care să deturneze atenția de la evenimentele de pe teritoriul ucrainean, concomitent cu generarea unei presiuni suplimentare pe Kiev și partenerii occidentali ai Ucrainei. Din această perspectivă, soluțiile au fost limitate:

- amplificarea nivelului de implicare în conflict a forțelor islamiste din Caucaz/ Cecenia; opțiunea este deja valorificată de liderul de la Kremlin, aspect confirmat de intensificarea zborurilor militare dinspre Groznîi spre F.Rusă;
- atragerea Transnistriei, regiune separatistă de pe teritoriul R.Moldova în conflict; dinamica de securitate din respectiva regiune pare să confirme aplicarea unei strategii care să aibă ca finalitate intrarea forțelor militare și de securitate ale Tiraspolului în conflictul ruso-ucrainean, alături de militarii ruși care fac parte din cele două contingente staționate pe teritoriul Autoproclamatei Republici Transnistrene.

(*sursa: www.bbc.com*)

Dintr-o perspectivă istorică, relația Chișinău-Tiraspol a fost, de la momentul conflictului de pe Nistru (1992), una constant tensionată, cu provocări repetate ale liderilor transnistreni la adresa statalității R.Moldova. Situația actuală este rezultatul unui acord de pace, semnat la 29 iulie 1992, de către președinții rus, Boris Elțin, și cel moldovean, Mircea Snegur, după aprox. 5 luni de luptă între rebelii pro-ruși susținuți de Armata a 14-a rusă/sovietică și armata noului stat moldovenesc. În baza acestui document, semnat cu 30 de ani în urmă, F.Rusă și-a asigurat pârghiile necesare exercitării unui control politic și militar consistent asupra tânărului stat de la est de Prut. Deși, în cele trei decenii de la terminarea conflictului, autoritățile de la Chișinău au derulat constant o campanie diplomatică internațională prin care au încercat să determine Moscova să-și retragă trupele de pe teritoriul Transnistriei, acestea nu au reușit atingerea obiectivului strategic. Cu o singură excepție, Summit-ul OSCE de la Istanbul din 1999, când F.Rusă a părut a face o concesie asumându-și obligația de a-și retrage militarii de pe teritoriul R.Moldova, Kremlinul a utilizat frecvent o politică de forță, materializată inclusiv prin constrângeri de ordin economic și energetic, prin care a determinat autoritățile de la Chișinău să accepte perpetuarea, de facto, a prezenței militare ruse. Situația s-a datorat și politicii extrem de precaute a UE și SUA de menajare a relației cu F.Rusă și de acceptare tacită a zonelor de influență rusă din zona sud-estică a Europei.

După preluarea puterii, în urma câștigării alegerilor din 2020, de către actualul președinte, Maia Sandu, și de formațiunile politice de factură pro-occidentală care i-au oferit susținerea, subiectul prezenței trupelor rusești pe teritoriul R.Moldova a fost repus pe masa negocierilor bilaterale. Ca de obicei, Moscova a tergiversat asumarea unei poziții tranșante.

În repetate rânduri, oficiali ruși au declinat solicitările legitime ale Chișinăului. Astfel, cu prilejul unei conferințe de presă (01.12.2020) ministrul rus de externe, Serghei Lavrov, a declarat că poziția R.Moldova „*nu este de natură să ajute la rezolvarea conflictului și nu vom putea accepta aceste solicitări iresponsabile*”. Ulterior (2022), un alt oficial rus, Elena Panina, membru al Comitetului pentru Afaceri Externe al Dumei de Stat, a declarat că „*retragerea trupelor rusești din Transnistria ar genera riscul reaprinderii conflictului moldo-transnistrean*”.

Invazia din Ucraina a oferit retrospectiv și explicația acestei atitudini: Transnistria a reprezentat și reprezintă un obiectiv strategic care permite articularea politicii externe a F.Ruse în zona de sud-est a Europei, un veritabil avanpost amplasat în proximitatea liniei de contact cu UE și NATO. Iar relevanța acestui avanpost pare să crească exponențial în contextul unei evoluții defavorabile Moscovei a războiului cu Kievul. Argumente în favoarea acestei ipoteze sunt furnizate atât de evoluțiile mediului de securitate din Transnistria, cât și de declarațiile recente ale unor înalți oficiali militari și politici ruși.

Referitor la primul aspect, în cursul lunilor aprilie și mai a.c., pe teritoriul Autoproclamatei Republici Transnistrene au avut loc atacuri asupra unor instituții publice, precum și asupra unor elemente de infrastructură, astfel:

- 25.04.2022, Tiraspol – a fost atacat cu armament de infanterie sediul așa-numitului Minister al Securității din Transnistria;
- 26.04.2022, proximitatea localității Majak (aprox. 50 km est de Chișinău), raionul Grigoriopol – au fost aruncate în aer două turnuri ale unui complex de transmisiuni;
- 05.05.2022, proximitatea localității Vărăncău - au fost lansate din dronă 2 dispozitive explozive;
- 07.05.2022, proximitatea localității Vărăncău – au fost executate 4 atacuri cu drone care au lovit un aerodrom nefuncțional din apropierea localității sus-menționate.

Un aspect interesant, care trebuie menționat, este faptul că primele explozii de pe teritoriul transnistrean s-au înregistrat în aceeași zi în care adjunctul ministrului rus de externe, Andrei Rudenko, a declarat că Moscova nu anticipează apariția unor riscuri de natură a duce la escaladarea situației din Transnistria.

Un alt aspect care poate releva existența unei strategii ruse care vizează escaladarea graduală a tensiunilor dintre Chișinău și Tiraspol este și

ordinul prin care ministrul apărării din așa-numita „republică transnistreană“ a ordonat mobilizarea tuturor bărbaților adulți cu vârste cuprinse între 18 și 55 de ani, pretextând că acțiunile Ucrainei în zona de sud sunt de natură a afecta inclusiv stabilitatea republicii transnistrene. Ordinul a fost dat cu 4 zile înaintea primelor incidente de la est de Nistru.

La o primă vedere, implementarea unui scenariu destabilizator în R.Moldova ar facilita deschiderea de către F.Rusă a unui nou front împotriva Ucrainei, care ar fi susținut de trupele rusești dislocate în Transnistria. Acestea ar putea fi implicate într-o ofensivă pe direcția est/sud-est, cu obiectivul Odesa. Practic, apariția trupelor rusești din Transnistria în proximitatea celui mai important port ucrainean ar genera o presiune suplimentară pentru armata ucraineană. Iar faptul că Moscova ia în calcul *„opțiunea transnistreană”* a fost exprimat de un general rus, Rustam Minnekaiev, care a menționat că „un control asupra sudului Ucrainei ar deschide o cale către Transnistria, unde sunt cazuri de opresiune a populației vorbitoare de limbă rusă”. Declarația oficialului militar rus este în deplină conformitate cu misiunea asumată public de președintele rus, Vladimir Putin, *„de a proteja toți etnicii ruși din spațiul ex-sovietic”*. Și R.Moldova a făcut parte din URSS.

Cu toate acestea, evaluarea obiectivă a premiselor unei strategii de implicare a trupelor rusești din autoproclamata „republică transnistreană“ indică un potențial redus de materializare:

- trupele rusești au un efectiv de 1500 – 2000 de militari, dotați cu echipament preponderent din perioada sovietică;
- armata ucraineană și-a concentrat forțe semnificative în zona Odesei, care este un obiectiv strategic major; acestea sunt înzestrate cu armament modern și au o bună pregătire de luptă;
- direcția de ofensivă est/sud-est implică tranzitarea unei părți a teritoriului ucrainean care a fost pregătit, din perspectiva infrastructurii, cu rol defensiv în scenariul implicării trupelor din Transnistria;
- F.Rusă menține interesul pentru cucerirea întregului litoral sudic al Ucrainei.

În consecință, strategia rusă poate viza prioritar scenariul unei destabilizări interne a R.Moldova, prin crearea de confruntări între susținătorii Chișinăului și cei ai Tiraspolului, respectiv Moscovei. Testarea acestui scenariu a avut loc cu prilejul manifestărilor din data de 9 mai a.c., când s-a încercat generarea unor conflicte între susținătorii partidelor de opoziție, rusofoni și rusofili, și câțiva reprezentanți ai formațiunilor de la putere, pro-europene. Scenariul pare că a fost dejucat, aspect ce determină o întrebare legitimă: în contextul în care Moscova deține pârghii semnificative în R.Moldova, care este explicația lipsei de eficiență a strategiei de destabilizare internă? O variantă de răspuns ar fi intenția Moscovei de a distrage atenția Occidentului de la o altă zonă din sud-estul Europei, cu un potențial exploziv mult mai mare: Balcanii de Vest.

ÎN LOC DE CONCLUZIE - BALCANII DE VEST ȘI REPETAREA ISTORIEI?

În Europa, secolul XX a început și s-a terminat în mirosul prafului de pușcă și în zgomotul armelor care au înroșit regiunea Balcanilor. De la războaiele din 1912-1913, care au deschis ușa unui secol sângeros, și până la conflictul din Kosovo, care a tras cortina peste una dintre cele mai dramatice perioade ale continentului european, spațiul balcanic a demonstrat că sintagma de *„butoiul cu pulbere al Europei”* este bine meritată. Cu toate acestea, Occidentul, în general, și Europa, în particular, par să nu fi învățat lecțiile istoriei recente: Balcanii par să ocupe, în continuare, un loc secundar pe lista de priorități geopolitice ale Washingtonului și Bruxellesului, proiectele integratoare ale UE și NATO adresate statelor din sud-estul Europei fiind formulate într-o manieră generică, neconformă cu realitățile regiunii în ansamblul ei.

Contextul a fost speculat de F.Rusă, care, cu resurse financiare puține, dar cu o strategie ofensivă, a reușit să se ancoreze puternic în spațiul balcanic, mizând preponderent pe

Harta Bosniei și Herțegovinei

două repere: ideologia panslavistă și religia ortodoxă. Recentele manifestații de susținere a acțiunilor militare ale F.Ruse în Ucraina, desfășurate la Belgrad și în Banja Luka (capitala R.Srpska/ Bosnia și Herțegovina), au evidențiat amplitudinea influenței Moscovei în spațiul balcanic, în special în teritoriile locuite de sârbi. Dintre acestea, entitatea sârbă/Republika Srpska din Bosnia și Herțegovina pare a fi candidatul perfect pentru generarea unui conflict de tip proxy, care să readucă în prim-plan un alt concept atașat Balcanilor, acela de *„pântecele moale al Europei”*.

Practic, la aproape 30 de ani de la terminarea războiului interetnic și interconfesional care a implicat toate cele trei etnii – sârbi, bosniaci și croați, Bosnia și Herțegovina pare că se regăsește într-o postură periculos de similară cu momentul 1992:

- o infrastructură administrativă pe criterii etnice, nefuncțională la nivel central și cu prerogativele uzurpate de autoritățile entităților;
- o dinamică economică bazată strict pe consum și finanțată din creditare și ajutoare internaționale, respectiv cele trimise de emigrație;
- structuri de securitate cu un grad scăzut de coeziune și un nivel aproape inexistent de interoperabilitate;
- formațiuni politice locale și centrale dezvoltate și consolidate exclusiv pe criterii etnice și religioase;
- o frustrare majoră la nivelul b-croaților, care nu se regăsesc într-o infrastructură administrativ-teritorială similară cu cele ale b-sârbilor și bosniecilor.

Cel mai recent argument în favoarea ipotezei potrivit căreia Moscova cunoaște la nivel de detaliu și exploatează aceste vulnerabilități este oferit de structura discursului politic al reprezentanților b-croați, respectiv al unor înalți oficiali de la Zagreb. Astfel, Dragan Covic, lider al comunității croate din Bosnia și Hețegovina, a afirmat public că „nu este suficientă influență rusă în Bosnia”. Ulterior, președintele Croației, Zoran

Milanovic, a declarat că se opune candidaturii Ucrainei la NATO, pe care a definit-o drept „una dintre cele mai corupte țări din Europa”.

Evident că reacția Rusiei nu a întârziat să apară, sub forma unor declarații de sprijin a demersurilor b-croate pentru modificarea legii electorale din Bosnia și Herțegovina, demers care va crea o serie de avantaje reprezentanților b-croați în zonele locuite majoritar de această comunitate și care este de natură a amplifica tensiunile interetnice, pe fondul unor frustrări manifeste ale etnicilor bosniaci. Dacă la aceste premise adăugăm demersul F.Ruse de creare a unui consulat la Banja Luka și intensificarea discursului de tip secesionist al membrului sârb al președinției tripartite de la nivelul Bosniei și Herțegovina, Milorad Dodik, putem creiona rapid un scenariu cu un potențial conflictual ridicat pe teritoriul bosniac, care în mod evident va fi util Moscovei. Și o Moscovă încolțită în Ucraina va valorifica, în mod cert, această oportunitate.

BIBLIOGRAFIE

1. BLAKEMORE Erin, ”What was the cold war – and are we headed to another one?”, nationalgeographic.com (23.03.2022).
2. BROWN Garrett W., Iain McLean and Alistair McMillan, *A Concise Oxford Dictionary of Politics and International Relations* (4 ed.), Oxford University Press, 2018.
3. LINDLEY-FRENCH Julian, Putin`s Ground Truth?, https://lindleyfrench.blogspot.com/2022/05/putins-ground-truth.html.
4. OSMANCZYK Jan Edmund, Anthony Mango, *Encyclopedia of the United Nations and International Agreements*, Abingdon, Routledge Books, 2002.
5. The National Archives, *Our documents:100 milestone documents from the National Archives*, Oxford University Press, Washington DC, 2006.

[1] Jan Edmund Osmanczyk, *Encyclopedia of the United Nations and International Agreements*, Abingdon, Routledge Books, 2002.
[2] Garrett W Brown, Iain McLean, and Alistair McMillan, *A Concise Oxford Dictionary of Politics and International Relations* (4 ed.), Oxford University Press, 2018.
[3] Daniel L. Byman – Senior Fellow/ Center for Middle East Policy, Washington DC.
[4] Erin Blakemore, ”What was the cold war – and are we headed to another one?”, nationalgeographic.com (23.03.2022).
[5] The National Archives, *Our documents:100 milestone documents from the National Archives*, Oxford University Press, 2006.

R.P. CHINEZĂ - LIDERUL UNEI NOI ORDINI MONDIALE?

Dragoș-Ștefan COCIȘ*

Abstract

Being one of the largest countries in Asia, China has continually struggled, both internally and externally, to become an important player on the world stage. The ascension to power of the Chinese Communist Party in 1921 marked a turning point of the way China tried to assert itself. Despite numerous struggles, China has developed slowly, reaching a point, in the XXI century, when it has finally been able to impose its own agenda both regionally and globally.

Keywords: *China; Chinese Communist Party; Taiwan; Tibet; Xinjiang; Inner Mongolia; world order.*

Motto:

"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."

Sun Tzu - The Art of War

CONTEXT

Având o istorie de peste 4000 de ani, China este una dintre puținele țări care au înflorit economic și cultural încă din primele etape ale civilizației. Mai impresionant este faptul că o bună parte din dezvoltarea culturală a Chinei s-a realizat cu o mică influență din exterior, singura excepție notabilă fiind reprezentată de introducerea Budismului, ajuns în spațiul chinez din India. Chiar și momentul marilor invazii Manchu a influențat într-o mică măsură cultura chineză, populațiile migratoare fiind absorbite în cultura Han.

Această izolare față de lumea exterioară a făcut posibilă înflorirea culturii chineze, însă, pe de altă parte, a lăsat China nepregătită în raport cu celelalte țări din emisfera vestică, superioare din punct de vedere tehnologic, începând cu a doua jumătate a secolului XIX. O consecință directă a acestui aspect a fost inabilitatea Chinei de a preveni și a răspunde expansionismului țărilor din emisfera vestică, țări aflate în superioritate tehnologică. Trauma reprezentată de această serie de evenimente din a doua jumătate a secolului al XIX-lea a devenit catalizatorul revoluției chineze de la începutul secolului al XX-lea împotriva vechiului establishment politic,

* ***Autorul este expert în cadrul Ministerului Apărării Naţionale.***

revoluție ce a culminat cu instalarea unui guvern comunist în anul 1949. Evenimentul continuă să producă reverberații la nivel global, modificând situația geopolitică din zonă și propulsând actuala R.P. Chineză în rândul celor mai influente țări din lume.

Încă de la înființarea Partidului Comunist Chinez, în anul 1921, liderii acestuia au avut convingerea că supraviețuirea și succesul statului chinez vor depinde, în mod intrinsec, de înțelegerea acelor țări și culturi care au capacitatea reală de a-l anihila, principalul competitor pe scena internațională fiind Statele Unite. Prin urmare, unul dintre obiectivele politicii externe definite de aceștia a fost studierea și înțelegerea acestor țări.

În contrast cu această orientare, elitele politice americane, cu câteva excepții notabile, până relativ recent, nu au acordat importanța necesară înțelegerii acelor factori care determină și ghidează politicile internaționale ale Chinei. Astfel, în timp, înțelegerea culturii chineze a devenit importantă pentru interesele naționale americane, însă foarte puțini americani au privit acest aspect ca esențial și, cu atât mai puțin, existențial. De exemplu, în a doua jumătate a secolului XX importanța relației SUA - R.P. Chineză a fost umbrită de competiția strategică dintre cele două superputeri (SUA și URSS) și de crizele multiple din Orientul Mijlociu. Toate acestea par să se schimbe odată cu începutul secolului al XXI-lea când, ca urmare a schimbărilor politice, economice și strategice, China s-a transformat dintr-un partener într-un competitor strategic pentru Statele Unite. Spre deosebire de această schimbare de viziune relativ recentă, liderii chinezi au manifestat de mult timp un așa-numit „realism strategic” în relația cu Washingtonul, înțelegând și admițând limitările colaborării strategice și economice cu SUA.

EVOLUȚII ALE RELAȚIEI SINO-AMERICANE ÎN SECOLUL XX

La începutul secolului al XX-lea, definindu-se drept putere anticolonială, Statele Unite au încercat să își creeze în China o imagine deosebită față de cea pe care o aveau europenii. Cu toate acestea, în ciuda faptului că guvernele americane

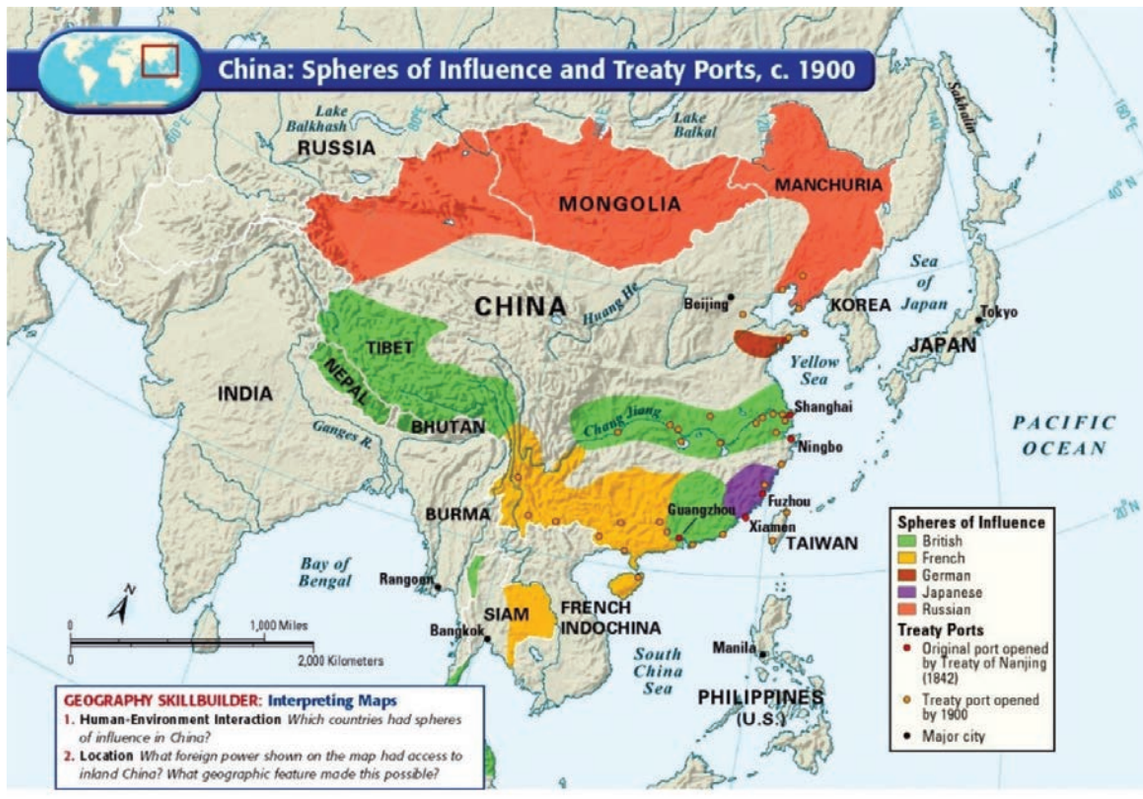


Fig. 1. Hartă cu concesiunile străine în China, în anul 1900 (http://wwww.endofempire.asia/wp-content/uploads/2015/11/0818.18.jpg)

protestau în mod regulat împotriva abuzurilor colonialiste la care se dedau puterile europene, emisarii SUA insistau asupra faptului că cetățenii americani trebuie să primească un tratament egal cu cetățenii celorlalte națiuni prezente pe teritoriul chinez. Mai mult decât atât, în timpul Rebeliunii Boxerilor din 1900, Statele Unite au trimis trupe alături de celelalte națiuni europene pentru a înăbuși revolta și pentru a proteja legațiile străine aflate pe teritoriul Chinei.

Odată cu înfrângerea Germaniei, la finalul Primului Război Mondial, președintele american Woodrow Wilson și-a anunțat programul intitulat „Cele paisprezece puncte”[1], în cadrul Conferinței de pace de la Paris. Unul dintre aceste puncte făcea referire și la dreptul popoarelor la autodeterminare, aspect care l-a transformat pe Woodrow Wilson în erou la nivelul opiniei publice chineze. Folosindu-se de nou-definitul drept la autodeterminare, patrioții chinezi au crezut că, în cele din urmă, vor putea să recupereze regiunea Qingdao și alte părți ocupate de Germania, zone în care cetățenii chinezi au fost priviți și tratați ca cetățeni de rangul al doilea.

Cu toate acestea, respingerea pretențiilor Chinei (în cadrul întâlnirii dintre Woodrow Wilson, David Lloyd George - primul ministru britanic și Georges Clemenceau - primul ministru francez) și decizia președintelui american de a ceda Japoniei provincia chineză Shandong au stârnit un val de furie în China. Principalul beneficiar politic al tratatului de pace a fost nou-formatul guvern bolșevic de la Moscova, Lenin refuzând să participe la conferința de pace și să semneze vreun tratat. De altfel, noul guvern sovietic a renunțat, în mod unilateral, la toate pretențiile teritoriale ale Rusiei în China, atrăgând imediat simpatia noilor partide politice care și-au făcut apariția pe scena politică chineză.

Spre deosebire de sprijinul primit de la Moscova, apelul lui Sun Yat-sen (primul președinte al nou-înființatei republici chineze) către președintele Warren Harding, în 1921, de a sprijini republica Chineză în cel mai critic moment al existenței sale, a rămas fără niciun răspuns. Dacă înainte Sun privise democrația americană drept model pentru dezvoltarea politică viitoare a Chinei, acum se afla în impas: singura țară către care se putea îndrepta pentru a cere sprijin era Rusia. Prin urmare a trimis la Moscova o delegație condusă de adjunctul său, Chiang Kai-shek, pentru a solicita sprijin. Astfel a început o competiție între Moscova și Washington în exercitarea influenței asupra liderilor chinezi, competiție ce avea să dureze mai bine de o sută de ani.

De-a lungul următorilor treizeci de ani, în perioada cuprinsă între semnarea Tratatului de la Versailles și proclamarea Republicii Populare Chineze (în 1949), viitorul Chinei a fost modelat de trei mari puteri: Japonia, SUA și Uniunea Sovietică. Invaziile Japoniei din 1931 și 1937 au pus în imposibilitate guvernul lui Chiang Kai-shek să modernizeze economia chineză și să demareze reforme sociale sau să facă tranziția către instituții liberal-democratice. În tot acest timp, Uniunea Sovietică și-a continuat relațiile politice și operaționale atât cu Kuomintangul, cât și cu Partidul Comunist Chinez.

Rivalitatea strategică dintre Washington și Beijing va continua până la momentul „deschiderii” față de R.P. Chineză promovate de Richard Nixon[2] și de Henry Kissinger, în anul 1971, relaxare sprijinită și de „diplomația de ping-pong”[3] promovată de Zhou Enlai (ministrul chinez al afacerilor externe) și de răspunsul pozitiv al lui Mao Zedong. Această schimbare radicală a fost generată și de deteriorarea rapidă a relațiilor sino-ruse, care își avea originea în denunțarea crimelor lui Stalin de către Nikita Hrușciov, în 1956, aspect care l-a înfuriat pe Mao Zedong.

Deschiderea față de Statele Unite a fost, prin urmare, o reacție la noile realități politice și economice din R.P. Chineză – realități generate, în foarte mare măsură, de consecințele economice și sociale ale „Marelui pas înainte” și ale Revoluției Culturale, dar și de noua realitate strategică în relația cu Uniunea Sovietică. Nimic din această deschidere nu a fost însă legat de reevaluarea valorilor liberale și democratice de către Partidul Comunist Chinez. Normalizarea diplomatică a relațiilor dintre cele două țări s-a realizat, în cele din urmă, în 1979, la șapte ani de la „Comunicatul din Shanghai”, principala divergență dintre cele două națiuni rămânând, pe mai departe, statutul insulei Taiwan. În legătură cu aceasta, SUA insista, pe mai departe, la renunțarea din partea statului chinez la

utilizarea forței pentru a determina reunificarea insulei cu China continentală. În același timp, administrația de la Washington semna o convenție ce promitea asistență militară Taiwanului, în cazul unei agresiuni chineze.

O urmare directă a normalizării relațiilor diplomatice a fost și acordarea de către Statele Unite a statutului „națiunii celei mai favorizate", ce permitea R.P. Chineze să aibă relații de schimb cu SUA la același nivel pe care aceasta le avea cu celelalte țări aliate din lume, ceea ce a însemnat acces direct la tehnologia, piețele și capitalul american. În acest mod a început marșul R.P. Chineze spre modernizare și dezvoltare economică. În plus, jucând „cartea Chinei", administrația de la Washington a avut un permanent atu în relația cu Uniunea Sovietică.

În pofida tuturor acestor considerente, Partidul Comunist Chinez considera noua relație cu SUA ca fiind doar o soluție temporară până în momentul în care Uniunea Sovietică nu ar mai reprezenta o amenințare directă pentru securitatea chineză și până când R.P. Chineză reușea să își consolideze economia națională și puterea militară. Contrar acestei viziuni pur pragmatice, Statele Unite nutreau aspirații mai profunde în ceea ce privea deschiderea Chinei, văzând în aceasta potențialul unei noi piețe pentru exporturile și investițiile americane, ceea ce ar fi favorizat tranziția treptată a acesteia către o economie de piață și ar fi pus bazele formării unei societăți libere.

Cu toate acestea, în decada imediat următoare normalizării diplomatice, tensiunile profunde ale relației dintre cele două țări începeau să iasă din nou la suprafață. Relația politică din această perioadă a rămas una fragilă, Partidul Comunist Chinez încercând, în permanență, să limiteze efectele pe care deschiderea către cultura occidentală le avea asupra studenților și intelectualilor din China. Astfel, expuși la o gamă largă de idei liberale, mulți dintre aceștia puneau sub semnul întrebării diversele aspecte ale ideologiei marxist-leniniste și ale partidului unic. Pe de altă parte, chiar și după „momentul Tiananmen" (aprilie-iunie 1989), sancțiunile americane, în măsura în care acestea au fost aplicate, au fost doar temporare, importanța relației economice și strategice cu Beijingul, dar și utilitatea acesteia împotriva Uniunii Sovietice și perspectiva unei piețe de desfacere în continuă creștere în R.P. Chineză, prevalând asupra celorlalte considerente.

Prăbușirea Uniunii Sovietice în 1991 a modificat în mod fundamental peisajul strategic al R.P. Chineze. În timp ce, din punct de vedere ideologic și politic, Partidul Comunist Chinez era oripilat de implozia comunismului de tip sovietic, fără ca americanii să fi lansat o singură bombă asupra Moscovei, colapsul Uniunii Sovietice a îndepărtat principala amenințare pe termen lung la adresa securității naționale a Chinei și, în același timp, a eliminat și principala motivație a normalizării și dezvoltării relațiilor dintre R.P. Chineză și Statele Unite. De fapt, apropierea dintre Beijing și Moscova începuse cu câțiva ani mai devreme, fiind declanșată de teama liderilor chinezi că vor crea o dependență excesivă față de Statele Unite, în special în ceea ce privește modernizarea forțelor armate. În plus, sancțiunile americane asupra exportului de tehnologie chineză, în domeniul nuclear și balistic, către țări precum Iran, Pakistan și Coreea de Nord au atras furia Beijingului, foarte interesat în sporirea veniturilor din exporturi. Mai mult decât atât, odată cu aplanarea tensiunilor dintre Beijing și Moscova, după 1991, liderii de la Kremlin s-au arătat din nou interesați să furnizeze echipamente militare forțelor armate chineze, fabricile de armament din F.Rusă fiind disperate după comenzi.

În acest timp, relația strategică dintre Washington și Beijing s-a deteriorat constant, atingând cel mai de jos nivel în anul 1996, când forțele chineze au lansat rachete în apele din jurul insulei Taiwan, în efortul de a descuraja alegerea pe cale democratică a candidaților taiwanezi în al căror program electoral apărea proclamarea independenței față de R.P. Chineză. Al doilea incident a avut loc în 1999, în timpul conflictului din Balcani, când cinci rachete ghidate au lovit ambasada chineză din Belgrad, omorând trei jurnaliști chinezi. Această realiniere strategică treptată a avut un impact profund asupra traiectoriei relației dintre R.P. Chineză și Statele Unite. Treptat, liderii partidului comunist chinez au concluzionat că existau mai multe puncte

comune cu F.Rusă decât cu Statele Unite, în pofida investițiilor și schimburilor comerciale și culturale dintre cele două țări.

Faptul că majoritatea administrațiilor americane de după cea a președintelui Nixon nu au privit relația cu R.P. Chineză din aceeași perspectivă pragmatică, precum liderii Partidului Comunist Chinez, nu era neapărat un semn de naivitate, ci era în concordanță cu opinia conform căreia creșterea nivelului de trai va crea, în timp, o clasă de mijloc solidă care va avea propria voce politică. Potrivit aceleiași opinii, în timp, democratizarea R.P. Chineze ar fi trebuit să determine administrația de la Beijing să accepte și să participe la implementarea ordinii internaționale liberale promovate de Statele Unite. În afara de aceasta, exista și speranța că, dacă vreodată R.P. Chineză va depăși puterea economică a Statelor Unite, la fel cum acestea din urmă au depășit puterea economică a Regatului Unit cu un secol înainte, tranziția va fi una pașnică, în baza valorilor comune care stau la baza ordinii mondiale globale[4].

Din multe puncte de vedere, criza actuală dintre Statele Unite și R.P. Chineză își are originea tocmai în aceste așteptări diferite între cele două părți: Beijingul a privit relația doar din punct de vedere tranzacțional, ca o metodă de a-și îmbunătăți securitatea și prosperitatea națională, în timp ce Washingtonul a privit relația ca fiind una transformațională, având obiectivul și posibilitatea de a schimba, în mod fundamental, natura Chinei comuniste.

OBIECTIVE ACTUALE ALE LIDERILOR CHINEZI

1. Asigurarea prosperității economice

Una dintre prioritățile importante ale liderilor chinezi este asigurarea prosperității economice, aflată în corelație directă cu stabilitatea politică. Misiunea declarată a Partidului Comunist Chinez este de a elimina sărăcia, de a crește standardul de trai la nivel național și de a spori veniturile guvernului, astfel încât să acopere cheltuielile cu educația, sănătatea și pensiile. În afară de acestea, un alt obiectiv prioritar îl reprezintă transformarea R.P. Chineze în lider global în știință și tehnologie și modernizarea forțelor armate. Creșterea economică susținută, undeva între cinci și șase procente anual, este, prin urmare, esențială pentru atingerea acestor obiective de bază[5].

Creșterea nivelului de trai și îmbunătățirea calității vieții sunt o componentă esențială a efortului de a păstra legitimitatea politică în era post-Mao. Acesta este, de fapt, și acordul nescris dintre partid și populație: aceasta va continua să tolereze un sistem politic autoritar atât timp cât nivelul de trai va continua să se îmbunătățească, Xi Jinping înțelegând foarte bine legătura directă dintre continuarea păstrării prosperității publice și prezența sa la cârma statului.

În ceea ce privește asigurarea prosperității economice, președintele chinez se confruntă, în prezent, cu mai multe provocări interconectate și care, uneori, intră în conflict unele cu altele: să mențină rata de dezvoltare economică atât de necesară creșterii nivelului de trai; să mențină un echilibru optim între stat și piață, fără a ceda noii generații de antreprenori controlul politic asupra pieței; să se asigure de reducerea inegalităților economice la nivel societal; să impună noi limitări privind emisiile de carbon, conform noii realități a schimbărilor climatice și să echilibreze presiunile economice din exterior, în special asupra comerțului, investițiilor și tehnologiei.

Pentru gestionarea acestor provocări și a potențialelor oportunități, economia R.P. Chineze a trecut prin trei etape distincte, aflându-se deja, în prezent, în cea de-a patra etapă[6]. Liderul chinez este convins de faptul că noua politică economică va fi suficientă pentru transformarea țării într-o superputere la nivel mondial, capabilă să iasă învingătoare din competiția cu Statele Unite ale Americii. Întrebarea cea mai importantă, care rămâne în discuție, totuși, este dacă toate aceste soluții impuse de la vârf și dacă obsesia lui Xi Jinping pentru control politic vor deveni o povară și nu un factor de creștere pentru dezvoltarea economică viitoare.

2. Asigurarea unității naționale

În ceea ce privește chestiunea unității naționale, putem identifica mai multe direcții de acțiune. Astfel, pe de o parte, se află problema Taiwanului, care ocupă zona centrală a

intereselor chineze, iar pe de altă parte, subiecte de preocupare sunt și provinciile Tibet, Xinjiang și Mongolia Interioară.

În problema Taiwanului, după criza din strâmtoarea Taiwan de la mijlocul anilor '90, predecesorii lui Xi Jinping au adoptat o politică de reunificare politică, prin crearea unei dependențe economice față de R.P. Chineză[7] și, ulterior, prin absorbție politică. Această politică de convergență a celor două economii într-una singură și de atragere a investițiilor din Taiwan în China continentală a avut câteva rezultate pozitive, însă este privită de administrația actuală de la Beijing ca fiind mult prea lentă. Strategia de absorbție economică graduală a avut un regres vizibil în anul 2019, atunci când guvernul de la Beijing a introdus un proiect de lege privind extrădarea și care a slăbit vizibil autonomia legală a Hong Kong-ului, conform modelului „*o țară, două sisteme*"[8]. Mișcările de protest din Hong Kong și, mai ales, represiunea brutală a acestora de către poliție a influențat și mai mult susținerea internă a modelului „*o țară, două sisteme*" de către Taiwan, orice încercare a unui posibil acord politic cu R.P. Chineză fiind acum sortită eșecului. Prin urmare, Xi Jinping a fost convins că modelul gradual a eșuat, percepție care a fost întărită și de refuzul președintelui taiwanez, Tsai Ing-wen, de a accepta formularea „*o singură China*" ca bază a continuării negocierilor dintre cele două părți[9]. Înfuriat și de afirmația lui Tsai potrivit căreia, în urma protestelor pro-democrație din Hong Kong, Taiwanului îi este imposibil să accepte vreodată modelul „*o țară, două sisteme*"[10], Xi Jinping a reafirmat public faptul că R.P. Chineză este pregătită să recurgă la toate mijloacele necesare, fără a exclude forța armată, în vederea reunificării[11].

În plan politic, oficialitățile de la Beijing s-au lansat într-o adevărată ofensivă diplomatică cu unicul scop de a reduce suplimentar numărul, și așa mic, de parteneri diplomatici ai Taiwanului. În același timp, relevante sunt și acuzațiile care i se aduc R.P. Chineze de interferență electronică asupra proceselor electorale din Taiwan și de declanșare a unei campanii susținute de dezinformare în presa din Taiwan[12].

Separat de statutul Taiwanului, problema centrală în accepțiunea liderilor chinezi, rămâne chestiunea provinciilor Tibet, Xinjiang și Mongolia Interioară. Fiecare dintre acestea reprezintă un cumul de factori de risc interni și externi pentru autoritățile chineze. Provincia Tibet, cândva sursa principală de tulburări sociale pentru R.P. Chineză, a fost pacificată prin folosirea unui set de măsuri dure de securitate, de implementare a unor tehnologii sofisticate de supraveghere și de politici de asimilare culturală. În prezent, provincia deține un rol strategic în relația cu India, luând în considerare atât faptul că aceasta din urmă l-a găzduit pe liderul tibetan exilat, cât și conflictele continue dintre cele două țări de la granița din Himalaya.

