Anul XV nr. 4/2023

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

CUPRINS

PERSPECTIVE GEOPOLITICE ȘI GEOSTRATEGICE

RĂZBOAIELE SECOLULUI XXI

INTELLIGENCE

RECENZII ȘI SEMNALĂRI

„CHINURILE" EPISTEMOLOGICE ALE REZILIENȚEI: REZILIENȚA STRATIFICATĂ FAȚĂ CU CRITICILE UNUI CONCEPT NETERMINAT

*Iulian CHIFU**

Abstract

Resilience has become a concept widely used and extensively abused in the current literature, ready to lose its original means and fighting to find and to prove its ***real added value and relevance.*** *Till the end of 2024, NATO has assumed to reflect and to decide if resilience can prove its epistemological use. Those "torments" of the resilience as a concept are partially behind us since* ***societal resilience***[1] *has proven its added value during Russia's war of aggression in Ukraine, being the one that* ***explains the concrete results***[2] *when one side has all figures on its side – manpower, capabilities, weapons and ammunition storages, ideological post – imperial upper hand – but* ***didn't succeed in wining the war***[3]***.*** *How those elements of* ***societal resilience*** *mix with other valid significances – like the* ***resilience of critical infrastructure*** *or* ***systems*** *that deliver specific services to the communities – is to be determined.*

Keywords: *resilience; layered resilience; societal resilience; intangibles; societal security.*

REZILIENȚA – CONCEPT LA MODĂ, SUPRAUTILIZAT, DILUAT ȘI NECONCRETIZAT EPISTEMOLOGIC

Reziliența este un ***concept complex***, în formare, legat cu preponderență de o caracteristică a comunităților umane – societate, națiune. În evaluarea acestui concept nu s-a ajuns, pe căile epistemologice și de delimitare, la o concluzie finală – lăsată la nivel NATO pentru finalul lui 2024 – în privința utilității sale și a diferenței specifice majore față de alte concepte înrudite, care să aducă plus valoare în cunoaștere. Reziliența se înrudește și este **valorificată cu preponderență în sfera securității**, confundându-se cu aceasta în mare măsură, când este considerată – în mod fals și reducționist – echivalentă cu **eliminarea sau diminuarea vulnerabilităților** sau cu caracteristica societăților/comunităților de a face față vulnerabilităților. Alții o asociază, după originea termenului din medicină și ecologie, cu **sustenabilitate**, cu **rezistență la schimbare și la șocuri** acute sau persistente și o împing până la confuzia și transferul unor **elemente de bună guvernare**.

Mare parte a componenței / a substanței conceptului de reziliență se referă, însă, la intangibile și nemăsurabile[4], la criterii de natură calitativă, descriptive, și la componente de securitate societală[5] – coeziune și identitate – care sunt fie elemente nemăsurabile, cu erori majore la modelele de măsurare, fie criterii calitative și nu cantitative. Am spicuit în cadrul acestui material componenta de indicatori care acoperă, pe cât posibil, partea tangibilă și măsurabilă.

Iulian Chifu este profesor la Universitatea Națională de Apărare și profesor asociat la Școala Națională de Studii Politice și Administrative. Este președintele Centrului de Prevenire a Conflictelor și Early Warning. A fost consilier de stat al prim-ministrului Guvernului României pentru afaceri externe, securitate și afaceri strategice în perioada 2021-2023. Anterior, a fost consilier prezidențial pentru afaceri strategice, securitate și politică externă (2011-2014).

Dar nu trebuie să uităm că nu orice realitate din natură se măsoară și că marile erori au apărut exact de la tendința de aproximare, măsurare și comparare, sau din modele cu erori majore, de unde inexplicabilitatea unor procese, erori majore de evaluare și surprize strategice[6]. Un caz relevant și caracteristic în acest sens este războiul de agresiune pe scară largă din Ucraina, un altul îl reprezintă intrarea masivă și atacul dezastruos al Hamas în sudul Israelului (7 octombrie 2023). Reziliența este un concept chemat tocmai să explice și să completeze această diferență, acest vid de înțelegere și cunoaștere, când evoluțiile sunt diferite sau chiar opuse celor pe care le-ar recomanda o comparație între componentele fizice, palpabile, măsurabile. De asemenea, ar trebui să acopere hiatusurile în explicarea unor evoluții diferite de cele rezultate din **măsurători și studii comparative**, neașteptate atunci când indicatorii sunt nepotriviți, insuficienți, cu erori comparabile cu valorile indicate, deci irelevanți.

Reziliența este privită ca o trăsătură, un proces sau un rezultat, și este adesea tentant să se adopte o abordare binară pentru a stabili dacă reziliența este prezentă sau absentă. Cu toate acestea, în realitate, este mai probabil ca reziliența să existe mai degrabă pe un continuum și poate fi prezentă în grade diferite în mai multe domenii ale vieții. Reziliența se poate schimba, în timp, în funcție de dezvoltarea societății și de interacțiunea cu mediul înconjurător.

Reziliența se referă la **caracteristica unei comunități umane** și presupune capacitatea continuă și în curs de dezvoltare a comunității de a răspunde vulnerabilităților sale și de a dezvolta capacități care să ajute comunitatea respectivă în prevenirea, rezistența și atenuarea stresului provocat de incidente de securitate, refacerea într-un mod care să permită restabilirea comunitară la o stare de autosuficiență și la cel puțin același nivel de sănătate și de funcționare socială după un incident de sănătate și folosirea cunoștințelor dobândite în urma unui răspuns anterior pentru a întări capacitatea comunității de a rezista la următorul incident.

La bază are componente cheie care afectează atât vulnerabilitatea unei comunități înainte de dezastru, cât și capacitatea sa de adaptare în vederea redresării, acestea incluzând sănătatea fizică și psihologică a populației, bunăstarea socială și economică, cunoștințele și aptitudinile individuale, familiale și comunitare în ceea ce privește autosuficiența și auto-ajutorarea, comunicarea eficientă a riscurilor, nivelul de integrare socială a organizațiilor guvernamentale și neguvernamentale în planificarea, răspunsul și redresarea, precum și legăturile sociale ale membrilor comunității.

Pentru a construi **reziliența comunitară** o comunitate trebuie să dezvolte capacități în: implicarea activă a părților interesate din comunitate în planificarea evenimentelor de sănătate și în pregătirea personală; dezvoltarea rețelelor sociale; crearea de oportunități de promovare a sănătății pentru a îmbunătăți sănătatea fizică și psihologică a comunității; planuri și programe care abordează și sprijină nevoile funcționale ale persoanelor aflate la risc (inclusiv ale copiilor); instituirea de planuri pentru a răspunde în mod eficient nevoilor de sănătate fizică și psihologică ale membrilor comunității după dezastru și planuri de reconstrucție pentru sistemele de sănătate și sociale care pot fi activate imediat[7].

Reziliența – ca formă neoliberală de guvernare, internalizează situațiile de urgență și normalizează pericolul prin producerea unei bio-optici care acceptă riscul și înlocuiește abordările de tip „siguranța mai întâi”. Astfel, reziliența seamănă cu un sistem de gândire care instruiește acceptarea unor riscuri globale incognoscibile, transferând, totodată, responsabilitatea asupra indivizilor[8].

Definiția rezilienței subliniază **capacitatea de a rezista, de a se recupera și/sau de a se dezvolta a unei societăți** în fața factorilor de stres și a cerințelor în schimbare și evidențiază trei aspecte. În primul rând, definiția se referă la reziliență ca fiind o abilitate, sugerând că aceasta nu vine ca o cantitate stabilă, neschimbătoare. În al doilea rând, reziliența cuprinde elemente atât de rezistență, cât și de dezvoltare, permițând nu doar recuperarea în urma factorilor de stres, ci și creșterea. Și în al treilea rând, definiția se concentrează pe cerințele în schimbare, sugerând că reziliența este un proces care apare în timp[9].

REZILIENȚA DEMOCRATICĂ – CONDIȚIE *SINE QUA NON* A REZILIENȚEI

Avem o întreagă literatură privind reziliența democratică, aspirația pentru ireversibilitatea democrației și a libertăților individuale, care definesc lumea în care suntem, bazată pe reguli și modul nostru de viață, dar și relația dintre guvernanță, democrație și reziliență[10] – decantată inclusiv de la actuala competiție declarată între democrații și autocrații și pretenția unor regimuri autocratice de a genera modele de guvernare mai reziliente prin represiune, centralizarea puterii și eficiența deciziei.

Procesul de consolidare a democrațiilor contribuie la promovarea rezilienței. Astfel, sprijinul pentru democrație în rândul elitelor și al cetățenilor este favorabil rezilienței democratice. Elitele tind să susțină normele democratice dacă au încredere că și adversarii politici vor respecta regulile. O astfel de încredere reciprocă este limitată în țările cu instituții democratice slabe și cu un istoric de autocratizare.

Studiile istorice comparative arată că recesiunea economică, dezvoltarea economică slabă, corupția și inegalitatea prezic nemulțumirea democratică și, mai departe, căderea în autocrație. Astfel, politicile care abordează în mod eficient aceste nemulțumiri pot fi considerate ca favorizând reziliența democratică[11].

Înțelegerea rezilienței democratice se bazează pe **capacitatea de a preveni regresul substanțial al calității instituțiilor și practicilor democratice.** Totuși, termenul nu are în prezent o specificație clară în literatura de specialitate, dar există unele conceptualizări ale rezilienței democratice.

Într-o primă etapă, a rezilienței inițiale, unele democrații sunt rezistente prin prevenirea deplină a autocratizării, ceea ce înseamnă că nu au înregistrat scăderi substanțiale sau susținute ale calităților democratice. În cazul în care reziliența la început eșuează, democrațiile trec printr-un episod de autocratizare. O democrație poate da dovadă de reziliență la dezintegrare, evitând diluarea democratică în a doua etapă.

Acest concept în două etape al rezilienței democratice este pragmatic și observabil din punct de vedere empiric și permite evaluarea democrațiilor care rezistă forțelor autocratizării și care au o reziliență în criză odată ce autocratizarea a început.

În general, **reziliența democratică** este definită ca fiind **persistența instituțiilor și practicilor democratice**. Din punct de vedere empiric, reziliența este măsurată ca fiind continuarea democrației, fără scăderi substanțiale sau susținute ale calității acesteia, adică **evitarea autocratizării**[12]. Iar la acest capitol, în cazul statelor democratice, **reziliența democratică este o condiție *sine qua non* a rezilienței**. Pe această dimensiune, astăzi există nenumărate criterii, indicatori, indici consacrați internațional pentru a acoperi reziliența democratică, referitoare la drepturile omului, economia liberă de piață și statul de drept, inclusiv independența justiției, încrederea în justiție și combaterea corupției.

Reziliența este indisolubil legată de reziliența democratică. Un sistem cu conducere autoritară poate fi rezilient pe termen scurt, poate fi chiar mai eficient (nu mai rezilient) decât un sistem democratic – care are nevoie de validări, dezbatere și convingere a majorității. Pe de altă parte, deciziile într-un sistem democratic sunt fundamentate pe elemente mai puternice de argumentație și reflecție a multiplilor actori, de acceptabilitate socială și, implicit, de susținere și implicare. De aceea, **pe termen mediu și lung, reziliența ne-democratică nu e durabilă** pentru că va îngloba tensiuni și divergențe (chiar dacă argumentele contrare includ și un anumit nivel de conformitate și schimbare a societății) și aceste acumulări vor izbucni tectonic, impredictibil, exploziv chiar, în momentele cele mai sensibile, de crize sau conflicte, în care e implicată acea societate.

REZILIENȚA INSTITUȚIONALĂ – LIMITELE CONFUZIEI CU REZILIENȚA *PER SE*

Reziliența instituțională – este încă un subiect profund discutabil și în dispută, în special pentru că intră în contradicție cu esența subiectului rezilienței, care este societatea umană, comunitatea, națiunea, nicidecum instituțiile, statul, organizațiile internaționale care sunt

instrumente pentru asigurarea serviciilor către indivizi, comunități și societate. Într-o societate democratică, reziliența democratică este un element critic în evaluarea rezilienței generale. Iar așezarea în mijlocul preocupărilor rezilienței a omului, comunității și societății este esențială.

Conceptul de **reziliență instituțională** se concentrează astfel asupra aspectului uman (sau social) al relației om-mediu și include nu doar întrebări și preocupări legate de resurse sau șocuri naturale, ci toate sursele posibile de instabilitate, inclusiv șocurile economice, politice și culturale endogene. Următoarea definiție generală, dar insuficient operaționalizată, poate fi utilizată pentru a oferi o perspectivă introductivă în această chestiune: reziliența instituțională este capacitatea unui sistem social (societate, comunitate, organizație) de a reacționa și de a se adapta la provocări abrupte (interne sau externe) și/sau de a evita derapajul treptat pe pante alunecoase distructive. Să detaliem relevanța instituțiilor pentru aceste trei componente: (1) capacitatea de reacție, (2) adaptabilitatea și (3) evitarea pantelor alunecoase[13].

Există **trei abordări posibile** ale conceptului de reziliență instituțională, consistente cu esența conceptului de reziliență (în condițiile rezilienței democratice, evident):

- privirea instituțiilor ca sumă de norme și proceduri, deci instituționalizarea ca proces nu ca finalitate – clădire, funcții, poziții pentru anumiți oameni;
- privirea asupra instituțiilor drept comunități în sine – tratarea rezilienței instituționale drept reziliență a acestor comunități, constituite din oamenii din instituții, pe criterii de sociologia organizațiilor – dar fără detașarea lor de comunitatea largă pe care o deservesc, în orice caz de reziliență democratică;
- abordarea instituțiilor ca instrumente ale rezilienței prin prisma serviciilor acordate comunităților, societății etc.

Instituțiile – adică regulile și normele care guvernează interacțiunea umană - sunt în mod inerent conservatoare[14]. Ele reduc incertitudinea ajutându-i pe indivizi să își bazeze așteptările pe acțiunile celorlalți[15]. Astfel, (sub)sistemul instituțional ghidează operațiunile tuturor ființelor umane în cadrul unui sistem social-ecologic (SES)[16]. Instituțiile oferă baza pentru utilizarea resurselor naturale și, astfel, leagă sistemele sociale de cele ecologice[17].

S-a dovedit utilă **distincția între instituțiile formale și cele informale**[18]. I**nstituțiile formale** sunt toate tipurile de norme obligatorii din punct de vedere juridic, cum ar fi constituțiile, legile și politicile din sistemul politic (de exemplu, structura de guvernare), sistemul economic (de exemplu, drepturile de proprietate) și sistemul de aplicare a legii (de exemplu, sistemul judiciar)[19]. Instituțiile formale pot fi împărțite în trei categorii, care se aseamănă cu grade diferite de continuitate și schimbare: reguli constituționale - care definesc autoritatea actorilor colectivi/se dezvoltă în decurs de câteva decenii; reguli de alegere colectivă - care permit alegeri colective cu privire la utilizarea resurselor de către actorii autorizați/se schimbă în decurs de câțiva ani sau decenii; și reguli operaționale - care definesc seturile de alegeri ale indivizilor/ se schimbă sau se deplasează în decurs de câteva luni sau ani[20]. În schimb, **instituțiile informale** includ normele culturale, cum ar fi obiceiurile, tradițiile și valorile morale – regulile împărtășite la nivel social care există și sunt aplicate în afara structurilor formale de guvernanță[21]. Instituțiile formale și informale pot spori sau diminua reziliența unui SES[22].

Un sistem instituțional (ca subsistem al SES) este rezilient dacă poate:

1. **să reziste la perturbări** și, astfel, să asigure stabilitate și să reducă incertitudinea în SES (de exemplu, prin definirea cotelor de captare a apei, astfel încât acestea să poată fi aplicate în anii de penurie de apă);
2. **să se schimbe** (și, astfel, să ofere flexibilitate) pe termen mediu și lung, pentru a reacționa la incertitudinile unui mediu în schimbare și/sau la schimbările din sistemul social (de exemplu, să ajusteze cotele de apă dacă disponibilitatea apei a scăzut pe o perioadă mai lungă de timp din cauza schimbărilor climatice)[23].

Reziliența instituțională sporește **diversitatea instituțională**. Această diversitate include un set de instituții relativ stabile, care nu sunt ușor de schimbat și care asigură

continuitatea (cum ar fi o Constituție) și altele care sunt mai ușor de schimbat și care, prin urmare, asigură **flexibilitatea** necesară **pentru a reacționa la schimbările externe** (cum ar fi politica în domeniul apei, normele de gestionare a apei)[24]. Reziliența instituțională constă, așadar, în gestionarea continuității și a schimbării pentru a adapta un sistem instituțional, fără a-l schimba atât de des încât părțile interesate să-și piardă încrederea în structura instituțională[25]. Combinația adecvată de continuitate și schimbare variază în timp și are ca rezultat perioade de persistență instituțională întrerupte de perioade de schimbări bruște[26].

Reziliența instituțională *per se*, pentru instituții, pentru guverne, pentru o majoritate politică, pentru o anumită guvernare, pentru instituțiile însele, este în contradicție flagrantă cu conceptul de reziliență în înțelesul său de caracteristică a unei comunități umane. 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. Disputa e cea a diferenței dintre anti-fragil și robust[27]: rezistența în fața amenințării și a vicisitudinilor justifică efortul menținerii formulei fizice de reprezentare a statului și instituției sau trebuie asigurată doar supraviețuirea și continuitatea serviciilor asigurate populației.

Dezbaterea nu este deloc trivială. Pentru prima variantă pledează componența simbolică și experiența istorică. Astfel, succesiunea statului trebuie menținută în ceea ce înseamnă definiția și condițiile apartenenței la comunitatea internațională și la 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)[28] înseamnă acest lucru reziliență? A supraviețuit acel stat? Sau guvernul Svetlanei Tsikhanouska are vocație de continuitate a statului Belarus dacă acesta ar fi înglobat în Rusia (eterna temă a legitimității guvernului în exil)?

Efectele secundare ale confuziei în privința rezilienței instituționale, de la reziliența pentru asigurarea serviciilor la nivelul societății către reziliență *per se*, poate crea monștri. În primul caz, ideea rezilienței guvernamentale, de exemplu, sau a celei instituționale *per se,* ar presupune instrumentarul pentru ca un guvern să nu cadă niciodată, ca o instituție să supraviețuiască pentru sine – pentru pozițiile publice, pentru factorul de putere sau cel de resurse pe care-l incumbă – și nu pentru serviciile acordate populației.

Aceasta este o falsă abordare a ideii de reziliență, în substanța și semnificația ei, pentru că o instituție poate fi schimbată – atunci când se reorganizează administrativ menținerea unui serviciu, dar într-o altă formă, cu altă abordare și alți decidenți. E și efectul secundar al stagnării și eternizării la putere, apărarea unei anumite puteri, guvernări sau persoane (vezi cazul dictatorilor și autocrațiilor) versus deservirea societății. Acestea nu sunt și nu vor fi niciodată parte a rezilienței, din cauza alterării fundamentale a rezilienței democratice, dar și a înțelesului exact al rezilienței.

CUM SE CIRCUMSCRIU ELEMENTELE REZILIENȚEI STRATIFICATE A NATO CU ESENȚA REZILIENȚEI SOCIETALE

Reziliența a fost **principalul subiect al summit-ului NATO de la Varșovia** (2016)[29] și a cuprins modul de definire, evaluarea rezilienței și întărirea ei. Reziliența este privită drept corolar sau chiar condiție – sunt auto-influențabile și se susțin reciproc – a descurajării și apărării aliate, ca 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 gestiona eficient mișcările necontrolate în migrație 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[30].

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 conceptul a fost prezent și în forma interimară a Conceptului Strategic al Alianței Nord-Atlantice, care a fost adoptat la Madrid (2022), și **Uniunea Europeană** și-a pregătit documentul strategic, Busola Strategică, care are prevederi referitoare la modul în care privesc cei 30 de membri reziliența[31]. Și temele explicite se referă la schimbările climatice, dezastre, urgențe civile. Pe dimensiunea rezilienței economice, temele sunt lanțurile de aprovizionare, rutele de transport, libertatea navigației, securitatea furniturilor.

Între **elementele de reziliență reținute la nivelul NATO și al UE** - prima organizație pentru a asigura serviciile de apărare colectivă către societățile statelor membre, iar cea de-a doua pentru a asigura politicile legate de schimbări climatice, dezastre și urgențe civile și pe cele de continuitate a fluxurilor de furnizori și rute de transport – putem identifica următoarele:

- Continuitatea guvernării, în sensul asigurării serviciilor către populație, intră în elementele de reziliență instituțională pentru societate, deci circumscrise sensului real și util epistemologic al rezilienței. La fel, în cazul continuității furnizării de alimente, apă și energie (cu elemente de reziliență a infrastructurii critice[32] și a lanțurilor de furnizări, reziliență economică), plus urgențe civile.
- Comunicațiile și transporturile intră direct la reziliența infrastructurii critice sau a sistemelor de asigurare a unor servicii pentru societate.;
- Crizele cu număr mare de victime, ca și urgențele civile, se circumscriu instrumentelor de tip decizie în criză. Reziliența, în acest caz, este marcată întotdeauna de limite pentru că gradul de „disrupție” al unei crize poate trece, dincolo de orice calcul de reziliență (vezi cazul Fukushima, lesne de plasat și la infrastructuri critice), în zona catastrofelor și dincolo de orice indicatori tehnici prevăzuți anterior.;
- Migrația este o temă aparte ce merită analizată cu atenție, fiind parte a rezilienței societale, dar care poate fi în contradicție cu reziliența instituțională, pentru că buna gestionare a fluxurilor migratorii (prin integrare și absorbție) poate intra (și a intrat) în contradicție cu reziliența societală. Desigur, la nivel de nuanță, putem vorbi despre elemente de toleranță și capacitate de integrare, în cazul unei națiuni puternice, care fac parte din reziliența societală, dar și acest lucru ține de politici guvernamentale adecvate care combină diversitatea, reziliența democratică a respectării opțiunilor și alegerilor cetățenilor și capacitatea de integrare reală)[33]. Deci reziliență societală și reziliență instituțională, dar cu multe necunoscute și posibile ciocniri de sensuri.
- În cazul criteriilor reținute de UE, avem de-a face cu una dintre semnificațiile originare ale rezilienței, reziliența de mediu, cu urgențe civile și decizie în criză, dar și cu reziliența economică, deja identificată mai sus, aferentă infrastructurilor critice și a sistemelor, lanțurilor de furnituri.

Problema epistemologică rezidă în a găsi modalitatea de „a potrivi” elementele rezilienței societale, cea care dă plus-valoarea și distincția conceptului de reziliență, relevanța și valoarea acestui concept, cu elementele de reziliență ale structurilor critice (reziliență inginerească) și reziliența sistemelor – în sensul rezilienței funcționale a acestor sisteme - pentru a asigura serviciile către populație și societate, deci pentru a îndeplini contractul social. Gestiunea crizelor – decizia în criză[34] și respectiv urgențele civile – intră, de asemenea, în responsabilitatea administrării sistemelor. Această epopee este critică pentru a valida relevanța și utilitatea conceptului de reziliență și locul său distinct, alături de alte concepte cu ale căror semnificații se confruntă, se suprapune sau chiar poate să se confunde.

BIBLIOGRAFIE

1. ALIGICĂ Paul Dragoș, Tarko Vlad, *Institutional Resilience and Economic Systems: Lessons from Elinor Ostrom's Work*, https://link.springer.com/article/10.1057/ces.2013.29.
2. BOESEA Vanessa A., Edgella Amanda B., Hellmeiera Sebastian, Maerza Seraphine F., Lindberg Staffan I., *How democracies prevail: democratic resilience as a two-stage process*, https://www.tandfonline.com/doi/epdf/10.1080/13510347.2021.1891413?needAccess=true.
3. CHIFU Iulian, *Decizia în Criză*, Editura RAO, București, 2019, ISBN 978-606-006-349-0, 335 p.
4. CHIFU Iulian, „Lecțiile conflictului din Ucraina și perspectiva rezilienței societale", *Infosfera*, nr. 2, 2022, ISSN 2065-3395.
5. CHIFU Iulian, Nantoi Oazu, Sushko Oleksandr, *Societal Security in the trilateral Region Romania-Ukraine-Republic of Moldova/ Securitate societală în regiunea trilateralei România-Ucraina-Republica Moldova*, ediție bilingvă, Editura Curtea Veche, Bucureşti, 2008, 320 p, ISBN 978-973-1983-00-4.
6. CHIFU Iulian, Ramberg Britta, *Crisis management in Transitional Societies*, Editura CRISMART SNDC, Stockholm, 2007, ISBN 978-91-85401-64-2, ISBN 1650-3856, 387p.
7. CHIFU Iulian, Ramberg Britta, *Managementul crizelor în societăţile în tranziţie. Cazul României*, Editura RAO, Bucureşti, 2008, ISBN 978-973-103-687-8, 352 p.
8. CHIFU Iulian, „Războiul hibrid și reziliența societală. Planificarea apărării hibride", *Infosfera*, nr. 1, 2018, ISSN: 2065-3395.
9 CHIFU Iulian, „Reziliența contemporană: competitivitatea națiunilor, capabilitatea statelor și securitate societală", *Infosfera*, nr. 3, 2022, ISSN 2065-3395.
10. CHIFU Iulian, „Reziliența în război și caracteristicile intangibile. Cazul războiului de agresiune al Rusiei în Ucraina", *Infosfera*, nr. 3, 2023, ISSN 2065-3395.
11. CHIFU Iulian, „Reziliență strategică: de la stabilitate și prevenție la acțiune pro-activă și adaptabilitate dinamică", *Gândirea Militară Românească*, nr. 1, 2021.
12. CHIFU Iulian, Simons Greg, *Rethinking Warfare in the 21-st Century. The Influence and Effects of the Politics, Information and Communication Mix*, Cambridge University Press, 2023, ISBN:9781009355247.
13. 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.
14. FOLKE C., L. Pritchard, F. Berkes, J. Colding, U. Svedin, *The problem of fit between ecosystems and institutions,* IHDP Working Paper No. 2, International Human Dimensions Programme, 1998.
15. *Grupul operativ UE-NATO privind reziliența infrastructurilor critice*, Raport de evaluare finală, iunie 2023, https://commission.europa.eu/system/files/2023-06/EU-NATO_Final%20Assessment%20Report%20Digital.pdf.
16. GUNDERSON L. H., C. S. Holling, L. Pritchard, G. D. Peterson, *Resilience in ecosystems, institutions, and societies: propositions for a research agenda,* Beijer International Institute of Ecological Economics, The Royal Swedish Academy of Sciences, Stockholm, Sweden, 1997.
17. GUPTA J., C. Termeer, J. Klostermann, S. Meijerink, M. van den Brink, P. Jong, S. Nooteboom, E. Bergsma, "The adaptive capacity wheel: a method to assess the inherent characteristics of institutions to enable the adaptive capacity of society", *Environmental Science and Policy*, vol. 13, nr. 6, 2010, p. 459–471, http://dx.doi.org/10.1016/j.envsci. 2010.05.006.
18. HELMKE G., S. Levitsky, "Informal institutions and comparative politics: a research agenda", *Perspectives on Politics*, vol. 2, nr. 4, 2004, p. 725–740, http://dx.doi.org/10.1017/S1537592704040472.
19. HERRFAHRDT-PÄHLE Elke, Pahl-Wostl Claudia, "Continuity and Change in Social-Ecological Systems: The Role of Institutional Resilience", *Ecology and Society*, 2012, https://www.jstor.org/stable/26269033.
20. HOLL C., *Entstehung und Wandel von Institutionen. North und Hayek im Vergleich,* Paper presented at the third workshop „Ordnungsökonomik und Recht" in Bleibach/Gutach, 11–12 Oktober 2002.
21. HOLLING C. S., L. H. Gunderson, "Resilience and adaptive cycles", pages 25–62, in L. H. Gunderson and C. S. Holling (eds.), *Panarchy: understanding transformations in human and natural systems*, Island Press, Washington D.C., USA, 2002.

22. LÜHRMANN Anna, *Disrupting the autocratization sequence: towards democratic resilience*, https://www.tandfonline.com/doi/epdf/10.1080/13510347.2021.1928080?needAccess=truehttps://www.tandfonline.com/doi/epdf/10.1080/13510347.2021.1928080?needAccess=true.
23. NORTH D. C., *Institutions, institutional change and economic performance,* Cambridge University Press, Cambridge, UK, 1990.
24. OSTROM E., *Governing the commons: the evolution of institutions for collective action,* Cambridge University Press, Cambridge, UK, 1990.
25. PAAVOLA J., "Institutions and environmental governance: a reconceptualization"*, Ecological Economics*, vol. 63, 2007, htt p://dx.doi.org/10.1016/j.ecolecon.2006.09.026.
26. 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.
27. PEJOVICH S., The effects of the interaction of formal and informal institutions on social stability and economic development", *Journal of Markets & Morality*, nr. 2, 1999, 164–181.
28. SHEA Jamie, *Resilience, a core element of collective defense*, document al NATO la https://www.nato.int/docu/Review/2016/Also-in-2016/nato-defence-cyber-resilience/EN/index.htm.
29. TALEB Nassim Nicolas, *Antifragil – ce avem de câștigat de pe urma dezordinii*, Editura Curtea Veche, 2014.
30. *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.
31. WILLIAMSON O. E., "The new institutional economics: taking stock, looking ahead"*, Journal of Economic Literature*, vol. 38, 2000, p. 595–613, http://dx.doi.org/10.1257/jel.38.3.595.
32. YOUNG O, "Institutional dynamics: resilience, vulnerability and adaptation in environmental and resource regimes", *Global Environmental Change*, vol. 20, 2010, p. 378–385, http://d x.doi.org/10.1016/j.gloenvcha.2009.10.001.
33. ZEGART Amy, "Israel's Intelligence Disaster. How the Security Establishment Could Have Underestimated the Hamas Threat", *Foreign Affairs*, October 11, 2023, at https://www.foreignaffairs.com/middle-east/israels-intelligence-disaster.

1 Iulian Chifu, „Războiul hibrid și reziliența societală. Planificarea apărării hibride", Infosfera, nr. 1, 2018, p.23-30, ISSN: 2065-3395.

2 Iulian Chifu, Greg Simons, *Rethinking Warfare in the 21-st Century. The Influence and Effects of the Politics, Information and Communication Mix*, Cambridge University Press, 2023, ISBN: 9781009355247.

3 Iulian Chifu, „Reziliență strategică: de la stabilitate și prevenție la acțiune pro-activă și adaptabilitate dinamică"*, Gândirea Militară Românească,* nr. 1, 2021, p. 10-21; Iulian Chifu, „Lecțiile conflictului din Ucraina și perspectiva rezilienței societale", *Infosfera*, nr. 2, 2022, p. 5-13, ISSN 2065-3395.

4 Iulian Chifu, „Reziliența în război și caracteristicile intangibile. Cazul războiului de agresiune al Rusiei în Ucraina"*, Infosfera*, nr. 3, 2023, p. 13-20, ISSN 2065-3395.

5 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.

6 Amy Zegart, "Israel's Intelligence Disaster. How the Security Establishment Could Have Underestimated the Hamas Threat", *Foreign Affairs*, October 11, 2023, at https://www.foreignaffairs.com/middle-east/israels-intelligence-disaster.

7 Chandra Anita et al., capitolul "Definition and Application of Community Resilience", în *Building Community Resilience to Disasters: A Way Forward to Enhance National Health Security*, RAND Corporation, 2011, p. 7–10. JSTOR, http://www.jstor.org/stable/10.7249/tr915dhhs.10.

8 Alicia Sliwinski, "Resilience", în *Humanitarianism: Keywords* (edited by Antonio De Lauri), Brill, 2020, p. 178–80. JSTOR, http://www.jstor.org/stable/10.1163/j.ctv2gjwwnw.87.

9 Meadows Sarah O. et al., "Understanding Resilience", în *Airman and Family Resilience: Lessons from the Scientific Literature*, RAND Corporation, 2015, p. 9–22. JSTOR, http://www.jstor.org/stable/10.7249/j.ctt19rmdbt.10.

10 Iulian Chifu, *Războiul hibrid și reziliența societală. Planificarea apărării hibride....*

11 Anna Lührmann, *Disrupting the autocratization sequence: towards democratic resilience*, https://www.tandfonline.com/doi/epdf/10.1080/13510347.2021.1928080?needAccess=truehttps://www.tandfonline.com/doi/epdf/10.1080/13510347.2021.1928080?needAccess=true.

[12] Vanessa A. Boesea, Amanda B. Edgella, Sebastian Hellmeiera, Seraphine F. Maerza, Staffan I. Lindberg, *How democracies prevail: democratic resilience as a two-stage process*, https://www.tandfonline.com/doi/epdf/10.1080/13510347.2021.1891413?needAccess=true.

[13] Paul Dragoș Aligică, Vlad Tarko, *Institutional Resilience and Economic Systems: Lessons from Elinor Ostrom's Work*, https://link.springer.com/article/10.1057/ces. 2013.29.

[14] Gupta J., C. Termeer, J. Klostermann, S. Meijerink, M. v. d. Brink, P. Jong, S. Nooteboom, E. Bergsma, "The adaptive capacity wheel: a method to assess the inherent characteristics of institutions to enable the adaptive capacity of society"*, Environmental Science and Policy*, vol. 13, nr. 6, 2010, p. 459–471, http://dx.doi.org/10.1016/j.envsci.2010.05.006.

[15] North D. C., *Institutions, institutional change and economic performance,* Cambridge University Press, Cambridge, UK, 1990.

[16] Holl C., *Entstehung und Wandel von Institutionen. North und Hayek im Vergleich,* Paper presented at the third workshop "Ordnungsökonomik und Recht" in Bleibach/ Gutach, 11–12 Oktober 2002.

[17] Folke C., L. Pritchard, F. Berkes, J. Colding, U. Svedin, *The problem of fit between ecosystems and institutions,* IHDP Working Paper No. 2, International Human Dimensions Programme, 1998.

[18] Williamson O. E., "The new institutional economics: taking stock, looking ahead"*, Journal of Economic Literature*, vol. 38, nr. 3, 2000, p. 595–613, http://dx.doi.org/10.1257/jel.38.3.595.

[19] Pejovich S, "The effects of the interaction of formal and informal institutions on social stability and economic development"*, Journal of Markets & Morality*, vol. 2, nr. 2, 1999, p.164–181.

[20] Holling C. S., and L. H. Gunderson, "Resilience and adaptive cycles"*,* pages 25–62, in L. H. Gunderson and C. S. Holling (eds.), *Panarchy: understanding transformations in human and natural systems*, Island Press, Washington, D.C., USA, 2002; Ostrom E., *Governing the commons: the evolution of institutions for collective action,* Cambridge University Press, Cambridge, UK, 1990; Paavola J., "Institutions and environmental governance: a reconceptualization"*, Ecological Economics*, vol. 63, nr. 1, 2007, p. 93–103, http://dx.doi.org/10.1016/j.ecolecon.2006.09.026; Helmke G., S. Levitsky, "Informal institutions and comparative politics: a research agenda"*, Perspectives on Politics*, vol. 2, nr. 4, 2004, p.725–740, http://dx.doi.org/10.1017/S1537592704040472.

[21] Helmke G., S. Levitsky, *Op. cit.*

[22] Gunderson L. H., C. S. Holling, L. Pritchard, G. D. Peterson, *Resilience in ecosystems, institutions, and societies: propositions for a research agenda,* Beijer International Institute of Ecological Economics, The Royal Swedish Academy of Sciences, Stockholm, Sweden, 1997.

[23] Young O, "Institutional dynamics: resilience, vulnerability and adaptation in environmental and resource regimes"*, Global Environmental Change*, vol. 20, nr. 3, 2010, p. 378–385, http://d x.doi.org/10.1016/j.gloenvcha.2009.10.001.

[24] Elke Herrfahrdt-Pähle, Claudia Pahl-Wostl, "Continuity and Change in Social-ecological Systems: the Role of Institutional Resilience", *Ecology and Society*, vol. 17, nr. 2, 2012, https://www.jstor.org/stable/26269033.

[25] Folke C &all, *Op.cit.*

[26] Elke Herrfahrdt-Pähle and Claudia Pahl-Wostl, *Op.cit.*

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

[28] 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.

[29] *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.

[30] Jamie Shea, *Resilience, a core element of collective defense*, document al NATO la https://www.nato.int/docu/Review/2016/Also-in-2016/nato-defence-cyber-resilience/EN/index.htm.

[31] EU, *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.

[32] *Grupul operativ UE-NATO privind reziliența infrastructurilor critice*, Raport de evaluare finală, iunie 2023, https://commission.europa.eu/system/files/2023-06/EU-NATO_Final%20Assessment%20Report%20Digital.pdf.

[33] Iulian Chifu, „Reziliența contemporană: competitivitatea națiunilor, capabilitatea statelor și securitate societală", *Infosfera*, nr. 3, 2022, ISSN 2065-3395.

[34] Iulian Chifu, *Decizia în Criză*, Editura RAO, București, 2019, ISBN 978-606-006-349-0, 335 p.; Iulian Chifu, Britta Ramberg, *Crisis management in Transitional Societies*, Editura CRISMART SNDC, Stockholm, 2007, ISBN 978-91-85401-64-2, ISBN 1650-3856, 387p.; Iulian Chifu, Britta Ramberg, *Managementul crizelor în societăţile în tranziţie. Cazul României,* Editura RAO, Bucureşti, 2008, ISBN 978-973-103-687-8, 352 p.