În ciuda stabilirii graniței comune ruso-chineze acum câteva decade în urmă, regiunea Mongolia Interioară reprezintă, de asemenea, o sursă de anxietate în relația dintre R.P. Chineză și F.Rusă, cele două state fiind în competiție, timp de secole, pentru influență în această regiune. În ciuda avantajelor economice și demografice, prezența etnicilor mongoli de-a lungul graniței chineze este un alt motiv de îngrijorare pentru Beijing. În vederea eliminării oricărui risc separatist, oficialii chinezi au derulat în regiune ample programe de impunere a culturii și limbii chineze.

Regiunea autonomă uigură Xinjiang este cea care a făcut obiectul celor mai severe măsuri de securitate, intrând astfel în atenția opiniei publice internaționale. Regiunea Xinjiang („*Noua frontieră*" în mandarină) reprezintă poarta de intrare a ceea ce R.P. Chineză definește ca fiind lumea ostilă a islamului din zona Asiei și a Orientului Mijlociu. Ideea de graniță cu această „lume ostilă" este accentuată și de îngrijorările, din ce în ce mai mari, privind pericolul separatist reprezentat de populația islamică locală, populație ce a încercat, în repetate rânduri de-a lungul istoriei, să își obțină independența față de China. Numeroasele tentative de obținere a independenței au inclus și acțiuni teroriste împotriva populației majoritare Han, atât în diferite regiuni ale Chinei, cât și în regiunea Xinjiang (inclusiv un atentat chiar în momentul când Xi Jinping era prezent în zonă), acțiuni

care i-au înfuriat pe liderii chinezi. Începând cu anul 2016, în regiunea Xinjiang a început implementarea unor noi măsuri de securitate dure, inclusiv prin instalarea de echipamente digitale avansate de recunoaștere facială și prin utilizarea unor „centre educaționale" în vederea controlării „grupurilor cheie" ale comunității locale.

Considerate împreună, Tibetul, Mongolia Interioară, regiunea Xinjiang, Hong Kong și Taiwan reprezintă, din perspectiva Beijingului, provocări majore la adresa unității naționale a R.P. Chineze. Însă, spre deosebire de predecesorii săi, Xi Jinping a adoptat o linie mult mai dură cu privire la acestea, considerând că imperativele securității naționale sunt mult mai importante decât costurile legate de imaginea și reputația regimului. Președintele chinez consideră, de asemenea, că restul mapamondului depinde acum de economia chineză într-o măsură atât de mare încât orice reacții politice internaționale, ca măsuri de răspuns la ceea ce se întâmplă în R.P. Chineză, vor fi doar superficiale, simbolice și cu caracter temporar. De altfel, conducerea de la Beijing încă își amintește că toate sancțiunile internaționale politice și economice la care a fost supusă R.P. Chineză după „momentul Tiananmen", din 1989, au dispărut treptat pe măsură ce Occidentul a realizat că putea realiza profituri în relația cu statul chinez.

3. Asigurarea supremației navale

De-a lungul ultimilor 180 de ani, cele mai mari amenințări la adresa securității naționale a Chinei au venit de pe mare. Astfel, în timpul primului și al celui de-al doilea război al opiului, China a fost atacată de către Franța și de către Marea Britanie dinspre mare. Tot dinspre mare, Japonia a lansat

Fig.2. Pretențiile teritoriale ale Chinei în Marea Chinei de Sud (https://en.m.wikipedia.org/wiki/Territorial_disputes-in-the-South-China-Sea)

o serie de campanii militare de succes între anii 1895 și 1945. Și, nu în ultimul rând, tot marea, dominată de forțele navale americane timp de zeci de ani, a împiedicat China comunistă să reanexeze Taiwanul. Nu este, prin urmare, surprinzător faptul ca zona maritimă aflată în estul Chinei este privită ca o zonă cu potențial ostil.

Din acest motiv, o componentă critică a programului președintelui chinez Xi Jinping este asigurarea supremației navale și, pe cât posibil, împingerea forțelor navale aparținând țărilor cu potențial ostil (în special Statele Unite) dincolo de arhipelagul Japoniei. Abilitatea americanilor de a-și mobiliza forțele militare în Oceanul Pacific este mult îmbunătățită tocmai de poziționarea acestor baze militare partenere. Prin urmare, R.P. Chineză și-a stabilit ca obiectiv strategic fracturarea alianțelor Statelor Unite în regiune pe cât de mult posibil, plecând de la raționamentul conform căruia Statele Unite, fără aliați, ar fi considerabil slăbite în zona Pacificului, tocmai acești aliați fiind cei care îi conferă un avantaj strategic extraordinar.

Elementul cheie al strategiei R.P. Chineze în vederea protejării periferiei sale maritime este tocmai expansiunea rapidă a capabilităților sale militare aeriene și navale, sprijinite de sisteme terestre de apărare și de implementarea unor sisteme performante de război electronic.

În plus, R.P. Chineză și-a folosit puterea economică și diplomatică împotriva acelor state care s-au dovedit a fi recalcitrante față de interesele declarate ale autorităților de la Beijing, limitându-le acestora accesul la piața internă (sau, în cazuri extreme, interferând cu activele acestora sau chiar arestându-le, sub diverse pretexte, cetățenii aflați pe teritoriul chinez) și transformându-le astfel, în accepțiunea chineză, în avertismente cu privire la prețul care va fi plătit de acele state care vor interfera sau se vor opune intereselor Beijingului. În același timp, liderii chinezi au încercat să recompenseze acele state care resping cooperarea politică cu Statele Unite.

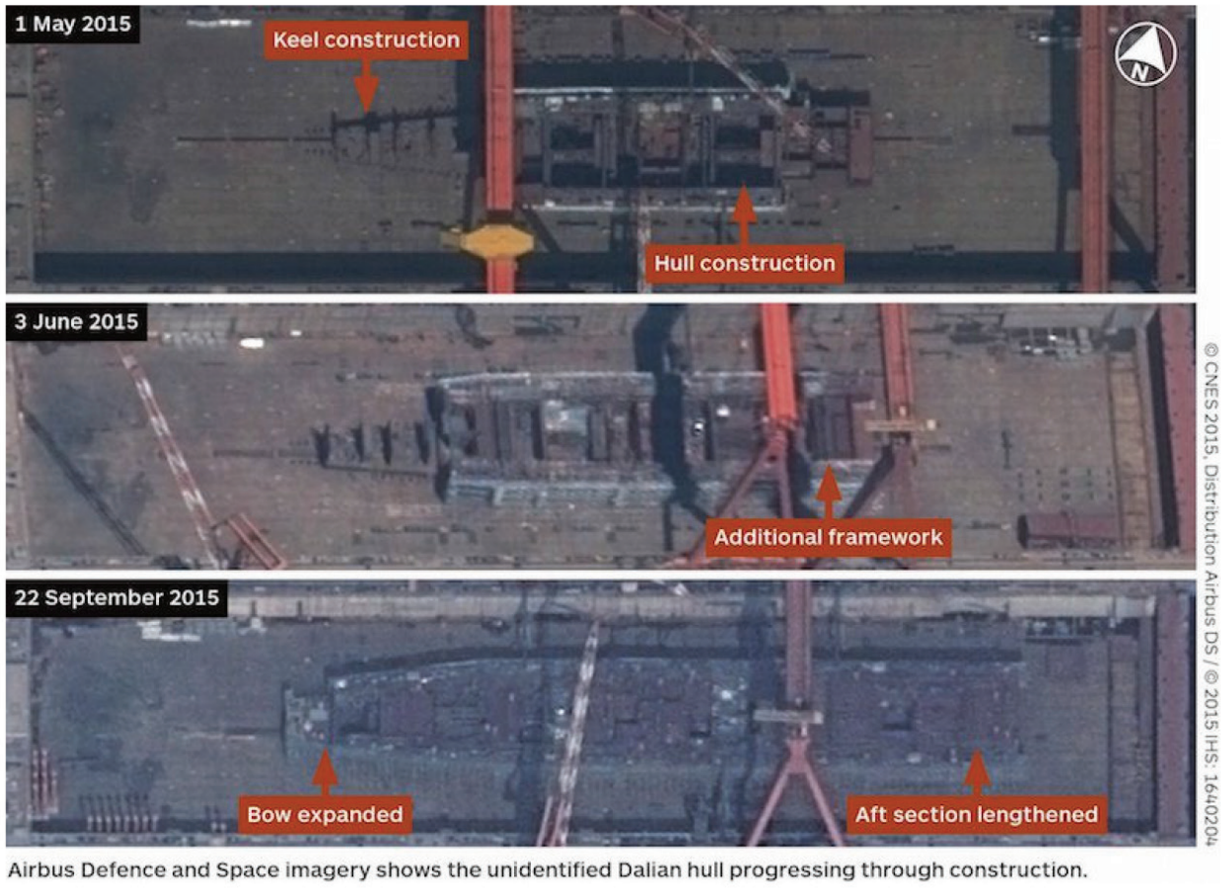


Fig.3.Imagini din satelit cu construcția primului portavion chinez (https://gcaptain.com/sattelite-images-may-show-chinas-first-domestically-built-aircraft-carrier)

4. Creșterea influenței comerciale

Un alt element cheie în consolidarea puterii internaționale a R.P. Chineze este creșterea sferei de influență economică. Pentru a-și atinge acest obiectiv, Beijingul s-a folosit de mai multe instrumente instituționale, precum Organizația de Cooperare de la Shanghai (SCO) sau de Conferința pentru măsuri de interacțiune și de creștere a încrederii în Asia (CICA). Cu toate acestea, principala măsură avută în vedere de R.P. Chineză este inițiativa „*Centura și drumul*"[13] (BRI) care include atât o componentă terestră - traseul trans-eurasiatic, cât și o componentă maritimă ce traversează Oceanul Indian, Marea Roșie și ajunge în Marea Mediterană. Inițiativa BRI încearcă să realizeze mai multe obiective în același timp. Pe de o parte, încearcă să îmbunătățească schimburile comerciale cu Europa și cu Orientul Mijlociu, asigurând astfel un climat strategic prietenos pentru R.P. Chineză și stabilizând zona centrală și zona sudică a Asiei (zone preponderent islamice). Pe de altă parte, liderii chinezi speră, de asemenea, să își asigure noi piețe în vederea atenuării consecințelor unei posibile excluderi viitoare din oportunitățile economice oferite de Statele Unite și de aliații acestora.

În ciuda criticilor, cel mai adesea întemeiate, privind capcanele BRI, de la proiecte construite defectuos, la nerespectarea standardelor de mediu, exploatarea forței de muncă locale, lipsa transparenței și adevărate capcane ale datoriilor țărilor partenere, inițiativa a fost adesea binevenită în multe zone emergente. De multe ori, BRI și instituțiile asociate acestei inițiative sunt singurele facilități de finanțare disponibile în multe țări, aspect luat în considerare de acestea, indiferent de câte probleme ar putea pune programele de împrumut oferite de Beijing. Astfel, realitatea este că singurul program, în contrapondere cu BRI, lansat de Administrația Trump (program numit *The Build Act*[14]) era în valoare de 100 miliarde USD, în timp ce BRI finanțase până în 2021 aproximativ 2600 proiecte în 100 de țări, cu un cost de 3,7 trilioane USD[15].

Din punctul de vedere al relației sale cu Europa, R.P. Chineză a privit de mult timp această legătură doar din perspectiva practică a

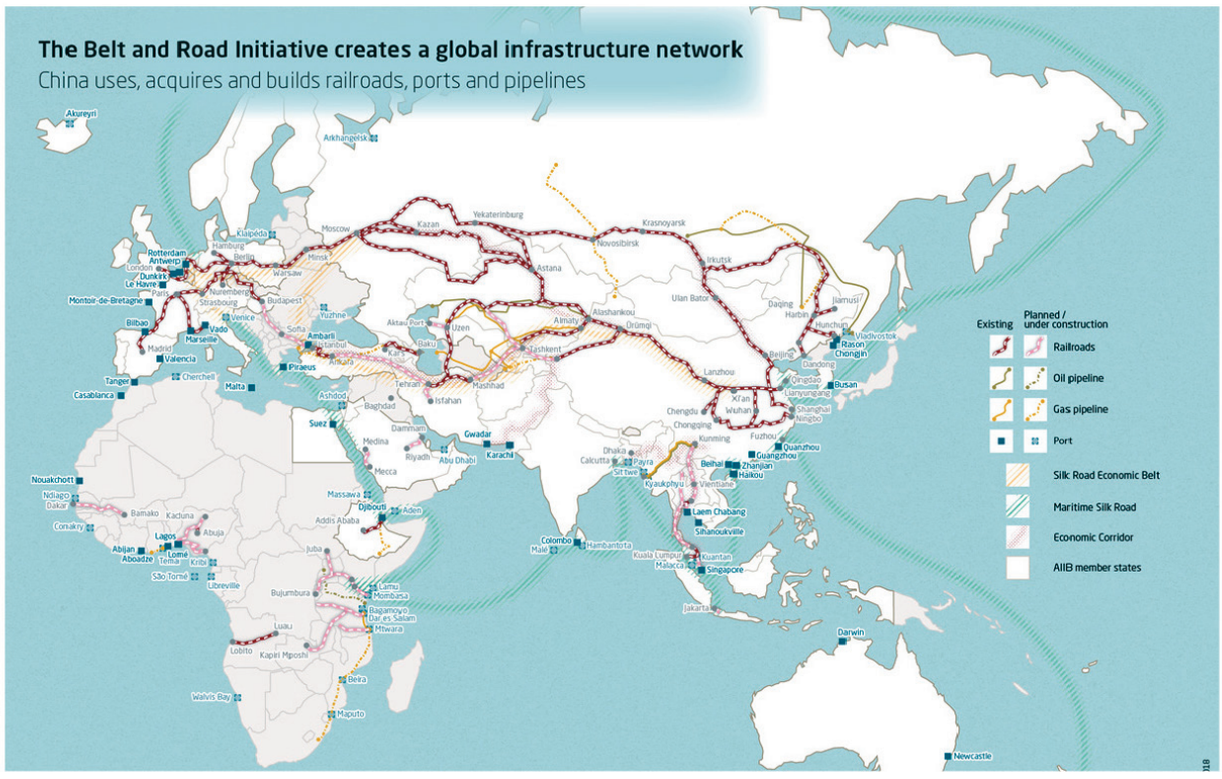


Fig.4. Inițiativa „Centura și drumul" (https://metrics.org/tracker/mapping-belt-and-road-initiative-where-we-stand)

oportunităților economice. Recunoscând faptul că la nivelul continentului european există multe puncte de vedere divergente legate de relația cu statul chinez, liderii de la Beijing au preferat să se concentreze pe statele europene mici, adică acolo unde influența chineză poate fi mai mare. În plus, prin cultivarea acestui tip de relații, R.P. Chineză a încercat să fractureze unitatea UE și NATO cu privire la chestiuni cheie legate de statul chinez. Administrația de la Beijing recunoaște importanța celor trei state europene mari: Germania, Franța și Marea Britanie, nu numai datorită influenței individuale globale a acestora, cât și datorită faptului că Berlinul, Parisul și, până mai recent, Londra, au jucat un rol important în conturarea pozițiilor adoptate de Bruxelles.

Dintre cele trei țări importante pentru politica externă a R.P. Chineze, Germania ocupă cea mai importantă poziție, datorită puterii economice, a stabilității politice și a influenței pe care o are la nivel european - influență care se observă și din simpla numire a fostului ministru al apărării german, Ursula von der Leyen, în funcția de președinte al Comisiei Europene în anul 2020.

R.P. Chineză percepe Europa ca singura entitate globală cu o potență economică și un grad de sofisticare tehnologică similare cu ale Statelor Unite. Însă, în timp ce ușile cooperării cu Statele Unite au fost închise, acestea sunt în continuare deschise în relația cu Uniunea Europeană. Pe de altă parte, liderii chinezi au identificat corect faptul că principiile universale ale respectării drepturilor omului sunt considerente centrale ale identității europene, Uniunea Europeană fiind, în viziunea Beijingului, cel mai mare apărător la nivel global al drepturilor omului. Acest rol a plasat Uniunea Europeană într-o poziție foarte problematică pentru autoritățile chineze, prin punerea sub semnul întrebării de către UE a politicilor interne și internaționale ale Partidului Comunist Chinez. Prin urmare, aplanarea criticilor UE cu privire la drepturile omului ar reprezenta o victorie majoră în lupta ideologică a PC chinez împotriva liberalismului politic, luptă care își are originile acum mai bine de o sută de ani, încă din primele zile ale înființării partidului.

În termeni economici agregați, comerțul este punctul forte al R.P. Chineze în relația cu Uniunea Europeană. În pofida unor tensiuni apărute relativ recent la acest capitol, inclusiv datorită refuzului Beijingului de a permite economiilor europene acces la piețele din spațiul chinez, Uniunea Europeană este cel mai mare partener comercial al R.P. Chineze începând din 2019, în urma războiului comercial sino-american. Astfel, în timp ce schimburile comerciale dintre R.P. Chineză și Statele Unite au scăzut la 419 miliarde USD[16], schimburile cu Uniunea Europeană au crescut la 437 miliarde USD[17].

Cu toate acestea, îngrijorările europenilor sunt, pe mai departe, legate de echitatea politicilor economice și de investiții ale R.P. Chineze. Din acest punct de vedere, obiecțiile Uniunii Europene sunt, în mare măsură, similare cu cele ale Statelor Unite, statele membre UE demarând instituirea unui regim mult mai restrictiv privind accesul pe piața europeană a societăților chineze deținute sau subvenționate de stat. Implementarea acestor măsuri a atins punctul culminant în martie 2019, atunci când Consiliul Europei a recomandat statelor membre să impună noi restricții cu privire la investițiile chineze în infrastructura-cheie sau în tehnologii de ultimă generație, în special în acele tehnologii care aveau acces la datele cu caracter personal ale cetățenilor europeni și la informații cheie pentru menținerea pluralismului politic în Europa[18] (a se vedea și cazul Huawei).

Relațiile bilaterale din ce în ce mai strânse dintre R.P. Chineză și F.Rusă reprezintă un alt motiv de îngrijorare al Uniunii Europene în legătură cu rolul din ce în ce mai mare pe care Beijingul este dispus să și-l asume la nivel mondial. Astfel, exercițiile navale comune ale forțelor ruse și chineze din 2017 în Marea Mediterană și în Marea Baltică[19], prezentate de media chineză ca o mulțumire față de solidaritatea arătată de Moscova în timpul exercițiilor chineze din anul 2016 din Marea Chinei de Sud, au sporit motivele de îngrijorare ale europenilor. Luând în considerare toate aceste aspecte și, în special, cooperarea din ce în ce mai strânsă cu Moscova, guvernele statelor europene au concluzionat că, în prezent, R.P. Chineză reprezintă o provocare în creștere pentru securitatea globală, în general, și pentru cea europeană, în particular.

CONCLUZIE

Ca urmare a aspectelor menționate anterior se remarcă două tendințe: R.P. Chineză este în proces de continuă schimbare, establishment-ul politic actual distanțându-se de politicile liderilor anteriori și promovând o imagine mai fermă, mai agresivă a Chinei, atât în plan regional, cât și în plan global. Modul de administrare a ultimelor crize, de la încercarea agresivă de a limita răspândirea Covid-19 (prin politica „zero Covid") la politicile severe de reeducare ale etnicilor uiguri sau la politica diplomatică agresivă adoptată recent de diplomația chineză denotă faptul că actualii lideri de la Beijing au schimbat tonul în relația cu celelalte state, încurajați fiind și de dependența economică din ce în ce mai mare de forța de muncă, de produsele și de piețele chineze.

Desigur, relația dintre R.P. Chineză și restul lumii este una complexă și include impactul cumulativ al unor factori precum istoria, rasa, cultura, identitatea și ideologia Chinei, însă ar fi o greșeală să fie tratată la modul simplist, liderii chinezi considerând deja secolul XXI ca fiind momentul de început al unei noi ordini mondiale, R.P. Chineză urmând să joace un rol decisiv în cadrul acesteia.

BIBLIOGRAFIE

1. COONEY, Sean, „Why Taiwan is not Hong Kong: A Review of the PRC's "One Country Two Systems" Model for Reunification for Taiwan", în *Washington International Law Journal,* vol. 6 (no. 3), 1997, p.497-548.
2. GAO Henry, „From the Periphery to the Centre: China's Participation in WTO Negotiations", în *China Perspectives,* No. 1 (89), 2012, p. 59-65.
3. GRIFFIN Nicholas, *Ping-Pong Diplomacy: The Secret History Behind the Game that Changed the World*, Simon & Schuster, 2014.
4. HU Angang. YAN Yilong, TANG Xiao, LIU Shenglong, *2050 China: Becoming a Great Modern Socialist Country,* Springer, Singapore, 2020, 105 p.
5. OVERHOLT H. William, *Hong Kong: The Rise and Fall of "One Country, Two Systems"*, Harvard Kennedy School, Ash Center for Democratic Governance and Innovation, 2019, 36 p.
6. PETTIS Michael, *The Four Stages of Chinese Growth*, 2014, https://carnegieendowment.org/chinafinancialmarkets/55947.
7. SORACE Christian, FRANCESCHINI Ivan, LOUBERE Nicholas (eds.), *Afterlives of Chinese Communism: Political Concepts from Mao to Xi,* Australian National University Press, 2019, 404 p.
8. SCHELLHORN M. Kai, "Asia after the End of the Cold War", în *Southeast Asian Affairs 1992*, Institute of Southeast Asian Studies (ISEAS), Singapore, p. 58-70.
9. ZAGORIA S. Donald, "The End of the Cold War in Asia: Its Impact on China", în *Proceedings of the Academy of Political Science*, Vol. 38, No. 2, 1991, p. 1-11.
10. www.bbc.com/news/world-asia-china-58854081.
11. https://news.cgtn.com/news/2021-09-06/China-s-vice-premier-says-country-will-support-private-sector-growth-13kumpnFnJS/index.html.
12. https://www.mfa.gov.cn/ce/cemy/eng/sgxw/t1840912.htm.
13. http://en.qstheory.cn/2021-07/08/c_641137.htm
14. http://www.chinatoday.com.cn/ctenglish/2018/hotspots/jdbn/202106/t20210629_800251275.html.
15. https://www.eastasiaforum.org/2021/0706/taiwans-china-dependency-is-a-double-edged-sword.
16. https://thediplomat.com/2020/10/from-china-to-the-us-the-self-reliance-slogan-is-back/.

17. https://thediplomat.com/2016/07/the-us-china-power-transition-stage-II.
18. https://www.mfa.gov.cn/ce/cemy/eng/sgxw/t1840912.htm.
19. https://policycn.com/21-06-21-common-prosperity-gongtong-fuyu/.
20. https://www.mfa.gov.cn/ce/cero/rom/xw/t1461266.htm.
21. https://www.mcc.gov/news-and-events/release/release-100518-build-act-signed-law.
22. https://www.reuters.com/world/g7-counter-chinas-belt-road-with-infrastructure-project-senior-us-official-2021-06-12/.
23. https://www.reuters.com/article/us-taiwan-anniversary-president.
24. https://www.reuters.com/article/us-taiwan-election.
25. https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/02/04/remarks-by-president-biden-on-americas-place-in-the-world/.
26. https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/12/fact-sheet-president-biden-and-g7-leaders-launch-build-back-better-world-b3w-partner.
27. https://www.reuters.com/article/us-usa-trade-china-details-factbox-idUSKBN1YK1QT.
28. https://www.visualcapitalist.com/china-displaces-u-s-as-the-eus-largest-trade-partner/
29. https://www.europarl.europa.eu/doceo/document/TA-8-2019-0156_EN.html.
30. https://www.nytimes.com/2017/07/25/world/europe/china-russia-baltic-navy-exercises.html.
31. https://en.m.wikipedia.org/wiki/Fourteen_Points.
32. https://en.m.wikipedia.org/wiki/1972_visit_by_Richard_Nixon_to_China.
33. https://en.m.wikipedia.org/wiki/Territorial_disputes-in-the-South-China-Sea.
34. http://wwww.endofempire.asia/wp-content/uploads/2015/11/0818.18.jpg.

[1] https://en.m.wikipedia.org/wiki/Fourteen_Points.
[2] https://en.m.wikipedia.org/wiki/1972_visit_by_Richard_Nixon_to_China.
[3] Nicholas Griffin, *Ping-Pong Diplomacy: The Secret History Behind the Game that Changed the World*, Simon & Schuster, 2014.
[4] https://thediplomat.com/2016/07/the-us-china-power-transition-stage-II.
[5] Hu A., Yan Y., Tang X., Liu S., "Conclusion: The Mission of the Communist Party of China", în *2050 China: Becoming a Great Modern Socialist Country*, Springer, Singapore, 2020, pp 89-90.
[6] Michael Pettis, The Four Stages of Chinese Growth, https://carnegieendowment.org/chinafinancialmarkets/55947.
[7] https://www.eastasiaforum.org/2021/0706/taiwans-china-dependency-is-a-double-edged-sword.
[8] William H. Overholt, *Hong Kong: The Rise and Fall of One Country, Two Systems,* Harvard Kennedy School, Ash Center for Democratic Governance and Innovation, 2019.
[9] https://www.reuters.com/article/us-taiwan-anniversary-president.
[10] Sean Cooney, "Why Taiwan is not Hong Kong: A Review of the PRC's "One Country Two Systems" Model for Reunification for Taiwan", *Washington International Law Journal*, vol. 6 (no. 3), 1997, pp.497-548.
[11] www.bbc.com/news/world-asia-china-58854081
[12] https://www.reuters.com/article/us-taiwan-election.
[13] https://www.mfa.gov.cn/ce/cero/rom/xw/t1461266.htm.
[14] https://www.mcc.gov/news-and-events/release/release-100518-build-act-signed-law.
[15] https://www.reuters.com/world/g7-counter-chinas-belt-road-with-infrastructure-project-senior-us-official-2021-06-12/
[16] https://www.reuters.com/article/us-usa-trade-china-details-factbox-idUSKBN1YK1QT.
[17] https://www.visualcapitalist.com/china-displaces-u-s-as-the-eus-largest-trade-partner/
[18] https://www.europarl.europa.eu/doceo/document/TA-8-2019-0156_EN.html.
[19] https://www.nytimes.com/2017/07/25/world/europe/china-russia-baltic-navy-exercises.html.

FORMATUL „BUCUREȘTI 9”: DIMENSIUNE A COOPERĂRII REGIONALE PENTRU ÎNTĂRIREA FLANCULUI ESTIC AL NATO

Andreea-Amalia STĂNICĂ*

Abstract

The aggressive policy pursued by the Russian Federation over the past two decades, which culminated in the invasion of Ukraine, has led states on the Eastern European side to lay the groundwork for regional cooperation, through which to strengthen unity, discouragement and defense. Based on both the common historical past and similar security objectives, Poland and Romania, in the position of strategic pillard of the North Atlantic Alliance, were the initiators of the Bucharest 9 (B9) format, along with Bulgaria, the Czech Republic, Estonia, Latvia, Lithuania, Slovakia and Hungary.

The main direction of research is to analyze the steps taken by the nine states engaged in the B9 format to strengthen NATO's eastern flank, from the development of the cooperation format to the present. Thus, the article will initially focus on addressing the strategic documents of each actor in order to identify how the threat posed by Russian state is stated. Subsequently, the measures taken by the B9 member states in terms of military cooperation and investment which are needed to counter a possible destabilization of the regional security climate, will be examined.

Keywords: *Bucharest 9; NATO; threat; Russian Federation; national strategy; eastern flank.*

INTRODUCERE

În contextul politicii agresive a Federației Ruse, concentrată pe ascensiune și revenire la statutul de superputere, statele membre NATO din flancul estic s-au implicat în dezvoltarea unor formate de cooperare, având ca obiectiv stabilizarea regiunii din punct de vedere al securității pe plan militar, politic, economic, social și informațional.

După inițiative eșuate de a recăpăta supremația asupra teritoriilor care au constituit în trecut Imperiul Rus, evenimentele din Georgia (2008), Crimeea (2014) și Donbas (2022) au condus la deteriorarea profundă a relațiilor dintre Federația Rusă și Alianța Nord-Atlantică, respectiv Uniunea Europeană. Politica externă agresivă a Federației Ruse a condus la reconsiderarea nivelului de securitate regională, determinând un mediu internațional imprevizibil și o retorică a rivalității binomului Est-Vest mult mai expansivă[1]. Aceste evoluții au determinat statele partenere ale NATO și UE să conlucreze permanent în vederea îndepărtării Kremlinului de atingerea dezideratului de a recâștiga influența în zona ex-sovietică. Din punct de vedere geopolitic, statele localizate la granița cu Federația Rusă prezintă un

Autoarea este doctorand al Școlii Naționale de Studii Politice și Administrative, București.

grad ridicat de vulnerabilitate, fiind nevoite să își alinieze obiectivele strategice de securitate[2].

Astfel, în contextul anexării Crimeii și turbulențelor înregistrate la nivel internațional, în anul 2014, România și Polonia au fost inițiatorii unui forum de dialog la Varșovia, încurajând statele situate pe flancul estic să intensifice cooperarea în vederea întăririi securității regionale. În noiembrie 2015, în cadrul Summit-ului de la București, dialogul dintre statele estice s-a concretizat prin adoptarea de către președinții Bulgariei, Estoniei, Letoniei, Lituaniei, Poloniei, României, Slovaciei, Ungariei și reprezentantul Cehiei a Declarației comune „Solidaritate Aliată și Responsabilitate Comună", document fondator al formatului „București 9"[3]. Prin declarația adoptată, au fost setate obiectivele în baza cărora vor fi angrenate în noul proiect, cele nouă state partenere urmărind intensificarea cooperării în cadrul Alianței Nord-Atlantice în vederea întăririi, din punct de vedere securitar, a flancului estic[4]. O altă întâlnire a fost desfășurată în iulie 2016 în capitala celuilalt stat fondator, Polonia, urmând ca ulterior, formatul de cooperare să cunoască anual o extindere. În noiembrie 2016, respectiv octombrie 2017, cele două summit-uri organizate la București, respectiv Varșovia, au fost extinse la nivel de miniștri de externe[5]. În anul 2018, capitala României a găzduit, în perioada 12-14 martie, prima întâlnire la nivel de reprezentanți ai apărării, participând atât oficiali ai Alianței Nord-Atlantice, cât și ai SUA[6]. În perioada 17-19 aprilie a aceluiași an, la București, a avut loc prima reuniune a formatului B9 la care au participat membrii ai structurilor legislative din cele nouă țări, precum și oficiali ai Franței și ai NATO[7]. O altă întâlnire organizată în anul 2018 a avut loc la Varșovia, întrunind președinții statelor membre și având ca finalitate semnarea unei declarații comune în cadrul căreia au fost afirmate următoarele obiective: consolidarea unității flancului estic, reîntărirea capabilităților statelor membre și implementarea „prezenței înaintate", menținerea caracterului descurajator și defensiv față de Moscova, precum și respectarea dreptului internațional, fiind luată în calcul opțiunea dialogului politic dintre actori[8].

În actualul context geopolitic, în februarie 2022, președintele României, alături de cel al Poloniei, au organizat un summit hibrid al formatului București 9 în contextul „agresiunii armate nejustificate, ilegale și neprovocate a Federației Ruse împotriva Ucrainei"[9]. În cadrul reuniunii, desfășurate în aceeași zi cu Summit-ul NATO, statele membre B9 au discutat despre necesitatea întăririi flancului estic al Alianței, prin adoptarea unor măsuri coerente și unitare, precum și despre sprijinul politic, economic și umanitar care urma a fi acordat statului ucrainean[10]. Ulterior, în martie 2022, a fost organizat la Bratislava un summit B9 al miniștrilor de externe, la care a participat atât Secretarul general-adjunct al NATO, cât și un reprezentant al SUA – asistentul secretarului de stat pentru afaceri europene și eurasiatice. Discuțiile au fost centrate pe agresiunea militară ilegală lansată de Federația Rusă împotriva Ucrainei și pe efectele acesteia[11]. De asemenea, a fost reiterat statutul Federației Ruse de principal furnizor de insecuritate la adresa partenerilor europeni și euroatlantici[12]. În urma acestei întruniri s-a stabilit organizarea unui nou summit găzduit de președintele României, împreună cu omologul său polonez, la București, în iunie 2022. De menționat faptul că această reuniune a avut loc în vederea enunțării unei poziții unitare a statelor membre ale formatului B9 pentru Summit-ul NATO de la Madrid (29-30.06.2022).

STRATEGIILE DE SECURITATE ALE STATELOR MEMBRE B9

Caracterul unitar al obiectivelor statelor din flancul estic, din punct de vedere al securității, ocupă un loc important în cadrul documentelor oficiale. De altfel, la nivelul strategiilor de securitate ale statelor membre se regăsește enunțată în diferite forme amenințarea orchestrată de Federația Rusă.

De exemplu, atât în cadrul Strategiei de securitate națională a Bulgariei, din anul 2018, cât și în cadrul Strategiei de Apărare, se pune accentul pe amenințările hibride conduse de Federația Rusă, încălcând regulile dreptului internațional, în contextul anexării Crimeii, în 2014[13]. La rândul său, Strategia de securitate națională a Estoniei, promovată în anul 2017, identifică amenințările Moscovei ca acțiuni cu

ascensiune constantă care agresează securitatea comunității europene[14]. Pentru atingerea dezideratului de hegemon, Estonia consideră că statul rus pune în prim-plan dimensiunea militară, concentrarea acestor elemente la granițele statelor baltice conducând la instaurarea unei destabilizări regionale[15]. În acest sens, Estonia salută în cadrul Strategiei sale eficiența sancțiunilor adoptate împotriva Moscovei și îndeamnă spre o intensificare a acestora[16]. Din punct de vedere al unității regionale, Estonia precizează în Strategie că trebuie consolidată unitatea statelor membre ale UE, fiind necesară crearea unui front comun pentru a contracara politica agresivă condusă de statul rus[17].

Letonia, în cadrul Strategiei sale de securitate națională, adoptată în anul 2020, se concentrează semnificativ pe agresiunea militară condusă de Federația Rusă în Ucraina și pe necesitatea aplicării unor măsuri de prevenire a unui scenariu asemănător împotriva sa. În vederea construirii unui climat de securitate stabil în interiorul granițelor sale, Letonia urmărește o cooperare mai strânsă la nivelul instituțiilor pe plan intern, asigurând astfel caracterul rezilient al statului[18].

Lituania își aliniază obiectivele de securitate cu celelalte state baltice, în cadrul Strategiei sale regăsindu-se, de asemenea, Federația Rusă în postura de stat agresor. În aceeași notă, Lituania consideră o amenințare politica statului rus de desfășurare a forțelor și capabilităților sale militare de-a lungul frontierei comune, respectiv pe teritoriul Kaliningradului[19]. Un alt punct cheie care se regăsește la nivelul documentului lituanian este conștientizarea existenței unui conglomerat de acțiuni care se încadrează într-un spectru multidimensional (energetic, informațional, economic, social etc.) direcționat împotriva statelor vecine, amenințare care destabilizează atât securitatea națională a Lituaniei, la nivel micro, cât și întregul climat de securitate euro-atlantic, la nivel macro. Având acest fundament, una dintre previziunile Lituaniei este utilizarea în viitor de către statul rus a acțiunilor hibride în vederea atingerii intereselor sale de politică externă.

Amenințarea generată de dislocarea capabilităților militare la frontiera cu un stat membru al B9 este enunțată și în cadrul Strategiei naționale de securitate a Poloniei (2020)[20]. La nivelul documentului, Federația Rusă este identificată drept principală amenințare, care prin intermediul consolidării dimensiunii militare și utilizării capabilităților în contexte precum ocuparea Abhaziei și Osetiei de Sud și a Crimeii, urmărește recăpătarea statutului de putere, respectiv reconstruirea Imperiului Rus. Alte acțiuni caracteristice Moscovei, utilizate împotriva statelor aliate la nivel european, sunt dezinformarea și atacurile cibernetice, acestea reprezentând amenințări atât pentru Polonia, cât și pentru întreaga comunitate internațională[21]. Utilizarea unor tactici ce se subsumează războiului hibrid au ca obiectiv subminarea dreptului internațional și recăpătarea influenței asupra statelor ex-sovietice. Tot din spectrul hibrid, Polonia identifică și presiunile energetice care pot fi aplicate de către Federația Rusă asupra statelor dependente de resurse externe[22].

Strategia națională de apărare a României, adoptată în anul 2020, pune accentul pe amenințarea generată de statul rus prin promovarea unei politici agresive la nivel internațional, cu accent asupra militarizării profunde a zonei Mării Negre[23]. Astfel, pentru a face față presiunilor existente în arealul estic, România promovează consolidarea cooperării regionale în cadrul Alianței Nord-Atlantice și Uniunii Europene. Alte formate de cooperare considerate a fi esențiale de către România sunt București 9 și Inițiativa celor Trei Mări, prin intermediul cărora țările de pe flancul estic pot întări mediul de securitate regional.

Slovacia, în cadrul documentului strategic actual, adoptat în anul 2021, încadrează acțiunile agresive din Georgia și Ucraina drept încălcări ale dreptului internațional, respectiv provocări semnificative la adresa sa[24]. În acest context, Bratislava consideră că un obiectiv principal care contribuie la climatul de securitate național este retragerea Federației Ruse din conflictul ruso-ucrainean, respectiv renunțarea la teritoriul Peninsulei Crimeea[25]. Pentru atingerea acestor deziderate, Slovacia susține măsurile de aplicare a sancțiunilor împotriva Federației Ruse, precum

și aspirațiile de aderare a statelor agresate în cadrul Organizației Nord-Atlantice[26].

În contextul formării noului guvern ceh din anul 2022 a fost adoptată o declarație în cadrul căreia este precizat că se vor reconsidera relațiile cu Federația Rusă[27]. Dacă în cadrul Strategiei naționale de securitate, adoptată în anul 2015, Cehia făcea apel la respectarea „integrității teritoriale a țărilor vecine", fără a pune accentul în mod concret pe situația din Ucraina, cel mai probabil noua Strategie națională de securitate va fi revizuită, extinzând mesajul transmis în cadrul declarației emise de noul bloc guvernamental[28]. Acest demers este susținut prin prisma poziționării Cehiei în fața unor acțiuni destabilizatoare ale Federației Ruse, precum și de mesajul și acțiunile ferme ale statului ceh de susținere a Ucrainei în contextul războiului izbucnit în februarie 2022.

Notă discordantă face statul ungar, care în cadrul documentelor strategice actuale nu consideră acțiunile Federației Ruse drept o amenințare. Ungaria, în cadrul documentului din anul 2020, definește Moscova ca unul dintre principalii piloni ai securității regionale și internaționale, promovând dialogul Vest-Est în vederea eliminării unui scenariu de escaladare a tensiunilor existente[29]. Prin adoptarea acestei poziții formale, cel mai probabil Ungaria urmărește atingerea intereselor sale economice și dialogul diplomatic favorabil. Cu toate acestea, apartenența sa la formatul București 9 poate defini în mod indirect alinierea cu viziunea celorlalte state membre.

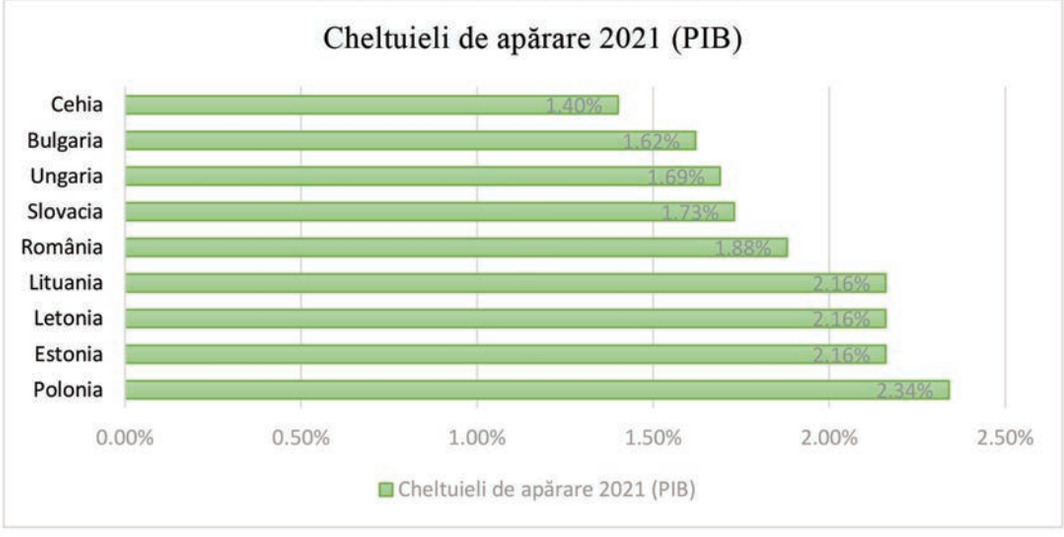
Prin scurta analiză a documentelor strategice ale celor nouă state membre ale formatului de cooperare regională, putem concluziona că obiectivele acestora modelează o conduită comună, aliniindu-se cu cele ale NATO în vederea dezvoltării unei politici de securitate stabile, care să reprezinte un pilon strategic împotriva amenințărilor orchestrate de statul rus în zona central-estică a continentului european. Astfel, prin raportare la actualul context geopolitic, reiese faptul că dezvoltarea formatului București 9 a fost și reprezintă, în continuare, o inițiativă strategică utilă care amplifică nivelul de cooperare regională.

MĂSURI ADOPTATE DE PARTENERII B9 ÎN VEDEREA CONSOLIDĂRII FLANCULUI ESTIC AL NATO

Pentru a pune în aplicare obiectivele enunțate în cadrul strategiilor de securitate, cele nouă state membre ale formatului de cooperare au inițiat demersuri de întărire a regiunii est-europene. Astfel, statele partenere au demarat acțiuni în trei direcții: au luat parte la exerciții militare, au crescut cheltuielile pentru apărare, alocând un procent mai mare din PIB (2% până în 2024) și au garantat modernizarea, respectiv dezvoltarea capabilităților militare din punct de vedere tehnic, prin creșterea bugetului aferent programelor de înzestrare (aproximativ 20% din buget)[30].

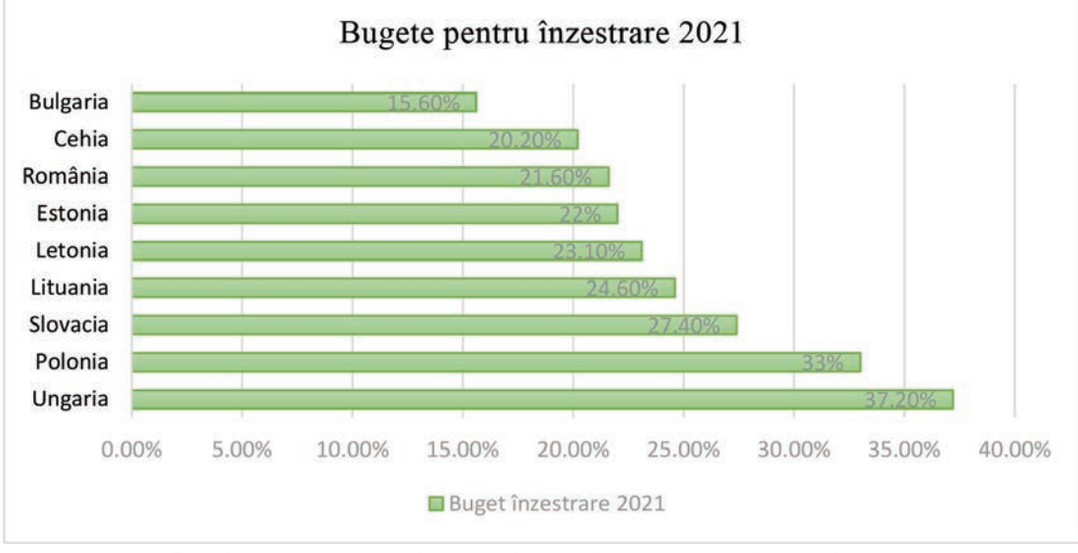
După anexarea Crimeii, în anul 2014, NATO, respectiv statele partenere ale Alianței, au sporit numărul exercițiilor militare. Astfel, prin participarea la exercițiile organizate în zona central-estică a Europei, statele membre contribuie la dezvoltarea cooperării din punct de vedere al securității și apărării flancului estic în fața provocărilor generate de acțiunile Federației Ruse. Dintre exercițiile militare cu implicare a statelor membre B9, desfășurate până în prezent, respectiv cele planificate în cursul anului 2022, putem numi următoarele: Riverine, Light Avalanche, Agile Spirit, Trojan Footprint, Saber Junction, Sea Breeze, Rapid Trident, Maple Arch, Nighthawk, Griffon Strike (04-29.04.2022, Lituania), Iron Wolf I-2022 (02.-20.05.2022, Lituania), Swift Response 22 (05-24.05.2022, Letonia, Lituania, Estonia, Polonia), Defender Europe 22 (16-27.05.2022, Polonia, Letonia, Lituania, Estonia, Slovacia), Baltops 22 (04-17.06.2022, vestul M. Baltice), Wind Spring 22 (20.06-05.07.2022, România), Platinum Lion 22 (01-30.07.2022, Bulgaria), Northern Coasts (NOCO) 22 (09-21.09.2022, M. Baltică), Poseidon 22 (04.11.11, M.Neagră, Bulgaria)[31], Seadfast Cobalt 22 (16.05-10.06.2022, Europa), Ramstein Legacy 2022 (05-06.07.2022, Polonia și statele baltice), Cyber Coalition 22 (07-12.11.2022, Estonia)[32]. Până în prezent, statele membre B9, prin participarea la aceste inițiative, au amplificat gradul de cooperare și interoperabilitate atât la nivel NATO, cât și în cadrul formatului București 9.

În ceea ce privește creșterea bugetului alocat apărării, conform datelor furnizate în cadrul unui raport recent (2021) al Bazei de Date a Cheltuielilor Militare SIPRI, Polonia și România se află pe locul 20, respectiv 40 la nivel mondial, cu bugete alocate de aproximativ 13.7 miliarde USD și 5.6 miliarde USD[33]. Conform datelor furnizate de NATO, din 2014 până în 2021 au fost înregistrate creșteri pentru cheltuielile de apărare ca pondere din PIB-ul statelor membre B9, cifrele aferente balanței din 2021 fiind regăsite în figura următoare[34]:



(Datele care au stat la baza realizării diagramei au fost preluate din *Defence Expenditure of NATO Countries 2014-2021, 2022*[35])

Încă de la începutul anului 2022 se remarcă intențiile de a face progrese la nivel european, cel mai probabil generate de lansarea invaziei ruse din Ucraina, Polonia și România (membre B9), alături de alte state Aliate anunțând planuri de creștere a bugetelor alocate de peste 2% din PIB. Argumentul central care a stat la baza demarării unor programe mari de achiziții de tehnică și echipamente militare în ultimii ani este proveniența sovietică semnificativă a celor deținute în prezent de statele membre. Astfel, conform datelor furnizate de NATO, până în prezent în statele membre B9 au fost înregistrate creșteri, procentele aferente anului 2021 regăsindu-se în figura următoare[36]:



(Datele care au stat la baza realizării diagramei au fost preluate din *Defence Expenditure of NATO Countries 2014-2021, 2022*[37])

Ținând cont de existența războiului ruso-ucrainean izbucnit în februarie 2022, statele B9 au acordat un ajutor semnificativ statului ucrainean agresat, înregistrându-se o serie de acțiuni și inițiative în vederea consolidării apărării pe flancul estic al NATO. Astfel, din punct de vedere al sprijinului cu tehnică și echipamente militare, partenerii B9 au avut o contribuție semnificativă, furnizând tancuri și blindate, sistemul de apărare antiaeriană S-300PMU, rachete sol-aer, rachete antitanc și muniție[38].

Prin analiza cantitativă efectuată, se remarcă o preocupare intensă a membrilor B9 în ceea ce privește consolidarea apărării pe flancul estic, atât din punct de vedere al cooperării regionale, cât și din punct de vedere al modernizării capabilităților militare. Direcțiile de acțiune ale celor nouă state sunt esențiale pentru stabilizarea climatului de securitate regional, contribuind atât la apărarea teritoriilor naționale, cât și la atingerea obiectivului NATO de asigurare a apărării colective, cu valențe internaționale.

CONCLUZII

Dezvoltarea formatelor de cooperare pe flancul est-european contribuie la stabilizarea climatului de securitate regional, însă pentru a putea contracara amenințările Federației Ruse este nevoie de o calibrare mai bună a acestora. În esență, București 9 creează premisele unei cooperări puternice, consolidând axa imaginară de la Marea Baltică la Marea Neagră, actorii regionali fiind capabili să contracareze prin intermediul unei viziuni și strategii unitare agresiunile conduse de Federația Rusă. Însă, pentru o mai bună capacitate de reacție a blocului de state angrenate în B9 este necesar să se depună eforturi în privința atingerii obiectivelor de înzestrare și alocarea a cel puțin 2% din PIB pentru bugetul de apărare de către fiecare actor. De asemenea, pentru consolidarea poziției regionale și a securității statelor membre, unii experți susțin extinderea în format B9+, prin cooptarea Georgiei, Republicii Moldova și a Ucrainei[39]. În actualul context geopolitic, intensificarea dialogului cu SUA, emiterea unor propuneri notabile și prezentarea premiselor de dezvoltare a unor proiecte de sprijin și ajutor-post conflict în cadrul Summit-ului de la Madrid din iunie 2022, ar putea spori credibilitatea și rolul B9 atât pe plan regional, cât și internațional.

BIBLIOGRAFIE

1. ORZELSKA-STACZEK Agnieszka, Piotr Bajda, *Security aspects of regional cooperation in Central Europe: Visegrad Group, Bucharest Nine, and The Three Seas Initiative*, Polonia, 2021, http://neweurope.centre.ubbcluj.ro/wp-content/uploads/2021/12/1.pdf.
2. *Allied National Exercises and Activities*, 2022, https://shape.nato.int/exercises/allied-national-exercises.
3. Calea Europeană, *Nine Heads of State Call on Alliance to 'Strengthen the Eastern Flank of NATO'*, 2015, https://www.atlanticcouncil.org/blogs/natosource/nine-heads-of-state-call-on-alliance-to-strengthen-the-eastern-flank-of-nato/.
4. MAE, Comunicat de presă, *Ministrul afacerilor externe Bogdan Aurescu a discutat cu aliații din Formatul București 9 reuniți la Bratislava consolidarea posturii de descurajare și apărare a NATO pe Flancul Estic, în actualul context de securitate*, 2022, http://mae.gov.ro/node/58277.
5. *Defence Expenditure of NATO Countries (2014-2021*), 2022, https://www.nato.int/nato_static_fl2014/assets/pdf/2022/3/pdf/220331-def-exp-2021-en.pdf.
6. *Defence Strategy of the Slovak Republic*, 2021, https://www.mosr.sk/data/files/4291_defence-strategy-of-the-slovak-republic-2021.pdf.
7. DA SILVA Diego Lopes, Nan Tian, Lucie Beraud-Sudreau, Alexandra Marksteiner, Xiao Liang, *Trend in World Military Expenditure*,

2021, https://www.sipri.org/sites/default/files/2022-04/fs_2204_milex_2021_0.pdf.
8. Embassy of Romania in the Republic of Poland, *Meeting of Foreign Affairs Ministers of the Bucharest 9 Format*, https://varsovia.mae.ro/en/local-news/1321.
9. *Government Resolution 1163/2020 (21st april), on Hungary's National Security Strategy*, https://honvedelem.hu/hirek/government-resolution-1163-2020-21st-april.html.
10. Kaitseministeerium, *National Security Concept*, 2017, https://kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_security_concept_2017_0.pdf
11. ANGHEL Liviu, *Summitul extraordinar al formatului București 9*, 2022, http://presamil.ro/summitul-extraordinar-al-formatului-bucuresti-9/.
12. Ministry of National Defence, *Bucharest-9 (B9) Defence Minister's Meeting*, https://english.mapn.ro/b9defence/.
13. BANASIK Miroslaw, *Bucharest nine in the process of strategic deterrence on NATO's eastern flank*, Polonia, 2021, https://apcz.umk.pl/CJPS/article/view/36524/30782.
14. *National Security Strategy of the Republic of Bulgaria*, 2011, https://www.me.government.bg/files/useruploads/files/national_strategy1.pdf.
15. *National Security Strategy of the Republic of Lithuania,* 2017, https://kam.lt/wp-content/uploads/2022/03/2017-national-security-strategy.pdf.
16. *National Security Strategy Of The Republic Of Poland*, 2020, https://www.bbn.gov.pl/ftp/dokumenty/National_Security_Strategy_of_the_Republic_of_Poland_2020.pdf.
17. *NATO Exercises and Activities*, 2022, https://shape.nato.int/nato-exercises.
18. HAȚEGAN Ovidiu, *Ce ajutor militar a oferit România Ucrainei în comparație cu celelalte țări din Europa și din lume*, 2022, https://www.g4media.ro/analiza-ce-ajutor-militar-a-oferit-romania-ucrainei-in-comparatie-cu-celelalte-tari-din-europa-si-din-lume-doar-casti-si-veste-anti-glont-slovacia-a-trimis-un-sistem-de-aparare-anti-aeriana-polonia.html.
19. *Policy Statement of the Government of the Czech Republic*, 2022, https://www.vlada.cz/assets/jednani-vlady/policy-statement/Policy-Statement-of-the-Government.pdf.
20. *Romania hosts Bucharest Format (B9) Summit at parliamentary level*, 2018, https://www.nineoclock.ro/2018/04/19/romania-hosts-bucharest-format-b9-summit-at-parliamentary-level-president-iohannis-national-parliaments-of-b9-countries-play-essential-role-in-equitable-sharing-of-burdens-inside-nato/.
21. România, Administrația Prezidențială, *Strategia Națională de Apărare a țării pentru perioada 2020- 2024*.
22. https://www.presidency.ro/files/userfiles/Documente/Strategia_Nationala_de_Aparare_a_Tarii_2020_2024.pdf.
23. *Security Strategy of the Czech Republic*, 2015, https://www.army.cz/images/id_8001_9000/8503/Security_Strategy_2015.pdf.
24. *Security Strategy of the Czech Republic*, 2015,
25. https://www.army.cz/images/id_8001_9000/8503/Security_Strategy_2015.pdf.
26. GERASYMCHUK Sergiy, *NATO's Bucharest Nine. Nothing quiet on the eastern flank*, 2021, http://prismua.org/wp-content/uploads/2021/12/B9-21_en_fin.pdf.
27. *The National Security Concept* (informative section), https://www.mod.gov.lv/sites/mod/files/document/NDK_ENG_final.pdf.
28. The Polish Institute of International Affairs, *The Bucharest 9: Delivering on the Promise to Become the Voice of the Wastern Flank*, 2018.
29. https://pism.pl/publications/The_Bucharest_9_Delivering_on_the_Promise_to_Become_the_Voice_of_the_Eastern_Flank.

[1] Agnieszka Orzelska-Staczek, Piotr Bajda, "Security aspects of regional cooperation in Central Europe: Visegrad Group, Bucharest Nine, and The Three Seas Initiative", 2021, http://neweurope.centre.ubbcluj.ro/wp-content/uploads/2021/12/1.pdf.

[2] Miroslaw Banasik, "Bucharest nine in the process of strategic deterrence on NATO's eastern flank", 2021, https://apcz.umk.pl/CJPS/article/view/36524/30782.

[3] Calea Europeană, "Nine Heads of State Call on Alliance to 'Strengthen the Eastern Flank of NATO", 2015, https://www.atlanticcouncil.org/blogs/natosource/nine-heads-of-state-call-on-alliance-to-strengthen-the-eastern-flank-of-nato/.

[4] Ibidem.
[5] Embassy of Romania in the Republic of Poland, *Meeting of Foreign Affairs Ministers of the Bucharest 9 Format*, https://varsovia.mae.ro/en/local-news/1321.
[6] Ministry of National Defence, *Bucharest-9 (B9) Defence Minister's Meeting*, https://english.mapn.ro/b9defence/.
[7] Romania hosts Bucharest Format (B9) Summit at parliamentary level, 2018, https://www.nineoclock.ro/2018/04/19/romania-hosts-bucharest-format-b9-summit-at-parliamentary-level-president-iohannis-national-parliaments-of-b9-countries-play-essential-role-in-equitable-sharing-of-burdens-inside-nato/.
[8] The Polish Institute of International Affairs, "The Bucharest 9: Delivering on the Promise to Become the Voice of the Western Flank", 2018, https://pism.pl/publications/The_Bucharest_9_Delivering_on_the_Promise_to_Become_the_Voice_of_the_Eastern_Flank.
[9] Liviu Anghel, *Summitul extraordinar al formatului București 9*, 2022, http://presamil.ro/summitul-extraordinar-al-formatului-bucuresti-9/.
[10] Ibidem.
[11] Comunicat de presă, *Ministrul afacerilor externe Bogdan Aurescu a discutat cu aliații din Formatul București 9 reuniți la Bratislava consolidarea posturii de descurajare și apărare a NATO pe Flancul Estic, în actualul context de securitate*, 2022, http://mae.gov.ro/node/58277.
[12] Ibidem.
[13] National Security Strategy of the Republic of Bulgaria, 2011, https://www.me.government.bg/files/useruploads/files/national_strategy1.pdf.
[14] Kaitseministeerium, National Security Concept, 2017, https://kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_security_concept_2017_0.pdf
[15] Ibidem.
[16] Ibidem.
[17] Ibidem.
[18] The National Security Concept (informative section), https://www.mod.gov.lv/sites/mod/files/document/NDK_ENG_final.pdf.
[19] National Security Strategy of the Republic of Lithuania, 2017, https://kam.lt/wp-content/uploads/2022/03/2017-national-security-strategy.pdf.
[20] National Security Strategy of The Republic of Poland, 2020, https://www.bbn.gov.pl/ftp/dokumenty/National_Security_Strategy_of_the_Republic_of_Poland_2020.pdf.
[21] Ibidem.
[22] Ibidem.
[23] România, Administrația Prezidențială, *Strategia Națională de Apărare a țării pentru perioada 2020-2024*, https://www.presidency.ro/files/userfiles/Documente/Strategia_Nationala_de_Aparare_a_Tarii_2020_2024.pdf.
[24] Defence Strategy of the Slovak Republic, 2021, https://www.mosr.sk/data/files/4291_defence-strategy-of-the-slovak-republic-2021.pdf.
[25] Ibidem.
[26] Ibidem.
[27] Policy Statement of the Government of the Czech Republic, 2022, https://www.vlada.cz/assets/jednani-vlady/policy-statement/Policy-Statement-of-the-Government.pdf.
[28] Security Strategy of the Czech Republic, 2015, https://www.army.cz/images/id_8001_9000/8503/Security_Strategy_2015.pdf.
[29] Government Resolution 1163/2020 (21st april), on Hungary's National Security Strategy, https://honvedelem.hu/hirek/government-resolution-1163-2020-21st-april.html.
[30] Sergiy Gerasymchuk, "NATO's Bucharest Nine. Nothing quiet on the eastern flank", 2021, http://prismua.org/wp-content/uploads/2021/12/B9-21_en_fin.pdf
[31] Allied National Exercises and Activities, 2022, https://shape.nato.int/exercises/allied-national-exercises.
[32] NATO Exercises and Activities, 2022, https://shape.nato.int/nato-exercises.
[33] Diego Lopes Da Silva, Nan Tian, Lucie Beraud-Sudreau, Alexandra Marksteiner, Xiao Liang, *Trend in World Military Expenditure*, 2021, https://www.sipri.org/sites/default/files/2022-04/fs_2204_milex_2021_0.pdf.
[34] Defence Expenditure of NATO Countries (2014-2021), 2022, https://www.nato.int/nato_static_fl2014/assets/pdf/2022/3/pdf/220331-def-exp-2021-en.pdf.
[35] Ibidem.
[36] Ibidem.
[37] Defence Expenditure of NATO Countries (2014-2021), 2022, https://www.nato.int/nato_static_fl2014/assets/pdf/2022/3/pdf/220331-def-exp-2021-en.pdf.
[38] Ovidiu Hațegan, *Ce ajutor militar a oferit România Ucrainei în comparație cu celelalte țări din Europa și din lume*, 2022, https://www.g4media.ro/analiza-ce-ajutor-militar-a-oferit-romania-ucrainei-in-comparatie-cu-celelalte-tari-din-europa-si-din-lume-doar-casti-si-veste-anti-glont-slovacia-a-trimis-un-sistem-de-aparare-anti-aeriana-polonia.html.
[39] Vasile Rotaru, Andreas Umland, "How Romania and Poland Can Strenghten NATO and the EU: The New Cooperation Initiatives Could Improve Regional Security", *Foreign Affairs*, 2017, în https://www.foreignaffairs.com/articles/central-europe/2017-11-10/how-romania-and-poland-can-strengthen-nato-and-eu.

PROVOCĂRI HIBRIDE DE NATURĂ CIBERNETICĂ

Paul MIHAI*

Abstract

From the perspective of the analysis of large-scale incidents of cyber terrorism and the growing influence of the Russian government, it was concluded that cyber attacks are threats to NATO member countries and have been included in the list of security threats identified in the New Strategic Concept of NATO since 2010. This conclusion makes terrorism have a new dimension, the cybernetic one, being an adaptation of terrorism to the new era and to be considered as a new field of defense - the cyber realm. In this article I will present and analyze the hybrid cyber challenges posed by the Russian Federation and materialized in cyber attacks on Estonia, Georgia and Ukraine from 2007-2014, to highlight and argue the similarities in the political context, methods, techniques and the tactics used in fulfilling the operational-strategic objectives.

Keywords: *cyber terrorism; terrorist organizations; cyber threats; cyber attacks; cyber space; Internet services; computer war; computer networks; virtual space.*

INTRODUCERE

Acțiunile de securizare a spațiului cibernetic reprezintă un efort comun al celor care aplică legea, al guvernelor, al capabilităților tehnologizate specifice și al indivizilor din societate. Pentru a reuși securizarea spațiului cibernetic este nevoie de o profundă înțelegere a fenomenului de terorism cibernetic, fenomen contemporan care are drept câmp de luptă spațiul cibernetic și este proliferat prin intermediul rețelei Internet, nevizând distrugerea fizică a rețelei, ci instituirea terorii în rândul actorilor statali și non-statali care o utilizează. Astfel, termenul ”cyber terrorism” face referire la utilizarea tacticilor și tehnicilor de război informatic de către organizațiile teroriste, afectând spațiul cibernetic. Mai mult, terorismul cibernetic operează exclusiv în spațiul virtual și nu distruge fizic infrastructura care susține existența spațiului cibernetic. Ritmul rapid de dezvoltare a terorismului cibernetic a impus crearea unor strategii la nivel global, responsabilitatea asigurării securității cibernetice revenind tuturor actorilor implicați în combaterea fenomenului criminalității informatice. După cum se observă, terorismul cibernetic nu diferă de terorismul convențional ca scop, este luat în serios de guverne și se dorește securizarea mijloacelor de operare, respectiv a rețelelor informatice și a structurilor critice interconectate.

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

ATACUL CIBERNETIC ASUPRA ESTONIEI

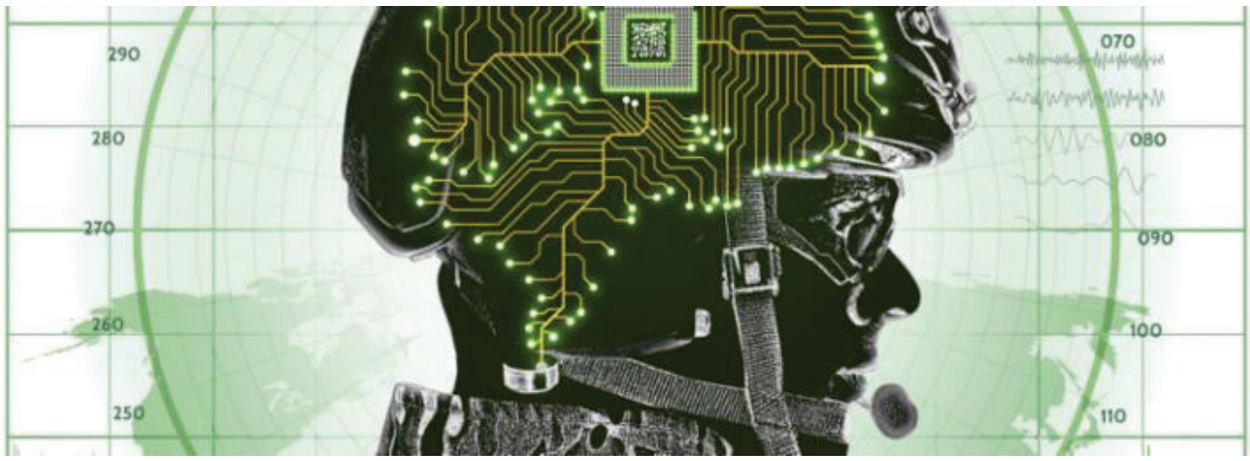
Primul atac cibernetic masiv în spațiul est-european a fost consemnat în Estonia, una dintre republicile baltice care a fost înglobată în Uniunea Sovietică în 1940. După dizolvarea Uniunii Sovietice, Estonia și-a recâștigat independența și a început rapid procesul de reforme economice, politice, sociale și militare. Aceasta a aderat la UE și la NATO, în scopul de a-și asigura securitatea națională. Autoritățile estone au văzut în F.Rusă cea mai gravă amenințare, iar integrarea cu structurile occidentale a reprezentat soluția pentru a depăși această amenințare. Una dintre principalele dispute în relațiile bilaterale a fost problema minorității ruse din Estonia, care reprezintă 26% din populație[1].

Începând cu luna aprilie a anului 2007, tensiunile dintre Estonia și F.Rusă au crescut semnificativ, ca urmare a deciziei autorităților de la Tallinn de a muta Monumentul Soldatului Sovietic din centrul orașului. Importanța acestui monument este legată de comemorarea soldaților sovietici care au eliberat Estonia. Odată cu mutarea statuii de bronz, au fost deshumați soldații Armatei Roșii ce fuseseră îngropați sub statuie și transferați într-un cimitir militar de la periferia capitalei. Pentru populația estonă, statuia reprezenta un simbol al opresiunii, iar pentru etnicii ruși mutarea a însemnat distrugerea patrimoniului cultural și lipsă de respect față de Armata Roșie, care a luptat împotriva Germaniei naziste în timpul celui de-al Doilea Război Mondial. După mutarea statuii, relația dintre Estonia și Rusia a devenit tensionată, Kremlinul acuzând autoritățile de la Tallinn că încalcă drepturile omului, fapt pentru care au cerut demisia premierului eston[2]. În același timp, au izbucnit ciocniri violente pe străzi între poliție și minoritatea rusă din Estonia, proteste în fața Ambasadei Estoniei din Moscova și, respectiv, o campania masivă de atacuri informatice.

Estonia era extrem de dependentă de Internet. În acea perioadă, aproape întreaga țară fusese acoperită de Internet prin WiFi, toate serviciile guvernamentale fiind disponibile online, iar 86% din populația estonă avea online banking. În 2007 a existat posibilitatea de a vota electronic, iar 5,5% din alegători și-au exercitat dreptul de vot în acest mod.

Începând cu seara zilei de 27 aprilie 2007 a fost semnalat un volum foarte mare de atacuri cibernetice pe ecranele de monitorizare ale operatorilor estoni, iar această zi a fost declarată ca fiind începutul masivului atac cibernetic. De la ora 22.00, organizațiile estone s-au confruntat cu mai multe tipuri de atacuri, fiind afectate servere de e-mail, servere web, servere de nume de domenii și alte servicii Internet. Sistemele au devenit foarte lente sau au fost blocate de un trafic de date neobișnuit de mare. Site-urile au suferit modificări vizuale, prima pagină fiind înlocuită cu cea a atacatorilor. Căsuțele de e-mail au fost umplute cu spamuri și e-mailuri de tip phishing. Traficul pe Internet a depășit de 10 ori media zilnică, generând funcționarea defectuoasă sau nefuncționarea serviciilor de Internet[3].

Atacurile s-au succedat astfel: în prima fază, coordonarea lor a fost realizată prin intermediul forumurilor, iar în cea de-a doua fază coordonarea a fost delegată serverelor de comandă și control ale rețelei de botnet[4]. A doua fază a ținut de pe 30 aprilie până pe 18 mai și a rulat în patru valuri cu intensități diferite, concentrându-se pe ținte variate și utilizând diverse tehnici de atac. Primul val de atacuri de pe 4 mai a constat în atacuri DDoS (Distributed Denial of Services) asupra site-urilor și sistemelor DNS (Domain Name System). Al doilea val, considerat vârf de atac, a avut loc pe 9 mai. Ulterior, numărul de acte ostile a început să scadă, iar de pe data de 11 mai au urmat patru zile de relativă liniște. Atacurile DDoS au inclus site-urile guvernamentale și cele de servicii financiare. Un al treilea val de atacuri a început pe data de 15 mai și a inclus atacuri DDoS de tip botnet împotriva site-urilor guvernamentale și a celor din domeniul financiar. Al patrulea val de atacuri a constat din nou în atacuri asupra site-urilor guvernamentale și asupra băncilor. Atacurile DDoS au vizat cu succes site-urile



Sursa:www.NATO.int

tuturor ministerelor, ale primelor două bănci mari din Estonia și ale mai multor partide politice. Hackerii au avut posibilitatea de a închide serverul de e-mail al Parlamentului și au dezactivat ATM-urile. Una dintre băncile estone care a fost victimă a atacurilor cibernetice a estimat pierderi în jurul valorii de 1 milion USD. Cu toate acestea, când au fost evaluate pierderile la încetarea atacurilor, s-a constatat în mod surprinzător că pagubele realizate de atacurile cibernetice au fost relativ scăzute[5].

Spre deosebire de atacurile din prima fază, cele din faza a doua s-au bazat pe botnet, care sunt considerate astăzi drept principalul vehicul și platformă pentru infracționalitatea cibernetică. Construcția și utilizarea botnet-urilor se bazează, de obicei, pe diviziunea muncii. Botnet-urile sunt create de așa-numiții „păstori de boți", care folosesc adesea kit-uri malware[6] create și vândute de programatori extrem de talentați. „Bot herders"[7] vând botnet-urile sau le închiriază pentru o anumită perioadă de timp unor părți terțe, care le folosesc pentru a trimite e-mail-uri de tip „spam" pentru a distribui malware sau, în cazul Estoniei, pentru a lansa atacuri DDoS. Timpul de închiriere devine vizibil între creșterea rapidă a traseului DDoS și scăderile rapide ce au loc la sfârșitul unui singur atac.

Din cele prezentate mai sus, majoritatea atacurilor asupra Estoniei a constat în DDoS, o tehnică cunoscută ce a produs o mulțime de incidente. Cu toate acestea, în Estonia a existat un mix inedit de atacuri, efectuate atât de hackeri profesioniști, probabil din rețeaua de afaceri ruse, care au folosit botnet, cât și de așa-numiții „hackeri patrioți" - tineri utilizatori de calculatoare individuale - care au fost indignați de decizia autorităților din Tallinn de a muta statuia de bronz. A existat un forum special în limba rusă de unde se puteau descărca instrumentele și instrucțiunile modului de efectuare a atacurilor cibernetice. În ciuda surprizei inițiale, Estonia a fost capabilă să organizeze rapid apărarea și, cu ajutorul CERT (Computer Emergency Response Team), a aliaților și a specialiștilor din Germania, Israel, Slovenia și Finlanda, a depășit pericolele.

Operația cibernetică (atacul cibernetic) din Estonia, din anul 2007, a fost intens dezbătută în mass-media și a fost numită „primul război cibernetic din istorie". Aceasta a arătat modul în care noua tehnologie ar putea fi folosită pentru a ataca o țară modernă. S-a dovedit că atacurile au venit din Rusia, cele mai multe atacuri DDoS fiind inițiate de la adrese IP ruse[8]. O mulțime de atacatori au utilizat calculatoarele din Estonia, ceea ce a indicat minoritatea rusă. Chiar dacă experții tehnici din cadrul Comisiei Europene și ai NATO nu au găsit nicio dovadă că atacurile au fost comise de către autoritățile ruse, aceste acțiuni au fost considerate, totuși, ca fiind coordonate de Kremlin. Un membru al organizației ruse de tineret NASHI, afiliată partidului lui Vladimir Putin, a mărturisit că „el a stat în spatele atacurilor"[9].

Obiectivul principal presupus al atacurilor cibernetice a fost influențarea autorităților de la Tallinn în scopul retragerii deciziei de îndepărtare a monumentului. Un alt obiectiv a fost de a testa capabilitățile ruse de război cibernetic și de a vedea reacția NATO atunci când unul dintre statele membre ale acestei organizații este atacat într-un domeniu nou. De asemenea, un al treilea obiectiv probabil a fost să demonstreze că NATO și UE nu ar apăra societatea estonă de atacul rus, iar rușii nu au nevoie de tancuri pentru a provoca daune Estoniei.

În urma acestor atacuri, obiectivele politice ale F.Ruse nu au fost atinse, monumentul nu a fost mutat, iar Estonia a devenit un lider în domeniul securității cibernetice. NATO a accelerat proiectele sale de apărare cibernetică și a creat Centrul de Excelență pentru Cooperare în Apărare Cibernetică, situat în apropiere de Tallinn. Estonia și aliații occidentali și-au asigurat sprijinul reciproc în cazul viitoarelor atacuri la scară largă asupra infrastructurilor IT&C (Tehnologia informației și a comunicațiilor), crescând astfel riscurile și costurile potențiale pentru un adversar care tolerează sau chiar utilizează grupuri de voluntari pentru a ataca infrastructurile de Internet străine. Drept urmare, Estonia a devenit mai apropiată ca niciodată de instituțiile de securitate occidentale, în timp ce influența culturală și politică a F.Ruse asupra Estoniei s-a redus. Chiar dacă Estonia era conectată în proporție mare la Internet, agenția guvernamentală CERT-EE, de răspuns în situații de urgență, avea doar doi membri. Acestora le-a luat trei săptămâni să oprească ritmul atacurilor, reușind să întărească apărarea statului eston cu ajutorul asistenței din partea altor state. Instrumente importante al politicii externe estone, precum canalele diplomatice, au fost utilizate pentru a configura agenda pe termen lung cu țările aliate.