EVOLUȚIA DOCTRINELOR MILITARE RUSE: DE LA RĂZBOI NELINIAR LA CONTROLUL HAOSULUI

Andrei Cristian MORARU*

Abstract

This article explores the evolution of Russian military doctrines in Europe over three distinct phases: the Gerasimov Doctrine (2013-2019), the Gerasimov Doctrine 2.0 (2019-2022), and the newly adopted doctrine (2022-present), that falls under the controlling chaos theory. The Gerasimov Doctrine, known for its hybrid warfare tactics, cyberattacks, and propaganda measures, aimed to destabilize European security. However, this doctrine was not solely implemented by the Russian Ministry of Defense; it was part of a broader plan orchestrated by Russian leader Vladimir Putin to maintain influence over the Euro-Atlantic region. During the implementation of Gerasimov Doctrine 2.0, Russian tactics shifted, reflecting the adaptability of their strategies, by using offensive cyber-attacks which affected the Ukrainian critical infrastructure. The current doctrine aims at creating social chaos in the Euro-Atlantic region, emphasizing on the creation of artificial chaos while maintaining a degree of regional control. The current article aims to analyze the evolution of the three military doctrines and the underlying reasons for these shifts, with implications for Euro-Atlantic security.

***Keywords**: Russian military doctrines; hybrid warfare; Euro-Atlantic security; Gerasimov Doctrine; Gerasimov Doctrine 2.0; controlled chaos theory.*

CONSIDERENTE GENERALE CU PRIVIRE LA POLITICA EXTERNĂ RUSĂ

Începând cu anul 2013 evoluția doctrinei militare a Federației Ruse a captat atenția comunității internaționale, marcând o transformare semnificativă în comportamentul acestui stat pe scena internațională. În ultimul deceniu, Rusia a jucat un rol central în conflicte regionale cheie, care au inclus anexarea Peninsulei Crimeea în anul 2014, implicarea în conflictul din Siria (începând cu anul 2015) și intervenția militară în Ucraina (2022). Aceste acțiuni au generat tensiuni semnificative între Federația Rusă și Occident, consolidând ideea că statul rus este hotărât să-și extindă sfera de influență în spațiul euro-atlantic.

Pe lângă dimensiunea geopolitică, Rusia a urmărit să impună și o influență ideologică, în special prin intermediul propagandei și a dezinformării, care a avut impact asupra opiniei publice europene. Metodele *soft-power* utilizate au avut drept scop subminarea coeziunii occidentale și promovarea unor valori specifice rusești. În plus, începând cu anul 2015, Rusia și-a intensificat prezența și în regiunea Orientului Mijlociu și Nordul Africii/ MENA, prin implicarea în conflictul din Siria.

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

Intervenția militară a venit în sprijinul guvernului sirian al lui Bashar al-Assad, forțele ruse având misiunea de a lupta împotriva grupărilor de opoziție și a celor extremiste.

Articolul de față se concentrează pe evoluția doctrinei militare a Federației Ruse și impactul transpunerii în practică a acesteia asupra stabilității în regiune. Obiectul general al studiului este investigarea și analizarea acestei evoluții în contextul securității euro-atlantice.

Studiul a pornit de la două întrebări inițiale de cercetare: „Ce beneficii are Federația Rusă ca urmare a creării unui haos social în regiunea euro-atlantică?" și „Cum sunt integrate acțiunile soft-power în doctrina militară a statului?".

În literatura de specialitate, există o serie de teorii care ar putea explica politica externă expansionistă manifestată de Federația Rusă.

Prin prisma teoriei lui Nicholas Spykman[1] („teoria țărmurilor"), Rusia încearcă să-și extindă influența în regiunea eurasiatică. Conform acestei abordări, din cauza absenței unui acces natural la mări cu climat cald, statul rus încearcă să pătrundă pe continentul european prin estul Europei. Această teorie, care a previzionat evenimentele geopolitice din ultimul deceniu, este bazată pe tendința Moscovei de a domina *heartland*-ul eurasiatic, pentru a-și întări influența în regiune și a se prezenta ca un stat-model, care va sta la baza reformelor sociale europene.

În perioada Războiului Rece, SUA a dezvoltat o strategie de „îndiguire" (*containment*)[2] pentru a contracara expansiunea și influența Uniunii Sovietice în spațiul european. În implementarea acesteia, a fost necesară cooperarea cu aliații vest-europeni pentru a limita politica externă expansionistă a URSS și pentru a proteja interesele occidentale.

Elementul cheie al strategiei de *containment* a fost expus în studiul diplomatului american George F. Kennan[3], prezentat sub anonimat în anul 1947. Astfel, într-un articol publicat în revista Foreign Affairs, autorul identifica riscurile generate de discursul lui Joseph Stalin din anul 1946, aspecte geopolitice care se puteau manifesta ca amenințări pentru securitatea eurasiatică.

DE LA „RĂZBOI NELINIAR" LA „OPERAȚII SPECIALE"

În martie 2013, generalul Valeri Gherasimov, șeful Statului Major al Armatei ruse, a publicat un articol[4] în care a prezentat avantajele „războiului neliniar", ceea ce în Occident a căpătat denumirea de „război hibrid"[5]. În fapt, articolul prezenta o transcriere a discursului propriu, în care susținea necesitatea utilizării războiului informațional, în coordonare cu acțiuni de tip *hard-power*, ca parte a unei concepții unitare a desfășurării conflictelor de tip „operații speciale". Republicat în anul 2016[6], articolul a stat la baza concepției de „new generation warfare"[7], prin intermediul căreia termenul de „război hibrid" era operaționalizat.

În perioada „Doctrinei Gherasimov" (2013-2019), Federația Rusă a implementat o serie de măsuri de tip *soft-power* subsumate războiului hibrid, care au inclus atacuri cibernetice și propagandă prin discursuri oficiale și mass-media. În acest sens, Ucraina a fost ținta unei serii de atacuri cibernetice de amploare în perioada 2014-2017, realizate de grupări precum Fancy Bear, Cozy Bear și Sandworm. În mai 2014, cu două zile înainte de alegerile prezidențiale, hackerii au pătruns în sistemul informatic folosit de Comisia Electorală Centrală din Ucraina și au dezactivat parțial rețeaua prin intermediul unui malware. Atacul cibernetic a fost reluat în același an, înainte de alegerile parlamentare din octombrie 2014, platformele online fiind blocate[8].

În 2015 și 2016 atacurile cibernetice rusești au vizat punerea în stare de nefuncționalitate a infrastructurii critice din Ucraina, respectiv afectarea companiilor responsabile de gestionarea rețelei de energie electrică. Au fost folosite metode asociate „spear phishing" pentru a distribui malware-ul „BlackEnergy" pe rețele securizate private. Ulterior au urmat atacuri cu malware-ul „KillDisk", care a provocat distrugeri și ștergerea permanentă a unor fișiere critice din rețea. Aceste atacuri au generat *black-out*-uri extinse, afectând aproximativ 230.000 de locuitori pentru o perioadă de până la șase ore, reprezentând primul atac cibernetic de succes asupra unei companii de energie electrică la scară globală[9].

Cel mai amplu și costisitor atac cibernetic asupra infrastructurii critice ucrainene a avut loc în anul 2017, când grupările rusești au utilizat malware-ul „NotPetya”, rezultat al combinării codului folosit în atacurile asupra rețelei de energie electrică cu malware-ul „Petya”. Grupările au avut acces la rețele comune private ale unor instituții bancare, aeroporturi și agenții guvernamentale din Ucraina.

Acest atac a generat pierderi financiare estimate la 10 miliarde de dolari și a afectat companii multinaționale precum Maersk, FedEx și Merck[10].

În ceea ce privește propaganda, „Doctrina Gherasimov” a direcționat utilizarea mijloacelor de transmitere a informațiilor către publicul european prin intermediul platformelor media rusești, care ulterior erau preluate și citate de presa europeană.

Credibilitatea surselor inițiale era întărită prin furnizarea de informații deja cunoscute sub o formă prelucrată, care includea evaluări și opinii negative asupra acțiunilor statelor europene pentru a modifica percepțiile occidentale. În acest fel, cetățenii europeni promovau ideile fabricate și generau insecuritate socială. De asemenea, prin intermediul discursurilor publice ale oficialilor ruși, Moscova a promovat o serie de mesaje cu conținut subversiv la adresa securității euro-atlantice, precum incapacitatea NATO de a-și îndeplini misiunile de apărare și de menținere a stabilității în regiune[11]. De asemenea, ulterior anexării Peninsulei Crimeea, Federația Rusă a desfășurat o campanie amplă de dezinformare, susținând că intervenția militară a fost justificată pentru a proteja populația rusofonă din regiune și pentru a preveni un „pericol fascist” în Ucraina[12].

Măsurile *soft-power* implementate în perioada 2013-2019 au demonstrat existența unor vulnerabilități în ceea ce privește măsurile de protejare a infrastructurii critice ucrainene, precum și lipsa unei culturi de securitate adecvate la nivelul unei bune părți a societății civile europene, care a devenit, în mod involuntar, un receptor al ideologiei ruse, facilizând atingerea obiectivelor strategice ale Federației Ruse.

UTILIZAREA PROPAGANDEI ÎN „OPERAȚIUNI INFORMAȚIONALE”

„Doctrina Gherasimov 2.0” a apărut în spațiul public în data de 4 martie 2019, prin intermediul ziarului oficial al Ministerului Apărării, Krasnaya Zvesda[13], la două zile după susținerea discursului șefului Statului Major General al forțelor armate ruse în cadrul conferinței anuale pe teme de apărare organizată de Academia Rusă de Științe Militare. Principalele puncte ale discursului lui Gherasimov au fost publicate și în limba engleză pe platforma oficială a publicației Sputnik[14].

Federația Rusă a continuat să includă propaganda în discursuri oficiale, dar a implementat și măsuri de influențare indirectă, sub denumirea de „operațiuni informaționale”[15], prin intermediul platformelor mass-media, cu accent pe manipularea opiniei publice (mai ales cu privire la capacitatea statelor europene de a menține stabilitatea în spațiul euro-atlantic). În acest mod, Federația Rusă a încercat modelarea dimensiunii sociale euro-atlantice spre o orientare pro-rusă și spre accentuarea valorilor ideologice promovate.

Una dintre campaniile de dezinformare implementate de statul rus, cu impact major asupra percepției populației europene cu privire la sistemul medical și de sănătate, a vizat lipsa de eficacitate a vaccinurilor în perioada pandemiei COVID-19[16]. Au fost promovate alternative rusești, fiind elaborate multiple articole în care vaccinul Sputnik V era prezentat drept superior celor occidentale[17]. Această campanie a avut și motivații de natură financiară, fiind dezvoltate platforme pentru atragerea de fonduri internaționale din partea societății europene, sub formă de fonduri de investiții, pentru finanțarea cercetărilor medicale[18]. Elemente propagandistice similare au fost îndreptate împotriva SUA și a statelor europene și pe timpul epidemiei HIV/SIDA din anii 1980[19].

O altă campanie inițiată de guvernul rus a avut loc pe timpul crizei din Belarus (2020). Pe timpul protestelor împotriva președintelui Aleksandr Lukașenko, Kremlinul a promovat, prin intermediul platformelor mass-media, imaginea statului ca fiind una de aliat de încredere al Moscovei[20], în ciuda imaginilor care demonstrau

încălcări ale Convenției de la Geneva (din 1949), fiind deschis focul asupra protestatarilor[21].

De asemenea, în perioada 2019-2022, au fost finanțate posturi de televiziune și platforme de știri europene[22], în vederea promovării unei viziuni pro-ruse. Ca reacția la aceste măsuri de proiectare a intereselor ruse, numeroase state europene au interzis difuzarea platformelor finanțate de Moscova, fiind retrase licențele acestora[23]. În ceea ce privește promovarea acestor interese în societățile occidentale cu un grad înalt de digitalizare, a fost intensificată prezența „boților" ruși pe platformele online de social media, cu accent pe Facebook, Instagram și Twitter[24]. Utilizatorii fictivi s-au alăturat grupurilor închise de discuții și forumurilor cu tematică politică și geopolitică europeană și au avut drept scop amplificarea dezinformării și crearea de teorii conspirative pro-ruse în rândul membrilor acestor comunități.

SUPREMAȚIE REGIONALĂ PRIN CONTROLUL HAOSULUI SOCIAL

În contextul conflictului ruso-ucrainean, începând cu data de 24 februarie 2022, președintele rus Vladimir Putin a efectuat un număr semnificativ de schimbări la nivelul conducerii militare a Federației Ruse. Conform analizei efectuate de Institutul American pentru Studiul Războiului (ISW)[25], cel puțin 17 comandanți de rang înalt au fost eliberați din funcții și înlocuiți, reprezentând o restructurare semnificativă a conducerii militare a statului. Procesul de restructurare a inclus demiterea unor lideri militari precum generalul Mihail Mizințev, cunoscut în spațiul public ca „Măcelarul din Mariupol", și generalul Rustam Muradov, care a condus atacul eșuat din Vuhledar, desfășurat în februarie 2023[26].

Generalul Serghei Surovikin, cunoscut sub numele de „Generalul Armaghedon", anterior comandant al campaniei militare desfășurate în Siria în anul 2015 și comandant al forțelor aerospațiale ruse din anul 2017, a fost numit în conducerea operațiunii militare din Ucraina începând cu luna octombrie 2022[27], înlocuindu-l pe generalul Gennady Zhidko.

Numirea acestuia a venit într-un moment marcat de instabilitate, ulterior bombardamentelor ruse asupra infrastructurii civile ucrainene și retragerii din regiunea Herson.

În luna ianuarie 2023, responsabilitățile acestui post au fost transferate către generalul Valeri Gherasimov[28], în timp ce generalul Surovikin a fost desemnat adjunct al acestuia. Acest aspect poate fi corelat cu faptul că, ulterior, Surovikin a fost anchetat în legătură cu o posibilă complicitate la revolta din 24 iunie 2023 organizată de Evgheni Prigozin, fostul lider al grupării Wagner[29] (începând cu luna august 2023, generalul nu a mai fost prezent în spațiul public). În conexiune cu aceeași anchetă, generalul Ivan Popov, fostul comandant al Armatei 58 de Forțe Întrunite, care luptă în Zaporojie, nu se mai află în poziția de conducere[30], după ce a făcut o serie de remarci în spațiul public cu privire la eșecurile planificării militare ruse din data de 12 iulie 2023[31].

În data de 24 iunie 2023, Evgheni Prigozin, fostul lider al grupării Wagner, a mobilizat aproximativ 5.000 de mercenari care au avansat către Moscova, generând o sursă puternică de instabilitate locală pentru Federația Rusă[32]. În ciuda acestui fapt, o analiză a ultimului deceniu sugerează că o cooperare strânsă între Federația Rusă și grupul Wagner reprezintă, în sine, un risc cu impact ridicat la adresa securității naționale a statului, prin impredictibilitatea acțiunilor mercenarilor care sunt motivați financiar, nu ideologic.

Demiterile conducătorilor militari, coroborate cu discursurile caracterizate de mesaje ostile adresate direct de către Vladimir Putin grupării Wagner[33], sugerau o diminuare a controlului situației regionale și interne din partea statului rus și o încercare urgentă de reimpunere a acestuia. În același timp, se poate observa o tendință prioritară a președintelui rus de a controla conținuturile informaționale difuzate către public, încercând în acest sens să proiecteze o imagine haotică a organizării Ministerului Apărării Rus, în vederea imposibilității prezicerii evenimentelor regionale ulterioare de către organizațiile euro-atlantice.

Aceste schimbări au determinat o serie de întrebări în rândul experților din domeniul militar,

fiind efectuate o serie de analize strategice în acest sens[34]. Implicațiile restructurării conducerii militare se pot răsfrânge asupra planurilor de acțiune propuse de Valeri Gherasimov, precum și asupra concepției generale de război hibrid a Federației Ruse. De altfel, comportamentul specific al statului rus a fluctuat pe timpul desfășurării conflictului ruso-ucrainean, însă o serie de adaptări ale doctrinei Gherasimov 2.0. au putut fi observate.

Astfel, în abordarea măsurilor de tip *soft-power* implementate de Federația Rusă, în cadrul campaniilor de dezinformare și propagandă a fost adăugat elementul de haos social, care este un rezultat direct al știrilor cu impact negativ asupra imaginii Uniunii Europene și NATO, promovate în spațiul euro-atlantic. Noua doctrină are drept scop menținerea controlului prin exploatarea haosului social generat în diferite state europene, care au o istorie comună din punct de vedere geopolitic, ideologic și religios cu cea a statului rus. Noua abordare vizează subminarea ordinii sociale și instituționale în cadrul statelor europene și a regiunii euro-atlantice. În acest mod sunt destabilizate elemente cheie care stau la baza funcționării și protejării infrastructurii critice.

Această interpretare este susținută inclusiv de Vladimir Putin, care, într-o adresă oficială, recunoștea puterea haosului social pentru generarea unor structuri instabile: *„Ca rezultat, în loc de democrație și libertate, au apărut haosul, izbucniri de violență și o serie de revolte. Primăvara Arabă s-a transformat în Iarna Arabă”*[35]. În cadrul acestui discurs, susținut la patru zile după anexarea Peninsulei Crimeea (2014), președintele rus a transmis societății necesitatea menținerii ordinii de către forțele ruse, în ciuda faptului că haosul social fusese deja pus în scenă prin intermediul propagandei realizate prin mass-media locală.

Fundamentul noii doctrine este asemănător, din punct de vedere al rezultatelor așteptate, cu teoria „controlului haosului” din domeniul analizelor statistice, care poate fi rezumată astfel: *„Dacă este adevărat că o mică perturbare poate genera răspunsuri majore în decursul timpului, este, de asemenea, adevărat că o alegere judicioasă a unei astfel de perturbații poate direcționa traiectoria acesteia pentru a produce o serie de stări dinamice dorite. Acesta este exact conceptul de <<targeting>>.”*[36]

În acest sens, noua doctrina propusă implică utilizarea mai multor platforme mass-media pentru îndeplinirea scopului campaniilor de dezinformare și propagandă, prin adăugarea în sfera de acțiune a Moscovei a unor agenții noi de presă, precum Pradva. De asemenea, începând cu anul 2022, propaganda realizată prin intermediul discursurilor oficiale s-a adaptat mediului informațional actual, prin postări de pe conturi oficiale rusești pe rețelele de socializare Telegram și Twitter[37].

Potrivit altei observații efectuate pe timpul analizei, conținuturile propagandistice sunt mai țintite, fiind menționate detalii necesare oferirii de credibilitate societății europene. Un exemplu în acest sens este declarația oferită de generalul Gherasimov în decembrie 2022[38], în care susținea că **România** este una dintre țările care livrează cele mai mari cantități de armament forțelor ucrainene.

Federația Rusă a mai adus în atenția societății europene o serie de „planuri emergente”[39] ale statelor NATO de a introduce contingente de menținere a păcii în zona de vest a Ucrainei, cu participarea directă a Poloniei și **României**[40]. Alte acuzații aduse organizațiilor euro-atlantice au făcut referire la așa-zise intenții ale Alianței Nord-Atlantice de a crea o „Asie Centrală Extinsă”, cu capitala la Kabul, sub conducerea SUA[41].

Propaganda statului rus a evidențiat și o serie de „greșeli”[42] efectuate de către forțele proprii, cu intenția de a sensibiliza societatea europeană și de a evidenția aspectul uman și propria failibilitate. În paralel, au fost utilizați termeni precum „ucrainenii teroriști” și narațiuni strategice subsumate Federației Ruse ca victimă[43].

CONCLUZII

Conform analizei întreprinse, precum și altor lucrări științifice[44], cele trei doctrine militare din perioada 2013-2023 sunt parte a unei strategii mai ample de menținere a controlului regional, care are ca scop secundar oferirea unor informații ușor de descifrat organizațiilor euro-atlantice cu privire la liniaritatea evoluției politicii externe a statului rus, similar statelor europene.

Doctrinele militare analizate, deși nu au fost confirmate de oficiali de la Moscova, au fost promovate de către platforme mass-media ruse – în acest fel, societatea europeană a asociat numele șefului Statului Major General al Federației Ruse, Valeri Gherasimov, cu doctrina fundamentală implementată de stat. În realitate, însă, strategia de destabilizare a instituțiilor euro-atlantice și a societății europene a fost coordonată, în mod direct, de către președintele rus, care, prin intermediul informațiilor vehiculate în mass-media și în discursuri oficiale, a oferit experților și analiștilor militari europeni aparența cunoașterii planurilor statului rus, din perspectiva măsurilor de *soft-power* asociate războiului hibrid.

Pornind de la „Doctrina Gherasimov" din anul 2013, trecând prin „Doctrina Gherasimov 2.0." din anul 2019 și noua doctrină militară din anul 2022, Federația Rusă a adaptat măsurile de tip *soft-power* implementate inițial (dezinformare, propagandă, discursuri cu caracter ideologic și influențare socială), precum și mijloacele utilizate (de la folosirea posturilor de televiziune europene la utilizarea platformelor online mass-media, de la conținuturi direct asociate discursurilor oficiale la posibile „scurgeri de informații" din întâlniri secrete în spațiul public) la realitățiile sociale și geopolitice ale anului 2023, folosind elementul de „haos social" pentru menținerea controlului asupra dimensiunilor afectate de instabilitatea provocată în spațiul euro-atlantic.

BIBLIOGRAFIE

1. ALSMADI Izzat, O'Brien Michael J., "How Many Bots in Russian Troll Tweets?", *Information Processing & Management,* vol. 57, nr. 6, 2020, doi:10.1016/j.ipm.2020.102303.
2. BĒRZIŅŠ Jānis, "The Theory and Practice of New Generation Warfare: The Case of Ukraine and Syria", *The Journal of Slavic Military Studies,* vol. 33, nr. 3, 2020, p. 355–380, doi:10.1080/13518046.2020.1824109.
3. BOCCALETTI S. et al., "The control of chaos: theory and applications", *Physics Reports,* vol. 329, nr. 3, 2000, p. 106-108, doi:10.1016/S0370-1573(99)00096-4.
4. BOGHARDT Thomas, "Soviet Bloc Intelligence and Its AIDS Disinformation Campaign", *Studies in Intelligence,* vol. 53, nr. 4, 2009, p. 1-24, disponibil la https://digitallibrary.tsu.ge/book/2019/september/books/Soviet-Bloc-Intelligence-and-Its-AIDS.pdf.
5. Centrul de monitorizare mass-media, *Știre falsă în presa rusă,* Inforadar, 2023, disponibil la https://inforadar.mapn.ro/42_stire-falsa-in-presa-rusa.
6. CERULUS Laurens, *How Ukraine became a test bed for cyberweaponry,* Politico Research and Analysis Division, 2019, disponibil la https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/.
7. CHALUPA Andrea, "Putin's Fabricated Claim of a Fascist Threat in Ukraine", *Forbes,* 2014, disponibil la https://www.forbes.com/sites/realspin/2014/04/04/putins-fabricated-claim-of-a-fascist-threat-in-ukraine/.
8. COPCEA Ionel, *Propaganda rusă duduie: surse ruseşti vorbesc despre existența unor planuri de introducere a unor contingente de menținere a păcii din Polonia și România în Ucraina de Vest,* Defense Romania, 2023, disponibil la https://m.defenseromania.ro/propaganda-rusa-duduie-surse-rusesti-vorbesc-despre-existenta-unor-planuri-de-introducere-a-unor-contingente-de-mentinere-a-pacii-din-polonia-si-romania-in-ucraina-de-vest_624442.html.
9. ECKEL Mike, *All The Kremlin's Men: Russian Officials Drop Out of Sight, Suggesting Post-Mutiny Purges,* Radio Free Europe Russia, 2023, disponibil la https://www.rferl.org/a/all-the-kremlins-men-russian-officials-drop-out-of-sight-post-mutiny/32484195.html.
10. ECKEL Mike, *, General Armageddon': Who Is The Brutal Russian Commander Charged with Winning the Ukraine War?*, Radio Free Europe Russia, 2022, disponibil la https://www.rferl.org/a/russia-brutal-general-ukraine-war-commander-surovikin/32075971.html.
11. ECKEL Mike, *Russian General Says He Was Fired After Accusing Commanders of Betraying Troops in Ukraine*, Radio Free Europe Russia, 2023, disponibil la https://www.rferl.org/a/russia-general-dismissed-complaints/32501538.html.

12. GERASIMOV Valery, "The Value of Science Is in the Foresight", *Military Review*, 2016, p. 23-29.
13. GERASIMOV Valery, "Vektory razvitiya voyennoy strategii", *Krasnaya Zvezda*, 2019, disponibil la http://redstar.ru/vektory-razvitiya-voennoj-strategii/.
14. GIURCHESCU Ileana, Tony Wesolowsky, *RT: interzis în Uniunea Europeană, concernul rus ar putea reporni din Serbia*, Radio Europa Liberă Moldova, 2022, disponibil la https://moldova.europalibera.org/a/rt-interzis-%C3%AEn-uniunea-european%C4%83-concernul-rus-ar-putea-reporni-din-serbia/31955221.html.
15. GREENBERG Andy, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, Wired, 2018, disponibil la https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.
16. IMEBAL, *А вот и доказательство подъехало, что ОМОН передвигается на машинах скорой помощи,* Joyreactor Russia, 2020, disponibil la https://polit.reactor.cc/post/4462068.
17. IONIȚĂ Crăișor Constantin, Stoenescu Gabriel, „Inteligența Artificială", în *Impactul noilor tehnologii asupra Artei Militare,* (coord. Florin Cîrciumaru), Editura UNAp „Carol I", București, 2021.
18. ISW PRESS, *Russian Offensive Campaign Assessment,* April 30, 2023, Institute for the Study of War, 2023, disponibil la https://understandingwar.org/backgrounder/russian-offensive-campaign-assessment-april-30-2023.
19. JOYAL Paul M., *Russians are masters of disinformation. Don't fall for their lies on social media,* The Miami Herald, disponibil la https://www.miamiherald.com/opinion/op-ed/article246096855.html#storylink=cpy
20. KENNAN George, "The Sources of Soviet Conduct", *Foreign Affairs,* 1947, p. 566-582, disponibil la https://www.foreignaffairs.com/russian-federation/george-kennan-sources-soviet-conduct.
21. KRAMER Andrew, *Russian General Pitches 'Information' Operations as a Form of War,* New York Times, 2019, disponibil la https://www.nytimes.com/2019/03/02/world/europe/russia-hybrid-war-gerasimov.html.
22. LAZĂR Mihnea, *Rușii au pierdut zeci de blindate într-un singur atac la Vuhledar, dar continuă să înainteze. „Dezastrul se repetă din nou și din nou",* Digi 24, 2023, disponibil la https://www.digi24.ro/stiri/externe/rusii-au-pierdut-zeci-de-blindate-intr-un-singur-atac-esuat-la-vuhledar-un-dezastru-e-in-desfasurare-si-se-repeta-din-noi-si-din-nou-2247789.
23. MARJEȚKI Serghei, *Восточная Европа может поучаствовать в разделе послевоенной Украины,* Publicația online Репортёр, 2023, disponibil la https://topcor.ru/31412-kak-vostochnaja-evropa-mozhet-pouchastvovat-v-razdele-poslevoennoj-ukrainy.html.
24. MARZHETSKY Sergey, *What are the three strategic mistakes made by Russia and Ukraine during the NWO,* Publicația Reporter, 2023, https://en.topcor.ru/38972-kakie-tri-strategicheskie-oshibki-sovershili-rossija-i-ukraina-v-hode-svo.html.
25. MARZHETSKY Sergey, *What infrastructure facilities in Russia can become targets of Ukrainian terrorists,* Publicația Reporter, 2023, https://en.topcor.ru/38909-kakie-obekty-infrastruktury-v-rossii-mogut-stat-celjami-ukrainskih-terroristov.html.
26. MORARU Andrei-Cristian, "Putin's Rhetoric of Power: Unveiling The Strategic Language of Regional Dominance", *International Conference RCIC'23 Redefining Community in Intercultural Context,* Brașov, 2023, pp. 112-120, disponibil la https://www.afahc.ro/ro/rcic/2023/RCIC'23/volum_2023/Volume_RCIC'23.PDF.
27. MORAWIECKI Mateusz, Post, Twitter, 27 august 2020, disponibil la https://twitter.com/MorawieckiM/status/1298973502482063360.
28. NBC NEWS, *Full speech: Putin defiant in address to nation after attempted armed rebellion,* 00:00-05:28, 2023, disponibil la https://www.youtube.com/watch?v=uL41UXVWQK0.
29. PRYAKHIN Vladimir, *Почему натовское оружие дало осечку,* Nezavisimaya Gazeta, 2023, https://www.ng.ru/armies/2023-08-21/8_8805_discussion.html.
30. PUTIN Vladimir, *Address by the President of the Russian Federation,* 2014, disponibil la http://en.kremlin.ru/events/president/transcripts/20603.
31. PUTIN Vladimir, *Presidential Address to the Federal Assembly,* 2018, disponibil la http://en.kremlin.ru/events/president/news/56957.
32. REDACȚIA AL JAZEERA, *'Not overthrowing power': Wagner boss Prigozhin defends uprising,* Al Jazeera Media Network, 2023, disponibil la https://www.aljazeera.com/news/2023/6/26/wagner-mercenary-leader-defends-march-on-moscow.
33. REDACȚIA SPUTNIK INTERNATIONAL, *Russia's Geopolitical Rivals Preparing for High-Tech Wars in Space* – Gen Staff, Sputnik International, 2019, disponibil la https://sputniknews.com/military/201903021072893281-russia-hightech-space-wars/.

34. REDACȚIA Смотрим, *Герасимов рассказал, сколько критически важных объектов поражены на Украине,* Publicația online Смотрим, 2022, disponibil la https://smotrim.ru/video/2535425.
35. SĂGEATĂ Radu, *Geopolitică,* Editura Universităţii „Lucian Blaga", Sibiu, 2008.
36. SHIPENKOV Maksim, *Autoritățile germane au interzis televiziunii RT să mai difuzeze în Germania,* Radio Europa Liberă Moldova, 2022, disponibil la https://moldova.europalibera.org/a/autorit%C4%83%C8%9Bile-germane-au-interzis-televiziunii-rt-s%C4%83-mai-difuzeze-%C3%AEn-germania-/31685056.html.
37. SPYKMAN Nicholas J., *The Geography of the Peace,* Editura Archon Books, New York, 1969.
38. THE RUSSIAN DIRECT INVESTMENT FUND, About Sputnik V, disponibil la https://sputnikvaccine.com/about-vaccine/.
39. THE RUSSIAN DIRECT INVESTMENT FUND, RDIF brings together the best Russian and international technologies in the fight against COVID-19, disponibil la https://www.rdif.ru/Eng_COVID-19/.
40. WALKER Shaun, *Belarus protests: Putin ready to send Lukashenko military support,* The Guardian, 2020, disponibil la https://www.theguardian.com/world/2020/aug/27/belarus-protests-putin-ready-to-send-lukashenko-military-support.
41. ZAKREVSKA Sophia, *„Everything is going according to plan": since the beginning of the full-scale war, Putin has changed commanders in Ukraine 17 times,* Obozrevatel Ukraine, 2023, disponibil la https://eng.obozrevatel.com/section-life/news-everything-is-going-according-to-plan-since-the-beginning-of-the-full-scale-war-putin-has-changed-commanders-in-ukraine-17-times-01-05-2023.html.
42. Военный Осведомитель, *Post,* Telegram, 2023, disponibil la https://t.me/milinfolive/103475.
43. Герасимов Валерий, *Ценность науки в предвидении,* VPK News Russia, 2013, disponibil la https://archive.ph/2019.03.05-173836/https://www.vpk-news.ru/articles/14632.
44. Минобороны России, Post, Telegram, 2023, disponibil la https://t.me/mod_russia/23355.

[1] Nicholas J. Spykman, *The Geography of the Peace,* Editura Archon Books, New York, 1969.
[2] Radu Săgeată, *Geopolitică,* Editura Universităţii „Lucian Blaga", Sibiu, 2008.
[3] George Kennan, „The Sources of Soviet Conduct", *Foreign Affairs,* 1947, p. 566-582, disponibil la https://www.foreignaffairs.com/russian-federation/george-kennan-sources-soviet-conduct.
[4] Герасимов Валерий, Ценность науки в предвидении, VPK News Russia, 2013, disponibil la https://archive.ph/2019.03.05-173836/https://www.vpk-news.ru/articles/14632.
[5] Crăișor Constantin Ioniță, Gabriel Stoenescu, „Inteligența Artificială", în *Impactul noilor tehnologii asupra Artei Militare,* coord. Florin Cîrciumaru, Editura UNAp „Carol I", București, 2021.
[6] Valery Gerasimov, „The Value of Science Is in the Foresight", *Military Review,* 2016, p. 23-29.
[7] Jānis Bērziņš, „The Theory and Practice of New Generation Warfare: The Case of Ukraine and Syria", *The Journal of Slavic Military Studies,* vol. 33, nr. 3, 2020, p. 355–380, doi:10.1080/13518046.2020.1824109.
[8] Laurens Cerulus, How Ukraine became a test bed for cyberweaponry, Politico Research And Analysis Division, 2019, disponibil la https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/.
[9] Ibidem.
[10] Andy Greenberg, The Untold Story of NotPetya, the Most Devastating Cyberattack in History, *Wired,* 2018, disponibil la https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.
[11] Vladimir Putin, Presidential Address to the Federal Assembly, 2018, disponibil la http://en.kremlin.ru/events/president/news/56957.
[12] Andrea Chalupa, Putin's Fabricated Claim of a Fascist Threat in Ukraine, *Forbes,* 2014, disponibil la https://www.forbes.com/sites/realspin/2014/04/04/putins-fabricated-claim-of-a-fascist-threat-in-ukraine/.
[13] Valery Gerasimov, „Vektory razvitiya voyennoy strategii", *Krasnaya Zvezda,* 2019, disponibil la http://redstar.ru/vektory-razvitiya-voennoj-strategii/.
[14] Sputnik International, Russia's Geopolitical Rivals Preparing for High-Tech Wars in Space – Gen Staff, Sputnik International, 2019, disponibil la https://sputniknews.com/military/201903021072893281-russia-hightech-space-wars/.
[15] Andrew Kramer, Russian General Pitches 'Information' Operations as a Form of War, *New York Times,* 2019, disponibil la https://www.nytimes.com/2019/03/02/world/europe/russia-hybrid-war-gerasimov.html.
[16] Paul M. Joyal, Russians are masters of disinformation. Don't fall for their lies on social media, *The Miami Herald,* disponibil la https://www.miamiherald.com/opinion/op-ed/article246096855.html#storylink=cpy
[17] The Russian Direct Investment Fund, About Sputnik V, disponibil la https://sputnikvaccine.com/about-vaccine/.
[18] The Russian Direct Investment Fund, RDIF brings together the best Russian and international technologies in the fight against COVID-19, disponibil la https://www.rdif.ru/Eng_COVID-19/.
[19] Thomas Boghardt, „Soviet Bloc Intelligence and Its AIDS Disinformation Campaign", *Studies in Intelligence,* vol. 53, nr. 4, 2009, p. 1-24, disponibil la https://digitallibrary.tsu.ge/book/2019/september/books/Soviet-Bloc-Intelligence-and-Its-AIDS.pdf.

[20] Mateusz Morawiecki, Post, Twitter, 27 august 2020, disponibil la https://twitter.com/MorawieckiM/status/1298973502482063360. Shaun Walker, Belarus protests: Putin ready to send Lukashenko military support, *The Guardian,* 2020, disponibil la https://www.theguardian.com/world/2020/aug/27/belarus-protests-putin-ready-to-send-lukashenko-military-support.

[21] Imebal, А вот и доказательство подъехало, что ОМОН передвигается на машинах скорой помощи, Joyreactor Russia, 2020, disponibil la https://polit.reactor.cc/post/4462068.

[22] Ileana Giurchescu, Tony Wesolowsky, RT: interzis în Uniunea Europeană, concernul rus ar putea reporni din Serbia, Radio Europa Liberă Moldova, 2022, disponibil la https://moldova.europalibera.org/a/rt-interzis-%C3%AEn-uniunea-european%C4%83-concernul-rus-ar-putea-reporni-din-serbia/31955221.html.

[23] Maksim Shipenkov, Autoritățile germane au interzis televiziunii RT să mai difuzeze în Germania, Radio Europa Liberă Moldova, 2022, disponibil la https://moldova.europalibera.org/a/autorit%C4%83%C8%9Bile-germane-au-interzis-televiziunii-rt-s%C4%83-mai-difuzeze-%C3%AEn-germania-/31685056.html.

[24] Izzat Alsmadi, Michael J. O'Brien, „How Many Bots in Russian Troll Tweets?", *Information Processing & Management,* vol. 57, nr. 6, 2020, doi:10.1016/j.ipm.2020.102303.

[25] ISW Press, Russian Offensive Campaign Assessment, April 30, 2023, Institute for the Study of War, 2023, disponibil la https://understandingwar.org/backgrounder/russian-offensive-campaign-assessment-april-30-2023.

[26] Mihnea Lazăr, Rușii au pierdut zeci de blindate într-un singur atac la Vuhledar, dar continuă să înainteze. „Dezastrul se repetă din nou și din nou", Digi 24, 2023, disponibil la https://www.digi24.ro/stiri/externe/rusii-au-pierdut-zeci-de-blindate-intr-un-singur-atac-esuat-la-vuhledar-un-dezastru-e-in-desfasurare-si-se-repeta-din-noi-si-din-nou-2247789.

[27] Mike Eckel, ‚General Armageddon': Who Is The Brutal Russian Commander Charged With Winning The Ukraine War?, Radio Free Europe Russia, 2022, disponibil la https://www.rferl.org/a/russia-brutal-general-ukraine-war-commander-surovikin/32075971.html.

[28] Минобороны России, Post, Telegram, 2023, disponibil la https://t.me/mod_russia/23355.

[29] Mike Eckel, All The Kremlin's Men: Russian Officials Drop Out Of Sight, Suggesting Post-Mutiny Purges, Radio Free Europe Russia, 2023, disponibil la https://www.rferl.org/a/all-the-kremlins-men-russian-officials-drop-out-of-sight-post-mutiny/32484195.html.

[30] Mike Eckel, Russian General Says He Was Fired After Accusing Commanders of Betraying Troops in Ukraine, Radio Free Europe Russia, 2023, disponibil la https://www.rferl.org/a/russia-general-dismissed-complaints/32501538.html.

[31] Военный Осведомитель, Post, Telegram, 2023, disponibil la https://t.me/milinfolive/103475.

[32] Redacția Al Jazeera, 'Not overthrowing power': Wagner boss Prigozhin defends uprising, Al Jazeera Media Network, 2023, disponibil la https://www.aljazeera.com/news/2023/6/26/wagner-mercenary-leader-defends-march-on-moscow.

[33] NBC News, Full speech: Putin defiant in address to nation after attempted armed rebellion, 00:00-05:28, 2023, disponibil la https://www.youtube.com/watch?v=uL41UXVWQK0.

[34] Sophia Zakrevska, „Everything is going according to plan": since the beginning of the full-scale war, Putin has changed commanders in Ukraine 17 times, Obozrevatel Ukraine, 2023, disponibil la https://eng.obozrevatel.com/section-life/news-everything-is-going-according-to-plan-since-the-beginning-of-the-full-scale-war-putin-has-changed-commanders-in-ukraine-17-times-01-05-2023.html.

[35] Vladimir Putin, Address by the President of the Russian Federation, 2014, disponibil la http://en.kremlin.ru/events/president/transcripts/20603.

[36] S. Boccaletti et al., „The control of chaos: theory and applications", *Physics Reports,* vol. 329, nr. 3, 2000, p. 106-108, doi:10.1016/S0370-1573(99)00096-4.

[37] Centrul de Monitorizare Mass-Media, Știre falsă în presa rusă, Inforadar, 2023, disponibil la https://inforadar.mapn.ro/42_stire-falsa-in-presa-rusa.

[38] Redacția Смотрим, Герасимов рассказал, сколько критически важных объектов поражены на Украине, Publicația online Смотрим, 2022, disponibil la https://smotrim.ru/video/2535425.

[39] Serghei Marjețki, Восточная Европа может поучаствовать в разделе послевоенной Украины, Publicația online Репортёр, 2023, disponibil la https://topcor.ru/31412-kak-vostochnaja-evropa-mozhet-pouchastvovat-v-razdele-poslevoennoj-ukrainy.html.

[40] Ionel Copcea, Propaganda rusă duduie: Surse rusești vorbesc despre existența unor planuri de introducere a unor contingente de menținere a păcii din Polonia și România în Ucraina de Vest, Defense Romania, 2023, disponibil la https://m.defenseromania.ro/propaganda-rusa-duduie--surse-rusesti-vorbesc-despre-existenta-unor-planuri-de-introducere-a-unor-contingente-de-mentinere-a-pacii-din-polonia-si-romania-in-ucraina-de-vest_624442.html.

[41] Vladimir Pryakhin, Почему натовское оружие дало осечку, Nezavisimaya Gazeta, 2023, https://www.ng.ru/armies/2023-08-21/8_8805_discussion.html.

[42] Sergey Marzhetsky, What are the three strategic mistakes made by Russia and Ukraine during the NWO, Publicația Reporter, 2023, https://en.topcor.ru/38972-kakie-tri-strategicheskie-oshibki-sovershili-rossija-i-ukraina-v-hode-svo.html.

[43] Sergey Marzhetsky, What infrastructure facilities in Russia can become targets of Ukrainian terrorists, Publicația Reporter, 2023, https://en.topcor.ru/38909-kakie-obekty-infrastruktury-v-rossii-mogut-stat-celjami-ukrainskih-terroristov.html.

[44] Andrei-Cristian Moraru, „Putin's Rhetoric of Power: Unveiling The Strategic Language of Regional Dominance", International Conference RCIC'23 Redefining Community in Intercultural Context, Brașov, 2023, p. 112-120, disponibil la https://www.afahc.ro/ro/rcic/2023/RCIC'23/volum_2023/Volume_RCIC'23.PDF.

MENTALITATEA POPORULUI RUS ÎNTRE TRADIȚIE ȘI EVOLUȚIE

Iulia BORISOV[*]

Abstract

The article is devoted to the issue of the mentality of the Russian people. The concept of "mentality", its structure and its basic components are analyzed. In this approach, the author refers to the works of Russian philosophers on this topic. Approaches to the mentality of the Russian people made by philosophers like V. Klyuchevsky, V. Solovyov, N. Berdyaev, N. Lossky and others are mentioned, emphasizing the inconsistency of the Russian character. Emphasizing the stability of the mentality, the author traces the manifestations of change and its evolution under modern conditions.

Keywords*: mentality; tradition; evolution; culture; archetype; intelligence; collectivism; religiosity; inconsistency.*

Filosofii ruși, reflectând intens asupra soartei Rusiei, a diversității ei, au încercat să determine trăsăturile specifice ale caracterului național rus. Cu mult înainte de apariția termenului de „mentalitate"[1] în filosofia străină, gânditorii ruși și-au concentrat eforturile asupra analizei „sufletului rus", a „sufletului întregului social", înțelegându-l ca pe un complex unicat de trăsături morale și psihologice specifice.

Conceptul de „suflet rus" este foarte important pentru cultura rusă, fapt confirmat de versatilitatea interpretării acestei sintagme: se referă la specificul spiritualității rusești („taina sufletului rusesc"), poate fi interpretat și ca lumea interioară a unei persoane („a-ți pune tot sufletul"), semnifică însuși individul ca element principal constitutiv („sufletul societății"), include și trăsăturile caracterului său („suflet bun"), se poate rezuma, pur și simplu, la fizicalitatea umană („niciun suflet în casă") sau/și începutul său nemuritor („gândește-te la suflet"), exprimă gradul de deschidere al individului („din toată inima"), dar și moartea socio-spirituală a unei persoane („suflete moarte") ș.a.m.d.[2]

În încercările lor de a soluționa chestiunea identității poporului rus, filosofii ruși au folosit conceptele de „suflet rus", „suflet al întregului social", „caracter al poporului rus" ș.a. Toate acestea pot fi utilizate ca sinonime pentru reprezentări ontologice naționale, modele culturale distincte de cele ale altor popoare. Aceste concepte le-au permis filosofilor ruși să exploreze ceea ce astăzi este definit ca mentalitate.

Conceptele de „mental" (ca substantiv) și „mentalitate" sunt relativ recente, dar au intrat complet în circulația științifică și sunt acum utilizate pe scară largă în literatura filosofică, antropologică și culturală. Noțiunile sunt necesare pentru a clarifica starea mentală a diferitelor epoci, a diferitelor popoare, a diferitelor grupuri sociale. Etimologia cuvintelor este latină: *mens* – minte, gândire, mod de a gândi, coerență mentală. Apariția lor a fost un fel de reacție la identificarea conștiinței cu mintea, caracteristică a Iluminismului. De fapt, „mentalul" este ceva obișnuit, care stă la baza conștientului și inconștientului, logicului și emoționalului, o sursă profundă, greu de fixat, de gândire și emoții.

[*] ***Autorul este doctorand al Universității din București.***

Acest concept combină o varietate de sensuri și semnificații asociate cu problema identității naționale și caracteristicile culturii naționale.

Pavel Gurevici[3] propune să distingem conceptul de „mentalitate" nu numai din perspectiva tipului de gândire, ci și din cea a stărilor de spirit manifestate la nivel social, a orientărilor axiologice și a ideologiei. Mentalitatea exprimă ceva mai mult sau mai puțin stabil – obiceiuri, tendințe, emoții colective. Ea se întoarce în profunzimile inconștiente ale psihicului, este greu de exprimat verbal. Natura mentalității este influențată de tradiție, cultură, inconștient, mediul coabitării, în special, de ecosistem. Conceptul de „mentalitate" ne permite să conectăm dialectic abilități analitice de gândire, forme dezvoltate de conștiință cu arhetipurile inconștientului, să descoperim opoziția dintre natural și cultural, emoțional și rațional, individual și colectiv. Este utilizat acest concept ca o caracteristică a unui set relativ holistic de gânduri, credințe, valori, abilități ale conștiinței, care se dezvoltă într-un fel de imagine a lumii, comună pentru oameni.

Cercetător al mentalității popoarelor lumii, Gheorghi Gacev[4] abordează acest concept prin prisma specificului național, care este determinat de sinteza a trei componente: Cosmo – Psiho – Logos: „...lucrarea mea – scrie Gacev – constă în a determina calitățile speciale ale fiecărui popor, substanța lui, caracterul gândirii, psihicului și al talentelor deosebite, pentru că popoarele sunt ca instrumentele muzicale, unul este o vioară, altul este un oboi, al treilea este o orgă ș.a.m.d. Toți sunt muzicieni, dar timbrul este diferit. Iar eu identific și definesc acest timbru."[5] (t.n.)

Mentalul este o caracteristică integrală a oamenilor care trăiesc într-o anumită cultură, cu modul lor special de a percepe lumea, cu propria manieră de gândire, cu o ierarhizare a valorilor ontologice, cu formele lor de comportament cotidian și social.

Mentalul unui popor este constituit din structurile profunde ale conștiinței sale, ce s-au dovedit a fi constante și stabile, unind diferite epoci istorice. Valorile umane de bază, comune tuturor popoarelor din diferite culturi, au varii semnificații și accente, asociate cu mentalitatea acestor popoare. Mentalul colectiv al unei națiuni se manifestă în cultura sa, dându-i o identitate națională.

La originile înțelegerii particularităților sufletului rusesc se află gânditori precum Vladimir Monomah, Nil Sorski, Grigori Skovoroda. O mare contribuție în abordarea specificului mental al poporului rus au avut-o Piotr Ceaadaev, Alexei Homiakov, Vladimir Soloviov, Feodor Dostoievski. De un interes deosebit sunt lucrările gânditorilor de la sfârșitul secolelor XIX-XX, care s-au orientat către analiza aspectelor contradictorii ale caracterului rus, care este o trăsătură specifică a mentalității sale.

Această particularitate a mentalității unui popor este indisolubil legată de factorii geografici, climatici și istorici, de poziția geopolitică. Caracterul național rus s-a format sub influența următorilor parametri:

1. Acceptarea creștinismului ortodox de sorginte bizantină;
2. Stăpânirea tătaro-mongolă, ale cărei urme sunt adânc înrădăcinate în memoria poporului rus;
3. Situarea geografică a Rusiei între civilizațiile din Occident și din Orient, care a devenit baza profundă a dualității sale; stând cu un picior în Europa și cu celălalt în Asia, Rusia a absorbit trăsăturile atât ale civilizației occidentale, cât și ale civilizației orientale.

Totodată, în Rusia au apărut idei și fenomene culturale atât de originale și specifice încât sunt străine de percepția atât a Orientului, cât și a Occidentului, ceea ce a dat naștere la dezbateri aprinse despre „misterul sufletului rus". Într-adevăr, în Rusia s-a format un arhetip cultural special, iar mecanismele profunde ale „inconștientului colectiv" (Karl Jung), deși sunt stabile, nu sunt conștientizate mereu și au devenit aproape imuabile. Drept urmare, aceleași trăsături și caracteristici ale comportamentului rușilor se regăsesc în diferite etape ale istoriei țării. Discreția și chiar catastrofismul din istoria Rusiei și a culturii ei (Rusia Kieveană, Țaratul Moscovit, Rusia sovietică și postsovietică) nu au zdruncinat arhetipul cultural deja cristalizat.

Istoricul Vasili Kliucevski constată contradicția dintre hărnicia și lenea rușilor. Rușii sunt obișnuiți cu efortul excesiv de forță pe termen scurt, să muncească din greu și rapid, ca apoi să se odihnească pentru o iarnă

lungă. Ei consideră că trebuie să se grăbească, să muncească din greu pentru a face multe într-un timp scurt. Niciun alt popor din Europa nu este capabil să muncească atât de mult pentru o perioadă scurtă de timp, dar nicăieri nu există și o asemenea lipsă de (auto)disciplinare cu munca uniformă, moderată, constantă. În poporul rus există „oblomovismul”[6], lenea și pasivitatea. „Oblomovismul” este o boală națională rusă, o trăsătură a caracterului rus. În supunerea față de simțul datoriei, rusul își dezvoltă în sine capacitatea de a lucra conștiincios, dar un aspect al oblomovismului rămâne în el (de exemplu, refuzul de a scrie scrisori).

Ortodoxia le-a influențat puternic rușilor și filosofia de viață a fericirii. Componenta suferinței este de cea mai mare importanță în această filosofie. În toată literatura clasică rusă a secolului al XIX-lea, în special în lucrările lui F.M. Dostoievski, tema suferinței este recurentă. Clasicul consideră că suferința este valoroasă pentru că purifică și înalță un individ. Suferința este pur și simplu necesară pentru a deveni om. După suferință, omul devine mental mai subtil, mai capabil să empatizeze cu ceilalți. Aceeași idee o regăsim și în lucrările filosofului rus Vladimir Soloviov. El scrie despre compasiune ca milă. Mila constă în faptul că o persoană „... simte într-un mod corespunzător suferința sau nevoia altcuiva, adică le răspunde mai mult sau mai puțin dureros, arătându-și astfel, într-o măsură mai mare sau mai mică, solidaritatea cu ceilalți”[7].

În cadrul mentalității ruse este importantă problema dreptului moral de a fi fericit. Nu doar chestiunea fericirii şi a suferinței se află în centrul filosofiei ruse, ci şi toate aspectele conștiinței și comportamentului moral. Unele dintre cele mai importante caracteristici ale mentalității ruse au vizat prevalarea conștiinței morale asupra celei juridice sau politice. Drept urmare, orice act de putere este evaluat de ruși din punctul de vedere al echităţii sale. De asemenea, conceptele economice ale rușilor sunt inseparabile de cele morale.

O mare contribuție la studiul mentalității ruse au avut-o filosofii din secolul al XIX-lea şi începutul secolului al XX-lea. Revenind la această chestiune, N.A. Berdiaev[8] a remarcat tendința spre comunitarism, colectivism, gregaritate, predeterminată tocmai de mentalitatea culturii ruse cu elementele specifice ei: unitarismul viziunii asupra lumii, maximalismul aspirațiilor, escatologismul (tendința de a pune întrebări „ultime”, „extreme” și de a găsi soluții în pragul vieții și al morții, al sfârșitului lumii și la Judecata de Apoi). Berdiaev consideră că o trăsătură invariabilă a caracterului rus este inconsecvența acestuia, antinomia, absența unei căi de mijloc între poli/ între extreme. Acest lucru se manifestă în orice: în atitudinea oamenilor față de putere, față de libertate sau față de cultură. Nikolai Berdiaev scrie cu acurateţe despre antinomiile caracterului rusesc:

1. Rusia este cea mai nestatală, cea mai anarhică țară din lume. Poporul rus este cel mai apolitic popor și pare să dorească nu numai un stat liber, libertate în stat, ci și libertate față de stat. Și coexistă din plin și reversul: Rusia este cea mai statală și cea mai birocratică țară din lume; totul în Rusia devine un instrument al politicii. Poporul rus a creat unul dintre cele mai puternice state din lume și un mare imperiu. Poporului rus aproape că nu i-a mai rămas putere pentru o viață creativă liberă, toată energia i-a fost canalizată spre întărirea și protejarea statului. Puterea birocrației din viața rusă a fost o invazie internă a popoarelor non-ruse. Poporul cel mai puțin statal a creat o statalitate atât de uriașă și puternică, încât și cei mai anarhiști sunt subjugați de birocrație.
2. Atitudinea față de naționalitate. Rusia este cea mai nonșovină țară din lume. Poporul rus nu este deloc caracterizat de naționalism agresiv. În acest sens, Rusia se distinge de orice altă țară din lume. Dar și aici există o antiteză. Rusia este cea mai naționalistă țară din lume, o țară cu o rodomontadă națională fățișă. Reversul smereniei rusești este o extraordinară aroganță rusească. Rusia este „Rusia cea sfântă”. Aceeași antinomie enigmatică poate fi urmărită în orice în Rusia. Este posibil să se stabilească un număr nenumărat de teze și antiteze despre caracterul național rus,

să fie dezvăluite numeroase contradicții ale sufletului rus. Natura umană a rusului, conform observațiilor lui Berdiaev, este foarte polarizată. Pe de o parte, smerenia, pe de altă parte, răzvrătirea; pe de o parte – compasiune, pe de altă parte – cruzime; pe de o parte – dragostea de libertate, pe de altă parte - o tendință spre robie[9]. Așa cum scria Ivan Bunin, „«din noi [rușii, n.a.], ca dintr-un copac, iese şi o bâtă, şi o icoană», în funcție de circumstanțe şi de cine prelucrează acest copac: Serghie din Radonej sau Emelka Pugaciov”[10]. (t.a.)

Celebrul filosof, scriitor şi publicit Ivan Ilin a remarcat, de asemenea, această dualitate, această incoerență atât în viața, cât şi în conştiinţa ruşilor: „Întreaga istorie a Rusiei este o luptă între o înclinaţie centripetă şi creatoare și o alta centrifugă, ce dezintegrează: între statalitatea ce impune sacrificiu şi disciplină și instinctul individualizator anarhic”[11]. Gheorghi Fedotov[12] a asemuit Rusia cu un centaur, referindu-se la bifurcația și inconsecvența sa inerentă.

Nikolai Losski[13], explorând caracterul poporului rus, a avut în vedere ceea ce este intrinsec conștiinței de masă: un singur complex de trăsături specifice, care sunt ferm înrădăcinate în structura poporului și se manifestă recurent de-a lungul istoriei. Studiind mentalitatea poporului rus, autorul este conștient de numeroasele aspecte ale acestei probleme: (1) evidențiază acele caracteristici de bază, care sunt cu adevărat inerente poporului rus și (2) aplică exemplul clasic de etică a virtuții (aretologia, ale cărei baze au fost puse de Aristotel, renaște în gândirea axiologică europeană din a doua jumătate a secolului al XX-lea atât în Occident, cât și în Europa de Est.). Losski, în lucrarea sa „Harakter russkogo naroda”[14], distinge între trăsăturile mentalității o pereche particulară de contrarii – între moral pozitiv și moral negativ. Apare un fel de evantai al virtuților și viciilor, cristalizându-se o imagine completă a caracterului național rus.

Ce trăsături de caracter ale poporului rus evidențiază Nikolai Losski ca fiind principale? În primul rând – religiozitatea, care include şi ateismul militant. Rușii vor să acționeze în numele a ceva absolut. În același timp, dacă au îndoieli cu privire la ideal, sunt capabili să treacă de la o incredibilă frică de Dumnezeu și ascultare la o răzvrătire nestăpânită. O altă pereche semnificativă de contradicţii se regăseşte în înclinaţia ruşilor spre forme extreme de experienţe: ateism, rebeliune. Mai departe: o voinţă înflăcărată dusă la maximum şi, în acelaşi timp, lene (oblomovism) şi pasivitate; libertate a spiritului în căutarea valorilor superioare și o tendință spre anarhie, nihilism (în rândul intelectualității), huliganism (în rândul oamenilor de rând); bunătate primordială și cruzime nestăpânită; o înzestrare genuină cu mentalitate satirică şi o tendință de autopedepsire; mesianism și carență de autodisciplină; lipsa simțului proporției și alternare bruscă de la o extremă la alta. Alături de „perechile antinomice”, Losski punctează și „punctele slabe” ale caracterului rus, care sunt frapante pentru străini: neglijență în muncă, nepăsare, critică și lipsă de acțiune, beție, samavolnicie și toleranță excesivă, predispoziție pentru acţiuni absurde, autodistrugere interioară și o râvnă pentru autoflagelarea nestăpânită.

Gheorghi Gacev[15] și-a dedicat opera sa fundamentală mentalităților popoarelor lumii. Remarcând rolul mare al Puterii, Statului și dezvoltării Rusiei în viața poporului rus, el scrie: „Acesta este stilul nostru, nu se poate face nimic în privința asta. Măcar dacă ar fi respectată măsura (subl. n. I.B.). Dar, cu principiul Măsurii, suntem mereu slabi...”[16]. (t.n.)

Despre caracterul contradictoriu al sufletului rus, despre lipsa unui simț al măsurii scrie şi Dmitri Lihaciov[17] în lucrarea sa „*Reflecții despre Rusia”*: caracterul național al rușilor „... este departe de a fi unit. Încrucișează nu numai trăsături diferite, ci și trăsături într-un «registru unic»: religiozitate cu ateism extrem, dezinteresare cu tezaurizare, caracter practic cu neputință totală în fața circumstanțelor exterioare, ospitalitate cu mizantropie, desconsiderare națională cu șovinism, incapacitate de a lupta cu manifestare bruscă a unei rezistențe magnifice la luptă”.

Lihaciov nu omite să analizeze şi gradul de inteligență al poporului său. În mentalitatea rusă se disting conceptele de „inteligență/deșteptăciune” și „intelect”. Pentru ruși, cuvântul „inteligență” include automat şi o evaluare morală și etică, iar cuvântul „intelectual” coincide semantic cu termenii similari europeni. Pentru ruşi, primul concept are o valoare incontestabilă. Calităţile principale ale unei persoane inteligente sunt modestia, decența, bunăvoința, bunătatea, onestitatea și dorința de a-i ajuta pe ceilalți. În plan

secund sunt situate erudiția, inteligența, educația, dragostea față de lectură. Nu este o coincidență faptul că rușii nu amestecă, ci separă, în toate modurile posibile, concepte precum „intelectual", „inteligență" și „intelect", „intelectualitate". Spiritualitatea, delicatețea, responsabilitatea, calitățile morale înalte caracterizează o persoană inteligentă, care nu trebuie să fie neapărat un intelectual, să aibă o diplomă de studii superioare și să susţină muncă mentală.

Deși mentalitatea este o structură stabilă, ea este supusă evoluției. Astfel, colectivismul este o trăsătură caracteristică arhetipului rus. Această caracteristică a mentalității ruse îşi are rădăcinile încă din vremurile păgâne. Multe proverbe populare reflectă orientarea colectivistă a comportamentului unui rus: „Singur pe câmpul de luptă nu eşti oştean"[18]; „Printre oameni şi moartea este roşie"[19] etc.

Astăzi observăm doar forme exterioare, urme ale trecutului colectivismului instituţionalizat. Sub dominația sovietică, sensul însuși al colectivismului a fost pervertit și, odată cu căderea sa, fiecare rus s-a trezit, în cele din urmă, că este lăsat în voia lui. Rușii se ajută foarte rar între ei în străinătate, nu formează „comunități rusești" așa cum fac alți apatrizi din întreaga lume. Realitatea sovietică nu a influențat în cel mai bun mod trăsăturile caracterului rus. După cum remarca Alexandr Soljenițîn, regimul sovietic a contribuit întotdeauna la ascensiunea și succesul celor mai rele persoane și la distrugerea celor mai bune.

Sunt greu de negat distrugerea și deformarea treptată a arhetipului tradițional rusesc sub influența dualității și a ipocriziei vieții sovietice. Acest lucru a întărit și mai mult inconsecvența inerentă a caracterului rușilor. Într-un singur rus se poate regăsi aproape totul: înclinație pentru naționalism, dar și deschidere către toate culturile; cruzime, dar și o milă ieșită din comun; capacitatea de a provoca suferință, dar și potenţial de a simpatiza profund cu durerea altcuiva; resurse intrinseci de a lucra dezinteresat, dar și pasivitate şi lene.

Schimbarea de mentalitate a oamenilor se manifestă în raport cu religia. Am menţionat anterior că Losski considera religiozitatea cea mai importantă trăsătură a caracterului rus. După perioada sovietică a istoriei Rusiei, dificilă pentru Biserică, originile religiei în Rusia au fost subminate complet.

Credința se transmite mereu prin educaţia din cadrul familiei, iar tradițiile educației religioase s-au pierdut. Astăzi, atitudinea rușilor față de religie și Biserică seamănă mai degrabă cu o modă, în ciuda misticismului lor.

Rușii au o percepție specială asupra timpului. Un rus este mai înclinat să discute despre trecut decât să facă planuri pentru viitor, se uită mai des în urmă decât se uită înainte. Pentru el, atât trecutul său este foarte important, cât și o tipică stare de nostalgie după copilărie, după tinerețe, după locurile în care a trăit. Odată cu prăbușirea Uniunii Sovietice, a apărut şi nostalgia faţă de vremurile sovietice când trăia într-un stat puternic, chiar și nostalgia pentru Rusia țaristă, pentru monarhia care se scufundase în uitare.

Este evident că această atitudine față de trecut este o frână a mișcării către viitor. Trăsăturile mentalității ruse explică dificultățile dezvoltării moderne a Rusiei actuale. Astfel, atitudinea față de bogăție a fost, în mod tradițional, una negativă. Acest lucru este valabil mai ales pentru generația mai în vârstă. Majoritatea consideră că averea personală nu se dobândeşte prin propria muncă, ci, pur și simplu, se însușește din domeniul public. Paremiologia autohtonă reiterează acest aspect: „Din munca celor cinstiţi nu poți face camere de piatră", „Fericirea nu este în bani"[20] etc.

Pe de altă parte, raporturile economice determinate de piața liberală formează noi valori, în special în rândul tinerilor. Din ce în ce mai mult, rușii recunosc că nu este rușinos să fii bogat, banii devin un parametru de evaluare a succesului în viață.

Antinomia mentalității rusești, descoperită de gândirea filosofică rusă, se păstrează şi în prezent, chiar dacă este într-o formă transformată. Studiul mentalității ne permite să afirmăm că se caracterizează prin constanță, stabilitate. Totodată, deşi este un proces dificil şi foarte lent, se schimbă şi evoluează odată cu societatea şi realitatea socială. În opinia noastră, (re)includerea Rusiei în comunitatea mondială şi modernizarea acesteia vor avea succes doar dacă reformarea societății se va realiza ținând cont de mentalitatea poporului rus.

BIBLIOGRAFIE

1. BERDIAEV N. A., *Smîsl tvorcestva,* Moscova, 1989.
2. LOSSKI N. O., „Harakter russkogo naroda", în *Uslovia absoliutnogo dobra*, Moscova, 1991.
3. ILIN I. A. *Naşi zadaci. Istoriceskaia sudba i buduşcee Rossii. Stati 1948 – 1954 godov*, Vol. 2, Moscova, 1992.
4. GACEV G. D., *Mentalnost narodov mira,* Moscova, Eksmo, 2003.
5. LIHACIOV D. S., *Razdumia o Rossii,* Sankt Petersburg, Logos, 2001.
6. OJEGOV S.I., Șvedova, N.I., *Tolkovâi slovar russkogo iazâka.* Ediția a IV-a revăzută și adăugită, Moscova, Azbukovnik, 1997
7. *Mentalnost rossian* (Speţifika soznania bolșih grupp naselenia *Rossii),* Moscova, Image-contact, 1997.
8. SOLOVIOV Vl. *Opravdanie dobra. Soci. v 2-h t,* vol. I, Moscova, 1988.

[1] Există o serie de particularități privind implementarea lingvistică a conceptului de *mentalitate* în sfera noțională a limbii ruse contemporane. Se pune problema cu privire la posibilitatea de a distinge reprezentările lingvistice ale acestui concept sub forma substantivelor *mental* (rus. *менталитет*) și *mentalitate* (rus. *ментальность*) în înțelegerea teoretică și în practica vorbitorilor nativi. Se remarcă faptul că incertitudinea conceptuală, semantică și stilistică în funcționarea cuvintelor *mental* și *mentalitate*, în practica de vorbire a nativilor limbii ruse contemporane, indică lipsa de stăpânire a termenului în conștiința culturală. Lingviștii au constatat că uneori are sens să vorbim despre „gravitarea" cuvântului *mental* la sensul „unei anumite categorii de conștiință" și a celui de mentalitate la sensul „unui mod de realizare a mentalității, un set de anumite proprietăți ale acestei categorii". Acest fenomen este dezbătut în articolul L.I. Jukovskaia, „Mentalitet vs. mentalnost: osobennosti iazâkovoi eksplikaţii konţepta v sovremennoi russkoi reci" [Mental şi mentalitate: particularităţi ale explicaţiei lingvistice a conceptului în limba rusă contemporană] (traducerea noastră), publicat în *Mir nauki, kulturî, obrazovaniia*, Nr. 6 (49), 2014, p. 326-328.

[2] Ojegov S.I., Șvedova N.I., *Tolkovâi slovar russkogo iazâka [Dicționarul explicativ al limbii ruse,* Ediția a IV-a revăzută și adăugită*]* (traducerea noastră), Moscova, Azbukovnik, 1997, p. 183.

[3] Pavel Semionovici Gurevici (1933-2018) - filosof, culturolog și sociolog sovietic și rus, specialist în antropologie filosofică, filosofie occidentală modernă, filosofie culturală, psihologie clinică, psihanaliză, psihologie transpersonală. Psihanalist certificat în practică. Cercetător al religiilor și cultelor netradiționale. Doctor în științe istorice, doctor în filologie, doctor în filosofie, profesor universitar. Membru cu drepturi depline al Academiei Ruse de Științe Naturale.

[4] Gheorghi Dmitrievici Gacev (1929-2008) a fost un filosof sovietic și rus, critic cultural, critic literar și estetician. Doctor în filologie, cercetător principal la Institutul de Studii Slave al Academiei Ruse de Științe, a consacrat conceptul de „dezvoltare accelerată" a literaturii.

[5] Gacev G. D., *Mentalnost narodov mira [Mentalitatea popoarelor lumii]* (traducerea noastră), Moscova, Eksmo, 2003, p. 440.

[6] Inactivitate generată de incapacitatera de a face efort; stare de apatie; spirit de stagnare. • /nm. pr. [erou principal al romanului omonim al lui I. A. Goncearov, devenit simbol al inerţiei şi al pasivităţii) ***Oblomov*** + *-ism,* după rus. *Обломовщина*, v. Eugenia Dima (coord. ştiinţ.), *Dicţionar explicativ ilustrat al limbii române (DEXI)*, Editura Arc/ Gunivas, Chişinău, 2007, p. 1291.

[7] Soloviov V.S., *Opravdanie dobra. Soci. v 2-h t. [Justificarea binelui. Opere în 2 volume]* (traducerea noastră), vol. I, Moscova, 1988, p. 97.

[8] Nikolai Alexandrovici Berdiaev (1874-1948) a fost un filosof, teolog și creștin existențialist rus, care a subliniat semnificația spirituală existențială a libertății umane și a persoanei umane.

[9] N. A. Berdiaev , *Smîsl tvorcestva [Sensul creaţiei]* (traducerea noastră), Moscova, 1989.

[10] Ivan Alekseevici Bunin, *Okaiannîe dni [Zile blestemate]*, http://az.lib.ru/, 27.01.2009, http://az.lib.ru/b/bunin_i_a/text_2262.shtml (data ultimei accesări: 18.10.2023). Autorul rus, laureat al Premiului Nobel, invocă două personalităţi marcante din istoria Rusiei: pe Serghei de Radonej (?-1392, înhumat în 1426), unul din cei mai populari sfinți în Biserica Ortodoxă Rusă, un simbol al smereniei, respectiv pe Emelian Ivanovici Pugaciov (1742- 1775), fost conducător al cazacilor de pe Don, el fiind renumit pentru revolta țărănească dintre anii 1773-1775 şi asociat cu spiritul de revoltă şi răzvrătire împotriva inechităţii.

[11] I. A. Ilin, *Naşi zadaci. Istoriceskaia sudba i buduşcee Rossii. Stati 1948 – 1954 godov [Sarcinile noastre. Soarta istorică şi viitorul Rusiei: articole din perioada 1948 – 1954]* (traducerea noastră), (Vol. 2), Moscova, 1992, p. 245.

[12] Gheorghi Petrovici Fedotov (1886-1951) a fost un filosof religios rus, istoric, eseist, autor al multor cărți despre cultura ortodoxă, considerat de unii ca fondator al „culturologiei teologice" rusești.

[13] Nikolai Onufrievici Losski (1860-1965), cunoscut și sub numele de N.O. Losski, a fost un filosof rus, reprezentant al idealismului rus, epistemologiei intuiționiste, personalismului, libertarianismului, eticii și axiologiei. El a dat sistemului său filosofic numele de intuitiv-personalism.

[14] Caracterul poporului rus (traducerea noastră).

[15] Gacev G. D., *Mentalnost narodov mira [Mentalitatea popoarelor lumii]* (traducerea noastră), Moscova, Eksmo, 2003, p. 364.

[16] Dmitri Sergheevici Lihaciov (1906-1999) a fost un medievalist și lingvist rus, fost deținut în Gulag. În timpul vieții sale, Lihaciov a fost considerat cel mai important savant al limbii și literaturii ruse vechi. El a fost venerat ca „ultimul dintre vechii petersburghezi" și ca „un gardian al culturii naționale".

[17] Lihaciov, D. S., *Razdumia o Rossii [Reflecţii despre Rusia]* (traducerea noastră), Sankt Petersburg, Logos, 2001, p. 47.

[18] În original rus: «Один в поле не воин» („nu poţi face singur o treabă pentru mulţi").

[19] În original rus: «На миру и смерть красна» („nu este înfricoșător să mori printre oameni, este ușor să suporţi totul nefiind singur, ci împreună cu alții").

[20] În original rus: «От трудов праведных не наживешь палат каменных»; «Не в деньгах счастье»/ traducerea noastră în text.

ALTERITATEA NATO/FEDERAȚIA RUSĂ. O PERSPECTIVĂ DIALECTICĂ

Floris-Adrian IONESCU[*]

Abstract

In the backdrop of contemporary political-military crises, this research delves into complex interplay in progress between Hegelian dialectics and the triad of contemporary conflictuality in the dynamic rivalry between NATO and the Russian Federation. Framed within the evolving tapestry of geopolitical tensions, this study undertakes a meticulous examination of the intricate relationship between dialectical elements (thesis, antithesis, synthesis) and conflictual states (symmetry, asymmetry, dissymmetry). It unveils a multifaceted interdependence and a network of causal dynamics between these seemingly disparate theoretical constructs. By drawing upon the foundations of Hegelian dialectics, renowned for its emphasis on contradiction and progressive development, while placing it within the framework of the trichotomy of contemporary conflictuality, this research reveals the seamless integration of philosophical theory with international security concepts. It elucidates how the evolution of specific dialectical elements can exert a discernible influence on the nature and intensity of conflictual states. Simultaneously, it reveals how these conflictual states, in a reciprocal manner, serve as forces guiding and shaping the trajectory of dialectical evolution. This interdisciplinary perspective not only deepens our comprehension of the intricate dynamics, underpinning the NATO-Russia Federation rivalry, but also accentuates the capacity of philosophical theory to enhance the analytical arsenal deployed within the domain of international security studies. By exploring the dialectical undercurrents inherent in contemporary crises, this research provides a profound insight into the deep interconnection between philosophical inquiry and the ever-evolving landscape of international relations.

Keywords: *rivalry; Hegelian dialectics; trichotomy; international security; crises.*

PROLEGOMENE SECURITARE

Stabilitatea strategică a continentului european, în pofida tensiunilor din timpul Războiului Rece, a fost bazată pe două repere importante. În primul rând, Uniunea Sovietică a reprezentat, în mod evident, o amenințare militară substanțială pentru NATO, care a trebuit, în aceeași măsură, să se confrunte cu probabilitatea ca orice război în Europa să poată escalada la stadiul de război nuclear global, caz în care victoria oricărei dintre tabere și-ar fi pierdut importanța ca urmare a efectelor catastrofale[1]. Acest prim aspect a condus la stabilirea unui *gentlemen's agreement* între cele două entități opozante, balanța de putere fiind caracterizată de o precauție excesivă. Un al doilea aspect care a facilitat stabilitatea își avea rădăcinile în omogenitatea Alianței din perioada respectivă (bazată pe valori politice comune, apărare colectivă și angajamentul Statelor Unite ale Americii față de securitatea europeană). Deși Războiul Rece a parcurs numeroase crize, care au adus lumea în pragul unui război cataclismic, chiar și în cele mai fierbinți momente ale sale a existat un interes comun în stabilizarea crizelor și găsirea unei stări de echilibru (riscurile de declanșare a unui război fiind în mod clar și răspicat asumate), asigurându-se un dialog continuu între cele două superputeri pentru a menține acea pace fragilă[2].

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

În ultimii ani, probabilitatea „apariției" unei surprize strategice s-a accentuat periculos, fiind mai mare decât în deceniile anterioare. Se întrevăd provocări pentru stabilitatea strategică în Europa pe fronturi multiple. Cea mai vizibilă, Federația Rusă a respins Occidentul, folosind (în mod deschis și asumat) brutalitatea intervenției militare în Georgia și Ucraina, susținând că Occidentul încearcă să controleze spații din regiuni de interes strategic pentru Moscova. Regimul lui Vladimir Putin protestează, în mod constant, împotriva pătrunderii instituțiilor și valorilor occidentale în fostul spațiu sovietic și consideră acest lucru ca fiind o amenințare directă la adresa intereselor naţionale ale Federației Ruse.[3] Capabilitățile militare și, cu precădere, cele nucleare sunt utilizate (inclusiv într-un mod propagandistic) cu scopul clar de a descuraja și de a ține continentul european în tensiune.

Odată cu creșterea posturii convenționale de luptă, Federația Rusă a dezvoltat și perfecționat, în plan secund, acțiunile non-militare, asimetrice/ hibride, care urmăresc, în principal, slăbirea rezistenței și afectarea rezilienței blocului european al NATO. Această abordare de tip hibrid combină elementele de luptă clasice/convenționale cu instrumente și tehnici pașnice (acțiuni ce țin de războiul informațional, propagandă, sancțiuni economice, acțiuni cibernetice, măsuri în plan diplomatic etc.), care vizează însă un spectru larg de domenii (politică internă/externă a unui stat, diplomație, comunicare strategică, politică economică/financiară).