Prima lecție învățată de estoni, precum și de lumea întreagă, a fost că securitatea cibernetică și apărarea rețelei naționale implică nu numai detalii tehnice ale atacurilor, ci și strategii și politici de natură tehnologică. Tacticile echipei CERT-EE au fost de a menține online site-urile critice, cum sunt cele bancare, și nu site-urile guvernamentale, chiar dacă nefuncționarea acestora era un semn de slăbiciune din partea guvernului țării și a însemnat un real succes pentru atacatori. O altă tactică a fost de a menține funcțional serverul de email al Parlamentului, chiar dacă a fost necesară mutarea fizică a serverului de la un furnizor de Internet la altul. Acest lucru a îndârjit atacatorii, care și-au pus toată atenția și energia în închiderea acestui server, fără a se mai preocupa de alte ținte din infrastructura critică.

În concluzie, eficiența acțiunii este o caracteristică de bază a atacurilor cibernetice. În cazul Estoniei, agresorii nu și-au atins scopurile politice. Principalul instrument al tuturor atacurilor a fost atacul brutal DDoS, care a avut loc, în primul rând, prin intermediul rețelelor masive de botnet și, mai târziu, al „hackerilor patrioți" cu ajutorul instrumentelor pregătite anterior. Ca urmare a acțiunii ostile, majoritatea serviciilor de Internet s-au prăbușit, iar restabilirea acestora a fost destul de greoaie. Totuși, societatea informațională estonă a fost destul de rezistentă, ceea ce a determinat ca aceasta să nu-și modifice radical politicile organizaționale și funcționale după aceste atacuri cibernetice.

ATACUL CIBERNETIC ASUPRA GEORGIEI

Al doilea atac cibernetic s-a desfășurat în Georgia și a fost denumit „*primul război în aer, pe mare, la sol și în spațiul cibernetic*". Georgia și-a recâștigat independența după destrămarea Uniunii Sovietice, această țară având o istorie lungă și o conștiință națională puternică, diferită de a celorlalte țări sovietice. De la începutul anilor `90, Georgia a dorit integrarea cu Occidentul. Această tendință a fost consolidată după anul 2003, când a avut loc „Revoluția Trandafirilor", iar președintele Eduard Shevardnadze a fost răsturnat de la putere. Noul președinte ales, Mihail Saakașvili, s-a angajat în apropierea de structurile occidentale și a încercat să reintegreze provinciile Osetia de Sud și Abhazia. Încercările sale au primit o reacție puternică din partea F.Ruse și au condus la declanșarea, pe data de 7 august 2008,

a unui război de cinci zile. În ciuda faptului că războiul era clasic și comportamentul armatelor de pe câmpul de luptă amintea de secolul XX, un anumit aspect al acestuia a reprezentat o noutate - a fost primul război care a avut loc în aer, pe mare, terestru și în spațiul cibernetic.

Primele atacuri informatice au avut loc cu mai multe luni înainte de izbucnirea războiului. La data de 19 iulie, firma de securitate cibernetică FireEye a informat despre atacurile DDoS împotriva site-urilor georgiene[10]. Un scenariu similar atacurilor anterioare a fost repetat la scară mai mare pe 8 august și a coincis cu intrarea trupelor ruse în Osetia de Sud. Atacul executat de hackerii ruși poate fi împărțit în două faze. *În prima fază*, aceștia s-au axat în principal pe site-urile georgiene de știri și cele guvernamentale. Rușii au folosit botnet pentru a efectua atacuri DDoS, iar rețelele georgiene au fost mai vulnerabile la acest atac decât cele estone. *În a doua fază* a atacurilor cibernetice, țintele au fost instituții financiare, întreprinderi, instituții de învățământ, mass-media occidentale și un site al unui hacker georgian. În afară de atacul DDoS, au existat, de asemenea, operațiuni de ștergere a datelor efectuate cu ajutorul unor injecții SQL (*Structured Query Language*) și operațiuni de spam masiv pe e-mail-urile publice, cu scopul de a le bloca. În cea de-a doua fază, o mulțime de „hackeri patrioți" s-au alăturat campaniei împotriva Georgiei. Până pe 10 august 2008, majoritatea site-urilor guvernamentale georgiene au fost nefuncționale, iar guvernul georgian nu a putut comunica cu restul lumii prin intermediul Internetului. Conținutul site-ului președintelui georgian a fost înlocuit cu imagini ce l-au descris pe Mihail Saakașvili drept Hitler. De asemenea, nici băncile și nici rețelele de telefonie mobilă nu au funcționat în Georgia. Conform opiniilor căpitanului Paulo Shakarian, din armata SUA, „hackerii ruși și-au testat abilitățile și capacitatea de a conduce atacuri limitate"[11].

Atacurile au venit de pe teritoriul F.Ruse și au fost un mix de acte efectuate prin utilizarea de botnet-uri și atacuri efectuate de „hackeri patrioți" care, în mod similar cazului Estoniei, au putut găsi informații și programe pe forumuri speciale. A existat o listă de ținte prioritare și informații cu privire la potențiale vulnerabilități, precum și la modul în care să se sustragă blocadei georgiene asupra conexiunilor la Internet din F.Rusă. Centrul acestei campanii de informare a fost site-ul *StopGeorgia.ru*, disponibil online pe 9 august 2008, unde amatorii au putut să găsească instrumente utile pentru a efectua atacuri DDoS[12].

StopGeorgia.ru nu a fost singurul forum implicat în hacking-ul naționalist, dar a servit ca un bun exemplu pentru modul în care această extindere recentă a războiului de stat funcționează în spațiul cibernetic. În plus față de acest forum, a fost creat un canal IRC (Internet Relay Chat) pe *irc.dalnet.ru*, numit *#stopgeorgia*. La *StopGeorgia.ru* a existat o ierarhie distinctă, în care liderii forumului au furnizat instrumentele necesare, au identificat vulnerabilități ale aplicațiilor georgiene și au furnizat liste-țintă generale pentru alți membri ai forumului care nu aveau cunoștințele necesare pentru a acționa.

Ca și în cazul atacurilor din Estonia, specialiștii nu au găsit o legătură clară între autoritățile ruse și atac, însă cei implicați în proiectul *Grey Goose* - o inițiativă OSINT (*Open Source Intelligence*) formată din 100 de voluntari - au declarat că „nivelul de pregătire avansat și de cunoaștere sugerează cu tărie că hackerii ruși au fost pregătiți pentru asalt de către oficialii din cadrul guvernului rus"[13]. Analiștii proiectului *Grey Goose* au avut o activitate de colectare foarte activă pe forumul *XAKEP.ru* și pe forumul *StopGeorgia.ru*, constatând o monitorizare activă a tuturor vizitatorilor, precum și a postărilor acestora. O posibilă explicație ar fi că hackerii ruși naționaliști nu sunt doar pe teritoriul F.Ruse sau că au avut loc recrutări numeroase printre emigranții rușii. Și pentru ca forumul să prevină atacurile hackerilor georgieni, acesta a fost dezactivat temporar în perioada 14-18 august, fiind găzduit pe un server din SUA, deținut de SoftLayer Technologies. Membrii forumurilor discutau frecvent utilizarea serverelor proxy, cum ar fi *FreeCap.ru*, pentru a putea ataca chiar în condițiile blocării IP-urilor ruse sau încercării de detectare.

Mai mult, au existat alte două aspecte interesante ale atacului cibernetic din Georgia.

Primul aspect este legat de coordonarea loviturilor convenționale cu atacurile cibernetice, care sunt de cele mai multe ori nesesizabile. Cu toate acestea, există două exemple care ar putea indica cooperarea dintre forțele clasice și cele cibernetice. Primul exemplu a fost faptul că atacurile convenționale au omis locațiile mass-media și de comunicații, lăsând aceste ținte pentru atacuri informatice. Al doilea exemplu a fost un atac asupra site-urilor de închiriere a generatoarelor electrice cu motor diesel, care să completeze lovitura convențională împotriva infrastructurii electrice din Georgia. Cel de-al doilea aspect, destul de interesant, include pregătirea instrumentelor informatice, instruirea, crearea site-urilor speciale pentru efectuarea acestor atacuri, ceea ce poate indica faptul că Moscova pregătea acest război de mai mult timp. Accesul la instrumentele disponibile pentru ruși și instrucțiunile de utilizare nu pot fi pregătite într-o singură zi. În urma unei întreruperi masive a funcționării site-urilor, autoritățile georgiene au încercat, în primul rând, să filtreze adresele IP din F.Rusă, dar aceștia au schimbat foarte repede tactica și au utilizat alte servere decât cele rusești. Mai târziu, autoritățile georgiene au cerut ajutor Statelor Unite, Poloniei și Estoniei, iar serverele georgiene au fost relocate.

Atacul cibernetic din Georgia a fost o manifestare a unui război informațional sau mediatic destinat întreruperii accesului autorităților georgiene și al societății la orice sursă de știri. Autorii au urmărit trei obiective principale. Primul a fost de a demonstra întregii lumi fragilitatea regimului Saakașvili, care a pierdut controlul asupra statului propriu și paralizarea statului în urma invaziei ruse. Al doilea, adresat societății georgiene, a fost menit să întrerupă orice sursă de informație și să prezinte propaganda proprie, cu scopul de a răspândi haos și dezinformare pentru a submina moralul și încrederea populației în guvern. Obiectivul al treilea este legat de cea de-a doua fază a atacurilor îndreptate împotriva sistemului economic. Cel mai probabil, s-a dorit provocarea unor daune grave pentru dezvoltarea economică a Georgiei și convingerea populației de a nu-l mai sprijini pe Saakașvili. Obiectivele nu au fost atinse, în principal datorită ajutorului din partea SUA și UE (CERT, CERT-EE, CERT-PL, CERT-FR). Site-urile guvernamentale au redevenit funcționale, iar societatea georgiană și-a redobândit accesul la informații. De asemenea, SUA a promis ajutor financiar guvernului georgian.

Lecția învățată în acest context a creat o schimbare de mentalitate la nivel global, și anume că securitatea cibernetică este realizată prin mijloace tehnice, dar este vorba despre oameni, strategie, angajament și nu despre calculatoare, acestea fiind simple instrumente, arme ale atacului. Participanții la atacurile DDoS din Estonia au fost motivați de factori precum aderarea la normele de grup, validarea socială și contagiunea, factori care au contribuit la succesul atacurilor. Influențarea atât de rapidă a populației prin mijloace online a fost pentru autoritățile ruse un exemplu bun de copiat, rafinat și utilizat, ceea ce s-a văzut un an mai târziu în atacul cibernetic din Georgia care a însoțit războiul convențional.

În acest caz, a apărut un element nou - propaganda online. Georgia era perfect conștientă de inferioritatea sa economică, militară și politică față de Rusia și, prin intermediul serviciilor firmei de relații publice *Aspect Consulting*, a utilizat propaganda media ca armă împotriva rușilor. Agențiile internaționale de presă și, în special, media occidentală au fost bombardate cu informații despre faptul că civilii georgieni erau atacați de trupele rusești, iar relatările mediatice generau dovezi favorabile Georgiei și defavorabile Rusiei. După ce tensiunile s-au mai liniștit, ziarele occidentale care au susținut poziția Georgiei și au acuzat F.Rusă, au devenit mai critice asupra împrejurărilor în care a fost declanșat conflictul, recunoscând drept falsă teoria referitoare la faptul că Georgia a fost victima inocentă a agresiunii ruse.

În concluzie, lecția învățată din punct de vedere militar și legislativ a fost că semnificația unui răspuns eficient pentru atacurile cibernetice de mărimea și tipul celor din Georgia este limitată de legislație. Mai important, răspunsul la aceste atacuri include promovarea unei cooperări tehnologice internaționale eficiente, deoarece nu

există nicio modalitate pentru o țară de a coordona apărarea împotriva unor astfel de atacuri. Trebuie însă ținut cont de faptul că nicio entitate națională sau internațională nu are autoritatea de a legifera în domeniul cibernetic, astfel încât eforturile naționale vor trebui conjugate cu instrumente internaționale din diferite domenii. În plus, tehnica atacului a fost interesantă. S-au observat similitudini care pot indica faptul că agresorul ar putea fi același, ca și în cazul Estoniei. Cu toate acestea, cazul Georgiei pare puțin diferit, în sensul că a fost un atac mai sofisticat. Au fost perturbate site-urile guvernamentale, precum și cele de servicii financiare, ale băncilor și ale ziarelor online. Ca urmare a acțiunii ostile, majoritatea serviciilor de Internet s-au prăbușit, iar restabilirea acestora a fost destul de greoaie.

ATACUL CIBERNETIC ASUPRA UCRAINEI

Al treilea atac cibernetic a fost cel din Ucraina, fiind considerat un caz de *spionaj cibernetic*. Înainte de revoluția din 2014, Ucraina a cunoscut o serie tipică de incidente cibernetice, dintre care cele mai frecvente au fost atacurile DDoS controlate de botnet. De multe ori, acestea au venit ca represalii pentru inițiativele guvernamentale nepopulare, precum încercarea autorităților de a închide site-ul de file-sharing *www.ex.ua*. Până la sfârșitul anului 2012, o parte din frustrarea publicului a fost canalizată în deteriorarea site-urilor motivate politic din spațiul virtual al guvernului ucrainean.

În anul 2013 a evoluat tot mai agresiv domeniul programelor malware, iar vandalismul de rețea a generat o creștere a spionajului cibernetic, pentru care societățile comerciale de securitate cibernetică au completat o „listă roșie" de nume, precum *RedOctober*, *MiniDuke*, *NetTraveler* și multe altele. După ce a început revoluția din februarie 2014, ucrainenii de rând au devenit familiarizați cu combinația de hacking și activism politic - *hacktivism*, în care atacatorii poartă războiul psihologic prin intermediul Internetului. Deși un număr mare de persoane au simțit presiunea evenimentelor politice importante ce au clătinat Ucraina, a fost greu să ignore publicarea de scurgeri de documente guvernamentale ucrainene. Cel mai influent grup *hacktivist* a fost *CyberBerkut*, al cărui atac faimos a creat probleme serioase infrastructurii țării.

Nikolay Koval, șeful CERT-UA (*Computer Emergency Response Team* din Ucraina), a găsit răspunsuri în multiplele incidente și a aflat că, prin deținerea de dovezi suficiente, este de obicei posibil să se înțeleagă natura generală a unui atac, inclusiv cine ar putea fi atacatorii și ce urmăresc aceștia. Durata, contextul, identitatea victimelor și gradul de sofisticare al malware-ului sunt indicatori buni. Acesta a subliniat faptul că „un spyware de ultimă generație este probabil să fie găsit pe calculatoarele oficialilor guvernamentali de rang înalt sau pe nodurile importante de rețea din cadrul infrastructurii critice naționale"[14].

CERT-UA, în colaborare cu firme de securitate de rețea, precum *Kaspersky Lab*, *Symantec*, *ESET*, a fost capabilă de a „detecta, izola și elimina amenințările grave la rețeaua de securitate din Ucraina"[15]. Unul dintre incidente a fost reprezentat de *atacul hacktivist* din timpul alegerilor prezidențiale din Ucraina. Pe 21 mai 2014, *CyberBerkut*, prin dezactivarea nodurilor de rețea de bază CEC (*Central Election Commission*), a compromis numeroase componente ale sistemului electoral. Timp de 20 de ore, software-ul care a fost proiectat să afișeze actualizări în timp real la numărătoarea voturilor nu a funcționat corect. La data alegerilor - 25 mai, cu 12 minute înainte de închiderea urnelor, atacatorii au postat pe pagina web a CEC o imagine a liderului ucrainean Dmitry Yarosh, susținând că el a câștigat alegerile. Această imagine a fost prezentată imediat pe canalele de televiziune ruse. Atacul nu a influențat voturile din Ucraina deoarece toți cetățenii au votat pe hârtie cu ștampilă de vot și toate voturile au fost verificate manual.

Aspectele tehnice ale atacului au dezvăluit faptul că atacatorii sunt profesioniști. CERT-UA a descoperit că, înaintea atacurilor asupra site-urilor, au fost executate acțiuni de spionaj cibernetic prin infectarea rețelei CEC cu malware de tip *Sofacy/APT28/Sednit*. Cele două aspecte, de distrugere și spionaj cibernetic, sunt

complementare, hackerii trebuind să realizeze un tur de recunoaștere a țintei înainte de a porni un atac serios. Astfel, *CyberBerkut* a declarat că „a găsit și a exploatat o vulnerabilitate de ziua zero în software-ul Cisco ASA de la CEC”[16]. Experții cred că „este imposibil ca un grup de hackeri non-statali să poată avea un asemenea nivel de expertiză pentru exploatarea unei vulnerabilități zero-day”[17], iar de aici s-a tras concluzia că grupul este sprijinit de un stat. Pregătirea acestui atac a început cu cel puțin două luni înainte de alegeri, iar nivelul de pregătire a atacatorilor a fost unul ridicat, aceștia reușind să pătrundă în rețeaua CEC cu rolul de administrator.

Au existat operațiuni de spionaj cibernetic semnificative, legate de interesele strategice ale F.Ruse, în special în ceea ce privește situația din Ucraina. Cu toate acestea, nu s-au văzut atacuri profilate, coercitive și dăunătoare similare cu cele desfășurate în Estonia în 2007 sau în Georgia în 2008. Exemplele raportate public de CNA (*Computer Network Attack)* în Ucraina includ, în principal, atacurile DoS și DDoS, proiectate pentru a submina infrastructura ucraineană de telecomunicații. Pentru atacatori, acestea au fost modalități cu risc scăzut în perturbarea fluxului de informații din spațiul național de securitate ucrainean, precum și o modalitate de reducere selectivă și temporară a traficului online. Câteva informații cu privire la aceste incidente cibernetice au fost sintetizate, astfel:

- noiembrie 2013: hackerii ruși au defăimat și au atacat prin DDoS site-urile mai multor posturi de televiziune din Ucraina, diverse alte posturi de știri și ale unor politicieni;
- februarie 2014: trupe ruse specializate au accesat cablurile de fibră optică din Ucraina și au inspectat Ukrtelecom, care a declarat că a pierdut capacitatea tehnică de a asigura conexiunea între peninsula Crimeea și restul Ucrainei (în Crimeea au fost afectate toate rețelele - telefonia fixă și mobilă, accesul la Internet);
- martie 2014: pe măsură ce trupele ruse au intrat în Crimeea, site-ul principal al guvernului ucrainean a fost închis timp de aproape 72 de ore, multe alte site-uri guvernamentale și mass-media oficiale au fost vizate în atacurile DDoS, iar telefoanele mobile ale multor parlamentari ucraineni au fost de asemenea atacate;
- mai 2014: grupul hacktivist pro-rus CyberBerkut a revendicat responsabilitatea atacului asupra sistemelor Comisiei Electorale Centrale din Ucraina cu malware care ar fi eliminat rezultatele alegerilor prezidențiale; cu toate acestea, SBU (Serviciul de Securitate al Ucrainei) a eliminat malware-ul și a înlocuit programul electoral înainte de vot.

În conflictul F.Rusă-Ucraina, din 2014, operațiunile în rețelele informatice nu s-au limitat la noțiunea de război cibernetic. O examinare a tensiunilor susținute sugerează că acesta a fost un război purtat pentru „furt strategic și manipularea informațiilor“ și nu pentru aplicarea pe scară largă a atacurilor cibernetice distrugătoare. Campaniile de spionaj cibernetic inițiate din Rusia, desfășurate de-a lungul timpului și împotriva a numeroase ținte, au, fără îndoială, un avantaj considerabil în înțelegerea, anticiparea și, în unele cazuri, depășirea inamicilor. Această abordare poate să fi făcut DDoS și alte atacuri distructive mai puțin necesare sau preferabile. Unul dintre cele mai importante aspecte ale celor trei cazuri este autorul acestora. Arhitectura spațiului cibernetic nu permite să se afirme fără echivoc cine a fost responsabil pentru atacurile cibernetice. Cert este că majoritatea atacurilor a venit din spațiul F.Ruse, iar acest lucru poate conduce către trei ipoteze.

Prima ipoteză se bazează pe presupunerea că atacurile au fost efectuate de către amatori ruși, *hackeri patrioți* care doreau să atace cibernetic pentru a-și exprima afrontul față de jignirea adusă de politicile Estoniei și Georgiei. Această ipoteză este puțin probabilă, mai ales din cauza lipsei de competențe tehnice ale acestor hackeri. În timpul atacurilor, botnet-urile avansate au constat în utilizarea a mii de computere ce sunt inaccesibile pentru utilizatorii medii de Internet. În plus, în cazul Ucrainei, rețelele sociale ruse ale hackerilor nu au fost implicate.

Cea de-a doua ipoteză a presupus că atacurile au fost efectuate de grupurile ruse de tip *crimă*

organizată cibernetică, pe cont propriu, în special de rețelele ruse de afaceri. Folosirea botnet-urilor avansate deținute de infractorii cibernetici ruși a subliniat angajamentul hackerilor ruși. Aceste grupuri urmăresc, în principal, obținerea unor sume de bani. Este greu de menționat potențialele beneficii financiare care ar fi putut fi obținute prin atacarea site-urilor georgiene, estone și ucrainene. Din această cauză, aceste ipoteze par improbabile.

Cea de-a treia ipoteză se bazează pe presupunerea că autoritățile ruse au angajat infractori cibernetici din *Rețeaua de Afaceri a Rusiei* pentru a conduce atacuri împotriva Estoniei, Georgiei și Ucrainei. Această teză pare cea mai probabilă din mai multe considerente. F.Rusă a vrut să pedepsească aceste țări, dar nu a putut, mai ales în cazul Estoniei - membru al NATO. Așadar, a fost convenabil să angajeze infractori cibernetici care au purtat campania ofensivă în numele autorităților ruse. Cel de-al doilea aspect important este controlul deplin al fluxurilor de Internet din spațiul rus de către autoritățile de la Moscova, astfel că un atac de o asemenea amploare nu ar fi putut trece neobservat de către autorități, deci au fost făcute cu acordul tacit al guvernului rus.

Lecția învățată în Ucraina a constat în lipsa fundamentală de înțelegere a securității cibernetice din partea utilizatorilor. Prin urmare, la fiecare instituție s-a încercat realizarea unei *campanii de instruire* despre malware pentru ca angajații să cunoască modul în care încep infectările în sistem și modul în care atacatorii pot controla ulterior computerele lor pentru a fura documente, toate prin intermediul unui program de dimensiuni mici, neautorizat, care poate fi greu de detectat. Lipsa de experiență și percepția privind amenințarea cibernetică, atât din partea populației, cât și a instituțiilor publice și private, sunt motivele-cheie pentru care realizarea unui consens internațional cu privire la elementele de securitatea cibernetică are, încă, multe deficiențe.

CONCLUZII

În urma analizei celor trei cazuri de atac cibernetic, putem afirma că există o tendință în ceea ce privește viitorul concurenței militare în spațiul cibernetic. Din punct de vedere militar, societatea informațională a determinat dezvoltarea unor cazuri specifice de atac în noul spațiu concurențial - ***spațiul cibernetic***. Asemănător acțiunilor clasice, sunt utilizate atât instrumente și acțiuni simple, cât și atacuri cibernetice desfășurate după reguli și legi hibride.

Pe baza lecțiilor de natură militară și juridică identificate și învățate din recentele atacuri cibernetice publice, se pare că o modalitate contemporană de a ataca cibernetic o țară este *utilizarea zonei gri*. Astfel, va fi nevoie de timp pentru a se ajunge la un consens suplimentar privind aspectele juridice de apărare cibernetică la nivel internațional. Mai mult, pregătirea țărilor în domeniul securității cibernetice este diferită și ține de gradul lor de dezvoltare economică și militară. Acele țări care au asistat și au experimentat atacuri cibernetice au recunoscut, de asemenea, că există restricții semnificative în ceea ce privește utilitatea reglementărilor privind criminalitatea cibernetică pentru astfel de atacuri.

Lecțiile învățate din aceste trei cazuri de atac cibernetic au arătat diverse fațete ale securității și apărării cibernetice din punct de vedere tehnic, legislativ, social, diplomatic și militar. Ca urmare, măsurile de securitate cibernetică trebuie să fie rezultatul unei uniri de forțe între specialiștii IT guvernamentali, cei din sectorul privat și public, precum și din partea altor actori statali specializați în securitate cibernetică.

Toate atacurile cibernetice ruse care au avut loc în perioada 2007-2014, precum și celelalte executate asupra unor state din afara spațiului est-european, inclusiv asupra SUA, au avut o mulțime de asemănări, precum contextul politic, metodele, tehnicile și tacticile folosite ori autorii ipotetici. Contextul politic înainte de atacuri era aproape similar. Toate cele trei țări, în acea perioadă, au avut relații tensionate cu F.Rusă.

Mediul operațional cibernetic va continua să evolueze, prezentând forțelor militare provocări variate sub forma amenințărilor generate de către oponenți, care desfășoară acțiuni al căror caracter variază de la convențional la neconvențional, cu capabilități care presupun armament și tehnologie

de ultimă generație. Acești oponenți pot include în compunerea lor forţe convenţionale extrem de bine pregătite pe componenta IT și echipate corespunzător, precum și forțe specializate în desfășurarea acțiunilor de luptă neregulate, rezultatul fiind o forţă care întrebuinţează amenințarea de tip hibrid. În plus, în cele mai multe cazuri, nu se poate conta pe sprijinul populației locale în eliminarea acestor amenințări.

Din punct de vedere militar, spațiul cibernetic a determinat apariția armelor cibernetice, utilizate în noi tipuri de operații militare, care diferă de cele clasice prin modul de manifestare, scopul fiind același - eliminarea adversarului. Oricare ar fi tipul de conflict în viitor, terorismul cibernetic va fi integrat în toate formele de război, convențional sau neconvențional. Din cauza caracterului transfrontalier al acțiunilor realizate pe Internet la adresa guvernelor, organizații precum NATO și UE au recunoscut importanța spațiului cibernetic și au lansat o serie de proiecte de cooperare între statele membre ce vizează securitatea cibernetică, instruirea și educarea în acest domeniu multidisciplinar.

BIBLIOGRAFIE

1. ASHMORE William C., *Impact of Alleged Russian Cyber Attaks*, SAMS, 2009, online http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-027.pdf, accesat 10 aprilie 2019.
2. CARR Jeffrey, *Inside Cyber Warfare*, O'Reilly Media, 2009, accesat 17 aprilie 2019.
3. DENNING Dorothy, *Cyberterrorism*, online http://palmer.wellesley.edu/~ivolic/pdf/Classes/ Handouts/NumberTheoryHandouts/Cyberterror Denning., accesat 11 aprilie 2019.
4. FOXALL Andrew, *Putin's Cyberwar: Russia's Statecraft in the Fifth Domain*, Russia Studies Centre Policy Paper No. 9, 2016, accesat 12 aprilie 2019.
5. GEERS Kenneth, *Cyber War in Perspective: Russian Aggression against Ukraine*, NATO CCD COE Publications, Tallinn 2015, accesat 16 aprilie 2019.
6. GREENBERG Andy, *The State of Cyber Security When Cyber Terrorism Becomes State Censorship*, Forbes.com, 2008, online http://www.forbes.com/2008/05/14/cyberattacks-terrorism-estonia-tech-security08-cx_ag_0514attacks, accesat 10 aprilie 2019.
7. KOZŁOWSKI Andrzej, "Comparative analysis of cyberattacks on Estonia, Georgia and Kyrgyzstan", *European Scientific Journal*, February 2014, Vol. 3, online http://www.eujournal.org/index.php/esj/article/view/2941, accesat 09 aprilie 2019.
8. NAZARIO Jose, *Politically Motivated Denial of Service Attacks*, NATO CCDCOE, 2014, online https://ccdcoe.org/sites/default/files/multimedia/pdf/12_NAZARIO%20Politically%20Motivated %20 DDoS.pdf, accesat 09 aprilie 2019.
9. Project-Grey-Goose-Phase-I-Report on Georgia.pdf, 2008, online https://www.scribd.com/doc/6967393/ Project-Grey-Goose-Phase-I-Report, accesat 16 aprilie 2019.
10. SCHMITT Michael, VIHUL Liis, *Tallinn Manual 2.0: On The International Law Applicable To Cyber Operations*, Cambridge University Press, 2017, accesat 16 aprilie 2019.
11. Tratatul Atlanticului de Nord, Washington DC, 4 aprilie 1949, online http://www.mae.ro/sites/default/files/file/pdf/Tratatul%2520Nord-Atlantic.pdf, accesat 12 aprilie 2019.
12. TIKK Eneken, KASKA Kadri, RÜNNIMERI Kristel, KERT Mari, TALIHÄRM Anna-Maria, VIHUL Liis, *Cyber Attacks Against Georgia: Legal Lessons Identified*, NATO - CCDCOE, 2008, online http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf, accesat 14 aprilie 2019.
13. http://www.ismlab.usf.edu/isec/files/Georgia-Cyber-Attack-NATO-Aug-2008.pdf, accesat 16 aprilie 2019.

[1] Andrzej Kozłowski, *Comparative analysis of cyberattacks on Estonia, Georgia and Kyrgyzstan*, European Scientific Journal February 2014, Edition Vol.3, European Scientific Journal (ESJ), disponibil online pe site-ul http://www.eujournal.org/index.php/esj/article/view/2941, pp. 238-239, accesat la 09.04.2019.

[2] Jose Nazario, *Politically Motivated Denial of Service Attacks*, NATO CCDCOE, disponibil online pe site-ul https://ccdcoe.org/sites/default/files/multimedia/pdf/12_NAZARIO%20Politically%20 Motivated %20 DDoS.pdf, p. 3, accesat la 09.04.2019.

[3] *Ibidem*.

[4] Un botnet este un grup de computere conectate în mod coordonat în scopuri rău intenționate. Acești roboți formează o rețea de computere compromise, care este controlată de o terță parte și utilizată pentru a transmite malware sau spam sau pentru a lansa atacuri. O rețea bot este cunoscută și ca o armată de zombi (Techopedia Dictionary).

[5] Jose, Nazario, *op.cit.*

[6] Software-ul rău intenționat, cunoscut în mod obișnuit ca malware, este orice software care dăunează unui sistem computerizat. Programele malware pot fi sub formă de viermi, viruși, troieni, spyware, adware și rootkit-uri etc., care fură date protejate, șterg documente sau adaugă software neaprobat de un utilizator (Techopedia Dictionary).

[7] Un *botnet herder* (sau *bot herder)* este o persoană care controlează și menține o rețea bot instalând software rău intenționat în numeroase mașini, punând aceste mașini sub controlul său. Aceste „turme" de mașini bot, numite și zombi, pot fi apoi folosite pentru a ataca sau infecta alte mașini (Techopedia Dictionary).

[8] William C. Ashmore, *Impact of Alleged Russian Cyber Attaks*, SAMS, 2009, disponibil online pe site-ul http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-027.pdf, din data de 21.05.2009, pp. 34-35, accesat la 10.04.2019.

[9] Andy Greenberg, *The State of Cyber Security When Cyber Terrorism Becomes State Censorship,* Forbes.com, disponibil online pe site-ul http://www.forbes.com/2008/05/14/cyberattacks-terrorism-estonia-tech-security08-cx_ag_0514attacks. html, din data de 24.05.2008, accesat la data de 10.04.2019.

[10] Andrew Foxall, *Putin's Cyberwar: Russia's Statecraft in the Fifth Domain,* Russia Studies Centre Policy Paper No. 9 *(2016*), The Henry Jackson Society, May 2016, disponibil online pe site-ul http://www.stratcomcoe.org/do wnload/file/fid/5212, p.12, accesat la data de 11.04.2019.

[11] Andrzej Kozłowski, *op.cit.*, p.240.

[12] Jeffrey Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld*, O'Reilly Media, 2009, p.15.

[13] Project-Grey-Goose-Phase-I-Report on Georgia.pdf, https://www.scribd.com/doc/6967393/ Project-Grey-Goose-Phase-I-Report, 17 octombrie 2008, p.8, accesat la data de 29.04.2019.

[14] Kenneth Geers (Ed.), *Cyber War in Perspective: Russian Aggression against Ukraine,* NATO CCD COE Publications, Tallinn 2015, pp.50-55.

[15] *Ibidem*, p.57.

[16] *Ibidem*, p.60.

[17] Michael Schmitt, Liis Vihul, *Tallinn Manual 2.0: On The International Law Applicable To Cyber Operations*, Cambridge University Press, 2017, p.162.

PSIHOLOGIA CRYPTOCURRENCY

*Cristian DOBRE**

Abstract

In the last period of time, it has been observed the emergence of a new branch of psychology – the psychology of cryptocurrency.

This article does not has a holistic approach but its intention is only to answer some specific questions relevant for defense domain, that – What is the relevance of this for the defense and security domain? Why should the defense professionals have to be prepared for interaction with this kind of new currency? What is going to be the impact of integration of cryptocurrencies on daily life.

Keywords: *cryptocurrency; block-chain; bitcoin; adaptation; psychology.*

DE UNDE A PORNIT ERA CRIPTOMONEDELOR?

Cu certitudine, abordarea domeniului criptomonedelor ar trebui să înceapă de la istoria sa. Astfel, în anul 1983, americanul David Chauma a creat primul sistem de „bani electronici", numit „ecash". Acesta l-a dezvoltat, ulterior, prin intermediul aplicației „Digicash", care permitea transmiterea electronică a banilor, la distanță, pe baza unor sisteme de chei criptate. În acest lanț puteau fi implicate atât băncile, cât și simplii cetățeni care aveau cont pe Internet. În anul 1998, chinezul Wei Dai a creat „Crypto++", care era o librărie criptografică ce permitea lansarea sistemului monetar „b-money" și a unui algoritm de autentificare asociat (VMAC). Apoi, în anul 2009, presupusul cetățean japonez Satoshi Nakamoto a creat prima criptomonedă descentralizată, cunoscută sub numele de „Bitcoin".

După această dată au început să apară și alte criptomonede descentralizate, astfel că la nivelul anului 2018 numărul acestora era de aproximativ 1800. Unele dintre criptomonede au reușit să supraviețuiască, dar altele au dispărut pe parcurs. În prezent, mediul virtual este „populat" cu numeroase astfel de criptomonede, care însumează o cifră de afaceri considerabilă, de ordinul miliardelor de dolari. Tranzacționarea lor a devenit sigură și din ce în ce mai facilă, materializându-se și în realizarea unor „cripto-bancomate", care permit, în cele din urmă, extragerea de bani cash de către orice cetățean, în moneda țării sale sau într-o valută agreată. Astfel de terminale pot fi întâlnite chiar și în România.

În paralel cu criptomonedele de tip „Bitcoin", mai viețuiesc în spațiul virtual și „altcoin"-urile, reprezentate de tokene (fungibile și non-fungibile) și alte tipuri de criptomonede, care permit realizarea mai rapidă a tranzacțiilor financiare, a contractelor inteligente și a conversiei criptomonedelor, cu ajutorul block-chain-urilor. „Ethereum", „Litecoin" și altele sunt doar câteva astfel de exemple.

Spre deosebire de banii clasici, tipăriți de bănci, în funcție de interesele emitenților, criptomonedele descentralizate nu aparțin unui

* *Autorul este expert în cadrul Ministerului Apărării Naţionale.*

stat sau unei bănci. Acestea sunt „minate”, adică sunt create de milioane de entități din întreaga lume, pe baza unor algoritmi criptați, care nu pot fi virusați, iar fiecare tranzacție este controlată de sute de milioane de „mineri” angrenați în acest proces inimaginabil de transformare a curentului electric în valoare. Asemenea banilor clasici, criptomonedele nu au valoare intrinsecă, dar, spre deosebire de banii clasici, a căror valoare este dată în mod centralizat și convențional de politicile monetare ale statelor, aceste criptomonede primesc valoare direct de la utilizatorii lor din întreaga lume, în mod liber și descentralizat.

În contextul acestei noi realități mondiale – în care tehnologia, finanțele, economia, sociologia și psihologia se întâlnesc – experți financiari, juriști și economiști de prestigiu au început să studieze noua creație financiară descentralizată, care „trăiește” pe „block-chain”, în mediul virtual și care se dezvoltă spectaculos, în paralel cu sistemul monetar centralizat, guvernat de bănci și de interesele de stat (Law, Sabett, Solinas, 1996). În același timp, o mulțime de țări, inclusiv România, au început să introducă în legislația proprie referiri la criptomonede (de exemplu, Codul fiscal). Pe de altă parte, unele guverne au interzis cu desăvârșire utilizarea criptomonedelor pe teritoriul lor (Algeria, Bolivia, Egipt, Irak, Maroc, Nepal, Pakistan, Emiratele Arabe Unite), iar altele au impus tot felul de restricții.