Rezultatul final are avantajul obținerii unei strategii care utilizează multiple abordări și tactici într-un mod flexibil, adaptate adversarului, reacțiilor sale și schimbărilor de mediu, în vederea creării unei stări de confuzie și ambiguitate la nivelul societății, influențării opiniei publice, slăbirii coeziunii interne, subminării instituțiilor naționale/internaționale ș.a. Un exemplu elocvent în acest sens sunt, pentru Europa, dezbaterile pe teme precum fenomenul migrației sau beneficiile economice ale aderării/ integrării în Uniunea Europeană. Sublinierea și repetarea constantă în spațiul public a problemelor/ dificultăților acestor teme a condus la slăbirea încrederii populației în justețea/ corectitudinea măsurilor adoptate de autorități, în eficiența organizațiilor transnaționale, facilitând reconectarea parţială a unor state la fenomenul naționalist. În pofida faptului că nu este un fenomen resimțit la nivelul majorității populației, efectele la scară redusă, la nivelul individului, sunt de natură să submineze instituțiile și autoritățile în cauză.[4]

Atitudinea Administrației Trump cu privire la angajamentul SUA față de securitatea transatlantică a ridicat îndoieli serioase în rândul aliaților europeni și a plasat durabilitatea angajamentului într-o postură îndoielnică, exacerbând forțele deja centrifuge care contestau coeziunea Alianței. Tocmai în lumina acestor luări de poziție, Administrația Biden a prioritizat întărirea angajamentului american pentru stabilizarea continentului european.

Stabilitatea continentală este din ce în ce mai slăbită prin modalități care ies din sfera clasică a războiului convențional. Accepțiunea generală aliată, fiind și cea mai lesne de metabolizat, este aceea conform căreia Federația Rusă manifestă un expansionism agresiv și probează o formă accelerată de ingerință distructivă în treburile interne ale statelor europene şi din spaţiul post-sovietic, principala preocupare fiind aceea de a provoca Occidentul.[5] Pe cale de consecință (imediată și chiar alarmantă), NATO trebuie să anticipeze și să prevină escaladarea crizei în registrul cinetic al acțiunilor militare, argumentul suprem fiind Articolul 5 al actului fondator al Alianței.[6]

Din această perspectivă, NATO trebuie să anticipeze și să prevină escaladarea crizei în registrul cinetic al acțiunilor militare, argumentul suprem fiind Articolul 5 al actului fondator al Alianței[7]. Pe de altă parte, făcând apel la forța militară ca instrument de intimidare, Federația Rusă amenință interesele de securitate ale NATO și încearcă să impună Occidentului un *statu-quo* redesenat. Aceasta este o formă clară de instabilitate strategică[8].

DIALECTICA RIVALITĂȚII ISTORICE

Relațiile internaționale și, cu precădere, crizele politico-militare, au fost dintotdeauna supuse analizei specialiștilor, stârnind un interes crescut datorită reverberațiilor decelate din interacțiunea actorilor, cea din urmă având consecințe continentale și, deseori, globale.

Demersul de față propune o ipoteză inedită pentru analiza rivalității dintre NATO și Federația Rusă - o abordare interdisciplinară care integrează cadrul filosofic și epistemologic (dialectica hegeliană) cu studiile de securitate (trihotomia conflictualității contemporane). Această interacțiune creează un cadru complex în care evoluția dialectică și stările conflictuale se influențează reciproc, generând o dinamică a rivalității geopolitice care transcende limitele teoretice și are implicații semnificative în arena relațiilor internaționale contemporane.

Primul element al tezei propuse este ancorat în **dialectica hegeliană**[9], teoria filozofică dezvoltată de Georg Wilhelm Friedrich Hegel în secolul al XIX-lea. Perspectiva sa a avut o influență semnificativă asupra gândirii filozofice, politice și sociale, iar în domeniul studiilor de securitate și al relațiilor internaționale a furnizat un cadru conceptual pentru înțelegerea evoluției evenimentelor și a raporturilor de putere. Viziunea dialectică este bazată pe ideea fundamentală a contradicției și dezvoltării. Hegel a susținut că dezvoltarea oricărei entități sau concept are loc prin intermediul unei contradicții inițiale între o *teză* și o *antiteză*. Această contradicție conduce la un proces de confluență și reconciliere, numit *sinteză*. Pe cale de consecință, dialectica hegeliană subliniază ideea că dezvoltarea și progresul sunt rezultatul contradicțiilor și conflictelor, iar aceste conflicte sunt parte integrantă a evoluției.

Un aspect important al dialecticii hegeliene este conceptul de *spirală dialectică*. Acesta din urmă sugerează faptul că toate contradicțiile și conflictele generează nu doar o rezolvare/ rezoluționare, ci deschid cursul de acțiune care facilitează o dezvoltare ulterioară, spre un nivel superior de înțelegere sau de organizare.

Din acest punct de vedere, teza filozofică tranșează continuitatea procesuală de dezvoltare a spiritului uman și progresul societal în dinamica istoriei.

În cazul studiului de față, dialectica hegeliană poate fi aplicată pentru a înțelege evoluția conflictelor și relațiilor dintre state, oferind o perspectivă inedită asupra alterității dintre NATO și Federația Rusă. Conflictul și contradicțiile pot determina schimbări semnificative în sistemul internațional și pot influența direcția în care se îndreaptă securitatea europeană și/sau mondială.

Teoria dialectică a conflictului sinusoidal dintre cei doi mari actori se reflectă și în **trihotomia conflictualității contemporane**, aceasta din urmă fiind decelată în trei stări distinctive: *simetrie*, *asimetrie* și *disimetrie*. Crizele şi conflictele contemporane au un grad de imprevizibilitate şi impredictibilitate din ce în ce mai crescut, acestea evoluând spre integrare (universalitatea conflictului), dar, în acelaşi timp, şi spre fărâmiţare (fiecare sistem/ proces având propria-i conflictualitate). De-a lungul istoriei, conflictul militar a parcurs următoarele faze: războiul antic de invazie, declanşat prin surprindere, cu armate specializate (conflict asimetric, întrucât popoarele nomade de războinici mobili atacau popoarele sedentare, iniţial neînarmate şi nepregătite pentru astfel de confruntări); războiul clasic, caracterizat prin înfruntarea cavalerească, de cele mai multe ori în limitele dreptului păcii şi al războiului, între două armate sensibil proporționate ca instruire, dotare şi strategie (conflict simetric, precum războaiele napoleoniene, Primul şi cel de-al Doilea Război Mondial); războiul modern, cu o mulţime de forme şi expresii, de la cele clasice, în general, simetrice, la cele non-contact, asimetrice și de la cele de sancționare/impunere a unui anumit comportament la cele teroriste.

Accepțiunea cea mai răspândită caracterizează ***simetria*** drept *„proprietatea unui ansamblu spaţial de a fi alcătuit din regularităţi; proporţionalitate, corespondenţă, armonie între părţile unui tot, între elementele unui ansamblu; corespondenţă exactă (ca formă, poziţie, etc.) între părţile (opuse) ale unui tot”*[10]. În domeniul militar, simetria presupune entităţi (forţe, doctrine, strategii şi resurse) asemănătoare sau

compatibile, cu o anumită proporţionalitate a acţiunii şi reacţiei. Simetria (proporţionalitatea) reprezintă deci o corespondenţă (compatibilitate) substanţială între entităţi, considerate sub formă de forţe, tehnologii, doctrine, strategii etc. care, de regulă, se opun unele celorlalte[11]. Alte dicţionare arată că prin simetrie se înţelege o corespondenţă a părţilor opuse în ceea ce priveşte mărimea, forma şi poziţia[12] ori o corespondenţă a poziţiei, formei, măsurii, în raport cu o axă, între elementele unui ansamblu sau între mai multe ansambluri[13].

Dacă dicţionarele generale sunt puse de acord unele cu altele, asigurând (aproximativ) aceeaşi semnificaţie termenului „simetrie", se poate afirma că, pe cale de consecinţă, prin conceptul ***asimetrie*** se înţelege lipsa simetriei în cadrul relaţiei corespondente. Asimetria este o expresie a raporturilor reale existente în natură, în societate şi în relaţiile umane. Ştiinţa modernă studiază prin mijloace specifice raporturile asimetrice, oferind modele şi paradigme din ce în ce mai avansate. Asimetria există şi se manifestă pretutindeni și dintotdeauna. În aceste condiţii, conflictele asimetrice nu sunt altceva decât un mod real de manifestare a asimetriei în beligeranţă, toate conflictele fiind, în esenţă, asimetrice. Asimetria, la fel de veche ca şi războiul, se bazează pe faptul că între adversari au existat diferenţieri care i-au plasat atât pe unii, cât şi pe ceilalţi, în poziţii avantajoase sau dezavantajoase, influenţând deznodământul conflictului. La nivel strategic, aceste diferenţieri generează asimetria strategică[14].

Toate aceste constatări sunt relative. Din ce în ce mai mult, conflictele prezentului şi, mai ales, ale viitorului vor fi asimetrice. Deşi natura creează simetrii, există, chiar şi în mediul înconjurător, numeroase spaţii asimetrice, caracterizate de evoluţii neliniare surprinzătoare, aleatorii. Ştiinţific, conflictul se poate asimila cu asimetria, care reprezintă acţiunea, organizarea şi gândirea (concepţia) diferită de cea a adversarului, în scopul maximizării propriilor efecte, al obţinerii iniţiativei sau câştigării libertăţii de acţiune. Aceasta poate fi asimilată la nivel strategic (politic, politico-militar şi militar), operativ şi tactic sau o combinaţie a acestora[15].

Disimetria (non-simetria) înseamnă, în general, disproporționalitate, incompatibilitate între două forţe care se confruntă sub toate aspectele (mijloace, informaţii, tehnologii, doctrine, strategii). Cu alte cuvinte, disimetria presupune decalaje mari între două forţe care sunt faţă în faţă, care nu pot fi acoperite în niciun fel[16]. Disimetria este specifică perioadei post-*Război Rece 2.0.*[17], constituind disproporţionalitate între două entităţi, efectul de falie generându-se pe fundalul adâncirii uriaşelor decalaje economice, financiare, tehnologice, informaţionale şi, nu în ultimul rând, militare. În completare, disimetria poate fi percepută (iluzoriu) ca un moment tranzitoriu în evoluția conflictelor către asimetrie, prin manifestarea acesteia atunci când una dintre părțile aflate în conflict utilizează un atu sau un avantaj sub o funcționalitate diferită de cea inițial generată sau prevăzută, transformându-l într-un instrument de avantaj strategic. Această adaptare a resurselor sau a capacităților existente poate avea loc sporadic, atrăgând cu sine un dezechilibru temporar în raportul de putere.

Sinergia celor două teorii de bază ale ipotezei enunțate anterior relevă o relație de cauzalitate și interdependență a elementelor constituente. Corespondența dintre cadrul filozofic care se concentrează pe transformarea perpetuă a ideilor/relațiilor și cadrul analitic care explorează natura conflictelor contemporane și tipologia relațiilor conflictuale se dezvoltă analogic. Teza originală este marcată de momentul aprilie 1949 - geneza NATO, însumarea nivelului de ambiție, dar și de tensiunile care urmau să marcheze cele trei paliere ale securității și apărării europene de după cel de-al Doilea Război Mondial: legătura transatlantică, redresarea Germaniei și drumul către Uniunea Europeană, cât și postura adoptată față de dorința expansionistă crescândă a Uniunii Sovietice. La acel moment istoric ne găseam în fața simetriei strategice, întărită ulterior de asumarea Tratatului de prietenie, cooperare și asistență mutuală (Tratatul de la Varșovia) drept răspuns continental răsăritean la teza nord-atlantică. Tensiunea echivalentă s-a extins pe tot parcursul Războiului Rece. Antiteza învederată intervine, în manieră contradictorie, prin tensiunile dintre actori după momentul

demantelării Uniunii Sovietice. Comprimarea sovietică și extinderea paradigmei occidentale au definit o schimbare a raporturilor de putere, o tranziție de la scena bipolară spre uni-polarism cu periferie anarhică[18], având atributul asimetric. Rezoluționarea momentelor/ipostazelor antitetice sintetizează un echilibru fragil, fundamentat (în mod teoretic) pe negociere spre reconciliere.

În prezent, ne aflăm în fața unei relații disimetrice, care definește și mai evident diferențele paradigmatice și modul în care fiecare dintre cei doi mari actori previzionează pacea și/sau războiul. Așadar, memoria imperială la care Federația Rusă face apel pentru compensarea lipsei de putere în valoare absolută, precum și acțiunile sale asertive și beligerante, se juxtapun rezilienței și inspirației statelor membre NATO care oferă sprijin material și doctrinar Ucrainei, simultan cu augmentarea posturii de apărare a flancului estic al Alianței.

REFLECȚII SECURITARE DIN PERSPECTIVA ORGANIZAȚIONALĂ

Amenințările actuale la adresa securității, precum riscurile și vulnerabilitățile cu care se confruntă statele din regiunea euro-atlantică, sunt complexe și adesea dificil de cuantificat sau definit. Acestea includ aspecte precum terorismul, traficul ilegal de droguri, persoane, arme și tehnologii, proliferarea armelor de distrugere în masă, extremismul militant și dezastrele naturale, doar pentru a menționa câteva. O caracteristică comună a acestor amenințări este natura lor transfrontalieră, ceea ce înseamnă că pentru a le gestiona și eradica este necesar un efort internațional coordonat. Această realitate subliniază importanța depășirii paradigmei izolaționiste și necesitatea implicării active a NATO.

Efortul depus de Alianță în direcția menținerii păcii și consolidării securității este întărit prin facilitarea și augmentarea relației transatlantice. Obiectivul este de a dezvolta o relație simbiotică, atât din perspectivă politică, cât și operațională, între partenerii americani și cei europeni. Cu toate acestea, este important de remarcat faptul că dominația doctrinară și financiară a Statelor Unite ale Americii exercită o influență determinantă asupra ritmului și direcției NATO, creând uneori disonanțe în funcționarea sa.

Totuși, prezentul organizațional se află în faza de căutări, în registrul de asumare și împărțire a responsabilităților. Sunt tot mai dese luările de poziție și negocierile pentru multiplicarea contribuției membrilor la efortul global pe trei paliere distincte și, totuși, interdependente – creșterea contribuției financiare (ținta este 2% din PIB pentru fiecare membru în parte)[19]; generarea și asumarea noilor capabilități în consens cu evoluția afacerilor militare; și implicarea crescândă în plan operațional (resurse pentru operații și misiuni).

Ciclicitatea istoriei readuce NATO la obiectivul inițial - temperarea expansionismului rus[20]. Astfel, zona europeană redevine punctul central al efortului operațional, după perioada războiului expediționar din Afganistan. Perceperea generală a Alianţei, la Moscova, drept simbol al înfrângerii blocului sovietic în plan strategic, accentuată de complexul celui înfrânt, a alterat interacțiunea celor două entități. La polul opus, NATO se proclamă alianța militară cea mai prestigioasă din istorie[21], însă evenimente ale istoriei recente au evidențiat anumite puncte sensibile.

Dialogul contradictoriu cu Federația Rusă, dublat de demonstrații de forță, transformate în lovituri violente în proximitatea arealului aliat, se va extinde pe termen lung în termeni de incluziune, excluziune, tolerare, acceptare. În plus, extinderea estică a NATO este întârziată/diminuată de reacția Moscovei, care se simte sufocată și amenințată la rândul ei.

Cel mai periculos scenariu este reprezentat de ostilități violente generale pe axa urii Est-Vest.[22] Temerile sunt legate de victimele din rândul beligeranților, dar, mai ales, cele colaterale. Am putea previziona un succes aliat, NATO având mecanismele și resursele necesare pentru o confruntare clasică, însă aspectele hibride și cele nucleare ar duce conflictul într-o zonă tragică. Ar urma să fim martorii unui dialog al titanilor, cu demonstrații de superioritate alternate, la limita maximă admisibilă.

Un alt aspect îngrijorător este cel al investițiilor în securitate. Prin reducerea, în

perioada post-război Rece, a bugetelor alocate apărării de către fiecare membru în parte s-a diminuat puterea militară conjugată a Alianței. În acest context, creșterea resurselor de apărare sau, măcar, eficientizarea raportului cost-efect ar influența fără echivoc îndeplinirea obiectivelor organizaționale. Evoluția constructivă a NATO trebuie să învedereze corelarea cu Politica de securitate și apărare comună (PSAC) a UE în aspecte de asumare optimă și simultană a sarcinilor de securitate, diviziunea echitabilă a muncii, interoperabilitate și cooperare.

Aducem în discuție un concept interesant, a cărui însemnătate poate crește odată cu derularea istorică - *NATO nelimitat*[23]; acesta descrie capacitatea NATO de a interveni în afara zonei tradiționale pentru prevenirea și managementul crizelor. Fiecare răspuns acțional aliat aduce cu sine transformări în ulterioarele reacții față de situații asemănătoare.

Vârful de lance al NATO va rămâne *apărarea colectivă*, menținerea argumentului fondator conferind stabilitate și autoritate în raporturile externe ale organizației. Desigur, mijloacele de realizare necesită adaptarea permanentă față de amenințările emergente. Suntem foarte curioși ce succede binomului *hibrid - contra-hibrid*... NATO va rămâne, cel mai probabil, garantul securității europene, considerând că este singura formulă continentală pentru dezlegarea dilemei securității, unitatea de efort rămânând o precondiție pentru efectul aliat.

Pe termen mediu și lung, ar putea fi avute în vedere trei abordări strategice pe care le poate adopta NATO, fiecare dintre ele integrând acțiuni politice și militare controlabile (într-o mare măsură), dar numai una dintre acestea va servi cu adevărat ca o abordare echilibrată a stabilității strategice.[24] În primul rând, Alianța s-ar putea ghida spre un scenariu de forță, prin capacitarea capabilităților militare și întărirea posturii de descurajare, în încercarea de a aborda relația de adversitate cu un oponent nuclear, desfășurat operațional la periferia Alianței. Însă, trebuie să luăm în calcul faptul că un astfel de comportament semi-agresiv ar aduce cu sine tulburări politice și economice al căror efecte nu sunt clar previzionate. Alternativ, NATO ar putea readuce în politica sa o „lecție învățată" a istoriei, întărind postura de apărare în paralel cu potențarea dialogului cu Federația Rusă (precum în anul 1967 - Raportul Harmel sau în cazul Tratatului privind forţele nucleare intermediare/ INF, când NATO a apelat la abordarea dual, bazată pe o apărare solidă și pe dialog). Cea de-a treia abordare, cea mai îndrăzneață, ar fi abordarea directă a celei mai proeminente instabilități strategice a Europei și facilitarea unei noi arhitecturi europene de securitate.

Plasarea NATO permanent (în mod aparent) la marginea prăpastiei existențiale este problematică din cel puțin trei rațiuni. Primul argument - narațiunea privitoare la o criză interioară este imprecisă; punctul terminal și disoluția NATO sunt aspecte la fel de irelevante. În al doilea rând, NATO a depășit momente de colaps iminent în dese rânduri, încât este improbabilă și nerealistă teza dispariției (demantelării). În ultimul rând, putem afirma că Alianța are o capacitate nesecată de recuperare sau regenerare. Bineînțeles, simpla supraviețuire nu este suficientă, este relevant cât de departe ființarea se reflectă în adaptarea la noile realități. Certitudinea descrie cel mai bine faptul că NATO este o organizație vie, transformațională și inspirațională, care și-a dezvoltat un sistem de răspuns la crize credibil.

BIBLIOGRAFIE:

1. AUST Tobias, *Modernized deterrence and revitalized dialogue: adapting the Harmel Report to the post-2014 Europe*, Research Paper No.146, NATO Defense College, Roma, mai 2018.
2. BARRIE Douglas, Barry Ben, Beraud-Sudreau Lucie, Boyd Henry, Childs Nick, Giegerich Bastian, *Defending Europe: scenario-based capability requirements for NATO's European members*, International Institute for Strategic Studies, aprilie 2019.
3. BROWNE Matt, Rohac Dalibor and Kenney Carolyn, *Europe's populist challenge: origins, supporters, and responses*, Center for American Progress, 10 mai 2018.

4. CHIFU Iulian, „Rusia în Balcani: ruptură, separatism şi un nou război în Bosnia-Herţegovina”, *Adevărul*, 10 noiembrie 2021.
5. FOERSTER Schuyler, Larsen Jeffrey A., *The need for a new NATO strategy in a more dangerous world,* NATO Defense College, 2021.
6. FOERSTER Schuyler, Larsen Jeffrey A., *Designing a coherent NATO strategy*, NATO Defense College, 2021.
7. FRUNZETI Teodor, Nicolescu Violeta, ”NATO - Back to Roots”, *Strategic Impact*, nr. 78, Editura Universităţii Naţionale de Apărare „Carol I”, București, 2021.
8. KRASTEV Ivan, ”Eastern Europe’s illiberal revolution: the long road to democratic decline”, *Foreign Affairs*, 16 aprilie 2018.
9. KOFMAN Michael, *Drivers of Russian grand strategy*, Frivärld, 2019.
10. MONAGHAN Andrew, *Dealing with the Russians,* Polity Press, Cambridge, UK, 2019.
11. MOTYL Alexander J., ”Putin may want to be an Emperor, but Russia isn’t an imperial power”, *Foreign Policy*, 28 octombrie 2019.
12. *** *Conceptul strategic NATO*, Madrid, 29 iunie 2022.
13. *** *Dicţionarul explicativ al limbii române*, Editura Univers Enciclopedic, Bucureşti, 1998.
14. *** *Hegel’s Dialectics*, Stanford Encyclopedia of Philosophy, 2020.of Philosophy, 2020.

[1] Mantra președintelui american Ronald Reagan – „*războiul nuclear nu poate fi câștigat și nu trebuie dus niciodată” –* a fost fundamentul relației sale (de prietenie) cu liderul Uniunii Sovietice, Mihail Gorbaciov. A se vedea Declarația comună URSS-SUA emisă pe timpul Summit-ului de la Geneva (21 noiembrie 1985). Disponibil la adresa on-line: www.reaganlibrary.gov/research/speeches/112185a.

[2] Schuyler Foerster, Jeffrey A. Larsen, *The need for a new NATO strategy in a more dangerous world,* NATO Defense College, 2021. Disponibil la adresa on-line: https://www.jstor.org/stable/resrep32245.8.

[3] Pentru aprofundarea atitudinii anti-vestice a regimului de la Kremlin, a se vedea Michael Kofman, *Drivers of Russian grand strategy*, Frivärld*,* aprilie 2019. Disponibil la adresa on-line: https://frivarld.se/wp-content/uploads/2019/04/Drivers-of-Russian-Grand-Strategy.pdf.

[4] Despre provocarea populismului la nivelul continentului european, a se vedea: Matt Browne, Dalibor Rohac and Carolyn Kenney, *Europe’s populist challenge: origins, supporters, and responses*, Center for American Progress, 10 mai 2018, disponibil la adresa on-line: https://www.americanprogress.org/article/europes-populist-challenge/; Ivan Krastev, “Eastern Europe’s illiberal revolution: the long road to democratic decline“, *Foreign Affairs,* 16 aprilie 2018, disponibil la adresa on-line: https://www.foreignaffairs.com/articles/hungary/2018-04-16/eastern-europes-illiberal-revolution.

[5] Iulian Chifu, *Rusia în Balcani: ruptură, separatism şi un nou război în Bosnia-Herţegovina*, Adevărul, 10 noiembrie 2021. Disponibil la adresa on-line: https://adevarul.ro/international/europa/rusia-balcani-ruptura-separatism-nou-razboi-bosnia-hertegovina-1_618b60715163ec427160d213/index.html.

[6] ***, *Tratatul Atlanticului de Nord*, Art. 5 – *„Părțile convin că un atac armat împotriva uneia sau mai multora dintre ele, în Europa sau în America de Nord, va fi considerat un atac împotriva tuturor și, în consecință, sunt de acord că, dacă are loc un asemenea atac armat, fiecare dintre ele, în exercitarea dreptului la autoapărare individuală sau colectivă recunoscut prin Articolul 51 din Carta Națiunilor Unite, va sprijini Partea sau Părțile atacate prin efectuarea imediată, individual sau de comun acord cu celelalte Părți a oricărei acțiuni pe care o consideră necesară, inclusiv folosirea forței armate, pentru restabilirea și menținerea securității zonei nord-atlantice. Orice astfel de atac armat și toate măsurile adoptate ca rezultat al acestuia vor trebui raportate imediat Consiliului de Securitate. Aceste măsuri vor înceta după ce Consiliul de Securitate va adopta măsurile necesare pentru restabilirea și menținerea păcii și securității internaționale*”. Disponibil la adresa on-line: http://www.orniss.ro/ro/legislatie/pdf/acorduri/state_nato.pdf. Textul integral al tratatului se regăsește în Anexa 1.

[7] Ibidem

[8] Douglas Barrie, Ben Barry, Lucie Beraud-Sudreau, Henry Boyd, Nick Childs, Bastian Giegerich, *Defending Europe: scenario-based capability requirements for NATO’s European members*, International Institute for Strategic Studies, aprilie 2019. Disponibil la adresa on-line: https://forumostwest.ch/alt/pdf/reports/DefendingEurope.pdf.

[9] Vezi *Hegel's Dialectics*, Stanford Encyclopedia of Philosophy, 2020. Disponibil la adresa on-line: https://plato.stanford.edu/entries/hegel-dialectics/

[10] ***, *Dicţionarul explicativ al limbii române*, Editura Univers Enciclopedic, Bucureşti, 1998, p. 988.

[11] Ion Mitulețu, „Atipic şi asimetric în acţiunile militare moderne", în *Buletinul Universităţii Naţionale de Apărare „Carol I"*, nr. 1/2006, p. 158.

[12] ***, *Webster's New World College Dictionary*, ediţie on-line. Disponibil la adresa on-line: http:/www.webster-dictionary.org/definition/symmetry.

[13] ***, *Larousse. Dictionnaires de français*, ediţie on-line. Disponibil la adresa on-line: http://www.larousse.fr/dictionnaires/francais/symétrie/76062?q=symetrie#75189.

[14] Vasile Paul, „Asimetria strategică", în *Observatorul Militar,* nr. 18/2001, p. 12.

[15] *Ibidem*.

[16] Ion Mitulețu, *Op. cit.*, p. 86.

[17] *Cold war 2.0: how Russia and the West reheated a historic struggle.* Disponibil la adresa on-line: https://www.theguardian.com/world/2016/oct/24/cold-war-20-how-russia-and-the-west-reheated-a-historic-struggle; vezi și Vladimir Kozin, *US-NATO's Cold War 2.0 with Russia. How to Reverse the Tide of Global Warfare?*, Voltaire Network, 2014. Disponibil la adresa on-line: http://www.voltairenet.org/article186250.html.

[18] Iulian Chifu, "Third generation conflicts", în *Millenium III*, nr. 8-9/2002, p.169-189.

[19] *Funding NATO.* Disponibil la adresa on-line: https://www.nato.int/cps/ro/natohq/topics_67655.htm.

[20] Teodor Frunzeti, Violeta Nicolescu, "NATO - Back to Roots", *Strategic Impact*, nr. 78, Editura Universităţii Naţionale de Apărare „Carol I", București, 2021, p. 7-18.

[21] Secretarul General al NATO, Jens Stoltenberg, s-a adresat Congresului SUA, cu ocazia celebrării a 70 de ani de la înființarea organizației; în original: "*So, the NATO alliance is not only the longest lasting alliance in history. It is the most successful alliance in history*." Vezi *NATO: good for Europe and good for America*, disponibil la adresa on-line: https://www.nato.int/cps/en/natohq/opinions _165210.htm?selectedLocale=en.

[22] *This is the simplest explanation of why Putin is so opposed to NATO.* Disponibil la adresa on-line: https://www.businessinsider.com/simplest-explanation-of-why-putin-hates-nato-2015-2.

[23] Floris Ionescu, *Considerations on NATO's response to crises*, Proceedings of the 12th International Scientific Conference *STRATEGII XXI – Strategic changes in security and international relations*, vol. 2, Editura Universităţii Naţionale de Apărare „Carol I", București, 2016, p.171.

[24] Vezi Tobias Aust, *Modernized deterrence and revitalized dialogue: adapting the Harmel Report to the post-2014 Europe*, Research Paper No.146, NATO Defense College, Roma, mai 2018. Disponibil la adresa on-line: https://www.ndc.nato.int/news/news.php?icode=1182; Schuyler Foerster, Jeffrey A. Larsen, *Designing a coherent NATO strategy*, NATO Defense College, 2021. Disponibil la adresa on-line: https://www.jstor.org/stable/resrep32245.9?seq=1#metadata_info_tab_contents.

PROIECTAREA PUTERII STATALE ÎN SPAȚIUL CIBERNETIC

Cornel ARGINT *

Abstract:

Nowadays, the international environment is becoming more and more complex, the states trying to achieve a better place by using all the resources. The cyberspace is one of the most suitable domains where the governmental agencies could act in order to accomplish their strategical objectives. It's clear that the most active states in foreign affairs are in the world top for cyberspace operational capabilities.

Keywords: *international environment; cyberspace; operational capabilities; strategical objectives; state and non-state actors.*

ASPECTE GENERALE

Unul dintre elementele definitorii care au modelat profund societatea contemporană este reprezentat de dezvoltarea exponențială a sistemelor de comunicații și informatice. Această dezvoltare și-a pus amprenta în toate zonele societății – de la aplicații casnice până la domenii tehnologice de vârf, inclusiv în sfera instituțiilor de stat.

Utilizarea acestor sisteme într-o gamă largă de domenii (politic, economic, financiar, militar, sănătate etc.) a condus la eficientizarea activității și la creșterea productivității. Practic, nu putem imagina un domeniu performant fără ca acesta să nu beneficieze de sprijinul tehnologiei digitale.

Totuși, pe lângă avantajele incontestabile aduse de digitalizarea societății, acest proces a venit la pachet cu apariția unor noi vulnerabilități, de neimaginat în trecut. Generarea, transportul și stocarea datelor și informațiilor în spațiul cibernetic a determinat apariția unor grupări ilegale care încearcă să exploateze breșele de securitate cauzate de dezvoltarea necontrolată a domeniului. Obiectivele urmărite sunt diverse, de la obținerea de avantaje financiare până la terorism și spionaj la nivel statal.

În plan geopolitic, acest progres s-a reflectat în apariția unor elemente noi, nemaiîntâlnite anterior: lipsa frontierelor statale, mediu operațional cibernetic de ducere a luptei, apariția unei noi piețe comerciale (piața on-line), creșterea relevanței actorilor privați în defavoarea statelor și apariția unei noi componente a securității naționale – securitatea cibernetică.

În prezent, în condițiile reașezării ordinii mondiale, supremația Statelor Unite este supusă unei uriașe presiuni, inclusiv în spațiul cibernetic, unde un număr tot mai mare de actori statali și non-statali încearcă să ocupe o poziție dominantă în acest nou mediu concurențial.

CONCEPTUL DE PUTERE STATALĂ

În termeni generali, puterea reprezintă un fenomen social fundamental, care constă în capacitatea de a lua decizii și de a asigura îndeplinirea lor prin utilizarea diferitelor mijloace de persuasiune și constrângere.

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

Puterea se exprimă într-o relație asimetrică (conducere–supunere și/sau dominare–subordonare) între factorii la nivelul cărora se manifestă.

În domeniul teoriei geopoliticii, puterea statală se referă la capacitatea de influență a unui stat asupra altor state și actori internaționali și reprezintă o măsură a resurselor, abilităților și poziției strategice ale unui stat în raport cu alții. Puterea statală este determinată de mai mulți factori, cei mai importanți dintre aceștia fiind dimensiunea, populația, resursele naturale, puterea militară, economia, diplomația și influența culturală. Geopolitica tradițională statuează faptul că puterea statală este rezultatul interacțiunii dintre spațiu și putere. Astfel, poziția geografică a unui stat și resursele teritoriale pe care le deține pot influența capacitatea acestuia de a exercita putere și influență asupra altor state. De exemplu, un stat cu o poziție geografică strategică, ca urmare a deținerii unui port maritim important sau un teritoriu situat într-o zonă bogată în resurse naturale, poate avea o putere mai mare în relațiile internaționale.[1]

Puterea statală este adesea analizată și înțeleasă prin prisma mai multor componente, cele mai importante fiind: puterea militară, puterea economică, puterea politică, puterea culturală și puterea geografică. Aceste componente ale puterii statale nu funcționează în mod izolat, ci sunt interconectate și interdependente. Puterea statală reprezintă tocmai rezultatul combinației și interacțiunii acestora într-un mod complex și dinamic.

Proiectarea puterii statale se referă la strategiile și acțiunile prin care un stat își extinde și consolidează influența și puterea la nivel internațional. Este un proces prin care un stat își planifică și implementează politici și acțiuni pentru a-și promova interesele, pentru a-și proteja securitatea și pentru a-și dezvolta și menține sfera de influență. Aceasta implică o evaluare constantă a contextului și o adaptare strategică pentru a-și menține relevanța și influența într-un mediu internațional în continuă schimbare.

Proiectarea puterii statale în geopolitică este un proces complex și dinamic, care implică o evaluare atentă a intereselor și obiectivelor naționale și utilizarea diverselor instrumente și abordări pentru a-și atinge scopurile într-un mediu internațional competitiv. Această proiectare implică o gamă largă de instrumente și abordări, care sunt construite pornind de la componentele puterii statale:[2]

- Puterea militară - dezvoltarea și utilizarea capacităților militare pentru a-și proteja interesele și a influența evenimentele la nivel internațional. Cele mai importante măsuri pentru proiectarea puterii militare sunt: modernizarea forțelor armate, dezvoltarea capacității de proiecție a puterii militare și stabilirea alianțelor și acordurilor de securitate pentru a-și consolida poziția și influența în regiune și în lume.
- Diplomație și relații internaționale - gestionarea și promovarea relațiilor internaționale prin intermediul diplomației și negocierilor. Statele utilizează diplomația pentru a stabili și menține alianțe strategice, a-și promova interesele economice și politice și a-și extinde influența în cadrul organizațiilor internaționale.
- Economie și comerț internațional - o economie puternică și o capacitate comercială semnificativă sunt instrumente importante în proiectarea puterii statale. Statele se angajează în politici economice pentru a-și dezvolta sectoarele-cheie, a atrage investiții străine, a stabili parteneriate comerciale și a-și maximiza influența și avantajele economice în relațiile internaționale.
- Influența culturală - promovarea valorilor, ideilor și culturii proprii. Se referă la abilitatea de a influența și a atrage, în mod voluntar, alte state și actori internaționali prin cultură, modele de succes și valori.
- Controlul asupra resurselor și spațiului geografic - controlul și exploatarea resurselor naturale strategice, precum și controlul asupra teritoriului și spațiului geografic. Statele se angajează în politici și acțiuni pentru a-și extinde sfera de influență și pentru a asigura accesul la resursele naturale esențiale, cum ar fi energie, apă sau materii prime.

Proiectarea puterii statale implică o serie de **strategii și tactici** pe care statul trebuie să le ia și care variază în funcție de contextul specific și obiectivele statului respectiv. Cele mai importante strategii folosite pentru proiectarea puterii statale sunt: identificarea intereselor naționale, dezvoltarea capacităților militare, abilitatea în diplomație și negocieri, adoptarea de politici economice și comerciale sustenabile, utilizarea factorului cultural și asigurarea controlului asupra resurselor și spațiului geografic.[3]

Acest proces începe prin identificarea clară a intereselor naționale și a obiectivelor pe termen lung, incluzând protejarea securității teritoriale, extinderea influenței economice, consolidarea poziției geopolitice în regiune sau asigurarea accesului la resurse naturale. Definirea clară a intereselor permite statului să-și concentreze eforturile și resursele în direcția strategică potrivită. În acest sens, un stat își poate asigura proiectarea intereselor proprii numai dacă stabilește strategii realiste pe termen lung și este consecvent în implementarea acestora.

De exemplu, România a avut succes atunci când și-a setat obiectivul strategic de a adera la organismele euro-atlantice, dar a suferit eșecuri când a fost vorba de modul de exploatare a resurselor subterane din cauza inconsecvenței clasei politice de a urma o anumită strategie.

Puterea militară rămâne un instrument esențial în proiectarea puterii statale. Statul trebuie să dezvolte și să mențină o forță militară modernă, eficientă și capabilă de a proiecta putere în regiune și în lume, în funcție de interesele naționale. Acest lucru implică investiții în tehnologie militară, dezvoltarea capacităților de apărare și atac, precum și stabilirea alianțelor și parteneriatelor strategice pentru consolidarea securității.[4]

Statul trebuie să-și asigure accesul și controlul asupra resurselor naturale esențiale, cum ar fi energie, apă sau materii prime, prin intermediul politicii externe, negocierilor și influenței geopolitice. De asemenea, trebuie să-și protejeze și să-și consolideze teritoriul și frontierele pentru a-și menține securitatea și influența regională[5].

SPAȚIUL CIBERNETIC

Până la mijlocul secolului trecut, mediile de confruntare consacrate erau cel terestru, naval și aerian. Ulterior, inovațiile din domeniul tehnologic au făcut ca cel de-al patrulea mediu operațional să fie reprezentat de spațiul cosmic pentru ca, în prezent, o atenție deosebită să fie acordată mediului (spațiului) cibernetic, recunoscut ca al cincilea mediu operațional.

Spațiul cibernetic este definit ca fiind mediul virtual, generat de infrastructurile cibernetice, incluzând conținutul informațional procesat, stocat sau transmis, precum și acțiunile derulate de utilizatori în acesta. [6] În acest context, prin infrastructuri cibernetice se înțeleg infrastructuri de tehnologia informației și comunicații, constând în sisteme informatice, aplicații aferente, rețele și servicii de comunicații electronice.[7]

Spațiul cibernetic se află la intersecția a patru domenii de bază: fizic, informațional, cognitiv și social[8]. Domeniul fizic este format din partea hardware (cum ar fi cabluri, computere, routere, comutatoare etc.). Un aspect important este faptul că statul deține drepturile legale asupra zonei fizice, iar utilizatorii acesteia trebuie să respecte legile statului în care echipamentele se regăsesc, acesta fiind singurul aspect legislativ major care ar putea avea implicații asupra utilizatorilor. Domeniul cognitiv este partea din spațiul cibernetic care deține un rol special în cadrul procesului decizional și în cadrul căruia sunt dezvoltate concepte, noțiuni, tehnici, proceduri, doctrine, legi etc. Acesta este domeniul în care se realizează conceptualizarea ideilor importante. Considerat ca fiind cea mai importantă parte a spațiului cibernetic, domeniul social este zona în care oamenii interacționează, împărtășesc informații, socializează, reacționează la diverse acțiuni, se întâlnesc virtual și colaborează pe diverse teme de interes, împărtășesc puncte de vedere legate de cultură, credință, valori spirituale etc.[9]

În cele din urmă, domeniul informațional este zona în care informațiile sunt create, manipulate, diseminate, colectate, stocate și transmise între diferiți utilizatori.[10] Putem aprecia în prezent că

cea mai mare parte a informațiilor generate de oameni se află în spațiul cibernetic. Acest lucru conferă avantaje evidente prin posibilitățile multiple de procesare, dar și dezavantaje, având toate informațiile într-un singur loc.

Cele mai importante elemente care caracterizează cel de-al cincilea mediu operațional sunt[11]:

- **Capacitatea de extindere** - spațiul cibernetic este locul în care mii de conexiuni sunt stabilite în fiecare minut în întreaga lume. De exemplu, în cazul domeniului fizic, infrastructura care stă la baza existenței mediului cibernetic este deosebit de complexă, în interconexiune cu alte sisteme sau izolate, implicând o mulțime de procese de instalare, operare, mentenanță etc. Pe de altă parte, în ceea ce privește domeniul informațional, o multitudine de procese (stocare, procesare, analiză, diseminare etc.) au loc în cadrul spațiului cibernetic care, în funcție de nivelul de cunoaștere al utilizatorului, pot constitui acțiuni foarte sofisticate.
- **Viteza** - nivelul crescut de dezvoltare a tehnologiei conexe domeniului cibernetic determină ca procesele și funcțiile din cadrul sistemelor de tehnologie a informației și comunicării să fie efectuate foarte rapid, conducând astfel la o diminuare a timpului necesar pentru îndeplinirea obiectivelor proprii. Cu toate acestea, există și un punct slab: viteza operațiunilor efectuate în spațiul cibernetic este limitată la viteza cu care utilizatorii operează aplicațiile, pe de o parte, și la viteza de procesare a sistemului tehnic, pe de altă parte.
- **Deschiderea** - această particularitate poate fi analizată din două perspective: una negativă și una pozitivă. Spațiul cibernetic este domeniul care facilitează, pentru toți utilizatorii, conectarea, împărtășirea de idei, exprimarea de sentimente, generarea de conținut informațional sau simpla utilizare a acestuia, fiind disponibil pentru orice subiect prin intermediul Internetului. Pe de altă parte, există și o latură negativă a acestei particularități, generată de faptul că există și indivizi sau grupuri cu interese care au, de asemenea, acces nelimitat la spațiul cibernetic și generează acțiuni ce pot reprezenta repercusiuni semnificative pentru ceilalți utilizatori.
- **Perfectibilitate** - spațiul cibernetic este rezultatul efortului și cunoștințelor umane, ambele fiind perfectibile. Toate componentele hardware utilizate în cadrul rețelelor care formează domeniul cibernetic sunt create de mintea umană, putând fi caracterizate astfel de un anumit nivel de imperfecțiune. Mai mult decât atât, și zona de software este rezultată din cunoașterea și efortul uman, astfel încât printre acei octeți ce stau la baza codurilor ce formează programele se pot regăsi nenumărate greșeli ce pot fi exploatate de persoane rău-intenționate.
- **Anonimitatea** - acest atribut poate fi atribuit tuturor utilizatorilor care operează în spațiul cibernetic. Anonimitatea în spațiul cibernetic poate conduce și la comportamente antisociale, prin faptul că generează o stare de dezinhibare a individului cibernetic. Acest fapt se naște ca urmare a procesului de dezindividualizare a persoanei care operează în cadrul acestui mediu, generat de particularitatea de a utiliza resursele din spațiul cibernetic sub protecția anonimatului. În acest sens, *„individul dezindividualizat, ce nu se mai simte unic, reperabil și responsabil, desfășoară comportamente impulsive și necontrolate”*[12].
- **Comunalitatea** - spațiul cibernetic este o resursă comună împărtășită de utilizatori din întreaga lume, ca rezultat al deschiderii. Există o situație specifică, cea a rețelelor private, neconectate cu altele; cu toate acestea, chiar și utilizatorii acestora utilizează în comun mediul cibernetic delimitat de zona de activitate privată, închisă.

Actorii cibernetici sunt persoane fizice cu identitate virtuală complexă care acționează în spațiul cibernetic în scopul îndeplinirii unor obiective personale/organizaționale. În literatura de specialitate au fost identificate o mulțime

de tipologii, dar majoritatea se referă la aceiași actori: statali, non-statali și supra-statali[13].

Există diferite tipuri de grupuri cibernetice. În primul rând, unele dintre acestea amintesc de grupurile hacktiviste pe fondul activităților online puternic legate de motive politice. În al doilea rând, grupurile mai organizate, cu o activitate semnificativă în zona virtuală (care include pirateria, atacurile de tip phishing, DDoS etc.), au un impact mai ridicat asupra securității cibernetice. În al treilea rând, grupările sofisticate utilizează activitatea online pentru a obține resurse financiare, dar combină acțiunile efectuate în sfera cibernetică cu activitatea desfășurată în lumea fizică. În cele din urmă, unele grupări activează mai ales în domeniul real, dar utilizează instrumentele cibernetice pentru a facilita o parte din operațiunile desfășurate în mediul fizic.[14]

Statele și grupurile sprijinite de stat sunt cei mai importanți actori din domeniul cibernetic, deoarece au la dispoziție toate resursele (umane, financiare, politice, tehnologice etc.) necesare pentru a efectua atacuri împotriva țintelor, dar cel mai semnificativ aspect este că dețin un nivel de planificare și coordonare suficient de bine pus la punct în vederea creșterii eficienței acțiunilor. Atacurile grupurilor cibernetice sponsorizate de stat au la bază o gamă largă de instrumente extrem de sofisticate, care pot asigura un nivel sporit de îndeplinire a obiectivelor. În general, grupurile sponsorizate de stat vizează breșele necunoscute anterior de la nivelul de codificare al software-ului, aceste atacuri fiind numite atacuri de tip *zero-days*. Severitatea și complexitatea care caracterizează acțiunile executate de grupurile cibernetice sponsorizate de stat au condus la denumirea acestora drept **amenințări avansate persistente**.[15]

Aceste aspecte au fost evidențiate și în Strategia de Securitate Cibernetică a României, unde principalii actori care generează amenințări în spațiul cibernetic au fost clasificați astfel[16]:

- persoane sau grupări de criminalitate organizată care exploatează vulnerabilitățile spațiului cibernetic în scopul obținerii de avantaje patrimoniale sau nepatrimoniale;
- teroriști sau extremiști care utilizează spațiul cibernetic pentru desfășurarea și coordonarea unor atacuri teroriste, activități de comunicare, propagandă, recrutare și instruire, colectare de fonduri, etc., în scopuri teroriste;
- state sau actori non-statali care inițiază sau derulează operațiuni în spațiul cibernetic, în scopul culegerii de informații din domeniile guvernamental, militar, economic ori al materializării altor amenințări la adresa securității naționale".

În concluzie, spațiul cibernetic dispune de toate elementele necesare pentru a reprezenta o dimensiune a proiectării puterii statale.

UTILIZAREA SPAȚIULUI CIBERNETIC PENTRU PROIECTAREA PUTERII STATALE

Dezvoltarea rapidă a tehnologiilor moderne de informații și comunicații – condiție *sine qua non* a edificării societății informaționale – a avut un impact major asupra ansamblului social, marcând adevărate mutații în filozofia de funcționare a economicului, politicului și culturalului, dar și asupra vieții de zi cu zi a individului. Practic, în prezent, accesul facil la tehnologia informației și comunicațiilor reprezintă una dintre premisele bunei funcționări a societății moderne.

Spațiul cibernetic se caracterizează prin lipsa frontierelor, dinamism și anonimat, generând deopotrivă oportunități de dezvoltare a societății informaționale bazate pe cunoaștere, cât și riscuri la adresa funcționării acesteia (la nivel individual, statal și chiar cu manifestare transfrontalieră). Cu cât o societate este mai informatizată, cu atât este mai vulnerabilă, iar asigurarea securității spațiului cibernetic trebuie să constituie o preocupare majoră a tuturor actorilor implicați, mai ales la nivel instituțional, unde se concentrează responsabilitatea elaborării și aplicării de politici coerente în domeniu.[17]

Printre numeroasele obiective strategice ce pot fi îndeplinite prin întrebuințarea facilităților conexe celui de-al cincilea mediu operațional se regăsește și impunerea politicii statale în funcție de directivele transmise de administrația centrală, indiferent dacă această politică reflectă anumite aspecte societale autohtone sau viziunea de externalizare a voinței/controlului asupra anumitor domenii, zone geografice, grupuri sau indivizi din exteriorul respectivei națiuni.[18]

Există mai multe state care exploatează intens spațiul cibernetic pentru îndeplinirea unor obiective strategice. Aceste state au înțeles pe deplin rolul strategic pe care-l ocupă noul mediu operațional pentru sprijinul intereselor naționale. Fiecare țară încearcă să obțină o poziție cât mai dominantă în spațiul cibernetic, care-i va permite să-și impună regulile proprii în această zonă nouă care, fiind la început, suferă de un vid de reglementare. Principalii actori statali care evoluează în spațiul cibernetic sunt: Statele Unite, China, Rusia, Israel, Marea Britanie, Iran și Coreea de Nord.

Statele Unite ale Americii sunt considerate unul dintre cei mai importanți actori în spațiul cibernetic la nivel global. SUA dețin o puternică capacitate cibernetică, atât în domeniul militar, cât și în cel al informațiilor. În acest sens, au fost adoptate și implementate o serie de politici și legi în domeniul cibernetic, care stabilesc cadrul legal și normativ pentru securitatea cibernetică, având stipulate inclusiv prevederi care permit desfășurarea de operații cibernetice ofensive.

SUA sunt, de asemenea, un centru mondial pentru cercetarea și dezvoltarea în domeniul cibernetic. Cele mai utilizate soluții software sunt dezvoltate în interiorul acestei țări. Universități și companii din SUA sunt la vârful inovației în ceea ce privește tehnologiile și soluțiile cibernetice avansate. Guvernul american, în colaborare cu sectorul privat, sprijină activitatea de cercetare și dezvoltare în domeniul securității cibernetice, promovând inovația și dezvoltarea de tehnologii avansate.

USCYBERCOM este responsabilă atât pentru protejarea rețelelor de comunicații ale Departamentului Apărării, cât și pentru desfășurarea unor operațiuni cibernetice ofensive atunci când este necesar. Această organizație lucrează în strânsă colaborare cu alte agenții de informații și cu industria privată pentru a contracara amenințările cibernetice și a asigura securitatea cibernetică a SUA. Pentru a asigura sinergia activităților, USCYBERCOM se află sub dublă comandă, șeful acestei agenții fiind chiar șeful NSA (National Security Agency), unul dintre cele mai importante servicii de informații.

Aceste aspecte permit SUA să ocupe o poziție de lider în spațiul cibernetic la nivel statal. Capacitățile lor avansate în domeniul IT&C, precum și angajamentul lor în securitatea cibernetică, au impus ca această țară să fie cel mai important actor în mediul digital.[19]

R.P. Chineză este al doilea actor major în spațiul cibernetic la nivel statal. Cu o populație mare și o economie în creștere rapidă, China a dezvoltat o puternică capacitate cibernetică și a investit masiv în domeniul tehnologiilor informaționale și cibernetice.

Guvernul chinez a recunoscut importanța spațiului cibernetic și a stabilit o serie de politici și reguli în domeniul securității cibernetice care să-i permită atât controlul intern al acestui spațiu, cât și proiectarea externă a intereselor naționale. Agenția de Securitate Cibernetică a Chinei (Cyberspace Administration of China) este responsabilă de gestionarea și reglementarea activităților cibernetice în țară, având un rol important în monitorizarea și controlul informațiilor și al accesului populației la Internet.

Una dintre cele mai cunoscute acțiuni ale Chinei în spațiul cibernetic este politica sa de cenzură a Internetului, cunoscută sub numele de „The Great Firewall". Acest sistem de cenzură restricționează accesul la anumite site-uri web și platforme sociale, blocând sau filtrând conținutul considerat inacceptabil sau dăunător pentru regimul politic chinez[20]. În același timp, China a fost acuzată de numeroase țări și organizații internaționale că desfășoară operațiuni cibernetice ofensive, cum ar fi spionajul cibernetic și furtul de proprietate intelectuală. Experții în securitate cibernetică susțin că există grupuri de hackeri chinezi afiliați guvernului care se implică în activități de hacking și spionaj cibernetic în scopul obținerii de informații sensibile sau de avantaje economice.

Pe de altă parte, China a investit și în dezvoltarea de tehnologii și capacități cibernetice avansate. Companii chineze precum Huawei, ZTE și Alibaba au devenit jucători globali în domeniul telecomunicațiilor și al tehnologiei informației. Aceste companii au fost, însă, și în centrul unor controverse legate de securitatea cibernetică, fiind

acuzate de implicare în spionaj sau de încălcarea drepturilor de confidențialitate.[21] Capacitatea Chinei de a opera în spațiul cibernetic, politica sa de cenzură și acțiunile de spionaj cibernetic fac din această țară un actor major în peisajul global al spațiului cibernetic.

F.Rusă este cunoscută pentru utilizarea tacticilor de dezinformare și propagandă cibernetică, prin intermediul cărora încearcă să influențeze opinia publică și să destabilizeze statele și organizațiile din străinătate. Astfel de acțiuni au fost observate în contextul alegerilor și referendumurilor din diferite țări, în special în Statele Unite și în statele membre ale Uniunii Europene.

Rusia a fost implicată și în atacuri cibernetice sofisticate și operațiuni de spionaj cibernetic. Grupuri de hackeri susținuți sau tolerați de guvernul rus, precum Fancy Bear și Cozy Bear, au fost acuzați că au efectuat atacuri cibernetice asupra unor organizații guvernamentale, instituții financiare, companii și infrastructuri critice din alte țări.[22]

De asemenea, Rusia a dezvoltat o capacitate defensivă puternică în domeniul securității cibernetice. Serviciul Federal de Securitate al Rusiei (FSB) și alte agenții guvernamentale au responsabilitatea de a proteja infrastructurile cibernetice ale țării și de a contracara amenințările cibernetice. În plus, Rusia a adoptat o poziție fermă în ceea ce privește controlul și supravegherea Internetului. Guvernul rus a impus reguli stricte privind stocarea datelor și monitorizarea comunicațiilor online, ceea ce a generat îngrijorări cu privire la respectarea drepturilor de confidențialitate și la libertatea de exprimare. Capacitatea sa cibernetică, utilizarea tacticii de dezinformare și propagandă, precum și implicarea în atacuri cibernetice sofisticate, au generat acțiuni cu impact asupra securității cibernetice globale.

Deși este o țară mică din punct de vedere geografic, **Israelul** a recunoscut importanța spațiului cibernetic, fiind considerat, în prezent, un lider în domeniul securității cibernetice. Una dintre principalele caracteristici care a contribuit la succesul Israelului în domeniul cibernetic este accentul pe inovație și tehnologie. Acest stat a investit masiv în cercetare și dezvoltare în domeniul cibernetic, iar rezultatele acestor eforturi se reflectă în numeroasele companii de securitate cibernetică înființate în țară. Companii precum Check Point Software Technologies, CyberArk și Palo Alto Networks sunt recunoscute la nivel mondial pentru soluțiile lor avansate în domeniul securității cibernetice.

Guvernul israelian și-a manifestat, de asemenea, angajamentul față de securitatea cibernetică prin crearea unui ecosistem favorabil în care companiile, academia și guvernul colaborează împreună. Există o strânsă cooperare între sectorul privat și agențiile guvernamentale, precum Agenția pentru Securitate Cibernetică a Israelului (Israel National Cyber Directorate), pentru a identifica amenințările cibernetice și a dezvolta soluții eficiente de protecție.

Israel este cunoscut pentru abilitatea sa de a detecta și contracara atacurile cibernetice. Aceasta se datorează, în mare măsură, programelor de învățare automată și de inteligență artificială dezvoltate de către experții cibernetici israelieni. Statul israelian a creat, de asemenea, unități specializate în cadrul forțelor armate și ale serviciilor de informații, care se concentrează pe operațiuni cibernetice și pe protejarea infrastructurilor critice.[23]

De-a lungul anilor, Israelul a fost supus unor atacuri cibernetice din partea unor actori ostili, cum ar fi grupurile de hackeri susținute de entități precum Iran și Hezbollah. Cu toate acestea, a reușit să-și consolideze apărarea cibernetică și să răspundă cu succes la amenințările cibernetice. Este important de menționat că Israelul este cunoscut pentru politica sa de securitate strictă și pentru protejarea informațiilor sensibile. Guvernul israelian impune reguli și standarde clare privind securitatea cibernetică în diferite sectoare, inclusiv în sectorul militar, energetic și financiar.[24]

Marea Britanie este renumită pentru expertiza sa în domeniul securității cibernetice, iar industria britanică de securitate cibernetică este una dintre cele mai avansate din lume. Există numeroase companii britanice specializate

în securitatea cibernetică, care dezvoltă soluții avansate pentru protejarea infrastructurilor critice, a datelor și a sistemelor informatice. De asemenea, universitățile britanice sunt recunoscute pentru cercetarea lor de înaltă calitate în domeniul securității cibernetice și pentru formarea de specialiști în acest domeniu.

Guvernul britanic acordă o mare importanță securității cibernetice și a recunoscut că amenințările cibernetice reprezintă o problemă majoră pentru securitatea națională și economia țării. Centrul Național de Securitate Cibernetică (NCSC), care face parte din GCHQ, este principala instituție responsabilă de gestionarea și coordonarea politicilor și activităților de securitate cibernetică în Marea Britanie. Agențiile guvernamentale au luat măsuri pentru a se proteja împotriva atacurilor cibernetice și a dezvoltat o serie de inițiative și strategii în acest sens.

O altă zonă în care britanicii excelează este cea a diplomației cibernetice. Marea Britanie cooperează strâns cu partenerii săi internaționali în domeniul securității cibernetice și este activă în cadrul organizațiilor internaționale, precum NATO și Uniunea Europeană, în abordarea amenințărilor cibernetice comune. De asemenea, Marea Britanie are parteneriate de securitate cibernetică cu alte state și organizații din întreaga lume pentru a promova schimbul de informații și bune practici în domeniul securității cibernetice.

Guvernul **Iranului** acordă o mare importanță dezvoltării capacităților în spațiul cibernetic și consideră acest mediu ca fiind un domeniu strategic pentru securitatea națională. Organizația pentru Securitatea Cibernetică a Iranului (Iranian Cyber Security Organization - ICSO) este principala entitate responsabilă de gestionarea politicilor și activităților de securitate cibernetică în țară.

Iranul este cunoscut pentru activitățile sale cibernetice, existând indicii că guvernul iranian are capacități cibernetice avansate și că desfășoară operațiuni cibernetice în interes strategic. Aceste operațiuni includ atacuri cibernetice, spionaj cibernetic, dezinformare și sabotaj cibernetic. Există grupuri de hackeri asociate cu Iranul, precum APT33 (Elfin) și APT34 (OilRig), care sunt implicate în activități cibernetice de amploare. Aceste grupuri au fost implicate în atacuri cibernetice asupra unor ținte din întreaga lume, inclusiv din sectorul energetic, infrastructură critică și sectoare guvernamentale.[25]

Iranul este, de asemenea, cunoscut pentru capacitatea de a utiliza tactici de dezinformare și propagandă cibernetică în scopuri politice și militare. Guvernul iranian a fost acuzat de răspândirea de propagandă și dezinformare, prin intermediul rețelelor de socializare și a altor platforme online, pentru a-și promova agenda și pentru a influența opinia publică internă și internațională. Acest lucru este foarte bine reliefat în cadrul conflictului dintre Israel și Hamas, în cadrul căruia Iranul a sprijinit puternic războiul informațional, reușind să câștige sprijinul lumii arabe.

Mai mult, Iranul a dezvoltat și propriul program de dezvoltare a capacităților cibernetice, inclusiv în domeniul operațiilor cibernetice. Universitățile iraniene și instituțiile de cercetare sunt implicate în activități de cercetare și dezvoltare în domeniul securității cibernetice, iar guvernul sprijină dezvoltarea de competențe și capacități cibernetice avansate prin intermediul programelor de formare și educație.

Coreea de Nord are capacitatea de a desfășura operațiuni cibernetice ofensive, inclusiv atacuri cibernetice și spionaj cibernetic. Grupurile nord-coreene de hackeri, cum ar fi Lazarus Group și Hidden Cobra, sunt considerate a fi implicate în activități cibernetice de amploare la nivel global. Aceste grupuri au fost responsabile de atacuri asupra instituțiilor financiare, companiilor din sectorul energetic, guvernelor străine și altor ținte strategice.

Coreea de Nord este suspectată că desfășoară activități cibernetice cu scopul de a obține resurse financiare, prin intermediul atacurilor asupra platformelor de schimb de criptomonede și a altor scheme frauduloase în mediul virtual. În acest mod, statul nord-coreean încearcă să-și îmbunătățească situația financiară precară în care se află. Guvernul utilizează, de asemenea, capacitățile cibernetice în scopuri de propagandă și dezinformare. Este important de menționat că, din cauza caracterului închis al regimului și a limitărilor în ceea ce privește accesul la informații, este dificil să obținem o imagine completă și exactă a capacităților și activităților cibernetice ale Coreei de Nord[26].

CONCLUZII

Contextul geopolitic actual este dominat de frământări sociale și conflicte locale generate de dorința unor state de a schimba ordinea mondială prin trecerea de la o lume unipolară la una multipolară.

În acest context extrem de complicat, actorii statali implicați încearcă să se folosească de toate instrumentele disponibile pentru atingerea obiectivelor naționale strategice.

În plan internațional, acest lucru se realizează prin utilizarea capabilităților de care dispune un stat pentru proiectarea puterii în scopul influențării altor state.

Spațiul cibernetic reprezintă cel mai nou mediu operațional în care actorii statali acționează pentru a-și proiecta puterea. Dezvoltarea unor capabilități credibile, atât defensive, cât și ofensive, permit statelor să desfășoare acțiuni care să contribuie major la îndeplinirea obiectivelor strategice. Spionajul militar, diplomatic și economic au condus la cunoașterea mai bună a adversarilor și crearea de avantaje competitive. Campaniile de operații cibernetice, în special cele de tip APT, au devenit din ce în ce mai sofisticate și reprezintă amenințări serioase la adresa securității naționale.

În acest context, la nivel statal, a apărut o nouă provocare – aceea de a dezvolta structuri specializate care să asigure un nivel adecvat de securitate cibernetică, dar să și exploateze oportunitățile oferite de noul mediu operațional.

BIBLIOGRAFIE

1. ARGINT Cornel, „Spațiul cibernetic – un nou mediu operațional”, *Infosfera,* nr. 3, 2018, București.
2. BOBRIC George, Cornel Argint, „Spațiul cibernetic - instrument de impunere a politicii statale”, *Infosfera,* nr. 1, 2022, București.
3. CLEMENTE Dave, „Fundamentals of Cyber Security”, în *Verification & Implementation*, 3G Evolution Ltd, Londra, 2015.
4. FRĂSINEANU Dragoș, *Geopolitică,* Ediția a II-a, București, Editura Fundației România de Mâine, 2007.
5. HLIHOR Constantin, *Geopolitica şi geostrategia în analiza relaţiilor internaţionale contemporane*, Bucureşti, Editura Universității Naționale de Apărare, 2005.
6. SIMILEANU Vasile, *Geopolitică şi centre de putere*, Bucureşti, Editura Top Form, 2011.
7. SIMILEANU Vasile, https://www.geopolitic.ro/2023/02/centre-de-putere-axe-si-faliigeopolitice-3/, 10.06.2023.
8. THOMSON Darren, William Altman, Lea Hricikova, *Understanding Criminal Cyber Threat Actors and Motivations*, CyberCube, 2022.
9. ***, Strategia de securitate cibernetică a României 2022-2027, București, 2021.
10. ***, Canadian Centre for Cyber Security, *An introduction to the cyber threat environment,* https://cyber.gc.ca/sites/default/files/cyber/ publications/Intro-ncta-2020_e.pdf, accesat în data de 08.05.2023.
11. Oficiul pentru Transformarea Forței, *The Implementation of Network-Centric Warfare,* Departamentul Apărării al SUA, 2005.

[1] Vasile Simileanu, *Geopolitică şi centre de putere*, Bucureşti, Editura Top Form, 2011, p. 112-114.
[2] Dragoș Frăsineanu, *Geopolitică,* Ediția a II-a, București, Editura Fundației România de Mâine, 2007, p. 156.
[3] Vasile Simileanu, *Op.cit.*, p. 135-138.
[4] Dragoș Frăsineanu, *Op.cit.*
[5] Vasile Simileanu, https://www.geopolitic.ro/2023/02/centre-de-putere-axe-si-falii-geopolitice-3/, 10.06.2023.
[6] ***, *Strategia de securitate cibernetică a României 2022-2027,* București, 2021.
[7] ***, Canadian Centre for Cyber Security, *An introduction to the cyber threat environment,* https://cyber.gc.ca/sites/default/files/cyber/ publications/Intro-ncta-2020_e.pdf, accesat în data de 08.05.2023.
[8] George Bobric, *Amenințări cibernetice din Zona Extinsă a Mării Negre la adresa securității naționale a României, Teză de doctorat,* București, Universitatea Națională de Apărare, 2022, p. 33-35.

[9] Constantin Nilă, Cornel Argint, ”Efectele pandemiei de COVID-19 în spațiul cibernetic”, *Infosfera*, nr.3, 2020, București.
[10] Oficiul pentru Transformarea Forței, *The Implementation of Network-Centric Warfare,* Departamentul Apărării al SUA, 2005, p. 20.
[11] Dave Clemente, ”Fundamentals of cyber security”*,* în *Verification & Implementation*, Editura 3G Evolution Ltd, Londra, 2015, p. 163-176.
[12] Ştefan Boncu, *Psihologie socială*, online: https://www.psih.uaic.ro/wp-content/uploads/cercetare/publicatii/ cursuri/ boncu_s_curs_psih_soc/Curs16.pdf, accesat în data de 01.04.2023.
[13] Darren Thomson, William Altman, Lea Hricikova, *Understanding Criminal Cyber Threat Actors and Motivations*, CyberCube, 2022, p. 13.
[14] Dave Clemente, *Op.cit.*, p.72.
[15] Cornel Argint, „Spațiul cibernetic – un nou mediu operațional”, *Infosfera*, nr. 3, 2018, București.
[16] ***, *Strategia de securitate cibernetică a României 2022-2027,* București, 2021.
[17] George Bobric, Cornel Argint, „Spațiul cibernetic - instrument de impunere a politicii statale”, *Infosfera*, nr.1, 2022, București.
[18] Darren Thomson, William Altman, Lea Hricikova, *Understanding Criminal Cyber Threat Actors and Motivations,* Editura CyberCube, 2022, p.135-136.
[19] Dave Clemente, *Op.cit.*, p.79.
[20] Darren Thomson, William Altman, Lea Hricikova,, *Op.cit.*, p.152.
[21] Dave Clemente, *Op.cit.*, p.110.
[22] Cornel Argint, „Spațiul cibernetic – un nou mediu operațional”, *Infosfera*, nr.3, 2018, București.
[23] Dave Clemente, *Op.cit.*, p.72.
[24] Darren Thomson, William Altman, Lea Hricikova, *Op.cit*., p.135-136.
[25] *Ibidem.*
[26] *Ibidem.,* p. 172.

ARMELE HIPERSONICE, RĂZBOIUL HIBRID ȘI OPERAȚIUNILE INFORMAȚIONALE

*Ștefan-Cristian NUȚU**

Abstract

Current geopolitical context presents a vast way for procedures regarding actions of disinformation and propaganda, as a base component of the hybrid warfare, especially in information warfare spectrum. This paper seeks to present the modes and ways of presenting the information regarding technical themes from the present Russian – Ukrainian war and their effects on the decision makers and population.

Keywords: *war; information; missile; hybrid war; information warfare; threats; international.*

Conflictul militar dintre Federația Rusă și Ucraina a adus în atenția publicului importanța apărării și securității naționale a oricărui stat suveran. De fapt, conflictul dintre cele două state era în desfășurare cu mult înainte, acțiunile desfășurate de ambele state, înainte de începerea operațiunilor militare, intrând în domeniul războiului hibrid.

Caracterul volatil și diversitatea acțiunilor pe care le include „războiul hibrid“ fac ca definirea acestui termen să fie deosebit de dinamică. Putem aprecia că războiul hibrid este caracterizat de *„activități coercitive și subversive, de metode convenționale și neconvenționale, care pot fi utilizate într-un mod coordonat de actorii statali sau non-statali pentru a realiza obiective specifice, rămânând însă sub limita pragului de stare de război declarată oficial “*[1].

Astfel, termenul poate fi înțeles ca o serie de acțiuni cu caracter destabilizator, realizate atât prin mijloace convenționale, cât și neconvenționale, utilizate pentru exploatarea vulnerabilităților identificate. Forma specifică a metodelor utilizate în războiul hibrid depinde de obiectivele și capacitățile actorilor implicați, de contextul politic și strategic și de vulnerabilitățile și oportunitățile specifice. Pentru exemplificare, putem include în sfera războiului hibrid următoarele acțiuni:

- *Agresiune militară*: utilizarea forței militare de către un actor statal/non-statal pentru a-și atinge obiectivele, fie direct, fie prin intermediul forțelor proxy, prin utilizarea de arme convenționale, neconvenționale sau cibernetice.
- *Subversiune politică*: subminarea stabilității politice a unui stat țintă prin operațiuni de dezinformare, propagandă sau alte forme de război psihologic.
- *Coerciție economică*: un actor statal/ non-statal poate folosi măsuri economice pentru a face presiuni asupra unui stat țintă, cum ar fi sancțiuni, restricții comerciale, preluarea controlului în domenii strategice.
- *Atacuri cibernetice*: desfășurarea unor atacuri, campanii, operațiuni cibernetice pentru a perturba infrastructura critică, pentru a exfiltra informații sau pentru a controla anumite domenii de activitate.
- *Criminalitate organizată*: acțiunile grupărilor de criminalitate organizată în sprijinul unor entități statale/non-statale prin derularea de acțiuni destabilizatoare, procurarea de materiale și echipamente prin canale de contrabandă, asigurarea unor fluxuri pentru persoane etc.

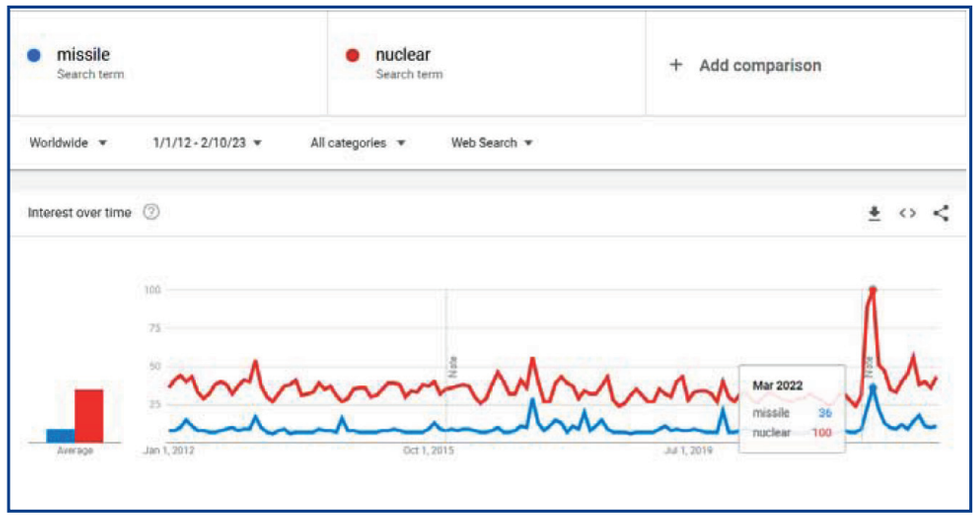
OPERAȚIUNI INFORMAȚIONALE ÎN RĂZBOIUL HIBRID

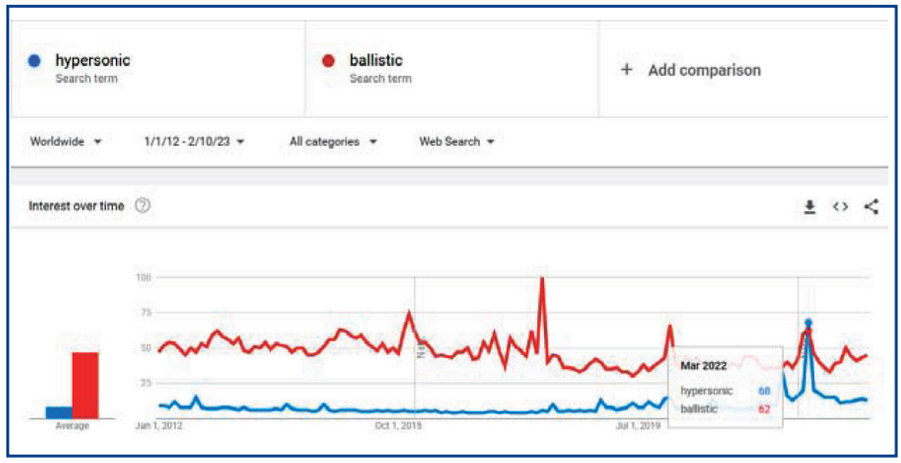
Analiza războiului hibrid are o importanță majoră în înțelegerea conflictelor și a modurilor de acțiune ale forțelor implicate. În această analiză, informațiile reprezintă resursa primară, astfel influențarea acestora poate constitui un avantaj major. Palierul informațional al războiului hibrid reprezintă o unealtă care nu are tangențe doar la nivel militar și politic, ci și în spectrul economic sau social. Orice acțiune de manipulare care poate influența informația finală se încadrează în sfera „*operațiunilor informaționale*", definite ca „*acțiuni de negare, exploatare, corupere sau distrugere a informațiilor inamicului pentru a influența, perturba sau uzurpa luarea deciziilor*"[2]. În afara acestor aspecte, pot exista și alte variante de folosire a informațiilor: prezentarea în momente specifice a anumitor informații; prezentarea unor informații doar în anumite contexte; expunerea unor informații parțiale referitoare la o anumită tematică; expunerea unor informații în contextul prezentării unor alte subiecte, cu care aparent nu au legătură.

Ne vom referi în continuare la ***tema armelor hipersonice***, prezentate în ultimii ani în spațiul public ca fiind capabilități militare moderne ale Federației Ruse, pe care intenționează să le folosească în conflictul cu Ucraina. Vladimir Putin, președintele Federației Ruse, a afirmat, în luna ianuarie a anului 2023, în contextul intrării în serviciu a fregatei „Amiral Gorșkov", faptul că „*acest tip de arme vor proteja F.Rusă de potențialele amenințări externe și vor contribui la asigurarea intereselor naționale ale țării noastre*"[3]. În luna februarie a anului 2023 ministerul rus al apărării a anunțat folosirea pentru prima dată a unei rachete hipersonice de tip Kh-47M2 Kinzhal, care a lovit un depozit al armatei ucrainene.

Referitor la utilizarea de către F.Rusă a armelor hipersonice, președintele Statelor Unite ale Americii, Joe Biden, a marcat faptul că această acțiune este motivată de pierderile masive survenite și că aceste arme nu constituie o diferență majoră privind capabilitățile focoaselor care pot fi utilizate, însă sunt mai greu de combătut datorită vitezei acestora.[4]

Ca urmare a expunerii subiectului în mass-media, s-a înregistrat un interes major al publicului pentru această tematică. În acest sens, putem analiza date oferite de motorul de căutare Google, prin intermediul paginii Google Trends. Această pagină stochează tendințele de căutare ale utilizatorilor, rezultatele fiind posibile accesării și analizării de către orice persoană interesată. Orice set de date furnizate de instrumentul web este obținut în urma selectării unui eșantion, care este considerat suficient pentru înțelegerea miliardelor de căutări zilnice (scalate într-un interval între 0 și 100), bazat pe proporția accesărilor în funcție de toate căutările înregistrate[5]. Pentru identificarea efectelor asupra populației au fost extrase cuvinte cheie în limba engleză, precum „missile" (rachetă), „hypersonic" (hipersonic), „nuclear" (nuclear) și „ballistic" (balistic). Intervalul de timp de luat în considerare este perioada 2012-prezent, raportat la căutările de pe Internet, referitoare la toate categoriile furnizate de Google.