În prezent, în paralel cu criptomonedele descentralizate, din ce în ce mai multe bănci au inițiat studii, protocoale și chiar criptomonede funcționale (de exemplu, Banca Chinei). Acestea din urmă, însă, sunt centralizate și controlate de respectivele bănci și de emitenți.

Dezvoltarea criptomonedelor a impus și o serie de cuvinte dedicate domeniului: „crypto-currency”, „block-chain”, „nodes”, „time-stamping”, „mining”, „e-wallet”, „anonymity”, „atomic swaps”, „public and private keys” etc. Toate aceste schimbări majore ale pieței financiare, de la nivel macro, unde se tranzacționează milioane de USD, până la nivel micro, în care oricare cetățean poate deține fracțiuni de criptomonede, cu valori de zeci de USD, pot să-i găsească pe cei mai mulți oameni nepregătiți din punct de vedere psihologic și economico-financiar pentru a face față noii realități. Uneori, aceste aspecte sunt perfect aplicabile și instituțiilor și firmelor, care pot prezenta lipsă de reziliență în fața acestei provocări, pe cât de imaterială pe atât de prezentă în viața noastră, a tuturor.

CARE ESTE „CICLUL EMOȚIILOR” ÎN PIAȚA CRIPTOMONEDELOR?

Angrenarea unei entități (individuale sau colective) în piața criptomonedelor presupune o serie de emoții. Acestea pot oscila pe o plajă foarte largă, de la extaz la agonie, în funcție de diagrama de evoluție a respectivei criptomonede. Mulți experți ai pieței financiare apreciază faptul că emoțiile au un rol de „motor” și de „modelator” în configurarea tranzacțiilor financiare, a bursei sau a investițiilor. Astfel, rezultanta fluctuațiilor emoțiilor entităților implicate într-o anumită piață financiară (investitori, comercianți, clienți, analiști economico-financiari etc.) creează „ciclul psihologic al pieței”. Atunci când aceste emoții sunt pozitive, piața are un trend ascendent, fapt cunoscut sub denumirea de ”bull-market”, iar când emoțiile entităților implicate devin negative, piața „intuiește” aceste sentimente și devine ”bear market”, iar ca rezultat, totul se prăbușește. Acest torent de emoții umane existent în piață este contagios și afectează mulțimi extrem de numeroase de oameni implicați în respectiva afacere.

Potrivit unei meta-analize efectuate pe articolele de specialitate publicate în ultimii ani, s-a putut observa următoarea tipologie a emoțiilor trăite de persoanele care au investit în criptomonede, în nume propriu sau al unei firme:

Neîncrederea. Aceasta este specifică, în general, celor care nu dețin cunoștințe despre acest instrument financiar și care au auzit tot felul de povești contradictorii. Această emoție mai este prezentă la persoanele care au pierdut bani pe seama criptomonedelor. Comportamental, aceste persoane nu investesc în criptomonede ori își retrag banii (cât au mai rămas!) din investiție și au o atitudine negativă față de viitorul criptomonedelor.

Speranța. Această atitudine îi caracterizează pe cei care au îndrăznit să investească în criptomonede și observă că banii lor sporesc constant în intervalul de timp ce urmează imediat după achiziția criptomonedei. Cei mai mulți se implică în piața criptomonedelor ca o reacție de conformism social, din următoarele motive: au observat la cunoscuții lor că și aceștia fac același lucru; este la modă/„trendy"; poate fi profitabilă (Oberstand, 2017). Această emoție mai este prezentă la persoanele care realizează faptul că deși au trecut printr-o perioadă financiară dificilă, generată de scăderea valorii criptomonedei în care au investit, aceasta începe, în cele din urmă, să crească sau, cel puțin, se oprește din scădere. Emoția de referință este asociată cu ideea că, probabil, în viitor, criptomoneda o să recupereze pierderea și o să revină la nivelul anterior, dacă nu chiar mai sus. Comportamental, aceste persoane așteaptă să vadă ce se va întâmpla cu evoluția criptomonedei în care au investit; ele dezvoltă o atitudine optimist-realistă cu privire la viitorul criptomonedei de referință și la viitorul sistemului "criptocurrency".

Optimismul. Se regăsește, de regulă, la persoanele care observă faptul că valoarea criptomonedei continuă să crească în mod constant, potrivit așteptărilor anterioare. Prin urmare, optimismul se asociază cu creșterea încrederii în moneda respectivă: comportamental, aceste persoane vor începe să investească în respectiva criptomonedă pe măsură ce încrederea lor crește. Atitudinea pozitivă față de "criptocurrency" se amplifică pe măsură ce valoarea investiției crește. Unele persoane își diversifică investițiile în criptomonede și încearcă și alte variante existente pe piață, iar sumele investite cresc gradual, pe măsură ce încrederea în criptomonede se consolidează. Totodată, crește interesul pentru a afla noi detalii teoretice despre piața descentralizată de valori.

Euforia. Este prezentă la persoanele care trăiesc creșteri spectaculoase, pe unitatea de timp, ale criptomonedei în care au investit. Comportamental, aceste persoane investesc și mai mult în "criptocurrency", își diversifică investițiile și în alte produse „cripto" și recomandă cunoscuților să procedeze în același fel. Ei devin vectori marcanți ai promovării criptomonedelor în toate mediile sociale, constituind, prin exemplul lor personal, modele de succes pentru comunitățile în care trăiesc. În numeroase situații, orbiți de euforia câștigului rapid, aceste persoane investesc irațional și cu lăcomie, tot ce au sau chiar se împrumută pentru a cumpăra și mai multe unități criptomonetare, în speranța multiplicării cât mai rapide a câștigului. Euforia se asociază, în cele mai multe situații, cu depășirea vârfului valoric anterior al criptomonedei respective și atingerea unuia nou, uneori nebănuit de mare. De exemplu, Bitcoin valora 10 USD la 2 iunie 2011, 100 USD la 1 aprilie 2013, 1.000 USD la 27 noiembrie 2013, 10.000 USD la 1 decembrie 2017, 63.347 USD la 16 aprilie 2021, pentru ca în august 2021 să oscileze în jurul valorii de 38.000 USD.

Calmul. Caracterizează persoanele care au investit în momentul în care valoarea criptomonedei scade un pic, dar valoarea acesteia își revine într-un timp relativ scurt. Aceste persoane se auto-liniștesc și își spun că este un fenomen normal, iar în scurt timp criptomoneda își va reveni, exact cum a făcut și în trecut. Comportamental, aceștia își monitorizează cu atenție investiția, iar volumul unor noi achiziții scade. Propagat în serie, asemenea unei reacții nucleare în lanț, fenomenul se amplifică la nivelul întregii piețe a respectivei criptomonede, iar aceasta stagnează.

Anxietatea. Apare atunci când trendul de scădere continuă dincolo de așteptările persoanei care a investit în criptomonede. În funcție de valoarea investiției și de personalitatea subiectului, nivelul anxietății poate fi mai mare sau mai mic. Acesta începe să-și facă reproșuri cu privire la comportamentul său anterior legat de creditarea prea mare a respectivei monede și de faptul că nu a urmat eventualele sfaturi ale cunoscuților de a se retrage la timp.

Negarea. Aceasta este o emoție ce apare în situația în care trendul descrescător al criptomonedei continuă. Ea se asociază cu un blocaj cognitiv, generat de faptul că subiectul refuză să creadă că toată investiția a fost în zadar.

Apar sentimente de speranță, care nu se sprijină, însă, pe date concrete. Comportamental, subiectul nu întreprinde nici un demers acțional, iar piața va continua să prăbușească criptomoneda, urmare a scăderii tranzacțiilor. Mulți investitori gândesc că „este deja prea târziu să vândă".

Panica. Aceasta se declanșează brusc și neașteptat, atunci când subiectul realizează că trendul descendent continuă vertiginos, valoarea criptomonedei se prăbușește sub nivelul investiției inițiale, iar fiecare secundă înseamnă pierdere sigură pentru el. Comportamental, el încearcă să salveze, în mare grabă, ce mai poate. Acțiunea unui asemenea investitor este însoțită de acțiunile a milioane de investitori care trăiesc exact aceleași emoții, în același timp. Așadar, panicați, investitorii vor vinde cât mai repede criptomoneda, accentuându-i și mai mult devalorizarea. Se spune că „piața a capitulat", chiar dacă, în cele din urmă, ea se stabilizează la o anumită valoare.

Dezamăgirea. Sentimentul se manifestă atunci când investitorii au trăit un minim istoric al respectivei criptomonede. De regulă, cei mai mulți au pierdut sume importante de bani sau s-au retras cu pagube incalculabile din respectiva investiție. Dezamăgirea este însoțită de furie îndreptată spre terțe ținte (pe cei care au manipulat piața, pe cei care ar fi putut să o salveze și nu au făcut-o, pe analiști, pe sine etc.). În funcție de personalitatea fiecărui investitor, dezamăgirii i se pot asocia și alte emoții negative, unele putând fi situate chiar la granița cu zona clinică.

Și totuși, criptomoneda își vede de drumul său sinusoidal, ascendent, descendent, ascendent etc., chiar dacă în unele situații reluarea sinusoidei poate să dureze mai mult timp. Cu alte cuvinte, mai există o emoție umană care nu permite respectivei criptomonede să iasă de pe piață. Aceasta este încrederea. Astfel, persoanele familiarizate cu acest ciclu de evoluție al criptomonedelor nu numai că își vor păstra banii investiți în acestea și vor aștepta ca ele să renască, potrivit paternului de evoluție specific al fiecărei criptomonede în parte, dar vor cumpăra criptomonedă atunci când toți sunt în panică (și prețul acesteia este foarte mic) și o vor vinde atunci când cei mai mulți sunt în faza de euforie (adică criptomoneda are cea mai mare valoare). Pentru a manifesta un astfel de comportament, însă, sunt necesare atât cunoștințe serioase cu privire la "criptocurrency" și o disponibilitate financiară a entității respective față de acest instrument financiar (pe cât de nou și de spectaculos, pe atât de provocator și perturbator), cât și o puternică stabilitate psihologică a „jucătorului" pe piața criptomonedelor.

Din punct de vedere psihologic, criptomonedele sunt atractive deoarece permit realizarea de profituri mari în intervale relativ mici de timp, cu efort minim sau economisirea banilor, la o rată pozitivă a dobânzii, pe termen lung. Din această perspectivă, pentru a menține un confort psihologic optim, se recomandă ca investitorii să țină seama de o serie de sfaturi utile, dintre care amintim:

- *analiza pragmatică a riscului* presupus de fiecare criptomonedă în parte, pe baza graficelor de evoluție ale acestora, pe durate cât mai mari de timp, și minimizarea acestuia cât mai mult posibil (investitorii ar trebui să-și seteze un nivel al riscului înainte de a-și utiliza banii în piața criptomonedelor);
- *diversificarea riscului*, în sensul că se recomandă investirea banilor clasici în mai multe criptomonede și nu într-un singur produs;
- *estimarea corectă a evoluției* criptomonedei – în mod normal, datorită volatilității sale mari, aceasta obișnuiește să aibă, frecvent, variații cuprinse între 20-25%/zi; dacă salturile, în special cele negative, sunt sub acest procent, atunci încrederea investitorilor în respectiva criptomonedă poate să scadă semnificativ, iar achiziționarea sa la un preț redus, dar generat de o scădere dramatică, poate să afecteze investiția deoarece respectiva monedă virtuală poate întâmpina probleme legate de refacere;
- *evitarea unor investiții păguboase* – investițiile masive într-o criptomonedă care crește spectaculos, cu peste 20-25%/zi,

sunt riscante, deoarece nu există controlul înregistrării maximului și apoi prăbușirii sale dramatice; de regulă, astfel de creșteri sunt „ajutate” de investitori strategici, uneori chiar instituționali, care au un interes specific în respectiva monedă;

- *păstrarea calmului*, atunci când toți și-l pierd, poate reprezenta o soluție bună de luat în calcul pentru evitarea panicii – o astfel de abordare se aplică, în special, atunci când investitorul respectiv dispune de o rezervă financiară confortabilă, care să-i permită existența chiar și în condițiile în care prețul criptomonedei scade sub cel de achiziție; evoluția sinusoidală, deja demonstrată a pieței „cripto”, reprezintă o garanție statistică a revenirii valorii respectivei criptomonede (acest aspect ciclic este creator de încredere);
- *luarea în considerare a bias-urilor cognitive* – atunci când oamenii au tendința de a se baza doar pe informațiile care le confirmă convingerile, ignorându-le pe celelalte, avem de-a face cu *bias*-ul de confirmare; asemenea acestui *bias*, se pot dezvolta și altele, care afectează judecata celor implicați în piața criptomonedelor, cu consecințe negative asupra investiției lor, în mod special, și a pieței, în general.

PE CE SE BAZEAZĂ PSIHOLOGIA PUNCTELOR FORTE ALE CRIPTOMONEDELOR?

Analiza punctelor forte ale criptomonedelor ne permite să punem în evidență și avantajele de natură psihologică, care definesc evoluția și chiar viitorul acestui nou instrument financiar.

Criptomonedele sunt valori monetare descentralizate, înregistrate pe block-chain-uri, prin contracte inteligente (acest sistem poate fi asimilat cu cel notarial mondial, doar că acesta ține evidența fiecărei tranzacții din spațiul virtual, la nivel mondial, fără nici un amestec din partea statelor). Astfel, dincolo de voința unei persoane, tranzacțiile sunt sigure, transparente și verificabile.

Criptomonedele asigură anonimatul investitorilor sau al celor ce le tranzacționează. Uneori, prin lege, băncile sunt obligate să pună la dispoziția autorităților date cu caracter confidențial cu privire la clienții lor. Sistemul ”cryptocurrency” nu poate fi interogat de nici un fel de autoritate statală sau supra-statală. Deși „portofelele virtuale” sunt perfect vizibile pe site-urile ”cryptocurrency”, numele real al deținătorilor nu este public.

Operarea cu criptomonedele este sigură. Acest lucru sugerează faptul că block-chain-ul nu poate fi corupt, virusat ori blocat, spre deosebire de sistemele financiare clasice ale băncilor, deoarece el este complet descentralizat și distribuit la nivel planetar, în milioane de calculatoare anonime.

Valoarea criptomonedelor este dictată direct de piața liberă și de încrederea investitorilor în ele, spre deosebire de banii clasici (FIAT), a căror valoare este stabilită prin politicile monetare ale statelor și organizațiilor financiare internaționale, în funcție de tot felul de interese politice ale momentului.

Viteza tranzacțiilor în criptomonede este mult mai mare decât prin utilizarea banilor clasici în cadrul sistemului bancar existent. Uneori, tranzacțiile de tip FIAT pot dura câteva zile până se materializează, iar taxele impuse de comisioanele bancare sunt destul de mari. În contra-partidă, tranzacțiile „crypto” sunt mult mai rapide, de cele mai multe ori oscilând de la câteva secunde la câteva minute.

Criptomonedele permit achiziționarea de bunuri din lumea reală, asemenea oricărei monede clasice. Acestea sunt echivalate, în cele din urmă, cu banii clasici, din perspectiva puterii lor de cumpărare.

Majoritatea criptomonedelor au ca valoare de referință dolarul american, o monedă clasică, recunoscută la nivel mondial, total convertibilă în orice altă valoare existentă pe piață. Acest lucru permite criptomonedelor să se țină la distanță de eventualele tendințe inflaționiste prezente în anumite economii, pe de o parte, și să evite crizele economico-financiare locale, regionale și chiar internaționale. În fapt, Bitcoin-ul a apărut ca o replică la criza financiară din 2008 din SUA, care s-a extins, apoi, la nivel mondial, cu o viteză impresionantă.

Bitcoin-ul are un mare potențial de creștere. Acest lucru a fost demonstrat de faptul că această criptomonedă a atins un vârf de 58.112 USD (21 februarie 2021), iar experții estimează că valoarea sa maximă ar putea depăși 500.000 USD, în câțiva ani (Strenlicht, 2021). În aceste circumstanțe, cu tot cu riscul de a prezenta salturi impredictibile de peste 35%, atât în sens pozitiv, cât și negativ, Bitcoin-ul rămâne extrem de atractiv pentru cea mai mare parte a fanilor criptomonedelor. În anumite situații, chiar adictiv.

Criptomonedele au devenit populare pentru o masă extrem de mare de oameni. Departe de a mai reprezenta un domeniu de nișă, criptomonedele au intrat în viața noastră de zi cu zi. Tânăra generație, mai familiarizată cu navigarea în mediul virtual, a fost prima care a îmbrățișat noua modă. Treptat, trendul ”cryptocurrency” s-a răspândit din cercurile elitiste spre marea masă de consumatori de Internet și nu numai. Astfel, în prezent, o mulțime de bunuri și servicii din piața reală pot fi achiziționate direct cu criptomonede.

Deținătorii de criptomonede nu sunt taxați/ impozitați de sistemele financiare ale statelor, atâta timp cât își păstrează investițiile în aceste active.

Viitorul aparține criptomonedelor. Deși pare greu de crezut, era digitală în care am intrat este orientată spre internaționalizare, multiculturalism, mediu virtual, descentralizare și companii multinaționale. În acest context, criptomonedele par a fi moneda viitorului.

Criptomonedele reprezintă inamicii publici principali ai sistemelor monetare clasice, în care mai puțin de 10% dintre bogații Planetei dețin peste 80% din resursele acesteia (inclusiv banii clasici). Astfel, băncile și guvernele vor lupta din greu pentru a discredita criptomonedele, pentru a nu produce dezechilibre în această ordine mondială a bunăstării.

În pofida tuturor interdicțiilor din unele state, *criptomonedele pot fi tranzacționate*. Astfel, prin utilizarea unor site-uri precum Paxful sau Bisq, pasionații de „crypto” își văd de treabă, în continuare. Acest element demonstrează că și cele mai drastice guverne nu se pot opune tranzacționării criptomonedelor. Mulți obișnuiesc să spună că viața criptomonedelor este tot atât de lungă și diversă ca a Internetului însuși.

PE CE SE BAZEAZĂ PSIHOLOGIA PUNCTELOR SLABE ALE CRIPTOMONEDELOR?

Analiza punctelor slabe ale criptomonedelor ne permite să punem în evidență și vulnerabilitățile de natură psihologică, care definesc evoluția și chiar viitorul acestui nou instrument financiar.

Criptomonedele sunt foarte volatile. Acest aspect face ca valoarea lor să oscileze foarte mult pe unitatea de timp.

Criptomonedele sunt sensibile la factorii de mediu. De exemplu, declarațiile unor formatori de opinie, ale unor oameni de afaceri de prestigiu, apariția unor legi anti-”cryptocurrency”, manipularea pieței de către „balene” (vând și cumpără masiv sume exorbitante de criptomonede) pot să le influențeze valoarea.

Criptomonedele sunt active speculative. Prețul lor poate fi crescut sau scăzut cu mare viteză, prin așa-zisele proceduri de tip ”pump or dump”. Așa ceva nu este posibil în cazul banilor clasici.

Criptomonedele au valoare zero sau chiar negativă, deoarece „ele nu numai că nu sunt recunoscute oficial de state ca având valoare, dar mai și consumă cantități impresionante de energie, pentru a fi produse.” (Roubini, 2021).

Criptomonedele nu pot oferi stabilitate, în situația stocării valorii. Afirmația se bazează pe volatilitatea foarte mare a activelor „crypto”.

Criptomonedele nu pot fi denominate într-un mod clar. Acest lucru face aproape imposibilă realizarea unui sistem de convertibilitate absolută între monedele de tip „crypto”.

Criptomonedele nu sunt scalabile. Faptul sugerează că dacă cineva și-a pierdut cheia privată de la portofelul virtual, și-a pierdut pentru totdeauna criptomonedele stocate în acesta. În cazul sistemului bancar clasic, atunci cineva își pierde cardul poate apela liniștit la banca emitentă, iar aceasta îi eliberează un nou card, fără să piardă nici măcar un cent.

Criptomonedele sunt controlate de monopoluri. Până a fi lansate pe piața liberă, emitenții criptomonedelor își opresc un stoc consistent din respectiva monedă, cu ajutorul căruia pot controla piața, la nevoie. În acest sens, este citat cazul Bitcoin-ului, al cărui creator deține un portofel virtual cu o valoare de aproximativ 30% din valoarea acestei monede existente pe piața liberă.

Criptomonedele nu reprezintă o investiție sigură pe termen lung, deoarece nu sunt stabile din punct de vedere valoric. Se spune că în caz de criză cele mai sigure active sunt: aurul, bunurile imobiliare, obligațiunile și chiar acțiunile unor companii serioase (Roubini, 2021).

Criptomonedele pot crea dependență, asemenea cu jocurile de noroc. Unele cercetări au arătat faptul că implicarea excesivă în tranzacționarea criptomonedelor poate genera aceleași efecte negative, cu influențe nocive asupra sănătății mentale (stres, anxietate, depresie, extaz adrenalinic, sinucidere, incapacitatea de a evalua realist riscul, activități obsesiv-compulsive etc.), fizice (oboseală cronică, boli cardiovasculare, boli sistemice, abuz de substanțe etc.), a relațiilor interpersonale (desocializare, orientarea puternică a interesului social spre zona virtuală, destrămarea familiei, reducerea activității sportive și în aer liber, tendințe infracționale – în cazul unor pierderi semnificative etc.), a carierei (dezinteres pentru activitatea desfășurată la locul de muncă, scăderea randamentului și a performanței profesionale etc.) și nu numai, ca în cazul jucătorilor împătimiți de pariuri sau jocuri de noroc (Strenlicht, 2021).

Criptomonedele au tendința de a crea "bubble market" (bule financiare în piață), adică de a fi supraevaluate în mod gratuit, fără un fundament real. Odată cu spargerea respectivei „bule" piața are tendința de a se prăbuși masiv, spre disperarea tuturor investitorilor implicați. De cele mai multe ori, apariția unei „bule" se datorează unor fenomene de natură psihologică: speranță, entuziasm, euforie etc.

Criptomonedele ar putea fi utilizate și de organizații situate în afara legii (crimă organizată, terorism etc.), deoarece tranzacțiile sunt anonime și greu de identificat.

EXISTĂ O SOCIOLOGIE A CRIPTOMONEDELOR?

În mod cert, una dintre cele mai interesante întrebări referitoare la criptomonede este „cine utilizează criptomonedele?" Astfel, realizând o meta-analiză a datelor prezente, se pare că utilizatorii majoritari se înscriu în următoarele pattern-uri sociologice: tineri și adulți până la 45 de ani; persoanele cu bani mulți, care au posibilitatea să și-i sporească și mai mult, rapid; persoanele din statele bogate, care utilizează criptomonedele pentru achiziții de servicii și bunuri; persoane din state în care nivelul inflației este foarte mare, iar valutele occidentale sunt greu de găsit; persoane din țări în curs de dezvoltare (în anumite astfel de state, Bitcoin a devenit o adevărată monedă națională – Columbia, Nigeria etc.); persoanele cărora le place riscul, având în vedere salturile valorice spectaculoase ale unor criptomonede; unele celebrități, care și-au făcut un obicei din a vorbi despre achizițiile lor în criptomonede (uneori, aceleași celebrități pot să le și prăbușească prețul în mod dramatic, așa cum a fost și cazul Bitcoin-ului după declarațiile incendiare ale lui Elon Musk din 2021).

Aceste date permit configurarea utilizatorului de criptomonede. Având în vedere media mică a vârstei utilizatorilor „crypto", mulți specialiști consideră că acest gen de activ va avea durată de viață mare, deoarece aparține, prin excelență, tinerei generații.

DE CE INVESTESC OAMENII ÎN CRIPTOMONEDE?

Analiza motivațiilor care îi determină pe oameni să investească în criptomonede dezvăluie un top selectiv al primelor motive, după cum urmează:

- Pe primul loc se situează *dorința de îmbogățire rapidă*. Multe persoane au realizat că dacă au noroc ori sunt inspirați, pot să-și sporească banii într-un mod rapid și ușor. Cu toate acestea, volatilitatea mare a criptomonedelor îi poate face și să piardă tot ce au, la fel de ușor și…simplu. Acest

motiv se asociază, deseori, cu nevoia de adrenalină dată de fluctuațiile mari ale valorilor criptomonedelor.

- Pe al doilea rând se situează *dorința de a face economii pe termen lung*. În acest sens, din analiza evoluției principalelor criptomonede, s-a observat că investițiile pe termen lung în criptomonede par a fi mai avantajoase decât depunerile bancare.
- Un al treilea motiv constă în *dorința de anonimitate și de eludare a taxelor*. Multe persoane se feresc să-și depună banii în bănci deoarece se consideră că acestea raportează organelor fiscale eventualele depuneri mai semnificative ale clienților. Acest motiv este citat mai ales de persoanele care obțin bani de pe piața neagră.
- Pe al patrulea loc se situează *ideea de modernitate și de viitor*. Mulți subiecți utilizează criptomonedele deoarece le consideră o legătură directă cu viitorul banilor. Aceștia obișnuiesc să invoce, în acest sens, ideea potrivit căreia, la apariția lor, criptomonedele nu valorau aproape nimic, iar în timp unele dintre ele și-au sporit valoarea chiar și de 990%.
- Următorul loc este ocupat de persoanele care dețin deja sume importante de bani în criptomonede și *au realizat potențialul investițional major în proiecte de tip „crypto”* sau în proiecte din lumea reală.
- În al șaselea rând regăsim motivațiile acelor *persoane care doresc să fie la modă* și au un coeficient mare de conformare la normele de grup. Acestea investesc în criptomonede deoarece mulți dintre cunoscuții lor o fac.
- Al șaptelea motiv face referire la subiecții care *au descoperit că pot crea valoare prin „minarea” de criptomonede*. Aceste persoane dețin echipamente sofisticate care permit rularea algoritmilor specifici creării de criptomonede, potrivit procedurilor specifice fiecărei crypto-currency.
- Locul opt în această selecție este ocupat de persoanele care au descoperit instrumentele financiare puse la dispoziție de diferite site-uri/companii specializate în „crypto” și *care au reușit să utilizeze criptomonedele în afaceri.*
- Ultimul loc în acest clasament este ocupat de motivația *persoanelor care detestă sistemele centralizate*, controlate de state și instituții financiare internaționale. Aceștia s-au orientat către lumea „crypto” descentralizată, găzduită de spațiul virtual și controlată prin block-chain-uri, la nivel mondial. Aceste persoane sunt mai rebele și nu suportă ideea controlului unei autorități centrale.

Acest „Top” poate să-și schimbe ierarhia motivațiilor, în timp, în funcție de tot felul de circumstanțe: efectele războiului dintre criptomonede și sistemele financiare clasice, fluctuațiile masive ale unor criptomonede, diversificarea instrumentelor financiare ce pot utiliza criptomonede, legătura criptomonedelor cu lumea reală, presiunile pieței, noile trenduri internaționale, câștigurile, respectiv pierderile pe care le pot avea pe unitatea de timp, personalitatea etc.

DE CE AR TREBUI SĂ ȘTIE MILITARII DESPRE CRIPTOMONEDE?

Deși domeniul criptomonedelor este, prin natura sa, unul economico-financiar, acesta a părăsit demult zona experților și a intrat puternic în fiecare societate, inclusiv în mediul securității. În acest context, apreciem util ca militarii să ia act de impactul psihologic al noului trend, în cazul în care sunt implicați ori vor dori să se implice. O evaluare justă a riscurilor personale îi va feri de șocuri psihologice majore, produse atât de creșterea, cât și de scăderea spectaculoasă a acestor criptomonede. Analiza motivațiilor și a sociologiei utilizării criptomonedelor a evidențiat că militarii se încadrează în zona de interes a potențialilor utilizatori.

Din perspectivă macro-economică, tranzacționarea masivă a criptomonedelor poate avea influențe majore și asupra sănătății afacerilor dintr-un anumit spațiu geografic și, de asemenea,

sursa: www.openaccessgovernment.org

poate influența chiar și securitatea națională și regională în anumite arii de interes (unele state sau entități non-statale pot să strângă rapid valută și pot accesa sisteme de arme și tehnologii la care nu ar avea acces în mod normal și legal, pot încălca embargouri, pot manipula piețele clasice, pot sponsoriza și derula acțiuni ostile etc.).

CONCLUZII

Departe de a fi epuizat subiectul, acest articol își propune să semnaleze implicațiile psihologice ale unei noi realități, care se construiește chiar acum sub ochii noștri, dar în spațiul virtual. Cel mai probabil, acest domeniu se situează la confluența dintre psihologia afacerilor/economică și cyber-psihologie (Dobre, 2020).

Confruntarea și coliziunea sistemului financiar clasic, centralizat, controlat de state și entități internaționale, cu cel descentralizat sunt la început de drum. Unii experți apreciază că apariția criptomonedelor reprezintă încă un succes al erei digitale, care a demonstrat, recent, pe timpul pandemiei de COVID-19, că multe lucruri de neimaginat cu puțin timp în urmă, au fost perfect realizabile (învățământul și munca de la distanță, tele-shopingul, tele-medicina, tele-psihologia etc.), în ciuda tuturor dificultăților de adaptare pe care le-am trăit.

Urmărirea cu atenție a acestor conflicte, a bătăliilor câștigate și pierdute de fiecare entitate în parte ne va putea ajuta să prognosticăm cât mai precis viitorul criptomonedelor și să ne adaptăm psihologic cât mai bine la lumea viitorului.

BIBLIOGRAFIE

1. DOBRE Cristian (2020), *PSYINT – Psychological Intelligence*, Editura CTEA, București.
2. HULBERT, M. (2021), *The psychology of a stock market bubble*, https://www.marketwatch.com/story/the-psychology-of-a-stock-market-bubble-11619198164.
3. LAW, L., Sabett, S., Solinas, J. (1996), How to Make a Mint: the Cryptography of Anonymous Electronic Cash, *The American Law Review* (Vol. 46, Issue 4), NSA.
4. LIN, M. (2021), *Why Investors are Irracional, according to behavioral finance*, https://www.toptal.com/finance/financial-analysts/investor-psychology-behavioral-biases.
5. STIEG, C. (2021), *Why people are so obsessed with bitcoin: The psychology of crypto explained*, https://www.cnbc.com/2021/01/23/why-people-invest-in-bitcoin.html.
6. STRENLICHT, L & Strenlicht, A. (2021). *Staring at Charts: Bitcoin and Cryptocurrency Addiction*, https://www.familyaddictionspecialist.com/blog/staring-at-charts-bitcoin-and-cryptocurrency-addiction.
7. OBERSTAND, P. (2017), *Psychological Biases you'll experience when it comes to traiding cryptocurrency*, https://medium.com/crobox/6-psychological-biases-youll-experience-when-it-comes-to-trading-cryptocurrency-8c7490086774.
8. *** (2018) https://letemspin.com/wall-street-cheat-sheet-psychology-of-a-market-cycle/
9. *** (2020) https://www.newsbtc.com/news/market-cycle-psychology-crypto-anxiety/
10. *** (2021) https://qz.com/2011333/the-psychology-behind-hodling-during-a-bitcoin-price-drop/
11. *** (2018) https://www.liteforex.com/blog/for-professionals/psyho/
12. *** (2021) https://www.zf.ro/business-international/economistul-prezis-criza-economica-2008-ataca-dur-bitcoin- valoare-19913408.
13. *** (2021) https://academy.binance.com/en/articles/the-psychology-of-market-cycles.
14. *** (2021) https://trading-education.com/the-psychology-of-trading-cryptocurrencies.
15. *** (2021) https://www.globalbankingandfinance.com/how-to-read-crypto-charts/
16. *** (2019) https://cryptotrade.blog/trading-psychology-greed-and-fear/
17. *** (2020) https://www.cornertrader.com/export/sites/cornertraderCOM/.content/.galleries/downloads/ website/tutorials/3-3-trading-psychology.pdf.
18. *** (2021), https://theinternationalpsychologyclinic.com/ the-psychology-of-crypto-currency-and-why-do-people-invest-in-bitcoin/

ACȚIUNILE PSIHOLOGICE - COMPONENTĂ PRINCIPALĂ A OPERAȚIILOR NON-CINETICE

*Alexandru-Dumitru PINTILI**

Abstract

In the 21st century, the world's leading states have moved to the next generation of wars, in which the emphasis is on the strategic confrontation of non-kinetic weapons. Obvious changes in the current security environment, emerging and disruptive technologies generate risks that lead to instability and confusion. Currently, almost all the armed forces of the developed states in their structured composition specialize in creating a psychological impact on military personnel and the enemy population. These structures use a set of methods and means of influencing people to change their psychological characteristics (points of view, opinions, value orientations, moods, motives, attitudes, behavioral stereotypes, etc.) Therefore, in addition to traditional military operations, non-kinetic operations of psychological, informational, cyber, economics etc., are becoming increasingly important because modern technologies are more sophisticated, integrated and interconnected. In this context, we will continue to focus on psychological actions as the main component of non-kinetic operations.

Keywords: *war; non-kinetic; technologies; operation; psychological; intelligence.*

INTRODUCERE

După apariția amenințărilor nucleare, războiul letal a devenit un mijloc ineficient în asigurarea dominației unui adversar. Armele nucleare au dus la excluderea câștigătorilor războiului tradițional, în condițiile în care războiul nuclear conduce automat la distrugerea civilizației umane. În prezent, limita războaielor tradiționale a fost atinsă, făcându-și apariția războaiele non-cinetice deoarece excluderea posibilității apariției unui război clasic a devenit sarcina universală a omenirii. Totodată, trebuie să realizăm faptul că umanitatea însăși nu poate opri conflictele de tip „război rece". Războaiele continuă, dar sub alte forme, ele fiind informaționale, cibernetice, diplomatice, economice, psihologice etc., în contextul în care actorii statali puternici creează în mod constant forme sofisticate de confruntare non-cinetică.[1]

În prezent, statele puternic dezvoltate economic pun accent pe conservarea armelor nucleare și dezvoltarea unor arme non-nucleare eficiente. Studiile și realizările din domeniile științific și tehnic, sociale și umanitare au condus la apariția unor noi tipuri de arme a căror utilizare nu cauzează daune umane sau materiale ireversibile. În acest sens, dezvoltarea așa numitor arme non-letale a ajuns în prim plan în obiectivele statelor puternice.

Unul dintre primele state care a lansat ideea dezvoltării unor astfel de arme este Statele Unite

* *Autorul este expert în cadrul Ministerului Apărării Naţionale.*

ale Americii. Un impuls suplimentar pentru dezvoltarea lor a fost dat și de lupta împotriva terorismului, traficului de droguri și persoane la nivel mondial. Imediat după Războiul Rece s-a lansat ideea utilizării unor acțiuni de tip psihologic și informațional care pot schimba conceptul de război făcând tranziția de la războaiele bazate pe exterminarea inamicului la războaiele din epoca informațională, accentul fiind pus pe cucerirea inamicului și controlul acestuia fără a-l distruge.

CE SUNT ACȚIUNILE PSIHOLOGICE, LA CE SERVESC ȘI CÂND SUNT EFECTUATE?

Orice putere nucleară încearcă în prezent să evite o catastrofă de acest gen și, prin urmare, recurge la noi modalități de atingere a obiectivelor. Tipurile distructive de operații militare au fost înlocuite de operații non-cinetice efectuate cu ajutorul unor mijloace, printre care și cele de tip psihologic, de influențare a conștiinței populației. Acestea pot include, de exemplu, televiziunea, presa scrisă și Internetul. Un efect de tip „soft power" al acțiunilor psihologice asupra țintei este mult mai eficient, cu costuri reduse și nu dăunează infrastructurii, mediului și populației în comparație cu câteva zeci de rachete nucleare de croazieră lansate într-o mare metropolă.

Acțiunile psihologice sunt asimilate, din ce în ce mai mult, în cadrul operațiilor non-cinetice, care la rândul lor sunt integrate războiului de tip hibrid sau asimetric. Pentru o mai bună înțelegere a obiectivelor care pot fi atinse cu ajutorul acțiunilor psihologice, vom detalia în continuare câteva caracteristici ale acestora.[2]

Scopurile și obiectivele acțiunilor de tip psihologic:

- prevenirea unui posibil conflict armat;
- slăbirea moralului personalului forțelor armate și al populației civile a inamicului;
- convingerea populației civile să refuze să participe la ostilități;
- crearea premiselor pentru realizarea obiectivelor politico-militare conturate cu pierderi umane minime și costuri materiale reduse.

Operațiile psihologice (PSYOPS) sunt principalele elemente ale războiului non-cinetic. Implementarea lor implică utilizarea unui set complex de obiective, sarcini, proceduri, forme, metode și tehnici de influență psihologică agreate, coordonate și interconectate.