Graficele intereselor rezultate consolidează ideea conform căreia orice acțiune militară duce la nevoia de cunoaștere a populației, pentru identificarea amenințării și posibilității de apărare împotriva acesteia. Se observă faptul că invazia pe scară largă a Forțelor Armate ale Federației Ruse în Ucraina, începând cu februarie 2022, a marcat momentul maximului interes al utilizatorilor de Internet asupra majorității cuvintelor cheie și noțiunilor folosite în discursurile factorilor de decizie la nivel global.

Ulterior lunii februarie 2022, căutările continuă un trend sinusoidal, marcat de nevoia de înțelegere a fenomenului.

ASPECTE TEHNICE PRIVIND ARMELE HIPERSONICE

Termenul „hipersonic" este asociat aparatelor de zbor ce se deplasează cu viteze de cel puțin cinci ori mai mari decât cea a sunetului/la viteze peste Mach 5 (la Mach 1, viteza de deplasare este egală cu viteza sunetului). Zborul hipersonic nu este o noțiune nouă întrucât proiectele din acest domeniu datează încă de la începutul secolului XX. Rachetele hipersonice sunt aduse în proximitatea țintelor de către rachete balistice și/sau rachete de croazieră și pot fi considerate ca treapta finală a vectorilor purtători. Vitezele hipersonice mari sunt obținute doar în proximitatea țintelor, la distanțe de ordinul kilometrilor, prin utilizarea unor motoare de tip scramjet[6] și necesită o lansare la o viteză cel puțin supersonică. Calitatea principală a rachetelor hipersonice este viteza pe care o pot atinge și, implicit, timpii de reacție foarte reduși pentru contracararea lor, care fac practic imposibilă capacitatea de a doborî o astfel de rachetă. O primă observație care se evidențiază este aceea că rachetele hipersonice pot intra și în înzestrarea cu armament a unor avioane de luptă, ceea ce conduce la o diversificare a posibilităților de utilizare și lovire. O a doua observație, colaterală primei, se referă la imposibilitatea combaterii unor astfel de rachete, care ar putea fi echipate cu încărcături nucleare. Consecința este că utilizarea acestor arme poate să inducă posibilitatea folosirii unor încărcături mult mai puternice, fără nici o posibilitate de reacție.

Sursa: Military TV, Youtube, https://www.youtube.com/watch?v=4pbKRgEgkzU&ab_channel=MilitaryTV

Principiile constructive ale motoarelor statoreactoare și/sau pulsoreactoare (motoare fără părți mobile), prin intermediul cărora se pot obține vitezele hipersonice sunt cunoscute de mult timp. Realizarea unor arme hipersonice este însă un proces îndelungat și care necesită multe resurse materiale și experiență tehnologică. Momentul ales însă pentru prezentarea acestor arme, la începutul conflictului, caută să evidențieze de fapt avansul tehnologic pe care și-l asumă Federația Rusă, cu scopul de a induce o stare de nesiguranță părții adverse. Este cert că, față de rachetele clasice, rachetele hipersonice au avantaje evidente, precum viteza, raza operațională crescută și precizie îmbunătățită și, în principal, timpul redus de reacție al inamicului. Utilizarea armelor hipersonice poate fi o modalitate de îmbunătățire a capabilităților militare ale unui stat. Aceste rachete pot fi folosite pentru o varietate de scopuri, inclusiv executarea de lovituri strategice.

Dezvoltarea și utilizarea rachetelor hipersonice ridică îngrijorări cu privire la impactul potențial al acestora asupra securității globale. Vitezele de deplasare și manevrabilitatea armelor hipersonice le fac dificil de detectat și interceptat, afectând capacitatea statelor și aliaților de a se apăra împotriva acestor amenințări. În plus, utilizarea rachetelor hipersonice de către națiunile rivale ar putea escalada tensiunile și ar duce la o cursă a înarmărilor cu implicații pentru stabilitatea întregii comunități internaționale. Înarmarea hipersonică poate fi înțeleasă printr-o analogie cu situația crizei rachetelor cubaneze din anul 1962, eveniment în care fiecare putere implicată (Statele Unite ale Americii și Uniunea Sovietică) căuta poziționarea tehnicii militare proprii cât mai aproape de teritoriul inamic, pentru a constitui o amenințare cât mai credibilă și eficientă. Exemplul actual, în cazul utilizării focoaselor nucleare, se încadrează perfect în tipologia conflictului din trecut, prin simpla schimbare a rachetelor balistice cu rachete hipersonice.

CONCLUZII

Tematica rachetelor hipersonice a fost expusă în discursuri care fac referire la protecția împotriva exploatării vulnerabilităților statului, conex cu protejarea intereselor acestuia, cu o formulare defensivă.

Aceste retorici au la bază acțiuni subversive, care contribuie la inducerea unor sentimente de teamă și nesiguranță, și care caută să destabilizeze percepția opiniei publice și a mediului politico-militar referitor la capacitățile și capabilitățile de apărare în fața noilor tipuri de armament. Cursa în domeniul armelor hipersonice rămâne una importantă pentru marii actori globali datorită noii dimensiuni a războiului pe care acestea o oferă în planul forței militare și în planul percepției avansului tehnologic cu impact social. Realitatea arată faptul că, de cele mai multe ori, evoluția tehnologică a sistemelor de atac sau de apărare are un efect imediat asupra populației și încrederii asupra factorilor de decizie, înainte de a influența situația pe *câmpul de luptă.* Astfel, amenințările hibride constituite de potențiala agresiune militară, prin tehnică inovatoare, alături de subversiunea politico-militară și în contextul unor campanii informaționale complexe, pot reprezenta un model acțional cu efecte imediate în plan social, politic și militar. Operațiunile informaționale (ca parte a războiului hibrid) referitoare la amenințările constituite de vectorii purtători (rachete intercontinentale, balistice sau hipersonice) au efecte imediate asupra populației civile. În context, crearea unei imagini de invincibilitate a rachetelor hipersonice în cadrul unor operațiuni informaționale poate avea efecte destabilizatoare atât asupra populației civile, cât și asupra organismelor militare, care vor fi nevoite să adopte măsuri de contracarare a noilor tipuri de amenințări.

---

[1] https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:52016JC0018, accesat în data de 14.02.2023

[2] Information Operations: Joint Publication 3-13, disponibil la adresa https://irp.fas.org/doddir/dod/jp3_13.pdf, accesat în data de 13.02.2023

[3] https://edition.cnn.com/2023/01/05/europe/russia-warship-hypersonic-missile-deployed-intl-hnk-ml/index.html, accesat în data de 14.02.2023

[4] https://www.businessinsider.com/biden-confirms-russia-used-hypersonic-missile-in-ukraine-2022-3, accesat în data de 14.02.2023

[5] https://support.google.com/trends/answer/4365533?hl=en, accesat în data de 14.02.2023

[6] https://www.nti.org/atomic-pulse/russias-kinzhal-hypersonic-missile-a-game-changing-weapon-or-a-distraction/, accesat în data de 13.02.2023

CRIPTOGRAFIA,ELEMENT ESENȚIAL ÎN ACTIVITATEA COTIDIANĂ

*Alexandru TATU**

Abstract:

The use of the internet as well as the exponential increase in the volume of information managed in the electronic environment led to the development and improvement of security measures. Cryptography is an essential tool for protecting the infrastructure specific to the IT&C field by preventing unauthorized acces. The use of cryptography is not limited only to the military field, today it is also used in everyday life, in various fields of activity.

Keywords: *cryptography; network security; encryption; decryption.*

DELIMITĂRI CONCEPTUALE

Societatea umană cunoaște profunde transformări ca urmare a apariției și dezvoltării noilor tehnologii specifice domeniului IT&C, care se regăsesc în majoritatea domeniilor activității cotidiene, influențând semnificativ dezvoltările criptografiei în domeniile educațional, medical, financiar-bancar, militar etc.

Criptologia, înțeleasă și acceptată ca o știință a scrierilor secrete, are o vechime de câteva mii de ani. Aceasta s-a dezvoltat și perfecționat odată cu matematica și, mai nou, prin intermediul tehnologiilor IT&C, cunoscând realizări exponențiale în ultima perioadă.

Primele texte *cifrate* descoperite, până în prezent, au o vechime de aproximativ 4.000 de ani și provin din Egiptul antic. În Grecia antică textele cifrate erau utilizate încă din secolul al V-lea î.e.n., iar în Roma antică protejarea informațiilor specifice domeniilor politic și militar se realiza utilizând scrierile secrete.

Criptologia a evoluat în mod diferit în funcție de gradul de dezvoltare economică a formațiunilor statale, în diferite momente ale istoriei. Printre cele mai cunoscute sisteme criptografice/ algoritmi utilizați amintim: cifrul lui Cezar; discul Alberti; multicilindrul Jefferson (discul lui Jefferson); cifrul Vigenere; mașina de criptare ENIGMA (utilizată în Al Doilea Război Mondial de către forțele armate ale Germaniei);

Fig. 1 - Enigma[1]

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

algoritmul de criptate **DES** (data encryption standard - standard de criptare a datelor); algoritmul criptografic **RSA** (Rivest-Shamir-Adleman - folosit în domeniul semnăturilor publice) și, nu în ultimul rând, **AES** (standard de criptare avansată - advanced encryption standard). În *criptografia* modernă vorbim de criptare pe curbe eliptice, folosită în mai multe domenii de activitate unde există nevoia de a transmite rapid date (ex: armata, serviciile financiar-bancare etc).

Principalele discipline responsabile de dezvoltarea criptografiei sunt matematica, informatica, fizica etc. Evoluția tehnicii de calcul (a infrastructurii IT&C), a algoritmilor și a metodelelor de criptare a impus creșterea rezistenței criptografice a echipamentelor utilizate pentru protecția informațiilor. În același timp, necesitatea sporirii securității informațiilor a determinat direct dezvoltarea criptografiei. Aplicațiile software, dispozitivele electronice realizate și utilizate în scop comercial privat, folosite pentru criptarea informațiilor, au devenit accesibile unei largi categorii de utilizatori, fapt ce a constituit atât un avantaj, cât și un dezavantaj, ajungându-se astfel în situația ca oricine să poată afecta/ influența viața privată a cetățenilor și chiar securitatea unui stat prin perturbarea infrastructurilor critice ale acestuia. Accesibilitatea informațiilor specifice domeniului criptografic sau a celor legate de funcționarea echipamentelor criptografice utilizate în infrastructuri critice poate aduce prejudicii deosebit de grave securității naționale.

Criptografia este o știință care a devenit o parte esențială a activității cotidiene, iar în lipsa sa, viața, așa cum o cunoaștem astăzi, ar fi extrem de diferită. Astfel, criptografia cuprinde activități specifice de cifrare/criptare, respectiv de decifrare/decriptare a unui fișier clar/criptat și este o componentă a unui domeniu mult mai larg, intitulat securitatea informației (information assurance).

Criptografia clasică este cea care se folosea înainte de apariția calculatorului. În *criptografia clasică*[2] algoritmii constau în caractere alfanumerice și într-o serie de transformări elementare (substituții, transpoziții) ale caracterelor textului în clar. Unii algoritmi foloseau aceste transformări în mod repetat, îmbunătățind în acest fel securitatea algoritmului de criptare. Pe de altă parte, în *criptografia modernă,* bazată pe tehnologiile IT&C, lucrurile au evoluat foarte mult, dar multe din principiile clasice au rămas valabile.

Criptologia reprezintă ansamblul conceptelor şi activităţilor specifice referitoare la criptarea informațiilor și la analiza criptografică (criptanaliză). Aceasta descrie și utilizează fundamente matematice pentru definirea și proiectarea metodelor criptografice, precum și principii de autentificare și restricționare a accesului la informații.

Criptanaliza[3] reprezintă ansamblul de activităţi care au ca scop obţinerea fișierelor clare din cadrul fișierelor criptate interceptate, fără a se cunoaşte integral sau chiar deloc cheia criptografică sau algoritmul criptografic utilizat. Criptanaliza reprezintă partea „ofensivă” a criptologiei, adică arta de a sparge sistemele de criptare utilizate de către adversar/inamic. Poate fi utilizată și în scop defensiv, ca ramură a criptologiei.

Un atac criptografic asupra unui echipament de criptare reprezintă o metodă utilizată cu scopul de a obține informațiile în clar din textul /fișierul criptat fără a avea acces la cheile de criptare sau la algoritmul criptografic utilizat. Succesul unui atac criptografic depinde de mai mulți factori: vulnerabilitatea sistemului utilizat; absența măsurilor de protecție specifice; neinstruirea personalului care utilizează sistemele criptografice.

Steganografia[4] este știința scrierilor secrete și reprezintă tehnica ascunderii/mascării informațiilor sensibile în alte mesaje, în așa fel încât existența acestora să nu poată fi sesizată. Pentru aceasta se pot utiliza anumite fișiere de tip audio sau video. De asemenea, există soft-uri care pot analiza fișierele gestionate în format electronic pentru a descoperi anumite informații criptate inserate în cadrul acestora.

Principalele funcții[5] asigurate de criptografie sunt:

- confidențialitatea;
- integritatea;
- disponibilitatea.

Confidențialitatea[6] reprezintă faptul că doar personalul autorizat poate avea acces la informații sensibile. Această funcție previne accesul la conținutul real al mesajului din partea entităților neautorizate prin criptarea informațiilor de către emitenți.

Integritatea datelor reprezintă proprietatea de a proteja orice modificare (inserare, ștergere, substituție) neautorizată a informației și garantează că informațiile transmise nu au fost alterate pe parcursul transmiterii.

Pentru a proteja informațiile se folosesc funcții matematice, specifice criptografiei, de tip Hash, precum și criptarea datelor.

Disponibilitatea informațiilor se referă la faptul că prin utilizarea serviciilor/funcțiilor specifice criptografiei, informațiile sunt accesibile utilizatorilor în orice moment și în condiții de securitate conform principiului necesității de a cunoaște.

Celelalte funcții specifice domeniului securității informațiilor sunt derivate din acestea.

TEHNOLOGII SPECIFICE CRIPTOGRAFIEI

Criptografia a devenit în ultimii ani o componentă esențială în protecția infrastructurilor critice la nivel național, guvernamental și militar, precum și bază a securității informațiilor gestionate în format electronic, în cadrul infrastructurilor specifice domeniului IT&C.

În context, criptografia a devenit o resursă critică deoarece există permanent necesitatea de a proteja informații sensibile, cantități mari de date.

Activitatea cotidiană este influențată în mod direct de tehnologiile specifice criptografiei.

Criptografia[9] implică conversia, cu ajutorul unui algoritm, a unui fișier de orice natură (audio, video, text, imagine, baze de date, etc.) într-un fișier criptat, procesul de conversie purtând denumirea de criptare (procesul invers de conversie a fișierului cifrat/criptat în fișier clar poartă denumirea de decriptare).

Principalele infrastructuri specifice[10] domeniului criptografic sunt: cheile criptografice, algoritmii criptografici, certificatele digitale, aplicațiile criptografice, instrumentele de autentificare, rețelele criptografice, librăriile criptografice, protocoalele și standardele criptografice etc.

Cheile criptografice[11] (de criptare) sunt folosite în combinație cu anumiți algoritmi criptografici pentru a proteja informații sensibile gestionate în cadrul infrastructurilor IT&C. Acestea reprezintă cele mai importante componente ale tehnologiilor specifice domeniului criptografic și pot fi o înșiruire de biți, numere etc.

Protocoalele criptografice cuprind un set de reguli utilizate între mai mulți indivizi sau organizații prin care se realizează operații

Fig. 2 – Tehnologii specifice criptografiei[7]

Criptografia[8] este, în prezent, un instrument indispensabil pentru securizarea sistemelor informatice utilizate în diferite domenii de activitate. Informațiile gestionate în format electronic în cadrul organizațiilor de orice tip, inclusiv cele militare, sunt protejate cu echipamente/dispozitive specifice domeniului criptografiei.

specifice privind autentificarea mesajelor, verificarea cheilor, transferul mesajelor sau cheilor. Acestea sunt utilizate pentru a asigura protecția criptografică a serviciilor din Internet. Printre cele mai importante sunt: **Ipsec** (Internet protocol security - protocol de securitate utilizat în Internet), **DNSSEC** (domain name server security protocol - protocol pentru servicii

de numire distribuite); **SSL** (secure sochet layer - protocol pentru conexiuni prin Internet securizate); **SHTTP** (secure hypertext transfer protocol - protocol de criptare pentru Internet mai modern decât SSL); **PKCS** (public key cryptography standards – grup de standarde de criptare cu chei publice); **TLS** (transport layer security – protocoale folosite pentru Internet pentru a oferi comunicații securizate) etc.

Certificatul digital este un document electronic folosit pentru a dovedi validitatea unei chei publice. *Certificatele digitale* oferă titularilor acestora identitate virtuală. Prin intermediul acestora, titularul poate crea ***semnături electronice (digitale)*** care sunt recunoscute în justiție, în conformitate cu legislația națională, și poate marca temporar un document electronic.

Algoritmii criptografici cuprind o serie de transformări prin care informațiile necesar a fi protejate sunt convertite (transformate) astfel încât să nu poată fi accesate. Cei mai importanți algoritmi cu cheie simetrică utilizați sunt **DES** (data encryption standard - standard de criptare a datelor) și **AES** (standard de criptare avansată - advanced encryption standard). Dintre algoritmii cu chei asimetrice reprezentativi sunt: **RSA** (Rivest-Shamir-Adleman) utilizat pentru semnături digitale, **DSA** (digital signature algorithm**), DSS** (digital signature standard) și **ECDSA** (elliptic curve digital signature algorithm – algoritm de semnătură digitală cu curbă eliptică).

Librăriile criptografice[12] conțin modalități și informații privind algoritmii care pot fi utilizați de către dezvoltatorii de aplicații software pentru a proteja informațiile sensibile. Aceste librării trebuie să îndeplinească anumite criterii de protecție pentru a putea satisface cerințele de securitate necesare asigurării infrastructurii.

Principalele tehnologii specifice criptografiei[13] **utilizate** sunt reprezentate de:

Smartcardul este un card de plastic (similar celor utilizate în domeniul bancar) care conține un cip criptografic care folosește algoritmi criptografici de tipul DSA/RSA pentru autentificarea pe anumite echipamente, scopul fiind limitarea accesului pe acestea. Dispozitivele sunt conectate prin intermediul unor cititoare de smartcarduri care sunt implementate la un echipament de tip PC. Există mai multe categorii și anume: carduri SIM – folosite pentru telefoane mobile; badge-uri utilizate la nivelul companiilor pentru identificarea persoanelor; carduri naționale de sănătate, permise de ședere, pașapoarte electronice etc.

Prin intermediul infrastructurilor de chei publice, utilizatorii autorizați pot folosi dispozitive de tip ***token*** pentru a se autentifica la anumite echipamente specifice. Pe aceste dispozitive sunt implementate soluții criptografice.

Token-ul USB de securitate este un dispozitiv care conține informațiile necesare autentificării la diferite infrastructuri sau echipamente. Băncile pot emite astfel de dispozitive pentru clienții săi, oferind protecție suplimentară în momentul în care aceștia utilizează servicii oferite de instituția bancară în mediul online. Dispozitivul are un anumit grad de autonomie față de alte tipuri similare. Necesitatea de a utiliza un cititor de carduri este eliminată și integrează atât procesorul criptografic (care conține elemente specifice cripto), precum și cititorul.

Mediile de stocare de tip USB criptate reprezintă măsuri de securitate pentru a proteja informațiile gestionate în format electronic prin intermediul acestor medii de stocare. Cele mai utilizate sau fiabile medii de stocare USB criptate sunt: Kingston Ironkeys, DiskAshur Pro, Aegis Secure keys, Secure Drive, etc. Mediile de stocare criptate pot fi și sub forma HDD externe care conțin informații sensibile și care beneficiază de aceste soft-uri configurate în vederea asigurării securității criptografice a datelor.

HMS[14] ***(hardware security module – modul de securitate hardware)*** poate fi conectat la un PC și este reprezentat de *dispozitive de tip black-box,* cu module hardware și software care asigură funcții criptografice în vederea protecției informațiilor gestionate în format electronic. Acest dispozitiv este de fapt un procesor cu funcții criptografice care asigură managementul cheilor criptografice, accelerează procese/funcții criptografice și garantează autentificarea pentru acces la anumite aplicații. Există două mari categorii de astfel de echipamente unele pentru PC-uri și altele pentru rețele. Aceste dispozitive sunt utilizate la bancomate, tehnologiile încorporate permițând retragerea banilor cash în

siguranță. Printre cele mai cunoscute și utilizate, la nivel național, se numără modulul de securitate hardware produs de Bitdefender.

Aplicațiile software criptografice asigură criptarea dispozitivelor de tip USB, HDD. Principalele aplicații[15] care asigură soluții/funcții de criptare a informațiilor:

- ***Axcrypt*** poate fi folosită și la nivel individual de către utilizatori pentru protecția informațiilor confidențiale/ sensibile. Utilizează algoritmi de criptare de tip AES-256 și poate rula pe dispozitive cu sistem de operare MacOS și Windows. Aplicația oferă versiuni specifice mediului de afaceri și la nivel de utilizator.
- ***DriveCrypt*** reprezintă, în accepțiunea specialiștilor, cea mai bună soluție software de criptare a informațiilor sensibile gestionate pe dispozitive de tip USB. Aplicația are funcții de securitate care permit autentificarea prin amprentare, principalul dezavantaj fiind prețul mare de achiziție.
- ***Rohos*** asigură protecția criptografică a informațiilor sensibile stocate pe dispozitive de tip USB, respectiv HDD. Există două versiuni: una care asigură criptarea dispozitivelor de tip USB și HDD și chiar a informațiilor stocate în cloud (Rohos Disk Encryption) și alta, Rohos Logon Key, care poate transforma un dispozitiv de tip USB sau chiar un echipament de tip Smartphone în instrument de autentificare, la dispozitivul criptat, prin intermediul aplicației Rohos Disk Encryption. Aplicația folosește algoritm de criptate AES 256 și poate rula pe sisteme de operare de tip Mac sau Windows.
- ***Gilisoft encryption*** permite utilizatorilor fără experiență să își asigure protecția criptografică a informațiilor sensibile gestionate pe dispozitive de tip USB. Asigură criptarea informațiilor cu algoritm criptografic de tip AES 256. Această aplicație software este disponibilă doar pentru sistemul de operare Windows.
- ***VeraCrypt*** asigură protecția informațiilor clasificate gestionate în format electronic. Această aplicație a fost cunoscută cu denumirea de TrueCrypt. Pentru protecția informațiilor se pot folosi algoritmi criptografici de tip Twofish, Serpent și chiar AES-256.
- ***Bitlocker*** este utilizat pentru a proteja informațiile gestionate în cadrul organizațiilor, precum și la nivel individual. Poate rula pe sisteme de operare de tip Windows și utilizează algoritmi criptografici tip AES 128 sau 256 și permite criptarea totală a HDD-urilor pe volume de date. Este inclusă în sistemul de operare Windows 10 și poate fi utilizată pentru a cripta o anumită partiție de pe HDD. Are implementate funcții de autentificare cu PIN sau parolă pentru utilizatori, precum și mod USB.

Aplicațiile criptografice prezentate mai sus nu sunt singurele de acest tip. Evoluția acestora este influențată direct de progresele înregistrate în dezvoltarea domeniului IT&C, constatându-se, totodată, și o largă aplicabilitate a acestora în diferite domenii de activitate (această realitate explică și rata exponențială de creștere a numărului acestora).

Principalele ***funcții ale dispozitivelor specifice domeniului criptografic*** sunt:

- asigurarea criptării diferitelor echipamente (HDD, router, USB, smartcarduri, token-uri, dispozitive 2FA);
- asigurarea protecției criptografice a serviciilor de mesagerie electronică;
- securitatea datelor și informațiilor confidențiale gestionate în format electronic în cadrul organizațiilor;
- protecția criptografică a serviciilor din Internet;
- securizarea diferitelor rețele;
- protecția criptografică a bazelor de date utilizate la nivelul diferitelor organizații;
- asigurarea securității criptografice a site-urilor;
- asigurarea securității serviciilor de email și a celor de mesagerie instant;
- implementarea serviciilor de semnături digitale;
- utilizarea algoritmilor criptografici în cadrul monedelor virtuale (criptomonede);
- autentificarea la diferite echipamente.

Este important să înțelegem faptul că funcțiile și principalele dispozitive utilizate pentru protecția criptografică a infrastructurilor IT&C **nu garantează protecția totală**.

DOMENIILE DE ACTIVITATE ÎN CARE CRIPTOGRAFIA ESTE UTILIZATĂ

Apariția și dezvoltarea continuă a utilizării calculatoarelor (tehnicii de calcul) în practic toate domeniile de activitate, existența și evoluția rețelelor specifice domeniului IT&C, la nivel național și internațional, globalizarea și dezvoltarea comunicațiilor, existența și dezvoltarea unor baze de date interconectate și actualizate în timp real, apariția și dezvoltarea comerțului electronic, a monedelor virtuale, constituie elemente de normalitate în activitatea cotidiană. Toate acestea indică o creștere extraordinară a volumului și importanței datelor gestionate și, implicit, determină multiplicarea vulnerabilităților specifice pe linie de securitate.

Criptografia este utilizată în viața de zi de zi. De exemplu, folosim servicii și produse specifice criptografiei în momentul în care transmitem email-uri, utilizăm servicii/produse bancare, ne conectăm la diferite echipamente electrocasnice din domeniul IoT (Internet of Things), accesăm diferite informații din Internet, participăm la cursuri online, semnăm documente în format electronic, folosim aplicații de mesagerie instant, achiziționăm diferite bunuri online etc.

Criptografia este utilizată pentru protejarea comunicațiilor guvernamentale/militare respectiv a infrastructurilor IT&C și mai mult pentru carduri bancare, plați de taxe, acces autorizat în clădiri sau la calculatoare, instrumente electronice de plăți electronice, drepturi de autor etc.

Principalele **domenii de activitate**[16] în care criptografia este utilizată:

- domeniul ***financiar-bancar*** (internet banking, transferuri bancare în mediul online, extrageri de numerar, etc);
- domeniul ***militar*** (echipamentele militare au integrate module criptografice care le permit să comunice în mod securizat);
- ***guvernamental*** (asigurarea protecției comunicațiilor guvernamentele de tip satelit, telefonie mobilă criptată, servicii de tip VOIP etc.);
- ***educațional*** (asigurarea protecției rețelelor informatice care asigură învățământ online, protecția criptografică a bazelor de date, a infrastructurilor specifice domeniului IT&C utilizate în procesul educațional);
- ***semnături electronice/digitale***[17] (o serie de algoritmi criptografici pentru implementarea unor soluții tehnice și anume algoritmi criptografici pentru generarea cheilor criptografice, pentru semnarea documentelor gestionate în format electronic, precum și algoritmi de verificare a semnăturilor electronice);
- ***comunicații mobile*** (dispozitive mobile criptate prin intermediul unor aplicații software sau dispozitive hardware care asigură protecția criptografică a informațiilor gestionate);
- ***servicii de mesagerie instant*** (mesageria criptată); cele mai utilizate servicii de mesagerie instant sunt WhatsApp, Wickr Me, Threema, Signal, Telegram, Ricochet etc;
- ***securitatea în Internet*** are la bază anumite protocoale și standarde criptografice care realizează securitatea informațiilor gestionate electronic; sunt utilizate protocoale criptografice pentru a proteja datele vehiculate în internet printre cele mai cunoscute regăsim: Ipsec (internet protocol security), SSL (secure sochet layer), TLS (transport layer security) etc;
- ***comerț electronic*** (transferul fondurilor electronice, procesarea plăților electronice, în sisteme de micro-plăți sau în carduri bancare); printre cele mai cunoscute procesatoare de plăți online sunt: PayU, Mobilpay, Amazon Paypal, 2Checkout etc;
- ***monede virtuale / criptomonede***[18] (transferul fondurilor bancare); utilizarea algoritmilor criptografici în cadrul criptomonedelor Bitcoin, Ethereum, Litecoin, Dogecoin, etc. Printre cei mai cunoscuți algoritmi criptografici sunt SHA-256 (introdus de Bitcoin),

Fig. 4 – Monede virtuale/criptomonede[19]

Cryptonight, Blake x11, Smartcontract, scrypt, x11, ECDSA, etc;

- ***servicii audio-video*** asigurate prin abonamente de televiziune (ex. Netflix, Amazon-prime, HBO, HULU), unde sunt necesare funcții de autentificare, chei criptografice etc.;
- domeniul ***sanitar*** (bazele de date ale pacienților care sunt stocate pe diferite servere, fiind necesare protejarea criptografică, infrastructura necesară implementării cardului de sănătate, a dosarului medical);
- ***securizarea infrastructurilor IT&C*** (criptarea echipamentelor de tip HDD, carduri de memorie de tip SD utilizate în cadrul telefoanelor mobile);
- ***IoT***[20]– asigurarea securității diferitelor dispozitive utilizate în locuințe personale (camere de supraveghere, echipamente electrocasnice inteligente, etc.);
- în ***biometrie***[21] este folosită ciparea/ tokenizarea și reprezintă o altă metodă de a permite dispozitivelor de a recunoaște utilizatorii autorizați (identificarea vocii, amprente digitale etc.);

Din prezentarea principalelor domenii în care criptografia este utilizată rezultă faptul că domeniul criptografic reprezintă o componentă de bază în activitatea cotidiană. O serie de dispozitive electronice (telefoane mobile, calculatoare, electrocasnice utilizate în scop casnic, ceasuri inteligente, routere etc.) au implementate anumite componente criptografice și algoritmi care ne asigură securitatea informațiilor gestionate în format electronic indiferent de spațiul în care ne desfășurăm activitatea sau de momentul în care realizăm acest lucru.

Odată cu achizițiile specifice din domeniul militar, în cadrul Armatei României va crește și ponderea echipamentelor specifice domeniului criptografiei, utilizate în sistemele de armament pentru asigurarea comunicațiilor securizare și pentru conducerea forțelor militare.

CONCLUZII

Importanța domeniului criptografiei în asigurarea securității infrastructurilor IT&C va crește și va influența activitatea cotidiană în ansamblul ei.

Achizițiile de tehnologii specifice criptografiei și implicit domeniului IT&C nu sunt suficiente fără a se asigura pregătirea și instruirea, într-un cadru instituțional, pentru personalul care va utiliza echipamente specifice acestui domeniu.

Principalele tendințe care vor asigura protecția datelor sensibile specifice domeniilor prezentate anterior, din sfera criptografiei, sunt cele legate de dezvoltarea *tehnologiilor cuantice* (calculatoare cuantice, criptare cuantică, criptanaliză cuantică), *tehnologiei cloud* (maniera în care aceste infrastructuri sunt protejate cu tehnologii specifice criptografiei) și, nu în ultimul rând, *tehnologia blockchain*.

Activitatea pe care o desfășurăm atât la nivel de individ, cât la nivel de organizație nu poate fi separată de impactul tehnologic asupra vieții.

Simpla deconectare a echipamentelor de la rețea nu mai este posibilă.

Dacă acum un număr de ani accentul se punea pe realizarea rețelelor de comunicații, a bazelor de date și a schimbului de informații, acum accentul s-a mutat pe protecția acestor infrastructuri specifice domeniului IT&C cu echipamente specifice criptografiei, care asigură pe lângă nevoia de conectare/de utilizare și protecția criptografică a informațiilor sensibile pe care le accesăm.

În concluzie, când ne gândim la criptografie putem face o analogie cu modalitatea în care ne protejăm casa și bunurile de anumite persoane rău intenționate, folosind sisteme de protecție fizică (încuietori, lacăte etc.). Folosim serviciile/ produsele criptografice pentru a proteja informații sau infrastructuri IT&C specifice domeniilor enumerate anterior. Aspectele menționate arată importanța acestui domeniu și rolul acestuia în activitatea cotidiană, precum și maniera în care criptografia se va dezvolta în viitor.

BIBLIOGRAFIE

1. *** „Cryptographic device”, disponibil la https://csrc.nist.gov/glossary/term/cryptographic_device;
2. *** „Definiția și istoria criptografiei”, disponibil la https://glennbouchard.com/ro/317-pengertian-dan-sejarah-kriptografi.html;
3. *** „Difference between classical and quantum cryptography” disponibil la https://www.geeksforgeeks.org/difference-between-classical-and-quantum-cryptography/?ref=rp, 22.06.2020;
4. *** „Difference between cryptography and cyber-security”, disponibil la https://geeksforgeeks.org/difference-between-cryptography-and-cyber-security/?ref=rp, 14.03.2023;
5. *** „Difference between stegangraphy and cryptography”, disponibil la https:/www.geeksforgeeks.org/difference-between-stegangraphy-and-cryptography/?ref=rp, 27.03.2023;
6. *** „O mașină de criptat Enigma folosită de naziști descoperită de scafandri germani în Marea Baltică”, disponibil la https://stirileprotv.ro/divers/o-masina-de-criptat-enigma-folosita-de-nazisti-descoperita-de-scafandri-germani-in-marea-baltica/, 05.12.2020;
7. *** „What are some exemples of cryptography. Cryptography in everyday life”, https://mgtblog.com/what-are-some-exemple-of-cryptography/;
8. *** „What are the applications of cryptography in information security”, disponibil la https://www.tutorialspoint.com/what-are-the-applications-of-cryptography-in-information-security, 04.03.2022;
9. *** „What is a cryptographyc key”, disponibil la https://www.cloudflare.com/learning/ssl/what-is-a-cryptographyc-key/;
10. *** „What is IoT?”, disponibil la https://www.oracle.com/internet-of-things/what-is-iot/.
11. BARRET Diane, Martin M. Weiss, *ComTIA Security+ SY0-501 Exam Cram*, 5th Edition, 26.12.2017, disponibil la https://www.pearsonitcertification.com/articles/article.aspx?p=2861453&seqNum=5;
12. BOUCHARD Glenn, „The CIA triad in cryptography”, disponibil la https:/www.geeksforgeeks.org/the-cia-triad-in-cryptography/?ref=rp, 13.03.2023;
13. CHAMBERALIN Austin, „Application of crytography”, disponibil la https://blogs.ucl.ac.uk/infosec/2017/03/12/application-of-crytography, 12.03.2017;
14. DE GROT Juliana, „What is USB control & encryption”, disponibil la https://digidalguardian.com/blog/what-usb-control-encryption, 02.08.2023;
15. ENISA (European Union Agency for Cybersecurity), *Artificial intelligence and cybersecurity research*, iunie 2023;
16. ENISA (European Union Agency for Cybersecurity), *Crypto assets, an introduction to digital currencies and distributed ledger tehnologies*, 09.02.2021;
17. ENISA (European Union Agency for Cybersecurity), *Digital identity standards, analysis of standard, Analysis of standardisation requirements in support of cybersecurity policy*, iulie 2023;

18. ENISA (European Union Agency for Cybersecurity), *Post-quantum cryptography, integration study*, octombrie 2022;
19. ENISA (European Union Agency for Cybersecurity), *Post-quantum cryptography, Current state and quantum mitigation*, mai 2021;
20. FANTESINI Arianna, „Digital euro advantages and risks of the Ecb's new virtual currency", disponibil la https://www.i-com.it/en/2020/10/16/digital-euro-advantages-and-risks-of-the-ecbs-new-virtual-currency, 16.10.2020;
21. GRUHN Diana, Julien Probst, „What is cryptoghrapy and why is it important?", disponibil la https://www.entrust.com/blog/2021/06/why-is-cryptography-so-important-heres-what-you-need-to-know/, 24.06.2021;
22. Ninel, „Cryptography in our daily usage", https://berty.tech/blog/cryptography-daily-usage, 16.10.2019;
23. PRASHANTH Reddy, „Real life applications of cryptography", disponibil la https://medium.com/@prashanthreddyt1234/real-life-applications-of-cryptography-162ddf2e917d, 08.11.2019;
24. PRATT Mary, „Learn the basics of cryptography in IoT", disponibil la https://www.techtarget.com/iotagenda/tip/Learn-the-basics-of-cryptography-in-IoT/, 19.10.2021;
25. RAWAT Soumyaa, „Characteristics, Types and Applications of Cryptography" disponibil la https://www.analyticssteps.com/blogs/characteristics-types-and-applications-cryptography, 03.10.2021;
26. Rezos, KristenS, kingthorin, „Cryptanalysis", disponibil la https://owasp.org/www-community/attacks/cryptanalysis;
27. Ronan, „5 every day applications of cryptoghrapy", disponibil la https://ronanthewriter.com/applications-of-cryptography-in-daily-life/, 09.06.2020;
28. ZAHORSKY Alexei, „The 5 best USB drive encryption software", disponibil la https://www.makeuseof.com/best-usb-encryption-software/, 08.06.2022.

[1] https://stirileprotv.ro/divers/o-masina-de-criptat.
[2] https://www.geeksforgeeks.org/difference-between-classical-and-quantum-cryptography/?ref=rp.
[3] https://owasp.org/www-community/attacks/cryptanalysis.
[4] https:/www.geeksforgeeks.org/difference-between-stegangraphy-and-cryptography/?ref=rp.
[5] https://www.tutorialspoint.com/what-are-the-applications-of-cryptography-in-information-security.
[6] https:/www.geeksforgeeks.org/the-cia-triad-in-cryptography/?ref=rp.
[7] https://glennbouchard.com/ro/317-pengertian-dan-sejarah-kriptografi.html.
[8] https://mgtblog.com/what-are-some-exemple-of-cryptography/
[9] https://geeksforgeeks.org/difference-between-cryptography-and-cyber-security/?ref=rp.
[10] https://csrc.nist.gov/glossary/term/cryptographic_device.
[11] https://www.cloudflare.com/learning/ssl/what-is-a-cryptographyc-key/
[12] https://www.entrust.com/blog/2021/06/why-is-cryptography-so-important-here-what-you-need-to-know/
[13] https://onlinedegrees.und.edu/blog/5-cryptography-tools/
[14] https://www.pearsonitcertification.com/articles/article.aspx?p=2861453&seqNum=5.
[15] https://www.makeuseof.com/best-usb-encryption-software/
[16] https://www.analyticssteps.com/blogs/characteristics-types-and-applications-cryptography.
[17] ENISA, Post-quantum cryptography, Current state and quantum mitigation, mai 2021, p. 23.
[18] Idem, Crypto assets, an introduction to digital currencies and distributed ledger tehnologies, februarie 2021, p. 16.
[19] https://www.i-com.it/en/2020/10/16/digital-euro-advantages-and-risks-of-the-ecbs-new-virtual-currency.
[20] Idem, Artificial intelligence and cybersecurity research, iunie 2023, p. 27.
[21] ENISA Digital identity standards. Analysis of standardisation requirements in support of cybersecurity policy, iulie 2023, p. 19.

IMPACTUL INTELIGENȚEI ARTIFICIALE ASUPRA CRIPTOGRAFIEI

*Ioana-Roxana DRAGOMIR**

Abstract

Artificial intelligence (AI) has a significant impact on the future of humanity in almost every field. With the help of AI, computers can process massive amounts of data and use them in the process of decisions' making.

The continuous evolution of AI technologies creates new opportunities and change the way we interact/communicate one another. It is difficult to assert with certainty in which domain the impact of AI will be more significant, as it can vary depending on numerous factors, including the level of technology used, government regulations, technological innovations and changes in market demand. There is an important connection between AI, cybersecurity, cryptanalysis and quantum cryptography, especially in the context of protecting data and communications in the digital age.

It is important to emphasize that the impact of AI will depend on how it is managed and implemented, as well as the decision made by society and governments worldwide regarding regulations and ethics.

Keywords: *Cryptanalysis; artificial intelligence; algorithms; quantum cryptography; cyber security.*

ZORII INTELIGENȚEI ARTIFICIALE – SCURTĂ INTRODUCERE

Sistemele de inteligență artificială[1] (IA) reprezintă configurații complexe și integrate de tehnologii hardware și software specializate, elaborate pentru a simula procese cognitiv umane precum învățarea, raționamentul, recunoașterea de tipare și luarea deciziilor. Aceste sisteme acționează prin colectarea informațiilor provenite din surse diverse, precum senzori, baze de date, dispozitive tip *Internet of Things* (IoT), apoi procesează aceste date pentru a le analiza, extrage semnificația lor și a genera răspunsuri sau acțiuni corespunzătoare.

Progresul tehnologic și informatic din secolele XX și XXI a fost marcat de evoluția rapidă a IA, aducând cu sine o transformare semnificativă în modul în care interacționăm cu tehnologia, învățăm din datele noastre și abordăm o gamă largă de provocări complexe.

Pionieratul în IA a început în anul 1950, când Alan Mathison Turing, matematician, informatician, criptanalist, în lucrarea sa „Computing Machinery and Intelligence”[2], propune Testul Turing[3] pentru a determina dacă o mașină poate imita inteligența umană.

În 1956, John McCarthy introduce termenul de „inteligență artificială” cu prilejul unei conferințe la Colegiul Dartmouth. Mai târziu, în același an, este realizat primul program software de către Allen Newell, JC. Shaw și Herbert Simon. Cercetătorii au dezvoltat primele modele de calculatoare capabile să imite procesele de raționament uman.

În anii 1970-1980, după o perioadă inițială de optimism, urmează o scădere a interesului în cercetarea IA din cauza unor dezamăgiri legate de limitările tehnologiei.

În perioada 1990-2000, cercetătorii fac progrese semnificative în dezvoltarea IA, în special în ceea ce privește învățarea automată. Sunt dezvoltate metode eficiente pentru antrenarea modelelor și pentru aplicarea lor în diverse domenii. În această perioadă, apare conceptul de „învățare profundă” (deep learning), care dezvoltă rețelele neuronale, fapt ce permite sistemelor IA să învețe din date. Dezvoltarea acestor tehnologii conduce la progrese în recunoașterea vocală și vizuală, procesarea limbajului natural,

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

vehicule autonome și altele. Companii mari, precum Google, Facebook și Amazon, investesc masiv în dezvoltarea IA, această tehnologie devenind o parte integrantă a multor aspecte ale vieții cotidiene, de la asistenții vocali de tip Siri (2011-Apple) și Alexa (2014-Amazon) la sistemele de recomandare pentru divertisment sau cumpărături online.

În 2016 apare primul „cetățean robot", numit Sophia, creat de Hanson Robotics, capabil să recunoască fețe, să comunice și să interpreteze expresii faciale.

Recenta explozie a IA este atribuită în mare măsură dezvoltării tehnicilor de învățare profundă și apariției rețelelor neuronale la scară largă, cum ar fi seria Generative Pre-Trained Transformer (GPT) de la OpenAI. GPT-3, lansat în 2020, este un exemplu excelent al modului în care IA a evoluat, acest model utilizând 175 de miliarde de parametri și demonstrând înțelegerea și generarea limbajului natural fără precedent. Succesul lui GPT-3 și al predecesorilor săi reprezintă dovada clară a potențialului IA, stimulând cercetarea și dezvoltarea permanentă a domeniului. Cea mai recentă iterație, GPT-4, se bazează pe predecesorii săi și prezintă capabilități și mai avansate, împingând granițele IA și mai departe.

Pentru a realiza mașini și programe care să fie capabile să simuleze sau să imite, într-o anumită măsură, funcțiile cognitive umane, IA se bazează pe diverse abordări și tehnici, cum ar fi:

➢ Învățare automată[4] (machine learning): implică dezvoltarea unor algoritmi care permit sistemelor să învețe și să adapteze modele din datele de antrenare pentru a face predicții sau pentru a lua decizii, fără a fi programate explicit pentru fiecare situație.

➢ Procesarea limbajului natural (NLP)[5]: se ocupă cu înțelegerea și generarea limbajului uman. Sistemele NLP permit computerelor să traducă limbi străine, să analizeze sentimentele din texte sau să interacționeze în mod natural cu oamenii prin vorbire sau scriere.

➢ Viziunea artificială: se concentrează pe dezvoltarea sistemelor capabile să recunoască și să interpreteze imagini și video. Tehnologii precum recunoașterea facială și identificarea obiectelor sunt câteva exemple de aplicații.

➢ Înțelegerea: se referă la capacitatea unor sisteme de a extrage informații și de „a înțelege" contextul din date structurate sau nestructurate, precum baze de date sau texte.

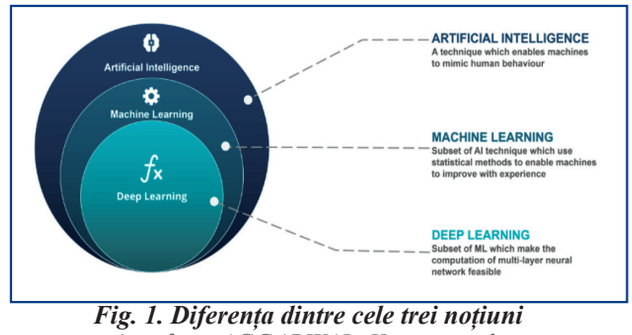


Fig. 1. Diferența dintre cele trei noțiuni
(*conform AGGARWAL, Karan, et al. Has the future started?)*[7]

➢ Învățarea profundă[6]: este o subramură a învățării automate care se concentrează pe rețele neuronale profunde și complexe pentru a îndeplini sarcini de învățare și recunoaștere;

➢ Robotica – include control, percepție, senzori și actuatori, precum și integrarea tuturor celorlalte tehnici în sisteme cyber-fizice capabile să efectueze sarcini complexe, precum intervenții chirurgicale asistate, asamblare, explorare etc.

Aplicațiile IA sunt diverse și cuprind domenii precum medicina, finanțele, transportul autonom, securitatea cibernetică, jocurile video și altele.

ETICA ȘI SECURITATEA IA

În ciuda progresului impresionant al IA, există încă provocări și preocupări etice care trebuie abordate pe măsură ce tehnologia continuă să evolueze. Confidențialitatea, securitatea și potențiala utilizare greșită a IA sunt probleme critice care necesită o reglementare atentă.

Etica și securitatea sunt aspecte interconectate și esențiale pentru a asigura dezvoltarea și utilizarea responsabilă a acestei tehnologii în viitor. Comunitatea internațională lucrează în prezent la stabilirea unor standarde și norme care să reglementeze acest domeniu.

În acest sens, Uniunea Europeană (UE) a acordat o atenție deosebită eticii și securității IA în cadrul eforturilor sale de a reglementa și implementa progresele tehnologiei. În continuare, vom prezenta pe scurt câteva aspecte relevante legate de etică și securitatea IA în UE.

Un prim domeniu de interes pentru UE se referă la dezvoltarea standardelor tehnice pentru IA. Aceste standarde sunt esențiale în asigurarea că toate sistemele IA dezvoltate sau utilizate în UE sunt conforme cu normele și valorile europene.

Planul coordonat privind IA, din 2018, reprezintă un angajament comun al Comisiei Europene și al statelor membre de a colabora pentru a maximiza potențialul Europei de a concura la nivel mondial. Revizuirea din aprilie 2021 a planului[8] coordonat a constituit următoarea etapă. Acesta reglementează diferitele utilizări ale IA, inclusiv cele cu impact ridicat, precum vehiculele autonome sau sistemele de recunoaștere facială, și stabilește cerințe stricte pentru dezvoltatori, inclusiv transparență, responsabilitate și evaluări de impact asupra drepturilor fundamentale ale cetățenilor, inclusiv dreptul la confidențialitate, nediscriminare și securitate.

UE a alocat resurse semnificative pentru cercetarea și dezvoltarea tehnologiei IA etice și securizate, precum și pentru stimularea inovației în acest domeniu, suma ridicându-se la cel puțin 1 miliard EUR pe an prin programele „Orizont Europa" și „Europa digitală în perioada 2021-2027".

Este important de menționat că aceste politici și inițiative se află într-un stadiu de dezvoltare continuă și pot evolua odată cu schimbările în tehnologia IA și nevoile societății. UE se angajează să creeze un cadru reglementat care să promoveze dezvoltarea și utilizarea responsabilă a IA în Europa.

În 2023 România era printre ultimele state ale UE fără o strategie națională în domeniul inteligenței artificiale, în timp ce alte țări europene se aflau deja la a doua iterație, revizuind strategiile naționale conform celor mai recente evoluții în domeniu. Pentru a recupera decalajul existent, a fost înființată Comisia Interinstituțională pentru Elaborarea Strategiei de IA a României, adoptată prin Hotărârea CSAT 148 / 27.09.2022.

Comitetul Român pentru Inteligență Artificială (AIRomânia) este o nouă structură în Guvern ce își propune să reunească experți, companii naționale și/sau de la nivel internațional. Structura este în prezent operaționalizată de Administrația Prezidențială a României, alături de Ministerul Cercetării, Inovării și Digitalizării, și are în responsabilitate coordonarea eforturilor de elaborare a strategiei de IA a României și a Planului de Acțiune pentru implementarea strategiei la nivel național. Scopul este să se poată utiliza progresul semnificativ realizat în proiectul „Cadru strategic pentru adoptarea și utilizarea de tehnologii inovative în administrația publică 2021-2027 – soluții pentru eficientizarea activității", coordonat de către Autoritatea pentru Digitalizarea României împreună cu Universitatea Tehnică din Cluj Napoca. De asemenea, se va construi un institut dedicat IA, în apropiere de centrul orașului Cluj-Napoca, care va avea o suprafață de 13.000 de metri pătrați, 30 de laboratoare, 15 săli de suport, mai multe săli de conferințe, dotate cu echipamente de înaltă performanță.

În SUA, Centrul Național de Excelență pentru Securitate Cibernetică (NCCoE), care face parte din Institutul Național de Standarde și Tehnologie (NIST), este un centru în care organizațiile din industrie, agențiile guvernamentale și instituțiile academice lucrează împreună pentru a aborda cele mai presante provocări: securitate cibernetică și IA.

NIST conduce și participă la dezvoltarea standardelor tehnice[9], inclusiv a standardelor internaționale, care promovează inovația și încrederea publicului în sistemele care utilizează IA.

INTELIGENȚA ARTIFICIALĂ ȘI CRIPTANALIZA

Criptanaliza este procesul de analiză și descifrare a datelor criptate fără a avea acces la cheia de decriptare corespunzătoare. Scopul acesteia este de a dezvălui informații secrete protejate în mod ilegitim. Criptanaliza este folosită în mod legitim în cadrul testelor de securitate pentru a verifica eficacitatea unui sistem de criptare, în investigațiile penale pentru a rezolva infracțiuni cibernetice, dar poate fi utilizată și ilegitim atunci când compromite securitatea unui sistem.

Există mai multe tehnici și metode de criptanaliză, iar succesul acestora depinde de diferiți factori, precum complexitatea algoritmului de criptare folosit, lungimea cheilor și resursele disponibile pentru atacatori.

Cea mai cunoscută metodă este criptanaliza cu forță brută, în care atacatorii încearcă toate cheile posibile până când o găsesc pe cea potrivită. Această metodă implică putere de calcul mare și, în consecință, devine ineficientă pentru sisteme complexe ce folosesc chei lungi.

O altă metodă o constituie criptanaliza prin analiza frecvenței cu care apar diferite simboluri sau caractere în criptogramă (textul cifrat).

Deși este adesea asociată cu încercările de spargere a securității, criptanaliza joacă un rol crucial în dezvoltarea și evaluarea sistemelor de criptare pentru a le face mai sigure și robuste împotriva unor potențiale atacuri.

IA poate avea un impact semnificativ asupra procesului de criptanaliză, atât în ceea ce privește eficiența atacurilor, cât și în ceea ce privește apărarea împotriva acestora. În continuare, vom descrie modul în care IA influențează / facilitează, în mod direct, câteva tipuri de atacuri:

➢ IA poate accelera procesul de criptanaliză cu forță brută, care implică încercarea tuturor cheilor posibile, prin utilizarea de calculatoare și hardware de înaltă performanță, reducând astfel timpul necesar pentru a sparge o criptare. Cu ajutorul rețelelor neurale sau a altor tehnologii IA, pot fi generate și testate combinații de chei într-un mod mult mai eficient.

➢ Prin algoritmii de învățare automată, IA poate detecta modele în datele criptate și poate ajuta la identificarea mai rapidă a caracteristicilor limbajului natural sau a altor modele prezente în textul clar, facilitând în final găsirea cheilor de criptare.

➢ IA poate dezvolta și implementa tehnici de criptanaliză avansate, cum ar fi rețele neuronale artificiale, pentru a încerca să descifreze datele criptate prin învățarea modelelor din datele disponibile. Cu suficiente date și resurse computaționale adecvate, IA poate învăța să descifreze informațiile.

În ultimul deceniu, tehnicile și abordările din învățarea automată și rețelele neuronale au devenit metode eficiente în „atacuri pe canale alăturate” (side channel attacks). Datorită relevanței sale practice ridicate pentru evaluarea securității implementărilor criptografice, BSI (Oficiul Federal pentru Securitatea Informației din Germania) urmărește în mod activ progresul în domeniul analizei „canalelor alăturate” cu metode IA și contribuie, de asemenea, la cercetarea în acest domeniu. De exemplu, cu ajutorul metodelor de IA, o echipă BSI a câștigat concursul international CHES Challenge în 2018, respectiv 2020. În cadrul unui alt proiect, „AI-assisted Analysis Methods for Symmetric Cryptography”[10], o echipă de la Ruhr-Universitat Bochum, condusă de Prof. Dr. Gregor Leander și Prof. Dr. Asja Fischer, analizează posibilitățile de utilizare a IA în analiza și evaluarea criptografiei simetrice. Unul dintre obiectivele proiectului este dezvoltarea de instrumente susținute de IA care pot contribui la evaluarea securității mecanismelor simetrice dezvoltate recent.

Pe de altă parte IA poate fi folosită pentru a întări securitatea criptografică și pentru a proteja împotriva atacurilor cibernetice, astfel:

➢ IA poate genera și gestiona chei criptografice puternice și complexe, făcând dificilă criptanaliza prin forță brută.

➢ IA poate detecta activitățile suspecte sau atacurile cibernetice asupra sistemelor de criptare prin identificarea de modele atipice în traficul de rețea sau în alte date.

➢ IA poate contribui la dezvoltarea de algoritmi criptografici mai siguri, mai rezistenți la atacurile criptanalitice, sporind securitatea sistemelor informatice.

În concluzie, IA poate juca un rol crucial în evoluția și complexitatea criptanalizei, atât ca instrument pentru atacuri, cât și ca mijloc de apărare împotriva acestora. Astfel, pe măsură ce IA continuă să se dezvolte, va exista o competiție constantă între criptografi, care dezvoltă algoritmi de criptare mai puternici, și criptanaliști, care utilizează IA pentru a încerca să spargă acești algoritmi.

IA poate avea un impact semnificativ asupra criptanalizei liniare și diferențiale, atât în ceea ce privește securitatea, cât și atacurile asupra sistemelor criptografice. Câteva situații des întâlnite, în care IA poate influența criptanaliza:

➢ Algoritmii de învățare automată pot ajuta la identificarea și exploatarea mai eficientă a corelațiilor liniare sau diferențiale din cadrul cifrurilor. Aceasta înseamnă că atacurile bazate pe aceste metode pot fi mai rapide sau pot necesita mai puține date pentru a dezvălui cheia secretă a unui sistem criptografic. Aceasta poate duce la dezvoltarea unor atacuri mai puternice și mai rapide asupra sistemelor criptografice care folosesc aceste tehnici.

➢ IA poate genera seturi de date relevante pentru criptanaliza liniară și diferențială. Generarea automată de date poate spori precizia și eficacitatea acestor tehnici de atac.

➢ IA poate optimiza parametrii și strategiile utilizate în atacurile de criptanaliză liniară și diferențială. Acest lucru poate duce la descoperirea mai rapidă a cheilor sau a informațiilor secrete.

➢ IA poate detecta eficient încercările de atac de tip liniar și diferențial. Sistemele de securitate bazate pe IA pot identifica mai rapid comportamentul suspect și pot reacționa în timp real pentru a contracara atacurile.

➢ Sistemele criptografice pot utiliza IA pentru a învăța din modelele de atac și pentru a se adapta la noile strategii de criptanaliză liniară și diferențială. Acest lucru poate face ca atacurile să fie mai dificil de realizat.

➢ IA poate dezvolta algoritmi criptografici mai rezistenți la atacurile de tip liniar și diferențial. Prin înțelegerea mai profundă a modului în care aceste atacuri funcționează, se pot dezvolta tehnologii de criptare mai sigure.

În concluzie, impactul IA asupra criptanalizei liniare și diferențiale poate fi dublu: poate face atât atacurile, cât și apărarea împotriva lor mai eficiente și mai complexe. Prin urmare, se impune o atenție deosebită în dezvoltarea și evaluarea sistemelor criptografice în era IA, pentru a asigura securitatea informațiilor și a datelor sensibile.

În ansamblu, IA aduce o dinamică semnificativă în criptanaliză, cu potențial de a spori atât atacurile, cât și de a îmbunătăți securitatea. Dezvoltarea și implementarea unor tehnici de criptografie rezistente la amenințările aduse de IA devin tot mai importante pentru a proteja informațiile și datele sensibile, într-o lume în continuă schimbare tehnologică.

INTELIGENȚA ARTIFICIALĂ ȘI CRIPTOGRAFIA CUANTICĂ

IA și criptografia cuantică sunt două domenii tehnologice distincte, dar ele pot avea interacțiuni și influențe semnificative unul asupra celuilalt.

O direcție emergentă în evoluția IA este progresul cuantic. Calculatoarele cuantice promit să accelereze semnificativ capacitățile de învățare automată și de analiză a datelor. Algoritmul lui Shor[11] va compromite protocoalele de comunicații folosite în prezent. Nu se cunoaște cu siguranță ritmul în care se vor dezvolta computerele cuantice, dar NIST recomandă utilizarea algoritmilor cuantici care sunt în curs de standardizare. Algoritmii selectați pentru standardizare au fost deja implementați în cele mai utilizate protocoale.

Algoritmii post-cuantici sunt dezvoltați pentru a rezolva probleme matematice considerate dificile pentru computerele cuantice. Criptografia bazată pe latice[12] este considerată una dintre cele mai solide probleme matematice de securitate post-cuantice, cu cel mai mare potențial în dezvoltarea unor noi mecanisme criptografice și cel mai intens cercetată de comunitatea academică. Există în curs de standardizare trei algoritmi bazați pe latice:

1. Algoritmul KYBER este un algoritm criptografic asimetric post-cuantic utilizat pentru schimbul de chei, care folosește latice pentru a obține securitatea. Acesta a fost propus inițial în anul 2017, în cadrul competiției NIST, iar în anul 2022 a fost selectat pentru standardizare. Se bazează pe o metodă publicată în 2005 de Oded Regev, dezvoltată de cercetători din Europa și America de Nord, care lucrează în universități, instituții de cercetare sau companii private.
2. Algoritmul CRYSTALS-Dilithium este unul dintre favoriții competiției NIST Post Quantum Cryptography (PCQ)[13] pentru semnătură digitală și face parte, ca și Kyber, din familia „Cryptographic Suite for Algebraic Lattices" (CRYSTALS). Acesta este proiectat să ofere un nivel ridicat de securitate și performanță. Este capabil să semneze documente de dimensiuni variabile, de la câțiva octeți până la gigaocteți, și poate funcționa cu chei de dimensiuni variabile.
3. Algoritmul FALCON (***F**ast **F**ourier **l**atticed-based **c**ompact signatures over **NTRU***) este un algoritm criptografic post-cuantic dezvoltat de Thomas Prest, Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Ricosset, Gregor Seiler, William Whyte și Zhenfei Zhang. Acesta tratează probleme matematice dificile: „Shortest Vector Problem" (SVP) și „Learning with Errors" (LWE).

Criptografia asimetrică nu mai este sigură; de aceea, sunt în curs de standardizare patru algoritmi cuantici: CRYSTALS-KYBER, pentru criptarea cu cheie publică și stabilirea cheilor, și CRYSTALS-DILITHIUM, FALCON și SPHINCS+ pentru semnătură digitală, câștigători ai etapei a treia din cadrul competiției PQC.

NIST lucrează în prezent la elaborarea standardului care ar trebui să fie gata în 2024 și recomandă ca să se facă trecerea la algoritmii cuantici selectați pentru standardizare, chiar dacă nu există încă un standard publicat. În acest sens, NIST va publica instrucțiuni pentru a se face tranziția cât mai repede la criptografia cuantică.

Cercetările din domeniul IA pot ajuta la dezvoltarea unor dispozitive cuantice mai eficiente și mai performante, care să accelereze procesul de factorizare folosind algoritmul lui Shor. De asemenea, IA poate contribui la accelerarea dezvoltării de tehnologii de criptare post-cuantice rezistente la atacurile cuantice.

IA poate fi folosită pentru a ajuta la dezvoltarea și optimizarea algoritmilor cuantici, inclusiv a algoritmului lui Shor. Utilizarea tehnicilor de învățare automată poate contribui la identificarea de noi abordări și tehnici pentru accelerarea acestor algoritmi.

Totodată, IA poate simula comportamentul sistemelor cuantice complexe, ceea ce poate facilita înțelegerea mai profundă a mecanismelor care stau la baza algoritmilor cuantici. Procesarea datelor generate de calculatoarele cuantice poate fi o provocare, iar IA poate fi folosită pentru a gestiona și analiza datele rezultate din execuția algoritmului lui Shor sau a altor algoritmi cuantici. Acest lucru poate ajuta la extragerea de informații relevante și la luarea deciziilor bazate pe rezultatele obținute.

În domeniul IA, BSI analizează deja tehnologiile viitoare, precum "Quantum Machine Learning QML (Învățare automată cuantică)"[14]. În linii mari, cercetătorii încearcă să valorifice și să examineze potențialele calculului cuantic în contextul învățării automate. Întrucât instruirea sistemelor moderne de învățare automată este un demers intensiv de calcul, ideea de a utiliza calculul cuantic în procesul de învățare automată atrage un interes din ce în ce mai mare. Primul rezultat fundamental îl constituie lucrarea „Quantum Machine Learning – State of The Art and Future Directions".

Prin urmare, IA și computerele cuantice sunt două domenii tehnologice cu o evoluție rapidă, iar interacțiunea lor duce la dezvoltări tehnologice semnificative și inovații în securitatea informațiilor, cercetarea științifică și multe alte domenii. Cu toate acestea, trebuie menționat că, în paralel cu dezvoltarea tehnologiilor cuantice, este important să se acorde atenție dezvoltării de tehnologii de criptare post-cuantice pentru a proteja datele și informațiile împotriva amenințărilor cuantice.

CONCLUZII

Sistemele de securitate bazate pe IA pot analiza comportamentul rețelelor și pot ajuta la identificarea și neutralizarea amenințărilor cibernetice în timp real, oferind o protecție mai bună împotriva atacurilor. De asemenea, tehnologiile IA pot fi folosite pentru a îmbunătăți criptarea datelor în tranzit, cum ar fi cele utilizate în comunicațiile online și în transferul de date între dispozitive.

IA poate fi utilizată în criptanaliză pentru a încerca să spargă sistemele de criptare folosind metode de forță brută sau algoritmi de învățare automată pentru a găsi vulnerabilități în criptare. Algoritmi de învățare automată pot fi folosiți pentru a identifica modele în datele criptate, ceea ce ar putea face mai ușoară spargerea cheilor criptografice. De asemenea, IA poate fi folosită pentru a dezvolta tehnologii de criptare mai sigure, care să reziste la atacurile cibernetice.

În concluzie, IA poate fi folosită atât pentru a îmbunătăți securitatea cibernetică și pentru a spori eficacitatea criptării, cât și pentru a încerca să spargă sistemele de criptare prin criptanaliză. Criptografia cuantică, pe de altă parte, reprezintă o paradigmă cu totul diferită pentru criptare și oferă o securitate ridicată în fața atacurilor cibernetice, inclusiv a celor bazate pe computere cuantice.

BIBLIOGRAFIE

1. AGGARWAL Karan et al., "Has the future started? The current growth of artificial intelligence, machine learning, and deep learning", *Iraqi Journal for Computer Science and Mathematics,* 2022, 3.1: 115-123.
2. BAUCKHAGE Christian, Rainer Bye, Ahmed Iftikhar, Christian Knopf, Merima Mustafic, Nico Piatkowski, Roland Stahl, Rafet Sifa, Eldar Sultanow, "Quantum Machine Learning State of The Art and Future Directions", Federal Office for Information Security, disponibil la http://www.bsi.bund.de.
3. Comisia Europeană, *Cartea albă privind inteligența artificială – O abordare europeană axată pe excelență și încredere,* COM(2020) 65 final, 2020.
4. GEORGESCU-MIHĂIȚĂ Adela, *Protocoale de grup în criptografia clasică și criptografia bazată pe latici,* teză de doctorat Universitatea din București, martie 2013, disponibilă la http://old.fmi.unibuc.ro/ro/pdf/2013/doctorat/rezumat_teza_Adela_Georgescu.pdf.
5. JIANG Yuchen, et al., Quo vadis artificial intelligence?, *Discover Artificial Intelligence,* 2022, 2.1: 4.
6. JURAFSKY D, Martin J.H., Speech and Language Processing. Prentice Hall, 2008.
7. MANNING C, Schtze H., *Foundation of Statistical Natural Language Procesing*, MIT Press, 1999.
8. NILSSON Nils (1998), *Artificial Intelligence: A New Synthesis,* Morgan Kaufmann, ISBN 978-1-55860-467-4. Archived from the original on 26 July 2020. Retrieved 18 November 2019.
9. NIST IR 8360, Machine Learning for Access Control Policy Verification, Vincent C. Hu Computer Security Division, Information Technology Laborator, September 2021, disponibil la http://nvlpuls.nist/nistpubs/ir/2021/NIST.IR.8360.pdf.
10. NISTIR 8105 „Report on Post-Quantum Cryptography", aprilie 2016.
11. NISTIR 8413-upd1 "Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process", july 2022.
12. NITAJ A., Rachidi T., Applications of Neural Network-Based AI in Cryptography, *Cryptography,* 2023, 7, 39, disponibil la http://mdpi.com/2410-387X/7/3/39;
13. OPREA A, Vassilev A, Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigation (National Institut of Standard and Tehnology, Gaithersburg, MD) NIST Artificial Intelligence, NIST AI 100-2e2023 ipd.
14. Regulament al Parlamentului European și al Consiliului de stabilire a unor norme armonizate privind inteligența artificială (legea privind inteligența artificială) și de modificare a anumitor acte legislative ale Uniunii, Bruxelles, 21.4.2021 COM(2021).
15. ROSPIGLIOSI Pericles 'asher', "Artificial intelligence in teaching and learning: what questions should we ask of ChatGPT?", *Interactive Learning Environments,* 2023, 31.1: 1-3.
16. RUSSEL Stuart J., Norvig Peter, (2021) *Artificial Intelligence: A Modern Approach* (4th ed.), Hoboken, Pearson, ISBN 978-0134610993, LCCN 20190474.
17. SAMUEL AL, Some studies in machine learning using the game of checkers. *IBM Journal of Research and Development,* 1959, 3:210-229.
18. SHOR W. Peter, "Polynomial-time algorithms for prime factorization and discrete logaritms on a qantum computer", *SIAM Journal on Computing*, 26 (5): 1484-1509, 1997.
19. TUFIȘ D., Algorithms and data design issues for basic NLP tools, in Nirenburg S. (ed.), *Language Engineering for Lesser-Studied Languages,* IOS Press, NATO Science for Peace and Security Series-D: Information and Communication Security 2009, 21:3-50.
20. TURING A., "Computing machinery and intelligence", Mind, 1950, 59:433-460.
21. .National Institute of Standards and Technology, U.S. Department of Commerce, *U.S. Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools.* Prepared in response to Executive Order, August 2019, 52 p.

[1] În acest articol vom apela pentru definirea conceptului la lucrările lui Stuart J.Russel, Peter Norvig, *Artificial Intelligence: A Modern Approach* (4th ed.), Hoboken, Pearson, 2021, și Nils Nilsson, *Artificial Intelligence: A New Synthesis,* Morgan Kaufman Publishers Inc.,1998.

[2] Lucrare publicată în 1950, în revista științifică MIND, editată de Asociația MIND și publicată de Oxford University Press.

[3] Testul, conceput de Alan Turing în 1950, este o metodă din domeniul inteligenței artificiale care își propune să răspundă la întrebarea „Pot (sau vor putea) mașinile să gândească?".

[4] Arthur L. Samuel, „Some studies in machine learning using the game of checkers", *Journal of Research and Development,* vol. 3, editor IBM, 1959, p. 210-229.

[5] În definirea conceptului de NLP am apelat la lucrările următoare: Chris Manning, Hinrich Schtze, *Foundation of Statistical Natural Language Procesing,* MIT Press, Cambridge, 1999; Dan Jurafsky, James H. Martin, *Speech and Language Processing,* Prentice Hall, 2008; Dan Tufiș, „Algorithms and data design issues for basic NLP tools", articol publicat în Nirenburg S. (ed.), *Language Engineering for Lesser-Studied Languages,* IOS Press, NATO Science for Peace and Security Series-D: Information and Communication Security 2009, p. 3-50.

[6] Așa cum a fost definit conceptul în lucrările lui Stuart J.Russel, Peter Norvig, *op.cit,* și Nils Nilsson, *op.cit.*

[7] Idem.

[8] Stuart J.Russel, Peter Norvig, *op.cit,* și Alan Turing, „Computing machinery and intelligence", publicat în revista Mind, Oxford University Press, vol. LIX, 1950, p.433-460.

[9] Detalii/analize/implicații asupra aspectelor dezbătute pot fi consultate în mai multe publicații coordonate de NIST de-a lungul timpului. În cadrul acestui articol au fost luate în calcul: 1) U.S. Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools. Prepared in response to Executive Order 13859, NIST, US Department of Commerce, 2019, http://nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf; 2) Alin Oprea și Apostol Vassilev, „Adversarial Machine Learning: A Taxonomy and Terminology of Attaacks and Mitigation", articol publicat de către NIST în NIST AI 100-2e2023 ipd, http://csrc.nist.gov/pubs/ai/100/2/e2023/ipd; 3) Vincent C. HU, Machine Learning for Access Control Policy Verification, NIST, Computer Security Division, 2021 http://nvlpuls.nist/nistpubs/ir/2021/NIST.IR.8360.pdf.

[10] Abderrahmane Nitaj, Tajjeeddine Rachidi, „Applications of Neural Network-Based AI", în Cryptography, 2023, http://mdpi.com/2410-387X/7/3/39.

[11] Algoritm de calculator cuantic pentru găsirea factorilor primi ai unui număr întreg. A fost dezvoltat (1994) de matematicianul american Peter Shor; Shor W. Peter, Polynomial-time algorithms for prime factorization and discrete logaritms on a qantum computer, *SIAM Journal on Computing,* 26(5): 1484-1509, 1997.

[12] 1) Obiecte geometrice care constau în aranjamente regulate de puncte în spațiul euclidian, asemănător spațiilor vectoriale. 2) Mulțimi parțial ordonate; Georgescu-Mihăiță Adela, *Protocoale de grup în criptografia clasică și criptografia bazată pe latici,* teză de doctorat, Universitatea din București, martie 2013, disponibilă la http://old.fmi.unibuc.ro/ro/pdf/2013/doctorat/rezumat_teza_Adela_Georgescu.pdf;

[13] Subiectul a fost abordat în cadrul NIST; pentru mai multe detalii a se vedea NISTIR 8105 „Report on Post-Quantum Cryptography", aprilie 2016, și NISTIR 8413-upd1 „Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process", july 2022.

[14] Christian Bauckhage, Rainer Bye, Ahmed Iftikhar, Christian Knopf, Merima Mustafic, Nico Piatkowski, Roland Stahl, Rafet Sifa, Eldar Sultanow, „Quantum Machine Learning State of The Art and Future Directions", Federal Office for Information Security, http://www.bsi.bund.de.

INTELIGENȚA POZITIVĂ. DINCOLO DE SABOTAJUL MENTAL ȘI AUTO-SABOTAJ

Nicolae SĂVULESCU[*]

Abstract

The article is intended to give an overall picture about that „the voices" in our head which generate negative emotions in the way we handle life's everyday challenges. These „voices" also known as „saboteurs", represent automated patterns in our mind for how to think, feel and respond. They cause all of the stress, anxiety, self-doubt, frustration, restlessness and unhappiness. They sabotage our performance, wellbeing and relationships. These „saboteurs" have a master, "The Judge", who is the universal one that afflicts everyone. The Judge works with one more Accomplice Saboteurs to hijack our mind and cause most of our setbacks. These Accomplice Saboteurs are nine of them and we are going to address each of them in the below article. The Saboteurs start off as our guardians that help us survive the real and imagined threats as children. By the time we are adults, we no longer need them, but they have become invisible inhabitants of our mind. Our Saboteurs patterns of thinking, feeling and reacting become soft-coded in our brain through neural pathways. When these neural pathways are triggered, we are „hijacked" by our Saboteurs and instantly feel, think and act using their patterns.[1]

Keywords*: Positive intelligence; mental sabotage behaviour; saboteurs; Judge; Stickler; Pleaser; Hyper-Achiever; Victim; Hyper-Rational; Hyper-Vigilant; Restless; Controller; Avoider.*

Multe din încercările pe care le facem pentru a ne crește șansele de succes și împlinire de sine se destramă la fel de rapid precum un bolovan ce se rostogolește la vale. Să ne gândim numai. Cum de renunțăm la a realiza o parte din lucrurile pe care ni le propunem la fiecare sfârșit de an? Cum se face că bucuria unei realizări importante este trecătoare, chiar dacă credeam că acel lucru ne va aduce fericirea pe termen lung? De ce aptitudinile ce țin de dezvoltare personală, pe care le dobândim în cadrul unor cursuri, se pierd în fața vechilor obiceiuri?

Suntem cu adevărat torturați și pedepsiți. Dar iată care e ideea. Este vorba de autotortură (în ascunzișul subconștientului monologul este realizat: deja nu-mi place, nu o să-mi iasă, deci nu-l fac pentru că nu-mi trebuie). Motivul pentru care multe din încercările noastre de a obține succes eșuează constă în faptul că ne sabotăm singuri. Mai exact mintea noastră face acest lucru. Mintea ne este atât cel mai bun prieten, cât și cel mai aprig dușman. „Sabotorii" ascunși din minte sunt responsabili pentru majoritatea nereușitelor noastre și fac acest lucru fără ca măcar să ne dăm seama[2].

INTELIGENȚA POZITIVĂ

Mentalul uman este un obstacol redutabil. În cea mai mare parte a timpului ne simțim hărțuiți de propriile îndoieli şi judecăţi tăioase, ce ne consumă energia într-un mod inutil, un conflict interior pe care îl hrănim constant, din care cu greu putem să ieșim, când şi când, ca să emitem cogniții şi, mai apoi, să facem acele lucruri care ne-ar putea pune pe traiectoria visurilor noastre.

Ar trebui să dezvoltăm o afacere, cu noi înșine, pe baza produselor gândirii, punând un mai mare accent pe crearea şi vânzarea de produse pozitive, de întărire emoțională: „Dar dacă nu o să vreau să-mi cumpăr propria idee? Reţeaua mea de distribuitori interni, sinapsele, nu îndrăznește să se dezvolte, pentru că mi se pare că nu prea mă pricep la auto-negocieri şi poate aș pierde mai mult decât aș câștiga. Modelul de lucru *part-time* nu există, fluxul este continuu, dar nu îndrăznesc, pentru că nu se face așa ceva şi pentru că nu vreau să-mi asum acest rol".