Clasificarea operațiilor psihologice

- după cronologie:
  - strategice (pe termen lung) – sunt de natură globală și se desfășoară pe o perioadă lungă de timp (de la o lună la câțiva ani); au un caracter politic pronunțat, reprezintă campanii de informare și propagandă, a căror țintă poate fi întreaga comunitate mondială, inclusiv populația propriei țări;
  - operaționale (pe termen mediu) – se desfășoară în sprijinul conflictului în timpul ostilităților;
  - tactice (pe termen scurt) - sunt efectuate în sprijinul operațiunilor de luptă ale unităților și formațiunilor trupelor proprii; obiectul unor astfel de acțiuni îl reprezintă gruparea de forțe inamice.
- în funcție de perioada conflictului:
  - în timp de pace (înainte de declanșarea conflictului) - este analog operațiilor psihologice strategice;
  - în timpul conflictului;
  - în perioada de menținere a păcii - efectuate în interesul prevenirii conflictelor militare sau pentru încetarea acestora.
- după concentrare:
  - îndreptate împotriva populației civile - se desfășoară din perspectiva impactului psihologic asupra populației țărilor neutre, precum și asupra populației civile din statul inamic;
  - îndreptate împotriva trupelor inamice - au ca scop dezorientarea echipelor de comandă ale inamicului, insuflându-le ideea inevitabilității înfrângerii, încălcării autocontrolului și, pe această bază, motivarea acțiunilor greșite;
  - acțiuni de asistare a forțelor opoziției - vizează crearea unor condiții favorabile, oferind sprijin moral și de altă natură forțelor de opoziție și elementelor disidente situate pe teritoriul inamicului;
  - acțiuni de expansiune culturală și sabotaj.

În prezent, acțiunile psihologice din cadrul unei operații psihologice sunt una dintre cele mai eficiente modalități de susținere a trupelor proprii. Structurile PSYOPS acționează și reacționează în baza impactului psihologic pe care îl au acțiunile lor asupra conducerii și a personalului forțelor armate ale inamicului, precum și a populației civile. Într-o situație de criză și odată cu izbucnirea conflictului, obiectivul principal al PSYOPS este de a reduce potențialul moral și stabilitatea psihologică a părții adverse și, prin urmare, să-și asigure victoria. După sfârșitul conflictului, PSYOPS vizează consolidarea societății, asigurarea loialității cetățenilor față de regimul de ocupație sau administrația interimară.

Teoria și practica operațiilor psihologice au trecut printr-o lungă istorie în dezvoltarea lor. Punctul de cotitură pe această cale a fost Primul Război Mondial. Această etapă istorică a fost caracterizată prin crearea, în diferite țări, a unor organisme speciale pentru desfășurarea propagandei în rândul trupelor și populației inamicului și dezvoltarea metodelor și tehnicilor de influență psihologică. În acest moment, războiul psihologic a fost recunoscut ca parte integrantă a artei războiului. În timpul celui de-al Doilea Război Mondial, acțiunile psihologice au început să fie văzute ca unul dintre factorii decisivi care ar putea fi folosiți pentru a învinge inamicul cu pierderi minime. Astfel, principalii actori care au demarat acțiuni de tip psihologic au fost Marea Britanie, Germania, URSS și SUA.

Conflictele armate de după cel de-al Doilea Război Mondial au fost caracterizate prin utilizarea pe scară largă a forțelor și mijloacelor PSYOPS. În acești ani, specialiștii americani au dezvoltat conceptul de „război psihologic“, conform căruia eficacitatea influenței psihologice este determinată de puterea și profunzimea depresiei inamicului, cauzate de efectul demoralizant al armelor în combinație cu propaganda subversivă.[3] În același timp, ostilitățile din Coreea, Vietnam, Afganistan și din Golful Persic au arătat că numai acele materiale informative care se bazează pe principiile de ideologizare, noutate, impactul integrat al aspectelor militare și psihologice și plauzibilitatea conținutului sunt capabile să atingă obiectivele stabilite de inițiator.[4]

Astăzi, specialiștii PSYOPS folosesc diverse mijloace, metode și tehnici de influență psihologică, care se bazează pe cele mai recente realizări ale gândirii științifice. În multe state au fost create și funcționează efectiv dispozitive speciale pentru acțiuni psihologice. Pregătirea specialiștilor PSYOPS se fundamentează pe o bază strict științifică și se desfășoară în instituții de învățământ, printre care se află și centre științifice internaționale. Unul dintre primele state care au dezvoltat structuri de tip PSYOPS sunt Statele Unite ale Americii. Aparatul de stat american și forțele armate americane au în prezent cele mai puternice și bine echipate unități de operațiuni psihologice, care au câștigat o bogată experiență în timpul numeroaselor conflicte armate din toate regiunile lumii.

Conform punctelor de vedere ale conducerii politico-militare a Statelor Unite ale Americii, în condiții moderne, organizarea și desfășurarea acțiunilor de tip psihologic constituie un element indispensabil al participării forțelor armate la conflicte de intensitate variabilă, de menținere a păcii, umanitare și de combatere a terorismului.[5]

În conformitate cu liniile directoare în vigoare în Forțele Armate ale SUA, operațiunile psihologice reprezintă programe de acțiune care influențează evaluările, opiniile și emoțiile țintelor inamice (guverne, organizații, grupări teroriste etc.) și care au sarcina de formare a conduitei în concordanță cu obiectivele politicii externe a SUA.[6]

Conform doctrinei operațiilor psihologice a SUA, acestea sunt o parte integrantă a operațiilor informaționale de tip non-cinetic. Activitățile PSYOPS sunt planificate, organizate și desfășurate înainte, în timpul și după conflicte de intensitate diferită. În trecut, au existat diferențe clare între cele trei niveluri ale managementului PSYOPS: strategic, operațional și tactic. În prezent, astfel de diferențe nu mai există, deoarece este aproape imposibil să localizezi o astfel de acțiune.[7]

Acțiunile psihologice de nivel strategic sunt definite ca având implicații globale și sunt

planificate, organizate și desfășurate la nivel statal. Operațiunile psihologice ale Armatei SUA trebuie să asigure și să sprijine comandanții în conformitate cu Planul Strategic PSYOPS Național, atât pe timp de pace, cât și în timpul războiului. Acțiunile psihologice de nivel operațional se desfășoară pe tot parcursul și pe toată zona unui teatru de operații militare și sunt în sprijinul comandanților respectivi sau în sprijinul unor unități tactice ale elementelor PSYOPS. Acțiunile psihologice de nivel tactic sunt acele acțiuni ale forțelor și mijloacelor PSYOPS, întreprinse în anumite zone cu un impact focalizat asupra unor obiective stabilite. Aceste acțiuni sunt conduse de unități mici și presupun distribuirea de pliante, difuzarea de programe de televiziune și radio la nivel local, efectuarea de transmisii prin stații de emisie de sunet și transmiterea de mesaje cu impact vizual (postere și bannere).[8]

Schemele strategice și operațional-tactice pentru utilizarea în luptă a unităților PSYOPS au fost testate de către trupele SUA într-o serie de operații militare, care diferă între ele prin amploare, perioadă de desfășurare, localizare geografică, obiective și părțile aflate în conflict. Astfel de operațiuni includ utilizarea forței militare psihologice a SUA în Grenada (1983), în Panama (1989), în Golful Persic (1990), în Haiti (1994), în Bosnia și Herțegovina (1995 - până în prezent), în Kosovo (1999).[9]

O operație psihologică presupune implicarea anumitor specialiști care au cunoștințe și o pregătire specială, inclusiv experiență în acțiuni psihologice. Acest concept reflectă conținutul și activitățile unor structuri ce exercită un efect psihologic asupra populației și (sau) asupra personalului militar al unui stat vizat pentru atingerea obiectivelor politice, economice, financiare și chiar a celor pur militare.

Cu exactitate, *esența unei operații psihologice* este exprimată în instrucțiunile filosofului și conducătorului militar chinez Sun Tzu (sec. VI î.Hr.):

- descompuneți tot ce este bun în țara adversarului;
- subminați prestigiul conducerii inamice și expuneți-o, la momentul potrivit, rușinii publicului;
- incitați certuri și ciocniri între cetățenii unei țări ostile;
- incitați tinerii împotriva bătrânilor;
- obstrucționați prin toate mijloacele aprovizionarea trupelor inamicului și menținerea ordinii la nivelul acestora;
- faceți tot posibilul pentru a devaloriza tradițiile inamicului și subminați credința în conducerea acestuia;
- cumpărați informații și complici/în general, nu economisiți bani sau promisiuni, deoarece acestea aduc rezultate excelente.[10]

DE LA OPERAȚII PSIHOLOGICE LA OPERAȚII NON-CINETICE ȘI RĂZBOI PSIHOLOGIC

În trecutul îndepărtat, oamenii au putut să se influențeze reciproc numai în procesul de comunicare directă, sugestionându-și interlocutorii prin cuvinte, intonație, gesturi, expresii faciale. Astăzi, metodele de influențare a conștiinței umane au devenit mult mai diverse, eficiente și sofisticate datorită experienței practice acumulate de-a lungul mileniilor, precum și prin crearea de tehnologii speciale pentru comunicare și interacțiune.

Termenul „război psihologic” în sensul său neștiințific (cotidian) poate caracteriza:

- activități politice ale indivizilor, grupurilor, partidelor, mișcărilor;
- campanii electorale ale candidaților pentru diferite posturi electorale;
- activități publicitare;
- confruntare politică, economică sau culturală între grupuri etnice opuse etc.[11]

În prezent, în multe state dezvoltate economic, forțele și mijloacele de influență psihologică sunt combinate într-un întreg, conceput pentru a atinge scopuri militare, ideologice și politice. Acest proces ia diferite forme, în funcție de tradițiile istorice, condițiile politice și economice dintr-o anumită țară. Unele țări urmează calea creării unităților de război psihologic cu personal bine instruit, echipat, pregătit pentru acțiuni oriunde și oricând. Aceste unități fac de obicei parte din forțele armate ale statului sau din serviciile sale speciale. Dacă este necesar, pot fi folosite

în timp de pace, inclusiv împotriva propriilor cetățeni. Această abordare a devenit răspândită în SUA, Federația Rusă, Germania, R.P. Chineză, precum și în alte țări. Deci, războiul psihologic este o combinație non-cinetică de diverse forme, metode și mijloace de influențare a oamenilor pentru a schimba caracteristicile lor psihologice în direcția dorită (puncte de vedere, opinii, orientări valorice, stări de spirit, motive, atitudini, stereotipuri de comportament).

Într-un război psihologic, impactul non-cinetic poate fi realizat prin mai multe metode:

- În primul rând, prin mijloace psihologice clasice. Astfel, în perioada de dinainte de război, guvernul oricărei țări, prin intermediul mass-media, încearcă să formeze puncte de vedere patriotice și convingeri în rândul populației sale (în special în rândul militarilor), pentru a asigura prioritatea obiectivelor politicii de stat în conștiința de masă. În același timp, potențialul adversar încearcă să insufle în mintea populației și a personalului militar al acestui stat, idei și stări de spirit opuse, care aduc beneficii proprii.[12] De exemplu, prin acțiuni care incită la prejudecăți naționaliste, nemulțumiri față de măsurile politice sau economice ale guvernului. Așa au procedat toate puterile mondiale în Primul și Al Doilea Război Mondial sau în timpul diferitelor conflicte armate, precum cele din Coreea, Vietnam, Orientul Mijlociu etc.[13]
- În al doilea rând, impactul psihologic poate fi realizat prin mijloace pur militare. De exemplu, Uniunea Sovietică și-a desfășurat trupele și rachetele în apropierea frontierei cu China, în Vietnam sau pe teritoriul Cubei.[14] URSS a căutat în repetate rânduri să își atingă obiectivele politice printr-o demonstrație a forței militare.
- În al treilea rând, pentru influențarea psihologică a adversarului, poate fi utilizat un sistem de sancțiuni comerciale și financiare, care vizează subminarea economică. De exemplu, sancțiunile economice împotriva Irakului, Cubei, Libiei, Sudanului etc., implică o scădere semnificativă a nivelului de trai al majorității populației, numeroase conflicte interne, o creștere a morbidității, malnutriției și, ca urmare, nemulțumirea în masă a cetățenilor față de situația existentă.[15]
- În al patrulea rând, impactul psihologic poate fi realizat prin mijloace pur politice. De exemplu, un marș demonstrativ al membrilor organizației naționaliste. „Unitatea națională rusă" a lui Barkashov a presupus o polemică acerbă între reprezentanții diferitelor forțe politice din Rusia și a intensificat confruntarea dintre acestea.[16]

Războiul psihologic implică utilizarea unor tipuri de acțiuni psihologice de tip non-cinetic. Desigur, niciuna dintre unitățile specializate în acest domeniu ale unui actor nu își va dezvălui secretele, dar totuși există o oarecare clasificare a acestor tipuri de acțiuni:

- Psihologice - această opțiune este utilizată peste tot, deoarece impactul are loc prin cuvinte și informații obișnuite, ceea ce înseamnă că poate fi aplicat tuturor segmentelor de populație. Obiectivele acestui tip de impact sunt stabilite la scară cât mai largă deoarece oamenii, prin natura lor, dezvoltă opinii politice diferite, pot să își schimbe ideologia și să dezvolte noi credințe. Datorită acestui fapt, psihicul maselor devine maleabil, iar emoțiile obișnuite pot fi transformate în anumite reacții[17]. În forma sa cea mai simplă, demersul informațional și psihologic arată ca un pliant.
- Psihogene - aplicarea acestui tip de acțiune necesită echipamente tehnice, instruire și cunoștințe științifice. Această acțiune se poate realiza în două moduri: printr-un impact fizic real asupra creierului unei persoane și, ca urmare, apar tulburări în funcționarea sistemului nervos, care modifică și activitatea mentală. De exemplu, o leziune cerebrală traumatică scoate o persoană din acțiune mult timp. Adesea, imaginile despre moarte și distrugere ating psihologic chiar și o

persoană pregătită[18]. Se poate pierde în spațiu și timp, iar în viitor va avea nevoie de ajutor specializat pentru a reveni la normal, pentru a lua decizii raționale.

- Psihanalitice - fiecare agenție de informații din lume are specialiști care pot influența subconștientul unei persoane. Cel mai adesea, în procesul de expunere, se utilizează hipnoza, sugestia în faza somnului profund, precum și tehnici pentru a pune informațiile dorite în mintea persoanelor vizate. Corecția poate fi declanșată de cuvinte, imagini, sunete și chiar arome[19].
- Neuro-lingvistice - în mod popular, această metodă este cunoscută sub numele de programare neurolingvistică și reprezintă introducerea anumitor idei în conștiința unui individ. Acesta este un proces destul de complex care constă în mai multe etape. Este construit pe contradicțiile interne ale unei persoane, care îi provoacă disconfort. Și aici factorul psihologic joacă un rol foarte important astfel că un specialist în domeniul programării neurolingvistice poate identifica aceste contradicții, apoi le șterge din subconștient. Pe fondul slăbirii funcțiilor de protecție a corpului, el introduce ușor noi programe comportamentale în subconștientul uman. Ca urmare, o persoană își schimbă complet atitudinea față de viață, convingerile sale, stabilește prioritățile diferit și, în general, devine diferită[20].
- Psihotronice - cel mai adesea, se aplică la nivel macro deoarece metoda de programare în sine a fost inițial concepută pentru mase mari de oameni. Influența psihotronică implică obținerea unui rezultat prin transferul de informații la un nivel inconștient. Toate aceste metode au un singur mecanism de acțiune - permit corpului să primească informații fără a le trece prin filtrul gândirii. Astfel, informația merge direct la creier și acționează asupra terminațiilor nervoase.
- Psihotrope - reprezintă diferite medicamente, substanțe chimice sau biologice. Mai mult, pot fi atât de origine naturală, cât și sintetizate în laboratoare. Se pot sintetiza și combina diferite mirosuri care pot afecta oamenii într-un anumit mod. De exemplu, o astfel de acțiune este utilizată cu succes în centrele comerciale: mirosul produselor proaspete provoacă dorința de a merge la o cafenea, iar aroma citricelor îmbunătățește starea de spirit și contribuie la cheltuieli mai mari[21]. Același principiu este folosit pentru a induce dezgust și vărsături într-un batalion militar[22].

CONCLUZII

Istoria războaielor și a conflictelor armate confirmă într-un mod convingător faptul că acestea sunt câștigate sau pierdute de oameni și nu de avioane, tancuri sau alte tipuri de tehnică militară. Traseul și rezultatul luptelor sunt, într-o măsură decisivă, determinate de modul în care sunt mobilizați și de capacitățile spirituale și fizice ale soldaților. Chiar și în cele mai vechi timpuri, cei mai talentați comandanți înțelegeau că victoria asupra inamicului putea fi obținută nu numai cu armele, ci și prin influențarea conștiinței, voinței, sentimentelor și, astfel, căutau să folosească mijloacele de influență psihologică pentru a submina moralul inamicului. Acesta este motivul pentru care, în prezent, în multe state s-au dezvoltat structuri puternice de influențare psihologică asupra trupelor inamice. Este o provocare pentru liderii militari ai unităților și subunităților specializate în PSYOPS, contracararea psihologică eficientă a inamicului, precum și reducerea eficacității acțiunilor sale.

Astfel de acțiuni reprezintă un tip independent de influență, o armă eficientă, a cărei utilizare poate face posibilă abandonarea totală a forței militare. Acțiunile psihologice reprezintă implementarea măsurilor prezentate mai sus, atât în timp de pace, cât și în timp de război, menite să submineze potențialul sau prestigiul inamicului. Psihologia ajută unitățile specializate în PSYOPS să identifice verigile slabe din moralul și psihicul inamicului și să construiască asupra lor tactici științifice de presiune psihologică. De asemenea, utilizarea la nivel macro a unor astfel de tactici duce la apariția

contradicțiilor naționale, sociale, religioase, precum și la alte tipuri de dificultăți cu care se pot confrunta trupele inamice (foamea, frigul, lipsa suportului material și tehnic etc.). Totodată, trupele PSYOPS pot să răspândească zvonuri și dezinformări despre superioritatea semnificativă a trupelor proprii și asupra pierderilor inamicului, putând de asemenea să lucreze activ cu prizonierii de război în beneficiul propriu. Acțiunea psihologică este un tip de influență independentă și eficientă asupra inamicului, utilizată pentru a atinge obiectivele militare cu ajutorul mijloacelor non-militare. În viitor, astfel de operații pot deveni principala formă de război.

Rezumând, putem remarca faptul că eficiența acțiunilor psihologice depinde, în mare măsură, de interacțiunea tuturor structurilor implicate, de capacitatea comandanților de la toate nivelurile de a utiliza forțele și mijloacele PSYOPS. Astfel, tot ce am prezentat mai sus ne permite să afirmăm că în prezent lumea se confruntă cu un nou tip de ostilitate, identificată prin aceste acțiuni psihologice reprezentate de arme și tehnici neletale, fiind o modalitate eficientă de a atinge anumite obiective politice, economice, diplomatice sau chiar militare. Aceste acțiuni nu ucid, nu distrug, dar îți permit să obții victoria cu pierderi minime. Este un tip de armă independentă, eficientă și relativ ieftină în războiul modern. O armată care va avea superioritate, în privința caracteristicilor calitative și cantitative ale acestor tipuri de acțiuni, va fi mai eficientă pe câmpul de luptă al războiului modern.

Comandanții armatelor moderne trebuie să fie conștienți de faptul că pentru a învinge inamicul nu este suficient să-l domini fizic, iar distrugerea armatei inamice nu este întotdeauna cea mai eficientă metodă. Succesul luptei moderne depinde, în mare măsură, de echilibrul real al capacităților morale și psihologice ale părților opuse. Găsirea mijloacelor de creștere a moralului trupelor proprii și a mijloacelor de afectare a stării morale și psihologice a trupelor inamice, efectuarea eficientă a unei presiuni psihologice continue, dure și epuizante asupra inamicului reprezintă câteva caracteristici ale unui lider militar modern și cerința unei practici moderne de luptă.

Astfel, statele ce au în componența armatei specialiști sau unități PSYOPS pot efectua acțiuni eficiente asupra inamicului pentru a-și atinge obiectivele militare prin mijloace non-militare. Operațiile psihologice au devenit o necesitate și un tip de acțiune decisivă în cadrul operațiilor militare moderne. Astfel de operații se pot transforma în principala formă de război în viitor, iar civilizația noastră, devenită în cea mai mare parte informațională, trebuie să ia în considerare aceste schimbări în doctrinele sale militare.

Sursa: serenoregis.org

BIBLIOGRAFIE

1. ANDERSON R.J., *"Dark Psychology: Master the Advanced Secrets of Psychological Warfare, Covert Persuasion, Dark NLP, Stealth Mind Control, Dark Cognitive Behavioral Therapy, Maximum Manipulation, and Human Psychology"*, ebook, 2018.
2. BADSEY Stephen, „Propaganda: Media in War Politics", disponibil pe https://encyclopedia.1914-1918-online.net/article/propaganda_media_in_war_politics, accesat la 12.03.2021.
3. „Cuban Missile Crisis", disponibil pe https://www.history.com/topics/cold-war/cuban-missile-crisis, accesat la 12.03.2021.
4. FM 3-05.301, „Psychological Operations Tactics, Techniques, and Procedures", Department of the Army, 2003, SUA.
5. GARETH Roderique-Davies, „Neuro-linguistic programming: cargo cult psychology?", disponibil pe https://www.researchgate.net/publication/242770183_Neuro-linguistic_programming_cargo_cult_psychology, accesat la 20.03.2021.
6. GOLDSTEIN F. Findley, B., Jr., *Psychological Operations. Principles and Case Studies*, Air University Press, Alabama, SUA, 1996.
7. GRAZIANO S.A Michael, Kastner Sabine, „Human consciousness and its relationship to social neuroscience", disponibil pe https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3223025/, accesat la 16.03.2021.
8. HOSMER Stephen, *„The information revolution and psychological effects"*, disponibil pe https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1016/MR1016.chap8.pdf, accesat la 20.03.2021.
9. "Psychological operations", disponibil pe https://www.goarmy.com/careers-and-jobs/special-ops/psychological-operations.html, accesat la 02.03.2021.
10. Joint Publication 3-57, „Civil-Military Operations", disponibil pe https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_57.pdf, accesat la 04.03.2021.
11. KRYSKO V.G., „Secrets of psychological warfare", disponibil pe https://kerchtt.ru/en/sekrety-psihologicheskoi-voiny-g-krysko-v-sekrety-psihologicheskoi/, accesat la 20.03.2021.
12. LONGLEY Robert, „An Introduction to Psychological Warfare", disponibil pe https://www.thoughtco.com/psychological-warfare-definition-4151867.
13. „Military Interventions by U.S. Forces from Vietnam to Bosnia", disponibil pe https://www.everycrsreport.com/reports/RL30184.html, accesat la 06.03.2021.
14. PINTILI D. Alexandru, Mitulețu Ion, „Delimitări conceptuale privind operațiile informaționale, cibernetice, non-letale și non-cinetice", în *Colocviu strategic*, nr.10/2020, Universitatea Națională de Apărare „CAROL I" București, octombrie 2020.
15. POLS Hans, Oak Stephanie, „War & Military Mental Health", disponibil pe https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2089086/, accesat la 12.03.2021.
16. „Psychoanalytic Understanding of War Trauma", disponibil pe https://apsa.org/war-trauma-series, accesat la 20.03.2021.
17. ROGERS S. Elizabeth, „Using Economic Sanctions to Prevent Deadly Conflict", disponibil pe https://www.belfercenter.org/publication/using-economic-sanctions-prevent-deadly-conflict, accesat la 15.03.2021.
18. STĂNCULESCU Cătălin, „Condiționare psihologică, manipulare și război psihologic", disponibil pe https://mythologica.ro/conditionare-psihologica-manipulare-si-razboi-psihologic/, accesat la 10.03.2021.
19. SUN Tzî, *Arta războiului*, disponibil pe https://ro.wikiquote.org/wiki/Sun_Tzu, accesat la 10.03.2021.
20. United States Department of State, „U.S. Department of State Country Report on Human Rights Practices 1999 – Russia" , 25 February 2000, disponibil pe https://www.refworld.org/docid/3ae6aa864.html, accesat la 15.03.2021.
21. WESSELY Simon, „Psychological effects of chemical weapons", disponibil pe https://www.researchgate.net/publication/5615466_Psychological_effects_of_chemical_weapons_A_follow-up_study_of_First_World_War_veterans, accesat la 20.03.2021.

[1] Alexandru D. Pintili, Ion Mitulețu – „Delimitări conceptuale privind operațiile informaționale, cibernetice, non-letale și non-cinetice”, în *Colocviu strategic*, nr.10/2020, Universitatea Națională de Apărare „CAROL I” București, octombrie 2020.

[2] Robert Longley, „An Introduction to Psychological Warfare”, disponibil pe https://www.thoughtco.com/psychological-warfare-definition-4151867

[3] „Psychological operations”, disponibil pe https://www.goarmy.com/careers-and-jobs/special-ops/psychological-operations.html, accesat la 02.03.2021.

[4] Goldstein, F., Findley, B., Jr., *Psychological Operations. Principles and Case Studies*, Air University Press, pg. 231-249 Alabama, SUA, 1996.

[5] Joint Publication 3-57, „Civil-Military Operations”, disponibil pe https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_57.pdf, accesat la 04.03.2021

[6] FM 3-05.301, *Psychological Operations Tactics, Techniques, and Procedures*, Headquarters, Department of the Army, 2003, SUA, pg. 7.

[7] FM 3-05.301, *Psychological Operations Tactics, Techniques, and Procedures*, Headquarters, Department of the Army, 2003, pg. 9.

[8] Ibidem, pg. 5-20.

[9] „Military Interventions by U.S. Forces from Vietnam to Bosnia”, disponibil pe https://www.everycrsreport.com/reports/RL30184.html, accesat la 06.03.2021.

[10] Sun Tzî, *Arta războiului*, disponibil pe https://ro.wikiquote.org/wiki/Sun_Tzu, aceesat la 10.03.2021.

[11] Cătălin Stănculescu, „Condiționare psihologică, manipulare și război psihologic”, disponibil pe https://mythologica.ro/conditionare-psihologica-manipulare-si-razboi-psihologic/, accesat la 10.03.2021.

[12] Stephen Badsey, „Propaganda: Media in War Politics”, disponibil pe https://encyclopedia.1914-1918-online.net/article/propaganda_media_in_war_politics, accesat la 12.03.2021.

[13] Hans Pols, Stephanie Oak, „War & Military Mental Health”, disponibil pe https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2089086/, accesat la 12.03.2021.

[14] „Cuban Missile Crisis”, disponibil pe https://www.history.com/topics/cold-war/cuban-missile-crisis, accesat la 12.03.2021.

[15] Elizabeth S. Rogers, „Using Economic Sanctions to Prevent Deadly Conflict”, disponibil pe https://www.belfercenter.org/publication/using-economic-sanctions-prevent-deadly-conflict, accesat la 15.03.2021.

[16] United States Department of State, „U.S. Department of State Country Report on Human Rights Practices 1999 – Russia”, 25 February 2000, disponibil pe https://www.refworld.org/docid/3ae6aa864.html, accesat la 15.03.2021.

[17] Michael S. A. Graziano, Sabine Kastner, „Human consciousness and its relationship to social neuroscience”, disponibil pe https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3223025/, accesat la 16.03.2021.

[18] Stephen T. Hosmer, „The information revolution and psychological effects”, disponibil pe https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1016/MR1016.chap8.pdf, accesat la 20.03.2021.

[19] „Psychoanalytic Understanding of War Trauma”, disponibil pe https://apsa.org/war-trauma-series, accesat la 20.03.2021.

[20] Gareth Roderique-Davies, „Neuro-linguistic programming: cargo cult psychology?”, disponibil pe https://www.researchgate.net/publication/242770183_Neuro-linguistic_programming_cargo_cult_psychology, accesat la 20.03.2021.

[21] Simon Wessely, „Psychological effects of chemical weapons”, disponibil pe https://www.researchgate.net/publication/5615466_Psychological_effects_of_chemical_weapons_A_follow-up_study_of_First_World_War_veterans, accesat la 20.03.2021.

[22] Krysko V.G., „Secrets of psychological warfare”, disponibil pe https://kerchtt.ru/en/sekrety-psihologicheskoi-voiny-g-krysko-v-sekrety-psihologicheskoi/, accesat la 20.03.2021.

PROCESUL DE SELECȚIE, ETAPĂ FUNDAMENTALĂ ÎN EFORTUL DE ÎMBUNĂTĂȚIRE A CAPITALULUI UMAN ÎN HUMINT

Alexandru KIS*

Abstract

HUMINT is a niche discipline, with a limited number of stakeholders and practitioners. The management of the HUMINT personnel is a complex enterprise that should properly address aspects of career development projection and planning, starting from the selection process, professional development, performance assessments/ evaluation, and ending with welfare aspects that can affect individual and group performances.

Developing a well-trained and skilled HUMINT operator means that an applicant will be able to manage long life educational process in many different areas (military, economics, psychology, culture, public affairs, human geography, etc.), with ability to deal with permanent physical and mental stress, while preserving its capacity to fulfil all tasks and missions assigned. This is the basis for further professional progress, to senior/ leadership positions, or possible shifts to other disciplines.

In this respect, as the HUMINT community within the Military is limited in number, the individual quality of the personnel matters, and each vacant position has to be occupied precisely by the right skilled applicant. The paper further describes the NATO HUMINT COE approach to the selection process and professional development in HUMINT.

Keywords: *HUMINT; Human Capital; selection.*

INTRODUCERE

Centrul de Excelență NATO în domeniul HUMINT (HCOE) din Oradea este activ implicat în procesul de dezvoltare a capabilității HUMINT la nivel NATO. Acest fapt presupune sprijinirea Alianței din perspectiva cererilor de suport primite pe mai multe paliere – dezvoltare doctrinară, dezvoltarea și experimentarea de noi concepte și tehnologii, managementul lecțiilor învățate, educație și instruire.

Un domeniu complex, transdisciplinar, la care HCOE este parte, îl reprezintă programul NATO pentru îmbunătățirea capitalului uman (Human Capital Enhancement Programme – HCEP). Astfel, specialiștii Centrului sunt angrenați în elaborarea unor studii conexe acestui deziderat, particularizate pentru domeniul HUMINT, urmărind creșterea nivelului de performanță a personalului, aplicarea unor principii moderne de management și leadership în actul de comandă și control la nivel de proiecte, dar și în cadrul

* ***Autorul este expert în cadrul Centrului de Excelență NATO în domeniul HUMINT; opiniile și ideile exprimate în acest articol aparțin autorului și nu reflectă neapărat politica NATO.***

organizațiilor de profil din NATO, îmbunătățirea nivelului de cooperare și coordonare, dar și optimizarea resurselor.

Cel mai recent studiu al HCOE în acest domeniu este dedicat activității de selecție și dezvoltare profesională în HUMINT. Acesta pornește de la modele existente la nivelul organizațiilor din spectrul *Intelligence* în statele NATO, urmărind să pună în valoare bunele practici ale acestora în cadrul unui algoritm de selecție optimizat, cu aplicabilitate generală (un gen proxim al procesului de selecție, adaptat în funcție de cerințele specifice, cultura organizațională și cadrul legal al fiecărei națiuni în parte). Mai departe, dezvoltarea profesională, identificarea talentelor și retenția personalului, precum și opțiunile inovatoare de exploatare a capitalului uman sunt abordate dintr-o perspectivă racordată la fluxul transformațional al structurilor de comandă și de forțe ale Alianței.

În continuare vom face o scurtă trecere în revistă a premiselor desfășurării activității de cercetare și documentare aferente studiului, principalele elemente ale acestuia și concluziile cu relevanță, atât în ceea ce privește o abordare holistică a problematicii capitalului uman în cadrul organizațiilor de profil naționale, cât și la nivelul NATO.

CAPITALUL UMAN ÎN NATO – NOI COORDONATE DE PERFORMANȚĂ

Programul NATO pentru îmbunătățirea capitalului uman (HCEP), lansat în 2020, urmărește să modernizeze politica de resurse umane în cadrul Alianței, antrenând o revizuire a statutului acesteia la nivelul fiecărei branșe, în baza unei abordări centrate pe performanța individuală, reziliență și asigurarea avantajului competitiv. Trebuie să recunoaștem în aceste principii axioma aportului de valoare pe care personalul o reprezintă în economia organizației, precum și actul de simbioză reprezentat de politicile de personal și oportunitățile puse la dispoziția angajaților de către organizație în vederea dezvoltării profesionale, dobândirii de noi abilități, autoperfecționării acestora. Astfel, o resursă umană dinamică, cu apetit de învățare, cu flexibilitate în materie de ”up-skilling” (perfecționare) și ”re-skilling” (recalificare), sensibilă la evoluția ergonomiei locului de muncă (înțelegând aici transformarea acestuia din perspectiva impactului noilor tehnologii, a emergenței spațiului virtual – de la comunicare online către transpunerea în Metaverse, a dimensiunii cognitive și capacității de analiză critică și, în cele din urmă, a adaptării funcționale raportat la mediul de activitate) devine un motor al evoluției organizației și al creșterii relevanței acesteia în relația cu beneficiarii.

HCEP are ca linii de efort: dezvoltarea leadership-ului (cadrul de formare a liderilor și îmbunătățirea procesului decizional), creșterea eficienței organizaționale (orientarea către viitor, asigurarea premiselor pentru dezvoltarea și bunăstarea personalului) și optimizarea metodologiei de învățare (atât din perspectiva dezvoltării de conținut, cât și cea a predării/furnizării materialului didactic), concretizate în cunoaștere, abilități, atitudini, experiență și capacitate cognitivă, capabile să asigure gradul necesar de operaționalizare a Alianței și să genereze valoare pentru aceasta.

Toate aceste deziderate își găsesc reflectarea în parcursul profesional al personalului militar, indiferent de specialitate, și capătă dimensiuni aparte în momentul delegării la post în cadrul structurilor de comandă sau de forțe ale Alianței. Dincolo de responsabilitatea națională referitoare la pregătirea în conformitate cu solicitările din fișa postului, în domeniul *Intelligence* apar o serie de cerințe generale și specifice de instruire în ceea ce privește standardele specifice NATO, cuprinse în STANAG 2555.

GESTIONAREA CAPITALULUI UMAN ÎN HUMINT – ÎNTRE PLANIFICARE ȘI OPORTUNITATE. O PERSPECTIVĂ CALITATIVĂ

Necesitatea asigurării resursei umane calificate în cadrul organizației este subiectul proiecției necesarului de forțe pe diferite orizonturi de timp și se concretizează în planuri de recrutare, armonizate cu politicile de mobilitate intra sau inter-instituționale.

În acest context, procesul de selecție (completat, ulterior, de strategiile de dezvoltare profesională) are ca obiectiv final angajarea candidaților ce corespund atât cerințelor postului, cât și profilului psiho-social specific specialității militare vizate.

În cadrul structurilor de informații militare există o mare varietate de posturi distincte prin natura activității, nivelul cunoașterii și competențele solicitate angajaților. Dincolo de evaluarea acestor aspecte specifice, selecția personalului abordează și elemente legate de profilul personal și profesional al candidatului, competențele transversale, abilitățile tehnice, dar și latura motivațională și potențialul de învățare și dezvoltare.

În HUMINT există două curente majore de evoluție profesională – unul este axat pe culegerea de informații (operatorii HUMINT) și management operațional, iar celălalt se centrează pe procesarea informației și elaborarea de produse de *intelligence* (asimilat termenului de *analist*) – care marchează profile relativ diferite din punct de vedere al competențelor necesare prin prisma solicitărilor particulare (tabelul nr. 1), dar ambele construite pe fundamentul psiho-social solid al unui model unic[1].

Tabelul nr. 1: Repere privind competențele profesionale în HUMINT[2]

Operatorul HUMINT	Analistul HUMINT
- Planificarea activităților de culegere de informații; - Documentare/ pregătirea activităților HUMINT; - Identificarea surselor umane; - Executarea de activități specifice din spectrul HUMINT; - Competențe socio-emoționale specifice[3]; - Exploatarea informației; - Folosirea instrumentelor și sistemelor tehnice (platformelor) de culegere/ exploatare a informației; - Întocmirea de rapoarte specifice; - Managementul OPSEC și INFOSEC la nivelul microstructurii.	- Planificarea activităților de procesare a informațiilor; - Documentare pentru activitățile de procesare a informației; - Gestionarea bazelor de date; - Procesarea datelor și a informațiilor; - Aplicarea de tehnici și proceduri analitice; - Utilizarea produselor software de procesare a informațiilor; - Elaborarea de produse de Intelligence; - Evaluarea produselor de Intelligence; - Diseminarea produselor de Intelligence; - Asigurarea asistenței de specialitate pentru factorii de decizie.

Activitatea de culegere a informațiilor din surse umane este solicitantă pentru operatori din mai multe puncte de vedere. Pe de o parte, aceștia trebuie să fie capabili să opereze independent, în medii mai mult sau mai puțin permisive, să dovedească aptitudini de gândire critică și capacitate de evaluare corectă a situației, să rezolve problemele apărute și să ia decizii rapide. În relația cu sursele (indiferent de context), operatorii trebuie să își dovedească măiestria în ceea ce privește controlul relațiilor interpersonale: păstrarea inițiativei în conversație, siguranța de sine, capacitatea de a construi o relație empatică, dar manifestând în permanență o atitudine adecvată situației (ce poate avansa până la asertivitate și un anumit nivel de constrângere[4]). Alte funcții în domeniul HUMINT necesită competențe diferite, orientate către procesarea/ analiza informațiilor, dovedirea de capacități manageriale sau a abilităților de lider.

Ca element de referință comun, manualul Forțelor terestre ale SUA (F.M. 2-22.3/2006[5]) pentru operații de culegere a informațiilor din surse umane amintește o serie de atribute ale profesioniștilor din domeniu: vigilența, gândirea critică, răbdarea și tactul, credibilitatea, obiectivitatea, adaptabilitatea, perseverența, inițiativa, însoțite de trăsături de caracter

bine definite, cristalizate atât din perspectiva experienței profesionale, cât și a experienței de viață. În acest context, competențele transversale (bazate pe trăsăturile individuale) sunt puternic valorizate și fac obiectul evaluării în cadrul procesului de selecție.

Ținând cont de transformările sociale și a comportamentelor umane („terenul uman" reprezentând câmpul de operare în HUMINT) în epoca Internetului și a tehnologiilor emergente - fapt ce reclamă o adaptare continuă a procedurilor HUMINT, implementarea de sisteme tehnice/ digitale, dezvoltarea unor platforme de securitate operațională îmbunătățită - specialiștii din acest domeniu trebuie să demonstreze deschidere permanentă spre acumularea de noi competențe și capacitate cognitivă: capacitatea de a învăța, acumula, înțelege, analiza, sintetiza, dezvolta și combina idei, precum și de a elabora enunțuri creative sau critice pentru fundamentarea deciziilor profesionale. Acest ansamblu este legat de triada cunoaștere – abilități – atitudini, într-un cadru complex: cultură generală, IQ, cunoașterea bazelor legale ale societății, gândire critică și argumentare logică, comunicare orală și scrisă, sociabilitate, cunoaștere științifică în multiple domenii – psihologie, sociologie, etnografie, antropologie, geografie umană etc.[6] În plus, competențele digitale sunt deja o necesitate consacrată în tot ce întreprindem din punct de vedere profesional, pornind de la documentare, comunicare, (auto-) dezvoltare, întocmirea de documente și rapoarte ș.a.m.d.; aplicațiile de pe telefoanele inteligente sunt un asistent important al rutinei zilnice, cu relevanță multiplă (gestionarea activităților, orientare și mobilitate, comunicare, informare, micro-learning etc.).

În general, abordarea privind activitatea de selecție în domeniul *Intelligence* (implicit în HUMINT) se bazează pe două strategii distincte:

- ocuparea posturilor disponibile (planificată în baza unei dinamici recunoscute și a unor prognoze, dar cu o componentă reactivă puternică, generată de necesitatea de a asigura resursa umană necesară pentru posturile disponibilizate);
- „vânătoarea de talente", unde identificarea potențialilor candidați ce corespund unui profil bine determinat este un proces deschis, permanent, completat de activitatea formală de evaluare desfășurată în funcție de interesele organizației.

Un exemplu privind formularea unui model al candidatului îl regăsim în Ghidul elaborat de SRI pentru promovarea activității proprii de selecție[7]; pe de altă parte, anumite abilități ale persoanelor interesate de activarea într-un serviciu de informații pot fi evaluate prin forme atractive de interacțiune, chiar sub formă de joc (figura 1).

Figura 1: "Agenția de spionaj" – interfață pentru evaluarea preliminară a potențialilor aplicanți pentru un post în cadrul SIE (https://www.sie.ro/AgentiaDeSpionaj/)

MODELE DE EVALUARE ÎN CADRUL PROCESULUI DE SELECȚIE

În general, procesele de selecție cuprind o serie de etape (*figura 2*) menite să filtreze progresiv numărul de candidați, astfel încât, la finalul evaluării, organizația să beneficieze de aportul unor angajați apți pentru executarea sarcinilor prevăzute în fișa postului.

Figura 2: Etape ale procesului de selecție (https://iedunote.com/selection-process)

Complexitatea activității specifice și calitățile cerute candidaților în domenii complexe, ce fac recurs la abilități variate, determină ca designul procesului de evaluare să fie o adevărată provocare pentru echipa de proiect. Pornind de la modelele clasice de evaluare, sistemul centrelor de evaluare (”*assessment centers*”) răspunde, în mod standardizat, unor cerințe complexe de măsurare a multiplilor parametri avuți în vedere, raportat la o serie de comportamente prestabilite.

Tehnicile specifice centrelor de evaluare cuprind: exerciții de simulare situațională, jocuri de rol, interviuri, teste psihologice și alte instrumente validate de psihodiagnoză[8], activități individuale și de grup etc. *(figura 3)* și sunt adaptate inclusiv pentru procesele de dezvoltare profesională și evoluție în carieră. În funcție de obiective, testările aferente pot fi susținute în format fizic, online, sau combinat.

În mod uzual, evaluarea în acest context succede etapelor inițiale, cu rol eliminatoriu (testare medicală, sportivă, verificarea de securitate, testul de cunoaștere al limbilor străine ș.a.m.d.), ale procesului de selecție.

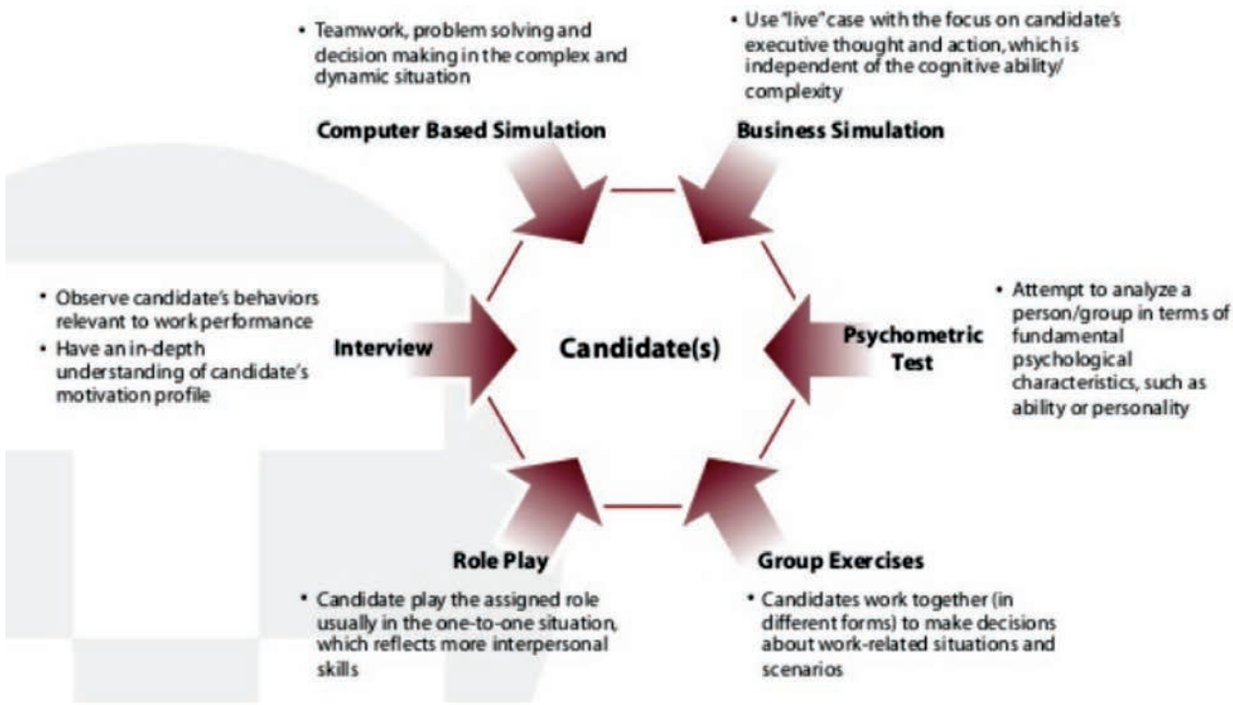


Figura 3: Testarea candidaților prin metoda centrelor de evaluare (https://www.slideshare.net/horatjitra/assessment-center-how-to-assess-select-and-develop-the-right-talent)

CĂTRE UN MODEL STANDARDIZAT PENTRU PROCESUL DE SELECȚIE ÎN HUMINT

La nivelul HCOE, interesul de elaborare a unui model privind procesul de selecție și dezvoltare profesională în HUMINT este bivalent. Pe de o parte, un astfel de model poate oferi o perspectivă de standardizare la nivelul națiunilor aliate: o abordare unitară a resursei umane, aceasta evoluând în carieră în baza unor programe de educație și instruire naționale și NATO standardizate, este de natură să asigure o dezvoltare comună a acestei capabilități la nivelul Alianței. Pe de altă parte, dincolo de prevalența națională în procesul de selecție, structurile de comandă și de forțe ale NATO, precum și alte organizații afiliate NATO (cum e cazul centrelor de excelență) pot beneficia de serviciile specialiștilor HUMINT proveniți atât pe filiera detașării la post de către națiuni, cât și prin servicii externalizate care să sprijine atât operațiile curente, cât și dezvoltarea capabilității la nivelul NATO în dimensiunile transformaționale consacrate: standardizare; dezvoltare conceptuală și experimentare; educație, instruire, exerciții și evaluare; lecții învățate.

Studiul dezvoltat de către HCOE analizează comparativ o serie de aspecte legate de particularitățile transnaționale ale procesului de selecție, pornind de la următoarele: bazinul de selecție, strategiile de abordare, concurența pe piața muncii și evaluarea atractivității serviciului în HUMINT, contractarea pe termen lung *vs.* contracte cu termen limitat (bazate pe managementul proiectelor și externalizarea unor servicii), criteriile de eligibilitate (un exemplu este reprezentat în tabelul nr. 2), aspecte privind testele eliminatorii (examenul medical, testul de pregătire fizică, examenul lingvistic, testul de cultură generală, testarea competențelor digitale) și constituirea profilului psihologic al fiecărui candidat, analiza factorului motivațional, importanța interviului de evaluare.

Astfel, pașii propuși în cadrul procesului culminează cu examinarea finală, la nivelul centrelor de evaluare, în cadrul cărora sunt evaluate – în condiții variabile și contexte particulare – competențele de comunicare orală și scrisă, calitățile de lider, abilitatea de relaționare cu diferite persoane, capacitatea de a anticipa evoluția situației și gradul de adaptabilitate la condiții variabile, capacitatea de gândire critică și

Tabelul nr. 2: Cerințe de bază pentru participarea în procesul de selecție pentru posturile HUMINT în cadrul US Department of Defence[9]

Basic entry requirements	Army	Navy	Air Force	Marine Corps
U.S. Citizen	Yes	Yes	Yes	Yes
ASVAB	GS + VE + MK + MC (ST score) = 101	WK +PC + AR = 107	WK+PC and AR = 33	VE + AR = 110 waiver based on performance
Age	18 years old	21 years old	21 years old	21 years old
Years experience	Specific HUMINT MOS selected upon enlistment	No specific HUMINT MOS, assigned HUMINT duties after enlistment	No specific HUMINT MOS, assigned HUMINT duties after enlistment	CPL or SGT with 1 year time in grade; selected from other MOS; selection based on interview
Language requirement	DLAB	DLAB	DLAB	DLAB
Clearance (TS/SCI)	Yes	Yes	Yes	Yes
Polygraph	Submit	Submit	Submit	Submit

abilitatea de a găsi soluții la problemele apărute, lucrul în echipă, performanța în condiții de stres etc.

În baza rezultatelor obținute, angajarea este legată de procesul adaptiv și evoluția abilităților specifice în cadrul unui curs de bază, ale cărui obiective vizează familiarizarea cu activitatea specifică în domeniul HUMINT și cristalizarea factorului motivațional pentru opțiunile de evoluție în carieră.

DEZVOLTAREA PROFESIONALĂ ȘI RETENȚIA PERSONALULUI ÎN DOMENIUL HUMINT

Dezvoltarea calității resursei umane și retenția personalului de valoare este un obiectiv general în organizațiile profesionale. În acest deziderat sunt implicate atât organizațiile, prin programe specifice de consiliere și mentorat, dezvoltare profesională și motivare, cât și angajații, care sunt încurajați să își dezvolte nivelul de cunoaștere și abilitățile prin efort propriu (care poate fi, la rândul său, stimulat de către organizație).

Capacitatea individuală de învățare, modalitatea de accesare a cursurilor de perfecționare, rezultatele așteptate în urma atingerii obiectivelor educaționale, „cultura educațională" în cadrul organizației sunt repere importante în definirea acesteia ca fiind una bazată pe cunoaștere. Așteptările actuale, în acest context, sunt legate de un ecosistem de învățare care favorizează complementaritatea soluțiilor educaționale formale și informale, asigură condițiile necesare pentru colaborare și învățare socială[10], se implică activ în activitatea de coaching & mentoring, asigură platforme de comunicare și lucru, fiind aliniate conceptului de învățare în ritmul activității lucrative.

Aplicarea acestor principii în organizațiile ce activează în domeniul informațiilor militare favorizează o schimbare de mentalitate, asociată cu o responsabilitate crescută la nivel individual (de unde și o importanță sporită în ce privește profilul angajaților). Dată fiind specificitatea activității în domeniul HUMINT și complexitatea pregătirii cadrelor de specialitate, retenția personalului în acest domeniu nu trebuie tratată cu superficialitate. Proiecția pe termen lung a carierei, păstrarea interesului pentru dezvoltare multilaterală (dar și de specializare în domenii de nișă) și dezvoltarea spiritului de corp sunt câteva repere legate de stabilitatea personalului și prevenirea carențelor în asigurarea cu personal. Pe de altă parte, pregătirea în a doua specialitate (HUMINT) a personalului militar din domenii ce presupun interacțiunea cu populația civilă (CIMIC, PSYOPS, jurnaliști militari etc.) poate fi o opțiune de augmentare a resursei umane în caz de nevoie.

În contextul disponibilității personalului în rezervă cu calificare în domeniul HUMINT pentru sprijinirea proiectelor curente din cadrul

organizațiilor de profil (participarea ca experți în conferințe, ateliere de lucru, echipe de redactare a unor standarde, lectori sau observatori/ instructori în cadrul cursurilor sau exercițiilor, specialiști tehnici, analiști, mentori etc.), HCOE a avansat în cadrul studiului ideea de constituire a unei platforme profesionale (de genul ”LinkedIn”) care să asigure conexiunea dintre oferta (pro bono sau plătită) celor dispuși și calificați să presteze anumite servicii și organizațiile interesate. O astfel de platformă capătă și mai multă substanță prin extinderea ei la nivelul întregii Alianțe și prin acoperirea tuturor specialităților militare, ca proiect aferent programului HCEP (cu respectarea cerințelor legate de acces pe platformă și securitate, certificare și asigurarea calității).

CONCLUZII

HCOE urmărește aplicarea principiilor HCEP legate de dezvoltarea capitalului uman în domeniul HUMINT, armonizate cu standardele NATO privind educația, instruirea, exercițiile și evaluarea. Acest fapt presupune o abordare multidimensională a acestei problematici și acoperă aspecte cantitative și calitative legate de selecția personalului, strategiile de dezvoltare profesională și portofoliul de cursuri aferent, evenimentele de instruire colectivă și exercițiile de integrare, suportul tehnic/tehnologii educaționale, modelarea și simularea în instruire, analiza caracteristicilor audienței și tehnicile de predare utilizate în instruirea individuală, opțiunile pentru autodezvoltare, strategiile de stimulare și motivare, activitatea de evaluare, politicile pentru certificarea competențelor, conceptul de mentorat și consiliere profesională, dar și aspecte privind resursa externă și valorificarea experienței rezerviștilor.

Relația cu mediul academic și cu organizațiile din domeniul industriei de apărare completează tabloul unei abordări comprehensive, puse în serviciul dezvoltării capabilității HUMINT în NATO, la care se adaugă componentele corectivă (managementul lecțiilor învățate) și prospectivă (cercetarea și dezvoltarea conceptuală), ce contribuie la procesul de îmbunătățire continuă aferent sistemului de asigurare a calității.

În acest context, implicarea HCOE în cadrul comunității de interes privind educația și instruirea HUMINT în NATO, precum și contribuția adusă la nivelul sistemului de management educațional în NATO, sunt general recunoscute la nivelul Alianței. Studiul privind selecția personalului și dezvoltarea profesională în HUMINT răspunde așteptărilor comunității profesioniștilor din acest domeniu, atât la nivel de reprezentanți naționali (prin asigurarea unui model de referință și promovarea unor bune practici ce pot fi asimilate), cât și în ceea ce privește entitățile NATO, prin aportul la creșterea calității capitalului uman pus la dispoziția Alianței de către națiuni și prin oportunitățile sugerate cu privire la exploatarea resursei reprezentate de către rezerviștii cu competențe certificate și recunoscute/validate.

Sursa: blog.ipleaders.in

BIBLIOGRAFIE

1. Department of the Army Headquarters, *FM 2-22.3 (FM 34-52) Human Intelligence Collector Operations*, September 2006, https://fas.org/irp/doddir/army/fm2-22-3.pdf.
2. HĂHĂIANU Florentina, *Explorarea competenței socio-emoționale* în *domeniul intelligence*, Editura Top Form, București, 2016.
3. https://iedunote.com/selection-process.
4. https://www.sie.ro/AgentiaDeSpionaj/
5. https://www.slideshare.net/horatjitra/assessment-center-how-to-assess-select-and-develop-the-right-talent.
6. KIS Alexandru, ARHIP Vasilică, TARCALA Oliver, ”Skills and traits of the HUMINT operator”, publicată în volumul celei de a 14-a Conferințe Științifice Internaționale “Defense Resources Management in the 21st century”, Brașov, Noiembrie 2019.
7. McLEOD, Saul, ”Albert Bandura’s Social Learning Theory”, 2016, în https://www.simplypsychology.org/bandura.html.
8. PERȚEA Gheorghe, *Testare psihologică. Psihodiagnoza personalității* (suport de curs), Facultatea de Psihologie, Universitatea Ecologică București, 2020.
9. Serviciul Român de Informații, Ghidul candidatului, 2022, în https://www.sri.ro/fisiere/ghidul_candidatului_2022.pdf.
10. TROPOTEI Teodor-Octavian, *Modelarea acțiunilor non-invazive de obținere a informațiilor din surse umane*, Editura Academiei Naționale de Informații ”Mihai Viteazul”, București, 2021.
11. WILKINSON Kevin R., *Unparalleled Need: Human Intelligence Collectors in the United States Army*, U.S. Army War College, Carlisle Barracks, PA, March 2013.

[1] Alexandru Kis, Vasilică Arhip, Oliver Tarcala, “Skills and traits of the HUMINT operator”, publicată în volumul celei de a 14-a Conferințe Științifice Internaționale “Defense Resources Management in the 21st century”, Brașov, Noiembrie 2019.

[2] Apud. Florentina Hăhăianu, *Explorarea competenței socio-emoționale în domeniul intelligence*, Editura Top Form, București, 2016, p. 99.

[3] F. Hăhăianu distinge două mari categorii de competențe socio-emoționale: dimensiunea intrapersonală (automotivarea, autocontrolul și conștiința de sine) și dimensiunea interpersonală (conștiința socială și abilitățile sociale), Op. cit.

[4] Kevin R. Wilkinson, *Unparalleled Need: Human Intelligence Collectors in the United States Army*, U.S. Army War College, Carlisle Barracks, PA, March 2013, pp. 6-7.

[5] Department of the Army Headquarters, *FM 2-22.3 (FM 34-52) Human Intelligence Collector Operations*, September 2006, https://fas.org/irp/doddir/army/fm2-22-3.pdf.

[6] Teodor-Octavian Tropotei, *Modelarea acțiunilor non-invazive de obținere a informațiilor din surse umane*, Editura Academiei Naționale de Informații „Mihai Viteazul”, București, 2021, pp. 234-235.

[7] Serviciul Român de Informații, Ghidul candidatului, în https://www.sri.ro/fisiere/ghidul_candidatului_2022.pdf.

[8] Gheorghe PERȚEA, *Testare psihologică. Psihodiagnoza personalității* (suport de curs), Facultatea de Psihologie, Universitatea Ecologică București, 2020.

[9] Kevin R. Wilkinson, Op. Cit., pp. 6-7; abrevieri utilizate: Armed Service Vocational Aptitude Battery (ASVAB), Top Secret Sensitive Compartment Information (TS/SCI), General Sciences (GS), Arithmetic Reasoning (AR), Word Knowledge (WK), Paragraph Comprehension (PC), Numerical Operations (NO), Coding Speed (CS), Auto Shop (AS), Mathematics Knowledge (MK), Mechanical Comprehension (MC), and Electronics Information (EI), Verbal Expression (VE).

[10] Saul McLeod, Albert Bandura’s Social Learning Theory, 2016, https://www.simplypsychology.org/bandura.html.

DEPARTAMENTUL SECURITĂȚII STATULUI ÎN ANII '70: COMPETENȚĂ ÎN FILAJ SAU DILETANTISM?

*Alin DREPTATE**

Abstract

State-sponsored surveillance has always been a subject of interest for the public, generating myths and heroes, portrayed with out of the ordinary skills, and in most cases, all of these were false or based on real facts, but grossly exaggerated. This article argues that except some of the activities of the State Security Department, which were against the Romanian population and had negative effects on the state development, other missions were legitimate and included proficient surveillance of individuals, especially foreigners, and their activities, which could have negatively affected national security. Based on researched documents, State Security Department exhibited critical and structured thinking in their missions and they were flexible to adapt to the requirements and the needs of the operational environment. The article argues the idea that State Security Department conducted surveillance operations professionally, with a limited impact from declamatory political influence, present in every institution in Romania before 1989.

Keywords: *State Security Department; Securitate; surveillance; foreigners; countersurveillance.*

INTRODUCERE

Începând cu anii '60, activitatea de filaj a Departamentului Securității Statului (DSS)[1], desfășurată la nivel central sau regional, sub coordonarea direcției specializate în acest sens, Direcția F Filaj și Investigații[2], devenea mai bine organizată și reglementată. Activitățile de filaj cuprindeau activități de supraveghere, dar și altele conexe, aspect oglindit de organigrama direcției, ce cuprindea birouri direcționate pe executarea efectivă a filajului, precum și pe desfășurarea de activități investigative sau de operații de tip reținere, percheziție sau management al celor arestați.

Prin instrucțiuni specifice structurii erau normate drepturile, obligațiile și restricțiile Direcției F, între primele fiind realizarea de investigații sau de percheziții secrete, rețineri de materiale sau de persoane (până la 48 de ore) sau arestări cu scopul descoperirii persoanelor „suspectate de activitate dușmănoasă"[3]. Toate acestea se realizau sub îndrumarea și aprobarea conducerii zonei în care se desfășurau, cu precizarea că după anul 1968 „prin reforma administrativ-teritorială, s-a renunțat la modelul sovietic cu raioane și regiuni, țara fiind împărțită în județe"[4] și un serviciu de filaj zonal putea avea în responsabilitate două-trei județe[5].

* *Autorul este cercetător acreditat la CNSAS.*

Restricțiile impuneau lucrătorilor Securității evitarea reținerii persoanelor ce ocupau poziții de autoritate, fără o aprobare prealabilă a DSS, precum și a celor care erau membri ai Comitetului Central al Partidului Muncitoresc Român (PMR)/ Partidului Comunist Român (PCR) sau a guvernului, respectiv a celor cu imunitate juridică/ parlamentară sau a diplomaților. Este necesară precizarea că reținerea diplomaților se putea face doar în „situații flagrante, compromițătoare”[6] sau prin diverse tertipuri, cum ar fi surprinderea unei soții de către soțul acesteia în timpul unei relații cu diplomatul, aspect exploatat prin reținerea diplomatului pentru câteva ore de către Miliție, pentru clarificarea situației. Recrutarea de colaboratori ai Securității se evita a se face dintre deputații „Marii Adunări Naționale”[7] sau dintre membrii partidului, toate acestea fiind însă doar linii directoare, excepțiile variind în funcție de dispozițiile primite și de existența aprobărilor suplimentare obținute din partea Primului Secretar al Comitetului Județean sau, după caz, de la Secretarul General al PCR[8].

Sub aspectul pregătirii, o parte din personalul Securității era absolvent de învățământ gimnazial, cu o mică parte dintre ei având pregătire universitară, cea din urmă impusă ca și condiție de activare în DSS după anul 1958. Cu toate acestea, chiar și după 1958 se remarca o preferință de a avea în structurile de conducere ofițeri „călițiîn lupta cu dușmanul de clasă”, un astfel de ofițer fiind, spre exemplu, generalul Pius Covaci, șef de direcție pe țară la filaj și investigație, fost miner cu doar patru clase[9]. Situația membrilor cu studii absolvite arăta că, spre sfârșitul anilor 1950, personalul cu studii superioare era sub 3,5% din întreaga structură, iar procentul celor ce dețineau un certificat de absolvire de șapte clase se apropia de 50%[10].

Ulterior, după anul 1964, când „se încheiase perioada dură a confruntării partidului cu dușmanii de clasă”[11], situația pregătirii universitare a cadrelor era mult mai bună[12], spre exemplu, activitatea Școlii Militare de Ofițeri de Informații de la Băneasa fiind orientată pe pregătirea de „profesioniști ai informațiilor și nu [de] slujbași ai partidului”[13]. Cadrele Securității erau selecționate și instruite pentru a avea „o bună pregătire profesională, juridică și de cultură generală, inclusiv cu o altă viziune asupra activității și a vieții în general”[14], având cursuri de „topografie militară, dactilografie, de identificare a persoanelor după scris, transmisiuni secrete prin radio, codificare și decodificare, conducere auto”[15] și „aplicații practice de scotociri în zone împădurite”[16]. Educația acestora cuprindea și participarea la prelegeri despre poezia modernă sau la spectacole de muzică și dansuri populare[17]. Rigurozitatea militară și diversitatea în pregătirea cadrelor Securității s-au perpetuat până spre perioada de final a regimului comunist, profesionalismul cadrelor Securității fiind îndeosebi observat în anii ’80, prin trecerea de la „bătaia, tortura, interogatoriile sălbatice pentru procurarea de probe”[18] la „probarea dovezilor, prezența procurorului” și existența de „măsuri prudențiale, preventive”[19].

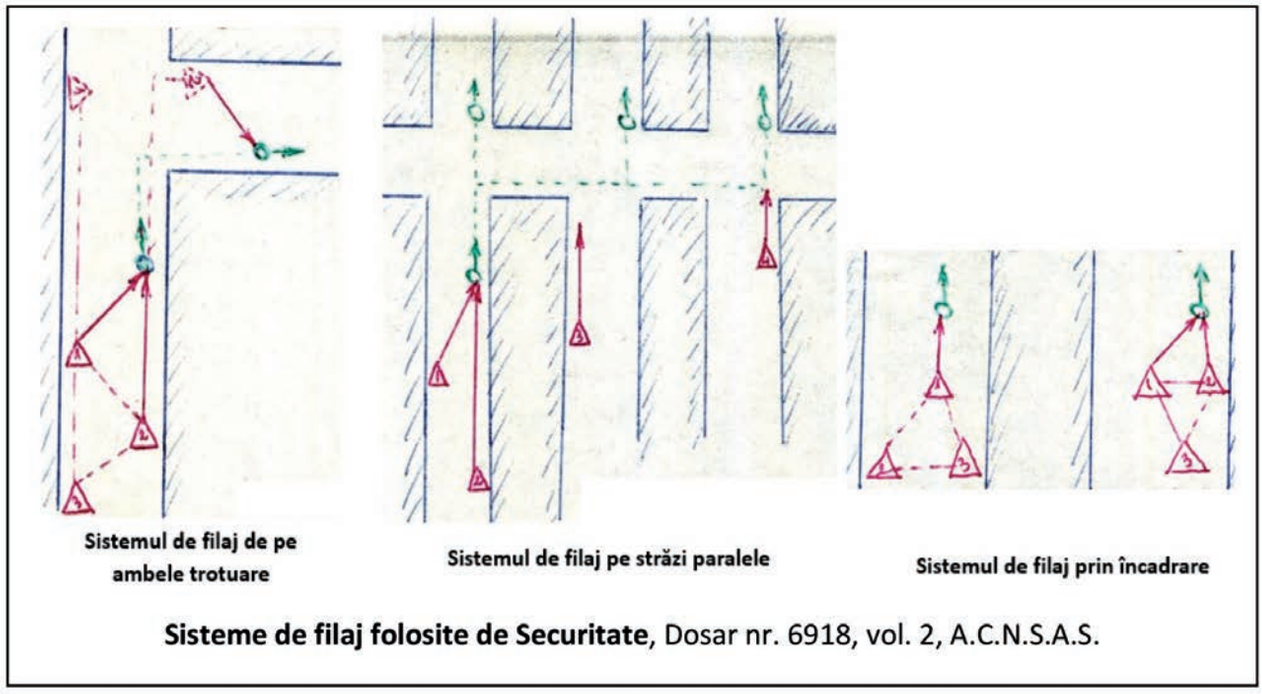
Din perspectiva activității operative, spre sfârșitul anilor ’60 activitatea DSS devenea mai pronunțată, îndeosebi în anul 1967, când Nicolae Ceaușescu și-a exprimat nemulțumirea că în acel an nu fusese descoperită nicio rețea de spionaj străină[20]. În cadrul unei „consfătuiri cu activul de bază al M.A.I.”, acesta accentuase necesitatea „îmbunătățirii pregătirii […] profesionale, ridicarea nivelului politic, ideologic [și] lărgirea orizontului […] de cultură generală”[21] ale organelor Securității. Astfel, în contextul creșterii numărului de vizitatori străini, datorită unei relaxări politice de scurtă durată și a riscului folosirii acestora de către agențiile de spionaj, precum și ca o posibilă reacție la nemulțumirile enunțate anterior de Ceaușescu, Direcția a IX-a din cadrul DSS a emis la data de 18 decembrie 1967 un documentar despre supravegherea cetățenilor străini. Acesta trata dificultățile întâlnite și modul în care serviciul s-a adaptat la provocările existente în activitatea de supraveghere[22]. Studiul de mai jos face o analiză a problematicii filajului, cu exemple din acel documentar, completate și detaliate cu fragmente din manuale, instrucțiuni și activități operative ale Direcției a IX-a a Securității.

CONCEPTUL DE FILAJ

Securitatea a definit conceptul de filaj drept o „activitate de urmărire secretă în teren, cu ajutorul unor mijloace și metode adecvate, a anumitor persoane și locuri care fac obiectul muncii de securitate”[23]. Printr-o astfel de activitate se încerca identificarea „elementelor dușmănoase”, a locațiilor acestora, a adreselor, a datelor personale sau a procedeelor folosite în activități ce aduceau atingere securității naționale. Astfel de activități au inclus, spre exemplu, identificarea unui transport de armament ce urma să fie folosit în executarea unui atac pe teritoriul României sau a unei mașini pline cu armament adus din Beirut și care urma să ajungă în Spania[24]. Procesul de filaj, așa cum era descris de Securitate, se structura pe mai multe etape, prima marcată de studiul sarcinii de filaj și a obiectivului[25] (locație, intrări ieșiri, orientare ferestre, străzi și direcții probabile de deplasare), urmată de identificarea locațiilor posibile de amplasare a posturilor de supraveghere și a bazelor de filaj și crearea planului și realizarea instructajului echipei[26], ulterior trecându-se la activitatea efectivă.

Filajul se realiza la cerere și, în funcție de situație, în cooperare cu alte structuri, cum ar fi cu cele de la contraspionaj și era, de regulă, stabilit pentru o perioadă limitată, în care se aștepta ca obiectivul[27] să desfășoare activități de interes pentru Securitate. În afara acestor perioade, obiectivul era trecut în „filaj de studiu”[28], presupunând preluarea acestuia în supraveghere, cu scopul verificării activităților lui, când se ivea o oportunitate (prezența sa într-un perimetru în care se afla și echipa de filaj), coroborată cu disponibilitatea echipei de filaj.

Tipurile de filaj folosite de Securitate, numite sisteme, erau bazate pe configurația trotuarelor, străzilor și pe tipuri de procedee utilizate în urmărirea obiectivului. Astfel, „sistemul de filaj de pe ambele trotuare”[29] era folosit în străzile semiaglomerate, filorii[30] deplasându-se pe ambele trotuare, iar sarcina de observare fiind trasată primului și celui de-al doilea filor, iar ceilalți necesitând a fi în contact cu aceștia și schimbându-se la intersecții, după nevoi, pentru preluarea obiectivului. În cadrul acestui dispozitiv, în sarcina ultimului filor era misiunea de a direcționa mașina de filaj și de a descoperi un eventual contrafilaj[31].



Sisteme de filaj folosite de Securitate, Dosar nr. 6918, vol. 2, A.C.N.S.A.S.

În mod similar, sistemul de filaj „pe străzi paralele”[32] folosit de Securitate prezenta avantajele folosirii unui număr de unu sau doi filori în urmărirea obiectivului, cu ceilalți deplasându-se pe străzi paralele și preluând obiectivul la schimbarea direcției de deplasare. Adițional, se putea folosi și sistemul de filaj prin încadrare, cu „vârful“ înainte sau înapoi, pe străzile foarte aglomerate, trioul monitorizând obiectivul, iar ceilalți filori fiind localizați mai în spate și acționând ca rezervă la cei din față. Sistemul de filaj în lanț a fost folosit pe străzile neaglomerate sau cu un singur trotuar, cu sarcina principală de a supraveghea obiectivul aparținând primului filor, iar ceilalți deplasându-se în urma lui și aflându-se la distanțe mai mari, predarea realizându-se succesiv, de la post la post.

Ca și particularitate, putea fi folosit și „filajul din față”[33], prin care filorul se afla în fața obiectivului și prin coordonarea cu cei din spatele obiectivului și aflați la o distanță mai mare, se anticipau mișcările acestuia. În acest fel a fost luat în supraveghere un cadru al unui serviciu de informații străin aflat sub acoperire diplomatică, care, cunoscându-se că se află într-o zonă aproximativă, a făcut greșeala de a utiliza un traseu de autoverificare folosit anterior. Fiind reperat pe acesta și prin folosirea filajului din față, echipa de supraveghere a descoperit legătura obiectivului cu un ofițer activ în Securitate și care, ulterior, a fost condamnat la 20 de ani de închisoare pentru trădare de țară. Astfel, această tehnică prezintă avantajul de a exploata autoverificările obiectivului direcționate spre spatele său și nu înainte, persoanele din față prezentând un interes redus.

În cele din urmă, sistemul de filaj pe posturi fixe a fost folosit îndeosebi în situațiile când se știa sau anticipa traseul obiectivului sau când acesta își lua măsuri de contra-filaj. Astfel, în cadrul unor misiuni de supraveghere în București, Securitatea, anticipând interesul unui străin pentru o zonă, a amplasat două dispozitive fixe de supraveghere, unul mascat într-un vagon de lucru al salubrității, iar celălalt într-o dubiță, ce au facilitat ulterior identificarea unei relații a străinului cu un cetățean român[34].

La acțiunile ce implicau contra-filajul, se atrăgea atenția asupra „complicelui” care putea veni înaintea obiectivului și supraveghea zona și persoanele din locație, comparând mediul înainte și după sosirea persoanei de interes. La nevoie, complicele și alți colaboratori monitorizau spațiul din jurul obiectivului, chiar pe timpul deplasării acestuia, spre identificarea echipei de filaj. Într-un astfel de caz, spre exemplu, soția unui cetățean român (agentă a serviciului de informații sovietic), iar el vizitator regulat al consulatului sovietic, a fost observată realizând contra-filajul. Aceasta se deplasa la aproximativ 50 de metri în spatele soțului ei, oprindu-se legendat la chioșcuri de ziare, monitorizând zona și notând numerele de mașini ce treceau[35]. În alte situații, în care obiectivul desfășura acțiuni de autoverificare, precum uitatul pe fereastră (de pe balcon sau de pe terasă), plimbarea în jurul domiciliului (pe străzi neaglomerate, drepte sau înguste) și folosirea de ganguri sau întoarceri bruște din mers, filajul devenea dificil, iar filorilor li se recomanda o atenție sporită, prioritatea constând în a nu fi identificați și astfel a nu compromite misiunea.

Alte modalități de supraveghere au inclus filajul în mijloacele de transport în comun, considerat dificil datorită particularităților asociate legendării[36] filorului sau nevoii de cunoaștere detaliate a traseului mijlocului de transport în comun. Prin comparație cu supravegherea în mijlocul de transport în comun, marcată de multe necunoscute, filajul în cadrul imobilelor era minuțios explicat în procedurile de lucru ale Securității, cu moduri de acțiune standardizate, particularizate la tipul de imobil sau la acțiuni specifice, cum sunt cele ce implicau folosirea scărilor sau a liftului. În ciuda tuturor precizărilor privind modul de acțiune, se accentua totuși că „prezența de spirit, calm, orientare, inventivitate, [...], legende verosimile”[37] erau de fapt ingredientele esențiale pentru reușita misiunii. Printre recomandările modului de lucru erau și acelea de a suspenda activitățile de filaj dacă exista pericolul deconspirării, iar personalul, pentru protecția și succesul misiunii, putea utiliza orice tip de ținută, nume conspirativ, legitimație de acoperire sau indicativ[38].