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

Pe baza unei idei ca aceasta, Shirzad Chamine[3], psiholog și doctor în neuroștiințe, a scris despre inteligența pozitivă, atenționându-ne asupra puterii sabotorilor mentali și auto-sabotajului, ca elemente prin care acceptăm regresia emoțională, fără să mai acționăm la timp spre reechilibrare.

Shirzad Chamine ne spune că *Inteligența Pozitivă* indică măsura în care deții controlul asupra propriei minți și măsura în care aceasta acționează spre binele tău.

El a creat termenul de PQ – Coeficientul Inteligenței Pozitive - care reprezintă „procentul din timp în care mintea ta acționează mai degrabă ca un prieten decât ca un dușman; sau, cu alte cuvinte, procentul din timp în care mintea te slujește, în loc să te saboteze".

COMPORTAMENTUL DE SABOTAJ MENTAL

Dacă facem referire la un astfel de mod de acțiune, Shirzad Chamine identifică o serie de sabotori interni, care reprezintă tipare mentale automate ce acționează împotriva propriei persoane. El arată că sabotorii sunt un fenomen universal și că întrebarea nu este dacă îi avem, ci pe care îi avem și cât sunt de puternici.

Acesta enumeră 10 sabotori: Judecătorul (Judge-the Master), Maniacul/Perfecționistul (Stickler), Binevoitorul/Conformistul (Pleaser), Hiper-ambițiosul (Hyper-Achiever), Victima (Victim), Hiper-rațonalul (Hyper-Rational), Hiper-vigilentul (Hyper-Vigilant), Neliniștitul/ Neobositul (Restless), Dominatorul/Autoritarul (Controller), Evitantul/Prudentul (Avoider).

Cum să recunoaștem dacă vocea din mintea noastră ne spune adevărul sau ne deformează realitatea? Acele tipare mentale, obiceiuri, credințe, prezumții lucrează de fapt împotriva interesului nostru. La care apelăm fără să ne dăm seama? În care să ne încredem…?

Dacă ar fi să mergem pe premisa pozitivismului, am putea afirma că reușita în viață se bazează pe gândirea pozitivă. Studiile au arătat că oamenii revin la ceea ce cercetătorii numesc „fericirile de bază", manifestate la scurt timp după anumite evenimente sau realizări care le cresc nivelul de fericire[4].

Să cunoaștem mai bine „sabotorii"

Fiecare dintre noi dezvoltă „Sabotori" de timpuriu (în copilărie) pentru a face față aparentelor amenințări ale vieții, la nivel atât fizic, cât și emoțional. Odată ajunși la maturitate, nu mai avem nevoie de EI, dar aceștia au devenit deja locatari invizibili ai minții noastre. De cele mai multe ori nici măcar nu suntem conștienți de existența lor.

Iată o scurtă descriere a fiecăruia dintre ei, menită să ne ajute să ne facem o idee despre cum funcționează fiecare:

1. Judecătorul (Judge): cel mai puternic (stăpânul/the master), cel care ne afectează pe toți, generează stres, furie, dezamăgire, rușine, învinovățire. Ne judecăm pe noi înșine, îi judecăm pe ceilalți sau circumstanțele. Astfel, vocea sa este des confundată cu vocea rațiunii.
2. Maniacul/Perfecționistul (Stickler): ține de nevoia de perfecțiune, ordine și organizare duse la extrem. Stârnește neliniște și încordare celor din jur, determinând o stare de frustrare celor cu care colaborează, prin faptul că ceea ce este efectuat nu e suficient de bine făcut.
3. Binevoitorul/Conformistul (Pleaser): te determină să obții acceptarea și afecțiunea celor din jur, prin recurgerea la flatare, la acțiuni menite să le facă pe plac celorlalți, în mod constant. Te face să pierzi din vedere nevoile proprii și creând, astfel, frustrare, începi să porți pică celorlalți. Îi încurajează pe colaboratori să se bazeze pe tine exagerat de mult.
4. Hiper-ambițiosul(Hyper-Achiever):creează dependență față de performanțele constante și față de rezultatele care susțin respectul de sine și auto-confirmarea. Conduce la tendința de a munci în mod exagerat, într-un ritm imposibil de menținut, căutând validare exterioară și uitând de controlul interior.
5. Victima (Victim): își dorește și reușește să fie emotivă și temperamentală, pentru a obține atenția și afecțiunea (validarea). Își irosește energia mentală și emoțională, iar ceilalți se simt frustrați, neputincioși și vinovați pentru că nu-l pot face niciodată fericit pe termen lung.

6. Hiper-raționalul (Hyper-Rational): implică o concentrare intensă și exclusivă doar pe procesele raționale ale tuturor lucrurilor, inclusiv a relațiilor. Te determină să devii nerăbdător când vine vorba de emoțiile oamenilor, pare rece și distant, manifestând aroganță intelectuală.
7. Hiper-vigilentul (Hyper-Vigilant): provoacă o neliniște puternică și continuă referitor la ce este și la ce ar putea fi. În permanență alert, nu se odihnește, ceea ce duce la stări de stres pentru el și pentru cei din jurul său.
8. Neliniștitul/ Neobositul (Restless): caută provocări din ce în ce mai mari, nu-și permite luxul să simtă mulțumirea reușitelor curente, generând situații care distrag atenția sa și a celor din jur. Pentru că nu se poate ține pasul cu el, se simte o răceală/distanțare față de acesta.
9. Dominatorul/ Autoritarul (Controller): funcționează pe baza unei nevoi anxioase de deținere a puterii, de preluare a controlului asupra situațiilor și de adaptare a acțiunilor oamenilor la propriile nevoi. Rezultatele obținute alături de acesta sunt bune, dar pe termen lung determină resentimente din partea celorlalți pentru că îi împiedică să-și manifeste abilitățile.
10. Evitantul/ Prudentul (Avoider): devine ezitant, se concentrează pe ceea ce este pozitiv și plăcut într-o manieră exagerată. Amână sau evită să facă anumite acțiuni dificile și neplăcute, amăgindu-se că e foarte bine așa[5].

Înțeleptul

„Înțeleptul" este de fapt partea noastră mai profundă și mai „deșteaptă", care poate trece peste conflicte și care rezistă tentației de a fi condusă de dramele și tensiunile momentului, evitând să devină victima păcălelii sabotorilor. Conform acestui mod de gândire, orice provocare cu care ne confruntăm este o oportunitate ce ne transformă, în mod activ, în „ceva sau cineva mai bun".

Dacă ne întrebăm „cum putem slăbi sabotorii?", atunci cel mai simplu, dar și cel mai eficient răspuns ar putea fi: prin forța și puterea *inteligenței pozitive*, reprezentate de Înțelept. Acesta apelează la cinci forțe importante ale minții pentru a „înfrunta" orice provocare ce vine din exteriorul sau din interiorul nostru, prin valorile de adevăr și importanța pe care o conferim acestora.

Dacă ne folosim de aceste forțe, pentru a depăși provocările, vom experimenta emoții și sentimente precum curiozitatea, creativitatea, bucuria, compasiunea, puterea de a lua/asuma decizii, echilibrul psiho-somatic și gândirea profundă.

Cele cinci puncte forte sau cele cinci forțe din mentalul nostru sunt:

1. Empatizarea (Empathize) – fii înțelegător cu tine, acceptă nereușitele; păstrează o atitudine pozitivă, cruță-ți energia;

2. Explorarea (Explore) – caută/descoperă motivele nereușitei proiectului tău; fi curios și păstrează o minte deschisă;

3. Inovarea (Innovate) – transformă descoperirile în soluții noi, creative; „banalul" altora este noua ta perspectivă;

4. Navigarea (Navigate) – alege o direcție nouă; înțelege că ceea ce ți se potrivește ție, alții vor respinge; fi curajos, conștient și calculat;

5. Acțiunea (Activate) – învinge-ți temerile, rămâi pozitiv în acţiunile tale; nu te lăsa influențat de ce a fost, ci concentrează-te pe ce este[6].

Comportamentul de auto-sabotare

Auto-sabotajul se referă la comportamente sau moduri de gândire care țin o persoană în loc și o împiedică să facă ceea ce vrea. Apare atunci când mintea logică și conștientă este în contradicție cu mintea subconștientă.

Comportamentele de auto-sabotare sunt alcătuite dintr-un set complex de acțiuni și gânduri care distrug intențiile bune și afectează negativ relațiile, angajarea, sănătatea, calitatea vieții și bunăstarea emoțională. Este important să înțelegem că, din moment ce comportamentele de auto-sabotare sunt inițial întărite, pe termen scurt permit o ușurare temporară a sentimentelor de anxietate și stres prin evitarea acestora, dar pe termen lung pot duce la posibile stări depresive, stimă de sine scăzută, abuz de substanțe, izolare, plafonare (neactualizarea obiectivelor de viață), înăbușind potențialul de dezvoltare al persoanei.

Auto-sabotajul este un termen umbrelă pentru tot ceea ce poate fi identificat ca având potențial de a dăuna/afecta negativ oportunitățile de carieră, relații sau dezvoltare personală. Sintagma se referă la un întreg flux de comportamente și modele dureroase, adânc înrădăcinate, care au la bază de fapt o iluzie, o credință responsabilă pentru blocajul sinelui adevărat.

Dacă facem referire la un astfel de mod de acțiune, avem în vedere[7]:

Iluzia de auto-sabotaj

Asigurați-vă că vă RECUNOAȘTEȚI și vă FELICITAȚI pentru auto-sabotajul realizat!!! Aceasta este o realizare care poate schimba viața. Recunoașterea acțiunilor de auto-sabotaj este ea însăși o realizare și un pas puternic în responsabilitatea comportamentală. Conștientizarea faptului că aveți o problemă este o declarație care pune transformarea în acțiune. Un contract, prin care acum sunteți dedicat schimbării.

Auto-sabotajul este FAKE NEWS.

Realitatea este că auto-sabotajul intervine atunci când credințele și modelele vechi intră în conflict cu versiunea ta, cea nouă, de „creștere". Obiceiurile și comportamentele noastre nu s-au adaptat la creșterea proprie, ÎNCĂ. Auto-sabotajul este o etichetă a scuzelor dăunătoare pe care le folosim pentru a nu ne oferi ceea ce merităm. Ceea ce par a fi daune provocate de sine, trebuie adesea înțelese la un nivel mai profund și explorate dacă tiparele urmează să fie contestate și schimbate permanent. Pentru a rupe lanțul, trebuie să mergem într-o călătorie de auto-descoperire și auto-acceptare.

Responsabilitate, schimbare și tipare

Realitatea este că, dacă suntem conștienți de comportamentele negative, atunci creăm o poziție prin care putem să devenim responsabili și să realizăm o schimbare. Narațiunea de auto-sabotaj este propriul facilitator personal. Pentru a scăpa de dramă, trebuie să lucrăm la mentalitatea și relația noastră cu acțiunea și transformarea. Să ne întrebăm ce am putea face diferit, în loc de ceea ce facem greșit.

Să învățăm să cerem ajutor și să nu ne mai temem de eșec, deoarece nereușita poate fi un bun profesor.

Dincolo de modelul dăunător al auto-sabotajului se află creșterea personală care ne va împuternici transformarea radicală. Dacă conștientizăm cum stau lucrurile, atunci vom avea puterea să le schimbăm.

Realitatea: procrastinare, valoare de sine scăzută și evitarea durerii

Auto-sabotajul este o justificare care limitează potențialul real. Este un ciclu crud de negare și durere. Alegerea iluziei va duce la frustrare, tristețe, furie și anxietate. Procrastinarea este un factor imens în auto-sabotaj. Înfruntarea realității în jurul motivelor pe care le folosim pentru a susține amânarea.

Auto-sabotajul ascunde, de obicei, o stimă de sine redusă. Această valoare scăzută provine din traume sau nevoi neîndeplinite. Auto-sabotajul permite oamenilor să aleagă o cale ușoară de ieșire, dar acest fapt este doar o buclă de evitare a durerii, care în final va crea perturbări interne serioase. Scopul dezvoltării de sine este să învățăm să avem încredere în noi, astfel încât să ajungem să învățăm din toate situațiile de viață și de la toți cei din jurul nostru, cu măsurarea pertinentă a investiției de timp și a realității pozitive.

Tu ești ce ai pus în tine.

Auto-reflecția și angajamentul față de schimbare reprezintă primii pași într-o călătorie a schimbării. Dezvoltarea personală nu este întotdeauna ușoară, totuși este plină de satisfacții, iar rezultatul primar dorit de multe ori se estompează pe măsură ce călătoria ne conduce la cine suntem cu adevărat.

Trebuie să ne aliniem cu adevărul asumat despre noi. Alinierea cu adevărul este o poveste a încrederii de sine în care ne recunoaștem adevărata valoare și începem să trăim în consecință. Schimbările de mentalitate pentru depășirea iluziilor de auto-înfrângere încep prin a recunoaște că nu ne limităm la etichetele prestabilite de către auto-sabotaj. Trebuie să creăm afirmații pozitive specifice felului de a fi.

Cauzele comportamentului de auto-sabotare[8] sunt:

- *frica de eșec;*
- *nevoia de control;*
- *modelele învățate prin exemplele familiale, instituționale și sociale;*
- *insuficienta îngrijire de sine și conexiune;*
- *lipsa de încredere în sine.*

Modalități prin care ne putem da seama dacă avem un comportament de auto-sabotare[9]:

- Dăm vina pe alții când lucrurile merg prost;
- Alegem să renunțăm atunci când lucrurile nu merg bine;
- Căutăm motive care să justifice amânarea/ întârzierea îndeplinirii unei sarcini;
- Creăm lupte inutile cu familia, prietenii și colegii;
- Simțim dificultate în exprimarea nevoilor.

Recomandări pentru depășirea acestui comportament[10]:

- identificarea și acceptarea acestui comportament;
- aflarea cauzelor;
- exersarea sentimentului de a fi confortabil cu eșecul;
- vorbirea despre acesta;
- identificarea dorințelor și planurilor pertinente pentru viitor.

Mulţi dintre noi ducem lupte grele cu sabotorii noștri şi adesea speranțele şi visurile noastre rămân în eter, rănite și uneori chiar ucise. Dar nu trebuie să fie aşa. Putem să învăţăm să ne împrietenim cu mintea noastră. Din fericire, domeniul psihologiei pozitive (acea ramură a psihologiei care studiază ceea ce trebuie să facem pentru a avea o viaţă fericită şi împlinită) aduce cu ea și remedii.

Principalele sugestii[11] propuse de către specialiști sunt:

Trei lucruri bune. Notează în fiecare zi trei lucruri bune care s-au întâmplat pe parcursul zilei sau trei lucruri pentru care eşti recunoscător. Pare un exerciţiu banal, poate inutil și plictisitor. Imaginează-ţi mintea ca pe o pajiște. Dacă treci de multe ori pe acea pajiște, la un moment dat se formează o cărare. Gândurile tale, prin concentrarea pe pozitiv sau pe negativ, pot crea un drum al crucii sau o potecă liniştită, cu pace şi alinare.

Darurile. Chiar dacă ai decis să te împrieteneşti cu mintea ta, lucruri negative o să se întâmple, fără îndoială. Atunci când o situaţie negativă apare în calea ta, gândeşte-te la felul în care ai putea să o transformi într-o oportunitate. Orice situaţie îţi poate oferi posibilitatea de învăţare sau de creativitate, dacă nu altceva. Te-ai certat cu un prieten? Cum îţi propui să îmbunătățești relaţia dintre voi, pentru ca astfel de certuri să nu mai fie posibile în viitor?

Etichetele. Etichetează gândurile şi sentimentele „Judecătorului", de fiecare dată când îl observi. Adică de fiecare dată când te judeci pe tine însăţi/însuţi sau pe cei din jur. „Nu sunt suficient de deşteaptă", „nu merit", „nu sunt un om bun", „băiatul ăsta e un incompetent", „mama iar se lamentează inutil", „m-ai pus într-o lumină proastă în mod intenţionat". Observă simplul fapt că mintea ta a creat aceste gânduri. E important să cunoşti conţinutul propriei tale minţi, dacă vrei să schimbi modul de gândire. Atunci când recunoşti gândurile nocive, poţi să îţi spui: „Sabotorul îmi spune că nu am nicio şansă.", versus „N-am nicio şansă!". Poţi să observi imediat diferenţa de nuanţă între cele două afirmaţii şi asta e destul ca să pună o distanţă mică, dar importantă, între tine şi gândurile negative.

CONCLUZII

Prin acest articol, nu se reliefează ceva nou, ci din contră, ceva ce cititorul știa deja și poate că nu era denumit astfel, în plan cognitiv. Cu toții ne identificăm un anumit număr de Sabotori, care ne afectează viața de zi cu zi, dar tot noi avem acest potențial extraordinar, numit Inteligență Pozitivă, prin care putem găsi calea cea mai eficientă și durabilă de a ne crește atât propria productivitate, cât și fericirea. Căci, nu-i așa, „de fericirea mea nu este nimeni responsabil, în afară de mine"? Și aici nu încape loc de egoism, ci întru totul este empatie.

Vestea bună este că acum Sabotorii tăi, probabil, nu mai sunt atât de confortabili și puternici, ținând cont că au fost scoși la lumină. Poate chiar li s-a diminuat din forță, prin simpla scoatere la iveală a felului mincinos/a tiparelor distructive de lucru. Poate „Înțeleptul" din tine a devenit conștient de propria prezență și forță și este mai pregătit să facă față modelelor autodistructive de gândire.

De fapt, multe din nefericirile noastre derivă din faptul că noi suntem „aici", dar mintea vrea să fie „acolo" în viitor sau „atunci" în trecut. A fi în prezent, aici și acum, implică acceptarea realității din momentul de față și sentimentul recunoștinței pentru ceea ce suntem[12].

BIBLIOGRAFIE

1. *** https://positiveintelligence.com/saboteurs, accesat la 08.09.2023.
2. *** „Comportamentul de auto-sabotare” disponibil la https://emcbuc.ro/2021-03-29/comportamentul-de-auto-sabotare/, accesat la 08.09.2023.
3. APOSTOIU Ana-Maria, „Rămâi ancorat în prezent. Viața este despre aici și acum”, disponibil la https://www.curteaveche.ro/carticheie/2020-03-18/rămâi-ancorat-în-prezent-viața-este-despre-aici-și-acum/, accesat la 08.09.2023.
4. DISPENZA Joe, *Distruge-ți obiceiurile nocive*, Curtea Veche, București, 2019.
5. LENNON Amanda, „Dincolo de auto-sabotaj este sinele tău adevărat”, disponibil la https://www.theportugalnews.com/ro/stiri/dincolo-de-auto-sabotaj-este-sinele-tau-adevarat/67099, 19.05.2022, accesat la 08.09.2023.
6. SHIRZAD Chamine, *Inteligența pozitivă*, Curtea Veche, București, 2017.

[1] *** „How We Self Sabotage”, disponibil la https://positive intelligence.com/saboteurs.

[2] Chamine Shirzad, *Inteligența pozitivă,* Curtea Veche, București, 2017 (pag. 13-14).

[3] *** https://www.curteaveche.ro/p/inteligenta-pozitivă--shirzad-chamine. Shirzad Chamine a absolvit inclusiv un master în inginerie electrică și un MBA la Universitatea Stanford. De asemenea, a fost CEO al celei mai mari organizații de coaching și training din lume - Coaches Training Institute (CTI). În prezent, susține cursuri la Universitatea Stanford, predând un program de formare și dezvoltare a Inteligenței Pozitive.

[4] Jonathan Haidt, *The Happiness Hypothesis: Finding Modern Truth in Ancient Wisdom,* Basic Books, New York, 2006.

[5] Chamine Shirzad, op.cit.,pag. 35-40.

[6] https://emcbuc.ro/2021/03/29/comportamentul-de-auto-sabotare/

[7] Amanda Lennon, „Dincolo de auto-sabotaj este sinele tău adevărat”, 19.05.2022, https://www.theportugalnews.com/ro/stiri/dincolo-de-auto-sabotaj-este-sinele-tau-adevarat/67099, accesat la 08.09.2023.

[8]-https://emcbuc.ro/2021/03/29/comportamentul-de-auto-sabotare/„Comportamentul de auto-sabotare” Concluziile studiului realizat pentru membri Ordinului Asistenților Medicali Generaliști, Moașelor și Asistenților Medicali din România/OAMGMAMR, filiala București, PSIHO-ASSIST.

[9] Idem.

[10] Idem.

[11] Joe Dispenza, *Distruge-ți obiceiurile nocive,* Curtea Veche, București, 2019.

[12] Ana-Maria Apostoiu, „Rămâi ancorat în prezent. Viața este despre aici și acum”, https://www.curteaveche.ro/carticheie/2020-03-18/rămâi-ancorat-în-prezent-viața-este-despre-aici-și-acum, accesat la 08.09.2023.

FOOD FOR THOUGHT

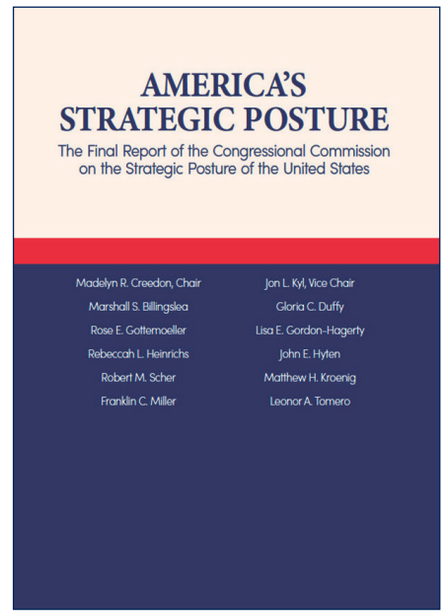
*Secțiunea **#foodforthought** cuprinde o selecție de resurse bibliografice (documente oficiale, cărți și rapoarte), publicate în ultima perioadă, cu impact semnificativ asupra domeniului studiilor de securitate și informații.*

Vasile CREȚU*

DOCUMENTE OFICIALE

Postura strategică a Statelor Unite ale Americii-

Congressional Commission on the Strategic Posture of the United States. "America's Strategic Posture". Final Report. Octombrie 2023. Disponibil online la https://armedservices.house.gov/sites/republicans.armedservices.house.gov/files/Strategic-Posture-Committee-Report-Final.pdf

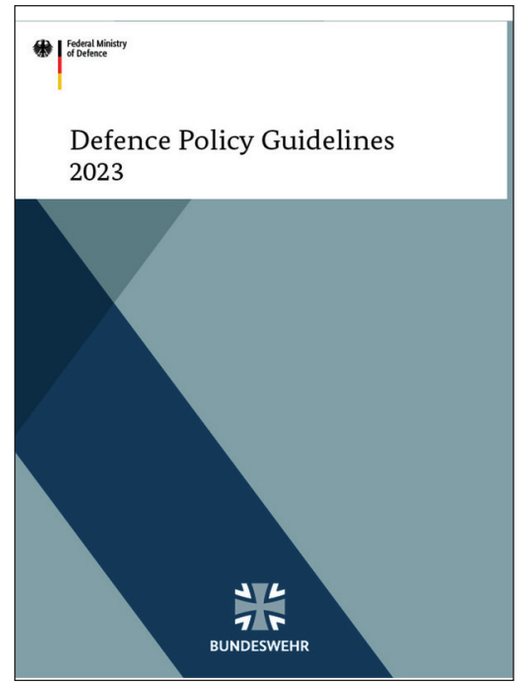


Comisia privind postura strategică a SUA, formată din 12 experți în domeniul apărării și politicii externe, special desemnați de Congresul american, analizează amenințările potențiale pentru perioada 2027-2035, concluzionând că statul american nu are, în acest moment, o strategie cuprinzătoare care să contracareze, simultan, provocările generate de R.P.Chineză și F.Rusă. În acest sens, Comisia stabilește o listă de 81 de recomandări în ceea ce privește (1) strategia; (2) postura strategică; (3) arhitectura și organizarea dimensiunii nucleare a securității naționale; (4) dezvoltarea capabilităților convenționale; (5) relația cu aliații și partenerii și (6) reducerea riscurilor. Referitor la cel de-al cincilea punct, Comisia recomandă Departamentului Apărării să crească interoperabilitatea sistemelor americane cu cele aliate pentru a maximiza descurajarea în diferite regiuni, prin sporirea cooperării tehnologice.

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

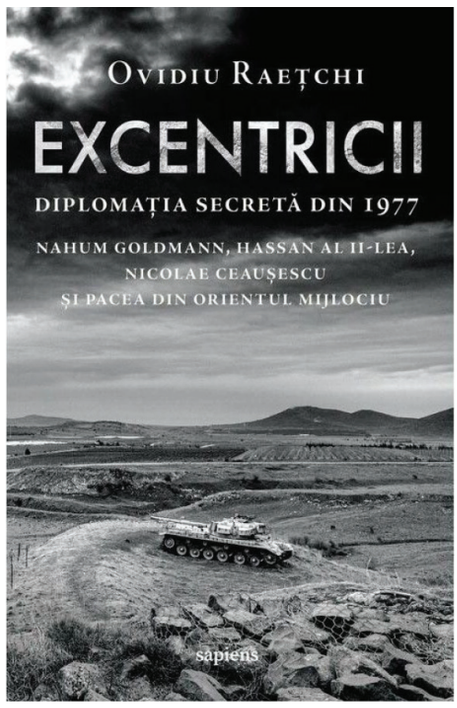
Orientările politicii de apărare a Germaniei

The Federal Ministry of Defence of Germany „Defence Policy Guidelines 2023". Noiembrie 2023. Disponibil online la https://www.bmvg.de/resource/blob/5702804/424c985d964341427afe0b7052090dff/defence-policy-guidelines-2023-data.pdf



Pornind de la prima strategie de securitate națională a Germaniei, adoptată în luna iunie 2023, *Orientările politicii de apărare* creionează locul și rolul Bundeswehr în contextul „schimbării istorice" (*Zeitenwende*), definind o sarcină de bază (apărarea națională și colectivă) și trei sarcini adiționale (promovarea stabilității și sprijinerea creșterii rezilienței partenerilor ca o contribuție la managementul internațional al crizelor; diplomația apărării, cooperarea internațională și dezvoltarea parteneriatelor; asigurarea securității interne și rol de sprijin). Potrivit documentului, Germania este „motorul economic" al centrului Europei, context în care Bundeswehr trebuie să devină „coloana vertebrală" a descurajării și apărării colective pe continentul european.

CĂRȚI



Diplomația secretă și Procesul de Pace din Orientul Mijlociu

RAEȚCHI, Ovidiu. *Excentricii. Diplomația secretă din 1977: Nahum Goldmann, Hassan al II-lea, Nicolae Ceaușescu și pacea din Orientul Mijlociu*, București: Editura Art, 2023

Publicată în contextul tensionării situației de securitate din Orientul Mijlociu, în urma atacului terorist al grupării Hamas din data de 7 octombrie 2023, cartea „*Excentricii*" aduce lumină asupra complexității Procesului de Pace, ilustrând eforturile diplomatice secrete ale României și Marocului (backchannel diplomacy) care au condus la lansarea dialogului oficial dintre Israel și Egipt din noiembrie 1977. Monografia este, de asemenea, reprezentativă pentru rolul de „conciliator" discret jucat de România pe timpul regimului comunist, evidențiind fundamentul obiectivului ulterior al lui Nicolae Ceaușescu de poziționare drept mediator recunoscut în plan internațional.

Consecințele globale ale războiului din Ucraina

BOCANCEA, Sorin (coord.). *Războiul din Ucraina. Un conflict regional cu efecte globale.* Editura Polis Books, 2023.

Volumul, coordonat de Sorin Bocancea, reunește perspectivele a 40 de specialiști din diverse domenii (istorie, științe politice, științe militare, relații internaționale, drept internațional, economie, jurnalism și comunicare) cu privire la cauzele, evoluțiile și consecințele războiului din Ucraina, atât asupra României, cât și la nivel global. Cartea oferă, așadar, o radiografie a conflictului ruso-ucrainean, contribuind la dezbaterea specifică din mediul academic românesc, pe următoarele dimensiuni: (1) istoria Rusiei și Ucrainei; (2) perspective istorice, culturale și ideologice asupra regimului Putin; (3) dispozitivele de război ale actorilor implicați; (4) cadrul juridic internațional; (5) implicațiile psihologice; (6) efectele resimțite în România și Republica Moldova; (7) reacții internaționale și (8) consecințe geostrategice.

RAPOARTE, STUDII

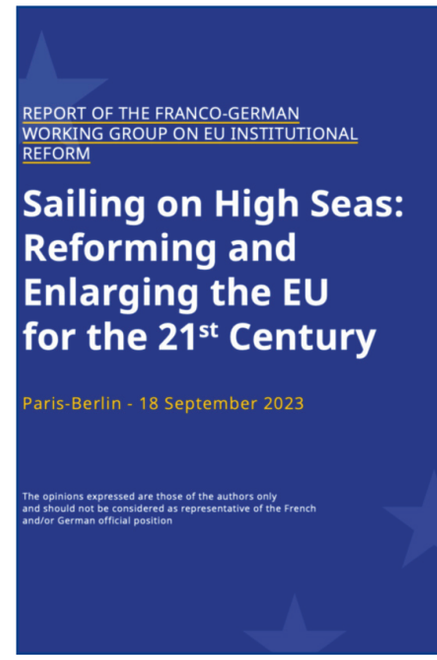
Tendințele transatlantice – opinii în rândul cetățenilor din 14 state

German Marshall Fund of the US. „2023 Transatlantic Trends". 12.09.2023. Disponibil online la https://www.gmfus.org/sites/default/files/2023-09/TT2023_digital-3.pdf

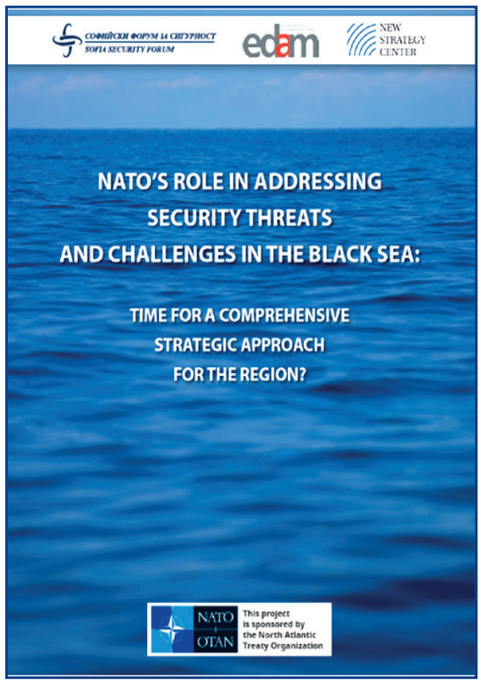
Cea de-a patra ediție a raportului „Tendințe Transatlantice", elaborat de German Marshall Fund of the US, prezintă rezultatele unui sondaj realizat în 14 state (Canada, Franța, Germania, Italia, Lituania, Marea Britanie, Polonia, Portugalia, Regatul Țărilor de Jos, România, Spania, Suedia, Turcia și SUA), evidențiind opiniile cetățenilor cu privire la ordinea globală, relațiile transatlantice, securitatea și apărarea internațională, relațiile cu China, precum și provocările globale. Printre concluziile studiului se remarcă: procentaje similare referitoare la percepția că SUA vor rămâne în continuare cel mai influent actor, respectiv că statul chinez va prelua această poziție; așteptările crescute privind consolidarea acțiunilor UE în domeniul apărării și securității; desemnarea migrației și schimbărilor climatice drept cele mai presante provocări de securitate.

Reformarea UE în perspectiva unui nou val de aderare

Franco-German Working Group on EU Institutional Reform. "Sailing on High Seas: Reforming and Enlarging the EU for the 21st Century". 18.09.2023. Disponibil online la https://www.auswaertiges-amt.de/blob/2617206/4d0e0010ffcd8c0079e21329bbbb3332/230919-rfaa-deu-fra-bericht-data.pdf



Grupul de Lucru Franco-German, format din 12 experți în afaceri europene, analizează maniera în care UE ar trebui să fie reformată pentru a crește capacitatea organizației de a acționa, a pregăti viitorul val de aderare și a întări statul de drept și legitimitatea democratică a constructului european. Raportul cuprinde atât recomandări pe termen scurt (până la alegerile europarlamentare din iunie 2024), cât și unele pe termen mediu și lung, propuse a fi implementate pe timpul următorului ciclu instituțional. Printre acestea, cele mai ambițioase sunt prevederile referitoare la revizuirea Tratatelor și generalizarea adoptării deciziilor cu majoritate calificată în Consiliul EU.



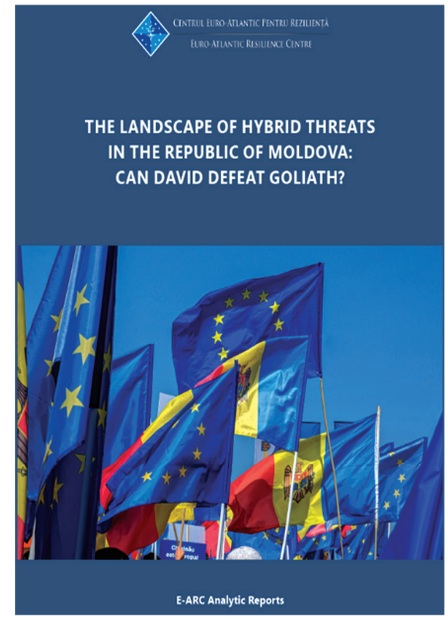
Rolul NATO în gestionarea amenințărilor și provocărilor din regiunea Mării Negre

The Centre for Economics and Foreign Policy Studies (EDAM), The New Strategy Center and The Sofia Security Forum. "NATO's role in addressing security threats and challenges in the Black Sea: Time for a comprehesive strategic approach for the region?". Noiembrie 2023. Disponibil online la https://newstrategycenter.ro/wp-content/uploads/2023/11/Security-threats-and-challenges-in-the-black-sea-web.pdf

Elaborat în comun de către trei think-tank-uri din România, Bulgaria și Turcia, raportul evidențiază principalele amenințări și provocări pe care statele din regiunea Mării Negre trebuie să le gestioneze și oferă recomandări de acțiune pentru cooperarea regională și pentru NATO. Printre acestea se numără: crearea unui cadru de cooperare militară regională pentru Marea Neagră, consolidarea capabilităților de interdicție regională și restricționare a accesului (A2/AD) și a celor anti-submarin, pregătirea pentru o potențială reocupare a Insulei Șerpilor de către F.Rusă și reflectarea unei atenții sporite asupra M.Negre în documentele strategice aliate.

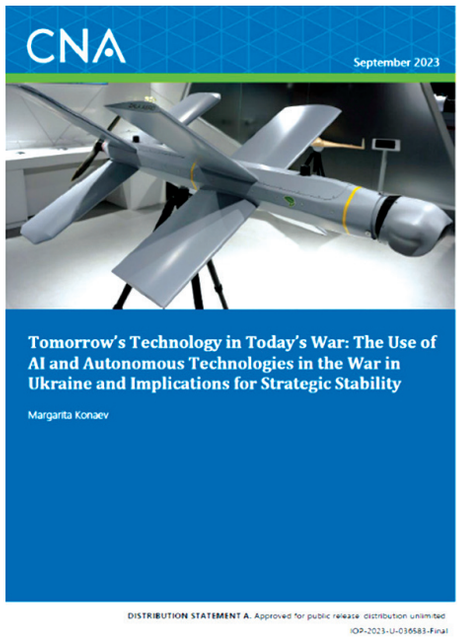
Manifestarea amenințărilor hibride ruse la adresa Republicii Moldova

The Euro-Atlantic Resilience Centre (E-ARC). "The Landscape of Hybrid Threats in the Republic of Moldova: Can David Defeat Goliath?". E-ARC Analytic Reports. Octombrie 2023. Disponibil online la https://e-arc.ro/wp-content/uploads/2023/10/THE-LANDSCAPE-OF-HYBRID-THREATS-IN-THE-REPUBLIC-OF-MOLDOVA.pdf



Uilizând cadrul conceptual privind amenințările hibride dezvoltat la nivelul UE, Centrul Euro-Atlantic pentru Reziliență analizează instrumentarul hibrid rus aplicat în Republica Moldova de la debutul războiului din Ucraina. Astfel, raportul evidențiază că strategia F.Ruse se bazează pe: (1) crearea și exploatarea dependențelor economice și a celor de infrastructură; (2) operații cibernetice; (3) încălcarea spațiului aerian și acțiuni militare și paramilitare; (4) crearea și valorificarea diviziunilor sociale; (5) sprijin politic; (6) acțiuni de dezinformare și propagandă.

Implementarea tehnologiilor viitorului în războiul din Ucraina



KONAEV, Margarita. "Tomorrow's Technology in Today's War: The Use of AI and Autonomous Technologies in the War in Ukraine and Implications for Strategic Stability". Center for Naval Analyses. Septembrie 2023. Disponibil online la https://www.cna.org/reports/2023/10/Use-of-AI-and-Autonomous-Technologies-in-the-War-in-Ukraine.pdf

Studiul, elaborat de Centrul pentru Analize Navale, oferă o imagine de ansamblu asupra utilizării inteligenței artificiale și a tehnologiilor autonome de către Ucraina și F.Rusă, atât pe câmpul de luptă, cât și în plan virtual, evidențiind, deopotrivă, acțiunile statale, precum și cele comerciale. Totodată, raportul pune accent asupra menținerii stabilității strategice, indicând necesitatea unor măsuri de creștere a încrederii (confidence building measures/CBMs) între SUA și F.Rusă, pentru a facilita transparența și a evita interpretări eronate care pot conduce la incidente și escaladarea situației.