Adițional la activitatea de supraveghere efectivă se recomanda folosirea deghizării, definită ca schimbarea aspectului exterior prin folosirea articolelor de îmbrăcăminte majore (uniforme, treninguri) sau a celor ușor de schimbat (canadiene, șepci), pentru o deghizare totală sau parțială. În cadrul acestei activități, machiajul era un element esențial pentru succesul misiunii, diminuând vizibilitatea ofițerului prin schimbarea aspectului feței, părului, toate acestea realizându-se cu luarea în considerare a distanței față de obiectiv, a iluminării în zonă sau a gradului de aglomerație. În unele cazuri, chiar dacă dotarea pentru deghizare sau machiaj era deficitară, cuprinzând „câteva mustăți, ochelari cu lentile de sticlă, câteva pălării”[39], aceasta era compensată prin „inventivitate, efort și profesionalism”[40].

Per ansamblu, sistemele de filaj folosite de Securitate indicau o abordare analitică a fenomenului supravegherii, pentru fiecare dintre ele fiind evidențiate particularități de folosire a procedeelor, cu avantajele și minusurile lor, cu scopul unei utilizări judicioase și uniforme, dar adaptabile la mediul operațional. Acestea asigurau, așa cum s-a observat în multe situații, compatibilitatea modului de acțiune între structurile Securității din zone diferite în a-și preda obiectivele, atunci când acestea traversau ariile de responsabilitate.

PROVOCĂRI ÎN FILAJUL ÎN HOTELURI ȘI COMPLEXE TURISTICE

Chiar dacă activitatea de filaj era reglementată în manualele, procedurile și instrucțiunile Securității, aceasta se confrunta totuși cu dificultăți. La începuturile acesteia, filajul se executa doar prin posturi exterioare imobilelor, fapt care necesita existența mai multor filori, a căror prezență era ușor de remarcat. De asemenea, lipsa dotării cu aparatură radio portabilă și absența personalului Securității în interiorul hotelurilor sau complexelor a creat probleme în identificarea obiectivelor, în monitorizarea activității în interiorul locațiilor și a îngreunat predarea acestora echipelor de filaj. Un prim pas în rezolvarea acestor aspecte a fost dotarea cu stații de emisie recepție portabile R.E.R. Storno și înzestrarea cu mijloace tehnice de semnalizare a plecării obiectivului echipei de filaj. Acestea au permis transmiterea semnalmentelor și a altor trăsături specifice obiectivului fără realizarea unui contact fizic între filori și preluarea acestora între echipe fără pierderea conspirativității sau a obiectivului, eficientizându-se predarea lui chiar și pe traseu.

Adițional înzestrării cu tehnică, angajarea ofițerilor de securitate în hoteluri pe poziții de recepționeri sau portari a permis executarea filajului în incinta hotelurilor (și folosirea acestora ca baze, la nevoie, pentru garderobe) și a ofițerilor pentru desfășurarea de activități de culegere de informații. Prezența filorilor în incinta hotelurilor, ca și angajați ai acestora, a facilitat identificarea persoanelor de interes încă din momentul cazării lor, concomitent cu obținerea unor date preliminare și realizarea unei prime evaluări a comportamentului lor[41]. Astfel, în interiorul restaurantului Lido din București, un ofițer sub acoperire al Securității a identificat comportamentul unui cetățean american ca fiind tensionat și din discuții cu acesta a aflat și cauza. În acest fel, prin introducerea unui alt ofițer sub acoperire și descriindu-l ca membru al Ministerului de Comerț Exterior a reușit să influențeze obiectivul în direcția dorită de statul român. În alte două cazuri, petrecute la hotelul Ambasador din București, au fost identificați un fost ofițer de informații din armata hitleristă și un cetățean străin care dădea sarcini unor cetățeni români și pe care îi remunera. În cazul fostului ofițer hitlerist, consumul excesiv de alcool, o provocare verbală bine lansată și prezența oportună a ofițerului de securitate, sub acoperirea de funcționar al hotelului, au permis determinarea trecutului acestuia și documentarea mai minuțioasă a motivului prezenței sale pe teritoriul României. La îmbunătățirea documentării acestor activități a contat și crearea, în interiorul hotelului, de posturi de fotografiere acoperite, aspect care a eficientizat și mai mult munca filorilor și

Obiectivul Tache, Timișoara, 28 aprilie 1967, A.C.N.S.A.S., Fond Informativ, Dosar 1943, filele 271,272, 274

a permis probarea acțiunilor obiectivelor și a legăturilor realizate de aceștia cu cetățeni români.

Spre deosebire de activitatea de filaj desfășurată în zona localităților, în cadrul complexelor hoteliere din zona litoralului, dispunerea grupată sau succesivă a acestora, alături de geografia restrictivă zonei, au permis o monitorizare eficientă a punctelor obligatorii de trecere din/ în zonă, dar au generat și anumite dificultăți[42]. Aceste piedici priveau supravegherea numărului mare de intrări/ ieșiri din hoteluri/ complexe, diversitatea mijloacelor de transport folosite (autocare, autoturisme, bărci, hidrobiciclete) sau provocarea adaptării vestimentației filorului la tipurile de activități, extrem de variate, specifice litoralului. Obstacolele menționate anterior erau oarecum diminuate de avantajele oferite de acest mediu diversificat, în care varietatea culturală asigura o conspirativitate foarte bună ofițerilor Securității.

Pentru a concluziona, provocările la adresa activității de supraveghere erau multiple, cauzate de lipsa aparaturii radio portabile și numărul redus de personal asociat nevoilor de filaj, ce afectau negativ coordonarea echipelor și monitorizarea obiectivelor. Geografia unei zone crea atât dificultăți, cât și oportunități, iar abilitatea de a exploata aceste oportunități era dependentă de gradul de pregătire al ofițerilor Securității. Din acest motiv, calitatea personalului Securității a reprezentat garanția succesului în astfel de activități, așa cum lipsa de pregătire a generat nereușite.

GREȘELI ÎN ACTIVITATEA DE FILAJ A SECURITĂȚII

Conștientizarea complexității tipurilor de medii operaționale și adaptarea permanentă la acestea nu au eliminat însă și eșecurile. Activitatea serviciului de filaj a avut și insuccese, așa cum au fost ele recunoscute de către Securitate[43]. Problemele erau generate de folosirea de procedee greșite în filajul obiectivelor la domiciliu sau la locul de muncă. Printre cele mai uzuale erau nerealizarea

unui studiu asupra locației de interes anterior supravegherii obiectivului, lipsa cunoașterii familiei extinse a obiectivului sau nepăstrarea unei distanțe suficiente în activitatea de supraveghere. Astfel, prezența unor ferestre orientate înspre echipa de filaj și neatenția la acestea au permis monitorizarea echipei de către obiectiv, iar existența unei intrări/ ieșiri secundare a luat prin surprindere echipa de filaj, care nu era conștientă de aceasta și de mișcările nesupravegheate ale obiectivului care o folosea. Adițional, conversațiile purtate de filori în apropierea unei rude a obiectivului, fără realizarea acestui fapt, a confirmat suspiciunile acestuia cu privire la motivul real al prezenței în zonă a echipei[44].

Similar, lipsa acordării de atenție procedurilor la deplasarea pe jos sau cu mijloace de transport în comun, respectiv a deghizării, au dus la deconspirarea echipelor de supraveghere. Astfel, o echipă de filori a supravegheat o persoană de interes într-un autobuz și, ulterior, în câteva magazine, iar lipsa alternării echipelor a dus la identificarea lor și la eșecul misiunii. Acest mod de lucru neprofesionist a fost completat în anumite situații de neschimbarea îmbrăcămintei, folosirea unor piese de îmbrăcăminte în culori stridente, care făceau lucrătorii Securității să iasă în evidență sau de îmbrăcămintea neadecvată misiunii. Spre exemplu, în cadrul unei operațiuni de supraveghere a unor diplomați, echipa a fost identificată de aceștia prin remarcarea numărului de persoane ce se urca, în mod repetat, în mașină (3-4) și lipsa de corespondență între mașina de lux folosită (Mercedes) și calitatea redusă a hainelor lor.

Drept urmare, existența instrucțiunilor specifice care reglementau activitatea de supraveghere operativă, în mod detaliat în unele cazuri, și perpetuul interes în actualizarea modului de lucru la dinamica realității, au creat premisele desfășurării adecvate a acestei activități, însă succesul misiunii depindea, în primul rând, de calitatea pregătirii personalului. Un cadru pasiv, apatic și mulțumit în a face ceea ce se normează printr-o instrucțiune, fără a înțelege ideea din spatele textului și necesitatea de a realiza ajustări în modul de operare, pentru a se adapta la specificul zonei, misiunii sau obiectivului, nu a generat rezultatul scontat. Din acest motiv, Securitatea a înțeles nevoia de recrutare a unui personal de calitate în rândurile sale și, cu mici excepții, a menținut această linie directoare, promovând competența în activitatea de filaj și diminuând, în mod gradat, numărul acelora care nu obțineau performanță.

CONCLUZII

Activitatea DSS în domeniul supravegherii a avut un început modest, dar spre sfârșitul anilor ’60, structura se afla într-un proces de reorganizare și modernizare. În cadrul acestei ultime perioade, personalul era selectat din rândul celor cu educație universitară, cu o pregătire „multilaterală”, unde calitatea umană era recunoscută ca fiind necesară în operaţiunile de supraveghere, ce implicau tact, calm, discernământ, putere de analiză, sinteză și adaptabilitate la mediul operațional. Sub această concepție, Securitatea a înțeles că pentru activitatea de filaj a străinilor, cel puțin în pozițiile ce presupuneau munca sub acoperire, era necesară cunoașterea limbilor de circulație internațională, motiv pentru care s-a promovat recrutarea unor persoane cu competențe lingvistice.

În concluzie, spre sfârșitul anilor ’60 și începutul anilor ’70, Securitatea a avut o structură de filaj bine organizată, reglementată doctrinar și conștientă de necesitatea adaptării permanente la mediu și la evoluțiile tehnologiei. Aceste calități o delimitează evident de acuzațiile de diletantism, cel mai probabil asociate prezenței, influenței sau activității unor politruci sau a unor persoane motivate mai mult de rea voință decât de obiectivitate.

BIBLIOGRAFIE

1. A.C.N.S.A.S, Instrucțiuni privind munca de filaj și investigații, Dosar 008712, Vol. 1P34, 1978, http://www.cnsas.ro/documente/materiale_didactice/D%20008712_001_p34.pdf. Accesat în data de 08.01.2022.
2. A.C.N.S.A.S, Ordinul M.A.I. 835 din 24.10.1971, Dosar arhiva operativă, Dosar 7, vol. 7.
3. A.C.N.S.A.S., Filajul - mijloc al muncii de securitate (temă în cadrul pregătirii ofițerilor), 1984, Secția a XII-a, Inspectoratul de Securitate al Județului Timiș, D.S.S., Dosar nr. 6918, vol. 2 , filele 264-287.
4. A.C.N.S.A.S, Notă de filaj privind deplasările obiectivului „Hary", la data de 23 mai 1970, între orele 6.00-21.30, Fond Informativ, Dosar 5423, vol. 2, fila 26, http://www.cnsas.ro/documente/judete/Alba/2.2.pdf. Accesat în data de 08.01.2022.
5. A.C.N.S.A.S., Filaje realizate de Securitatea din Cluj, Fond Informativ, Dosar 18291, vol. 14, filele 231-231v, http://www.cnsas.ro/documente/judete/Cluj/1.6.pdf. Accesat în data de 08.01.2022.
6. A.C.N.S.A.S., Timișoara - fotografii de filaj efectuate în cadrul acțiunilor de urmărire efectuate în cazul scriitorului Sorin Titel, Fond Informativ, 28 aprilie 1967, Dosar 1943, filele 271, 272, 274, http://www.cnsas.ro/documente/judete/Timis/1.10.pdf. Accesat în data de 01.01.2022.
7. A.C.N.S.A.S., Instrucțiunea Nr. D – 00190/1987 privind organizarea și desfășurarea activității informativ-operative a organelor de Securitate, Fond Documentar, Dosar 123, vol. 41, filele 3-25, 24 iunie 1987, http://www.cnsas.ro/documente/istoria_sec/documente_securitate/directive_instructiuni/1987%20Instructiuni_2.pdf. Accesat 08.01.2022.
8. A.C.N.S.A.S., Index de termeni și abrevieri cu utilizare frecventă în documentele Securității, http://www.cnsas.ro/documente/arhiva/Dictionar%20termeni.pdf. Accesat în data de 08.01.2022.
9. A.C.N.S.A.S., Metode folosite în filajul cetățenilor străini cazați la hotelurile din București și complexele turistice de pe litoral, Ministerul Afacerilor interne, Departamentul Securității Statului, Direcția a IX-a, Dosar D 013448, vol. 1, filele 122-139.
10. A.C.N.S.A.S., Ordinul Președintelui Consiliului Securității Statului nr. 35 din 20.06.1968, Dosar nr. D 3626_005, filele 216-227.
11. A.C.N.S.A.S, Ordinul Președintelui Securității Statului nr. 35 din 20 iunie 1968, http://www.cnsas.ro/documente/acte_normative/D%203626_005%20fila%20216-227.pdf. Accesat în data de 08.01.2022.
12. BURDULEA Ioan, *În slujba adevărului*, Editura Bibliotheca, Târgoviște, 2016.
13. COIFESCU Vasile (Gl.bg.rtg.), „O zi din viaţa unei echipe de filaj", *Vitralii - lumini și umbre*, nr. 8, 2011, pp. 11-18.
14. COIFESCU Vasile (Gl.bg.rtg.), „Oameni din sud la hotelul „Nord", *Vitralii - lumini și umbre*, nr. 9, 2011, pp.119-122.
15. COIFESCU Vasile (Gl.bg.rtg.), „Alte amintiri", *Vitralii - lumini și umbre*, nr. 22, 2015, pp. 85-86.
16. COIFESCU, Vasile (Gl.bg.rtg.), „Acţiunea Suveica", *Vitralii - lumini și umbre,* nr. 26, 2016, pp. 109-112.
17. Consiliul de Stat, Decretul nr. 130/1972 privind înființarea, organizarea şi funcționarea Ministerului de Interne, 19 aprilie 1972, https://lege5.ro/Gratuit/gyydonbr/decretul-nr-130-1972-privind-infiintarea-organizarea-si-functionarea-ministerului-de-interne. Accesat 14.01.2022.
18. DOBRE Florica (coord.), Banu Florian, Bărbulescu Theodor, Ivan-Duică Camelia, Țăranu Liviu, *Securitatea. Structuri/Cadre, obiective și metode*, *vol. I (1948-1967)*, Editura Enciclopedică, București, 2006.
19. IANCU Mariana, „Cum îi spiona Securitatea pe turiștii străini care veneau în România: ghizi transformați în colaboratori, microfoane și în hoteluri, și pe plajă", 27 aprilie 2016, https://adevarul.ro/locale/constanta/cum-spiona-

securitatea-turistii-straini-veneau-romania-ghizi-transformati-colaboratori-microfoane-hoteluri-plaja-1_5720a16f5ab6550cb865352c/index.html. Accesat în data de 01.01.2022.

20. PATRICHI Viorel, *Ochii și urechile poporului. Convorbiri cu generalul Nicolae Pleșiță*, Editura Lumea, București, 2001.
21. RAȚIU Daniela, „Cum îi fila Securitatea pe cetățenii străini cazați la hotelurile din București și de pe Litoral“, 15.02.2021, https://m.ziare.com/nicolae-ceausescu/securitatea-filarea-cetatenilor-straini-ofiteri-acoperiti-metode-de-supravehgere-ministerul-de-interne-1661974. Accesat în data de 01.01.2022.
22. TVR1, Adevăruri despre trecut: Securitatea, brațul înarmat al partidului. Interviuri cu Mădălin Hodor – istoric, general maior (rtg) Dumitru Bădescu, general de brigadă Vasile Mălureanu, https://www.youtube.com/watch?v=hlpC3OEcJuI. Accesat în data de 01.01.2022.
23. ȘOVU Ion, „Rateu la sprânceană”, *Vitralii - lumini și umbre*, nr. 28, 2016, pp. 61-64.
24. ȚĂRANU Liviu, *Intelectualii și Securitatea. Studiu de caz: anii '80*, http://www.romania-actualitati.ro/intelectualii_si_securitatea_studiu_de_caz_anii_80-121912. Accesat în data de 15.01.2022.

[1] În baza decretului nr. 130/1972 privind înființarea, organizarea și funcționarea Ministerului de Interne, se înființează Ministerul de Interne prin fuziunea Consiliului Securității Statului cu Ministerul Afacerilor Interne și se constituie Departamentul Securității Statului (DSS), inclus în structura Ministerului de Interne. Termenul de DSS este înlocuit uneori în text cu Securitate.

[2] Direcția „F” (1951-1956), Direcția a VII-a (1956-1967), Direcția a IX-a (1967-1972), Unitatea Specială „F” (1973-1989); Florica Dobre (coord.), Florian Banu, Theodor Bărbulescu, Camelia Ivan-Duică, Liviu Țăranu, *Securitatea. Structuri/Cadre, obiective și metode*, *vol. I (1948-1967)*, Editura Enciclopedică, București, 2006, p. IX.

[3] Dobre et al., p. 43.

[4] Ioan Burdulea, *În slujba adevărului*, Editura Bibliotheca, Târgoviște, 2016, p. 76.

[5] Burdulea, op.cit., p. 79.

[6] Ion Șovu, „Rateu la sprânceană”, *Vitralii - lumini și umbre*, nr. 28, 2016, p. 63.

[7] Dobre et al., p. 43.

[8] Burdulea, op.cit., p. 186; TVR1, Adevăruri despre trecut: Securitatea, brațul înarmat al partidului. Interviuri cu Mădălin Hodor-istoric, general maior (rtg) Dumitru Bădescu, general de brigadă Vasile Mălureanu, min.8-12, https://www.youtube.com/watch?v=hlpC3OEcJuI. Accesat în data de 01.01.2022.

[9] Ibid. p. XXIII, după Viorel Patrichi, *Ochii și urechile poporului. Convorbiri cu generalul Nicolae Pleșiță,* Editura Lumea, București, 2001, p. 153.

[10] Dobre et al., p. XXII.

[11] Burdulea, op.cit., p. 41.

[12] Ordinul Președintelui Consiliului Securității Statului nr. 35 din 20.06.1968, Dosar A.C.N.S.A.S. D 3626_005, filele 216-227, pp. 1-13, disponibil online la http://www.cnsas.ro/documente/acte_normative/D%203626_005%20fila%20216-227.pdf. Accesat în data de 01.01.2022.

[13] Burdulea, op.cit., p. 50.

[14] Ibid., p. 41.

[15] Ibid, pp. 50-51.

[16] Ibid.

[17] Ibid, p. 60.

[18] Liviu Țăranu, *Intelectualii și Securitatea. Studiu de caz: anii '80*, http://www.romania-actualitati.ro/intelectualii_si_securitatea_studiu_de_caz_anii_80-121912. Accesat în data de 15.01.2022.

[19] Ibid.

[20] Mariana Iancu, „Cum îi spiona Securitatea pe turiștii străini care veneau în România: ghizi transformați în colaboratori, microfoane și în hoteluri, și pe plajă“, 27 aprilie 2016, disponibil online la https://adevarul.ro/locale/constanta/cum-spiona-securitatea-turistii-straini-veneau-romania-ghizi-transformati-colaboratori-microfoane-hoteluri-plaja-1_5720a16f5ab6550cb865352c/index.html. Accesat în data de 01.01.2022.

[21] C.N.S.A.S., Metode folosite în filajul cetățenilor străini cazați la hotelurile din București și complexele turistice de pe litoral, Ministerul Afacerilor interne, Dosar D 013448, vol. 1, filele 122-139, Departamentul Securității Statului, Direcția a IX-a, p. 2.

[22] Ibid., p.1; Daniela Rațiu, „Cum îi fila Securitatea pe cetățenii străini cazați la hotelurile din București și de pe Litoral“, 15.02.2021, disponibil online la https://m.ziare.com/nicolae-ceausescu/securitatea-filarea-cetatenilor-straini-ofiteri-acoperiti-metode-de-supravehgere-ministerul-de-interne-1661974. Accesat în data de 01.01.2022.

[23] A.C.N.S.A.S., Filajul - mijloc al muncii de securitate (temă în cadrul pregătirii ofițerilor), Dosar nr. 6918, vol. 2 , filele 264-287, 1984, Secția a XII-a - Inspectoratul de Securitate al Județului Timiș, D.S.S, p. 1.

[24] Vasile Coifescu, „Oameni din sud la hotelul „Nord”, *Vitralii - lumini și umbre*, nr. 9, 2011, pp.119-122.

[25] Obiectivul este definit ca o persoană, grup de persoane sau instituție în supravegherea informativă a Securității.

[26] A.C.N.S.A.S., Filajul, pp 2-5.

[27] Termen folosit pentru a desemna persoana urmărită, folosit interșanjabil cu persoană de interes.

[28] Vasile Coifescu, „O zi din viața unei echipe de filaj”, *Vitralii - lumini și umbre*, nr. 8, 2011, p.13.

[29] A.C.N.S.A.S., Filajul, p. 6.

[30] Persoană din structura de filaj a Securității care executa activități de supraveghere.

[31] Activitate de identificare a activității de supraveghere/ filaj.

[32] A.C.N.S.A.S., Filajul, pp. 7-10.

[33] Coifescu, „O zi din viața unei echipe de filaj“, pp. 14-15.

[34] Coifescu, „Alte amintiri”, *Vitralii - lumini și umbre*, nr. 22, 2015, pp. 85-86.

[35] Coifescu, „Acţiunea „Suveica”, *Vitralii - lumini și umbre,* nr. 26, 2016, pp. 109-110.

[36] În baza instrucțiunii Nr. D – 00190/1987, legenda informativă este definită ca „versiunea verosimilă folosită cu scopul de a asigura conspirarea și secretizarea muncii de securitate și a realiza inducerea în eroare a dușmanului”.

[37] A.C.N.S.A.S., Filajul, p. 12.

[38] Dobre et al., p. 44.

[39] Burdulea, op.cit., p. 92.

[40] Ibid.

[41] Dobre et al., p. 5.

[42] Ibid., pp. 13-18.

[43] Ibid.

[44] Ibid.

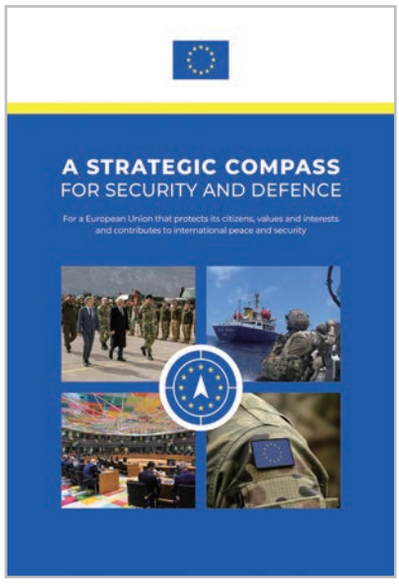
FOOD FOR THOUGHT

*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 de intelligence.*

DOCUMENTE OFICIALE

Busola strategică a UE - autonomia strategică și viitorul apărării europene

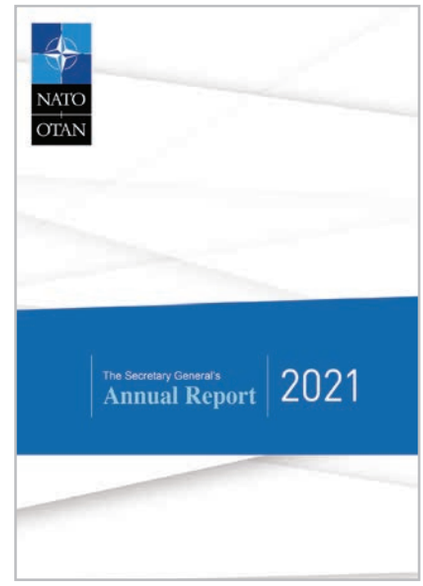
EU. "A Strategic Compass for Security and Defence: For a European Union that protects its citizens, values and interests and contributes to international peace and security", 21.03.2022.



Busola Strategică, document aprobat după o lungă reflecție privind viitorul apărării europene, dar și la scurt timp după izbucnirea războiului ruso-ucrainean, stabilește un plan de acțiune pentru consolidarea politicii de securitate și apărare comune (PSAC), într-o „lume multipolară contestată". Pentru întărirea autonomiei strategice, Busola trasează măsuri în următoarele domenii: (1) acțiune – crearea Capacității de desfășurare rapidă a UE, sporirea mobilității militare, consolidarea misiunilor și operațiilor PSAC; (2) securitate – consolidarea capacităților de analiză de intelligence, dezvoltarea unor instrumente pentru contracararea amenințărilor hibride, elaborarea unei strategii privind domeniul spațial, consolidarea rolului UE în domeniul securității maritime; (3) investiții – îmbunătățirea cheltuielilor pentru apărare, investiții în capabilități de nouă generație, promovarea inovării tehnologice, reducerea dependențelor tehnologice și industriale; (4) parteneriate – consolidarea cooperării cu NATO, ONU și partenerii regionali, dezvoltarea de parteneriate bilaterale cu statele like-minded și parteneriate adaptate diferitelor regiuni.

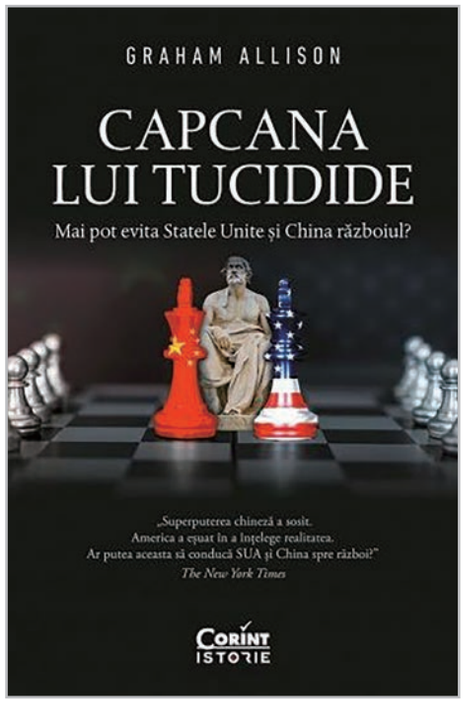
Activitatea NATO în anul 2021

NATO. ”The Secretary General’s Annual Report for 2021”, 21.03.2022.



Raportul Anual al Secretarului General, publicat la finalul lunii martie 2022, evidențiază principalele activități derulate de Alianță în anul 2021, în privința posturii de descurajare și apărare, investițiilor în domeniul apărării, precum și pe linia implementării măsurilor incluse în Agenda de adaptare NATO 2030. De asemenea, Raportul prezintă rezultatele sondajului realizat anual în cele 30 de state membre, evidențiind astfel un sprijin sporit din partea cetățenilor statelor NATO pentru apărarea colectivă (71% dintre aceștia consideră că ar trebui să-și apere țara dacă este atacată, în timp ce 64% sunt de părere că țara lor ar trebui să intervină dacă un aliat este atacat).

CĂRȚI



Războaiele și competiția dintre marile puteri

Graham Allison. *Capcana lui Tucidide: Mai pot evita Statele Unite și China războiul?*, Ed. Corint, 2022.

Publicată în 2017, ”Destined for War. Can America and China Escape Thucydide’s Trap?”, carte de referință în relațiile internaționale, a fost tradusă recent și în limba română (Ed. Corint, 2022). În cele 480 de pagini, Graham Allison pune în context teoria „creșterii pașnice a Chinei”, arătând, prin sintagma deja consacrată („capcana lui Tucidide”), cum în 12 cazuri din 16, competiția strategică dintre un hegemon și o putere emergentă rivală a condus, de-a lungul istoriei, la izbucnirea unui conflict armat. Cartea, intens dezbătută în mediile academice, este deopotrivă elogiată pentru fondul documentar și rigoarea analitică, precum și criticată/ contestată atât din perspectiva celor 12 recomandări, de la finalul lucrării, pentru evitarea „capcanei”, cât și a aplicabilității conceptului la rivalitatea sino-americană actuală.

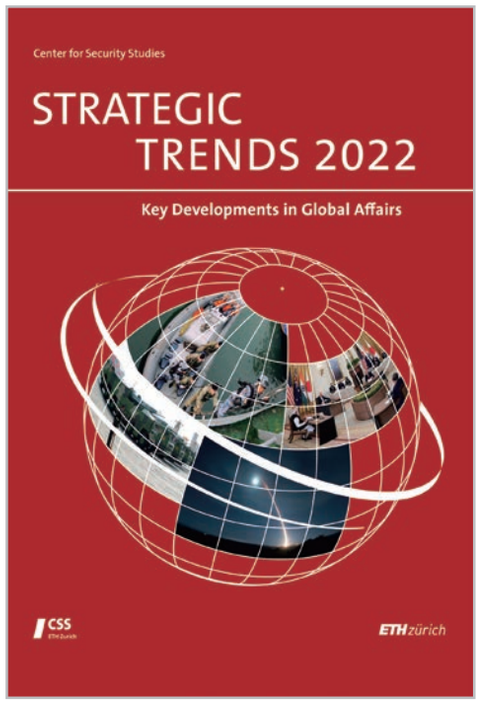
Cooperarea și conflictul – teme recurente în relațiile internaționale

Radu-Sebastian Ungureanu et al. *Cooperare și conflict în relațiile internaționale. O introducere,* Ed. Institutului European, Iași, 2021.

Cooperarea și conflictul sunt, probabil, laitmotivele teoriei relațiilor internaționale, dezvoltarea principalelor concepte fiind motivată și strâns legată de evoluția acestor două realități. Volumul, publicat la finele anului 2021, aduce în atenție, prin textele semnate de cercetători români, temele-cheie de cercetare din domeniu, într-o abordare didactică, tratând subiecte precum: evoluția teoriei, mediul anarhic și diplomația coercitivă, războiul interstatal, rolul organizațiilor internaționale, amenințările non-statale. Volumul este, astfel, bogat atât prin abordarea științifică și sumarizarea principalelor concepte, cât și prin bibliografia relevantă (mare parte disponibilă în limba română).

RAPOARTE, STUDII

Tendințe strategice

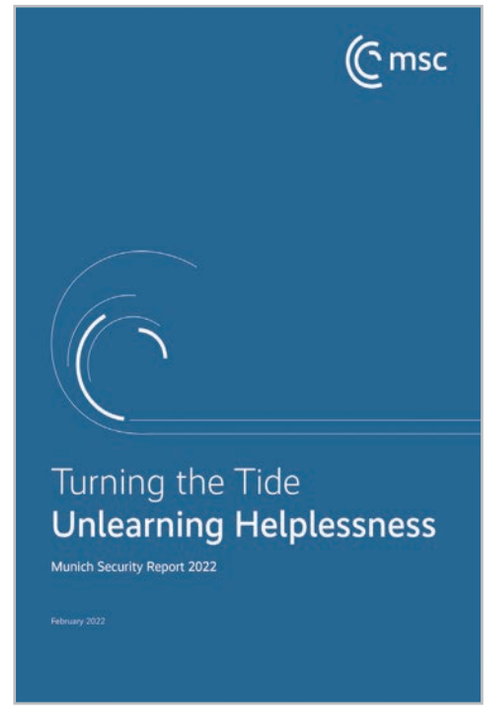


Center for Security Studies. ”Strategic Trends 2022: Key Developments in Global Affairs”, ETH Zurich, 2022.

Cea de-a 13-a ediție a raportului *Strategic Trends* analizează evoluțiile majore din politica globală, cu accent asupra securității internaționale. Astfel, raportul din 2022 este structurat în patru capitole (un al cincilea capitol nu a putut fi publicat pe fondul dinamicii războiului din Ucraina), care tratează: (1) impactul relațiilor dintre China și Rusia asupra securității asiatice; (2) rolul tehnologiilor hipersonice în competiția strategică dintre SUA, China și Rusia; (3) modalitatea în care războiul lansat de Rusia împotriva Ucrainei afectează regimul de control al armamentelor, precum și necesitatea unității transatlantice în acest context; (4) implicațiile strategice ale redefinirii conceptului „Indo-Pacific”, prin tranziția de la agenda pur economică la problemele specifice securității.

Conferința de Securitate de la Munchen: „Dezvățarea de neputință”

”Munich Security Report 2022: Turning the Tide. Unlearning Helplessness”, 18.02.2022.



Conferința de Securitate de la Munchen dă tonul, în fiecare an, dezbaterilor care domină agenda relațiilor internaționale, raportul publicat cu această ocazie impresionând prin realism și conceptele utilizate. Ediția din 2022 dorește să combată „neputința colectivă” care pare să caracterizeze democrațiile liberale și relația transatlantică, făcând apel la „dezvățarea de neputință” prin raportare la: (1) lecțiile învățate în urma misiunilor din Afganistan și viitorul prezenței occidentale în Mali, Sahel, Cornul Africii și Golful Arabiei; (2) arhitectura europeană de securitate și pretențiile ruse asupra Europei de Est; (3) riscul la adresa lanțurilor de aprovizionare din domeniul tehnologic; (4) accentuarea inechităților globale, în contextul pandemiei și schimbărilor climatice.

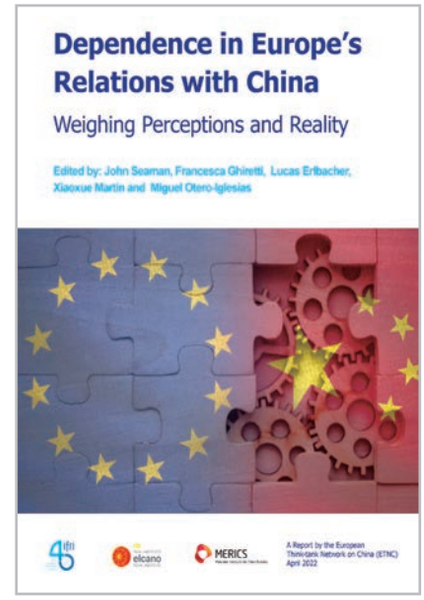
Cooperarea în domeniul securității în contextul competiției dintre marile puteri

Mazarr, Michael J. et al. ”Security Cooperation in a Strategic Competition”. Santa Monica, CA: RAND Corporation, 2022.

Cercetătorii RAND analizează modalitatea în care competiția strategică influențează dinamica activităților de cooperare din domeniul securității, atât din perspectiva intereselor strategice ale furnizorilor de securitate (SUA, China și Rusia, în principal), cât și prin raportare la o serie de studii de caz (India, Indonezia, Malaezia, Serbia, Thailanda și Vietnam). Studiul, de tip *policy paper*, este orientat către analiza aspectelor practice ale cooperării (obiective, instrumente, domenii), fiind amănunțit documentat.

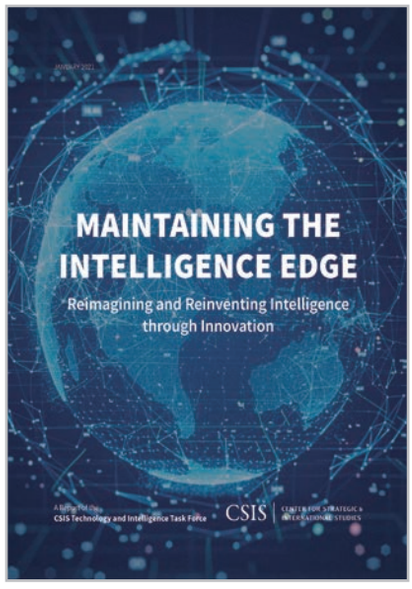
Dependența europeană față de China – între percepții și realitate

John Seaman et. al. (Ed.). ”Dependence in Europe’s Relations with China: Weighing Perceptions and Reality”, European Think-Tank Network on China (ETNC), April 2022.



Volumul, elaborat de o rețea a think-tank-urilor cu specialiști pe subiectul relației dintre statele europene și China, evidențiază demersurile europene pentru consolidarea rezilienței în cadrul relațiilor politice și comerciale cu statul chinez, în special în baza lecțiilor învățate pe timpul pandemiei de COVID-19. Studiul oferă, astfel, o imagine de ansamblu asupra noului context post-pandemic și a implicațiilor asupra Europei, dar și concluzii relevante privind perspectivele relației Europa – China prin analizarea dezbaterilor cu privire la reducerea dependenței la nivelul UE și în 18 state europene (17 din cadrul UE, alături de Marea Britanie).

Impactul noilor tehnologii asupra activității de intelligence



CSIS Technology and Intelligence Task Force. ”Maintaining the Intelligence Edge: Reimagining and Reinventing Intelligence through Innovation”, Center for Strategic and International Studies, January 2021.

Noile tehnologii (emergente și disruptive) vor schimba fundamental domeniul apărării și securității, atât prin diversificarea surselor de risc, cât și prin modalitățile ingenioase de implementare și armonizare cu doctrinele militare. În cazul activității de intelligence, inteligența artificială, *cloud computing*, senzorii avansați și *big data* vor transforma natura amenințărilor la care comunitatea de informații trebuie să răspundă, precum și posibilitățile de detecție și răspuns. Studiul, destinat comunității americane de intelligence, are ca obiectiv înțelegerea noilor tehnologii și a impactului acestora, concluzionând că principalul obstacol în fața inovării nu este reprezentat de lipsa resurselor financiare sau de limitările tehnologice, ci de cultura organizațională.