Anul XVIII nr. 1/2026

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

TRANSFORMAREA MILITARĂ

INTELLIGENCE

CULTURĂ ORGANIZAȚIONALĂ

SECURITATE ȘI TEHNOLOGII EMERGENTE

DESCURAJAREA ADAPTIVĂ ÎN MAREA NEAGRĂ. INTELIGENȚA ARTIFICIALĂ, COERCIȚIA MARITIMĂ ȘI LOGICA PARADOXALĂ A SECURITĂȚII EXTINSE A ROMÂNIEI

Silviu NATE*

Abstract

This article proposes an integrated analytical framework for adapting Romania's security posture to the defining challenges of modern conflict by integrating Artificial Intelligence (AI) into kinetic military operations, using maritime blockade and coercion as pressure tools below the threshold of armed conflict, and capitalizing on emerging geoeconomic dynamics articulated around the TRIPP Corridor and trans-Caspian connectivity. The approach leverages a triptych of complementary analyses consisting of a study of the AI-based maritime security architecture in the western Black Sea, a comparative analysis of blockade and quarantine scenarios in the Taiwan Strait and the Black Sea, as well as an examination of the "paradoxical logic" from Edward Luttwak's conceptualization applied to the extended Black Sea space against the backdrop of China-Russia strategic convergence.

The central argument is that Romania is at the intersection of three structural transformations such as the military AI revolution, the consolidation of the coercive arsenal of revisionist powers below the threshold of war, and the reorientation of transcontinental connectivity routes that simultaneously generate increased vulnerabilities and unprecedented opportunities for anchoring in the Western security architecture. The appropriate strategic response cannot be one-dimensional, but based on an adaptive deterrence architecture, which combines AI capabilities, anti-blockade resilience, asymmetric deterrence, and connectivity diplomacy.

Keywords: *Artificial Intelligence; Black Sea; Romania; maritime blockade; TRIPP Corridor; paradoxical logic; adaptive deterrence; China-Russia tactical convergence; gray area; Neptun Deep; Montreux Convention.*

* ***Conf. univ. dr. Silviu NATE este directorul Centrului de Studii Globale, Universitatea „Lucian Blaga“ din Sibiu.***

CONFIGURAȚIA UNEI CONJUNCTURI STRATEGICE EXCEPȚIONALE

În 03 ianuarie 2026, forțele speciale americane au executat în Caracas un raid care a dus la capturarea președintelui venezuelean Nicolás Maduro. Dincolo de relevanța sa geopolitică imediată, operațiunea a marcat un moment de inflexiune în istoria militară modernă, respectiv admiterea publică a utilizării unui model de inteligență artificială comercial – Claude, dezvoltat de compania Anthropic – în fluxul decizional operațional al unei acțiuni cinetice clasificate, prin intermediul Platformei AIP a Palantir Technologies, pe rețelele de nivel Impact Level 6[1] [2] [3]. Această integrare nu a fost un experiment de laborator, ci o demonstrație operațională în condiții reale, cu implicații directe pentru modul în care forțele armate moderne vor fi organizate, echipate și adaptate, inclusiv doctrinar, într-un viitor nu foarte îndepărtat.

Simultan, în bazinul Mării Negre se petreceau evoluții cel puțin la fel de semnificative. Drone rusești violau spațiul aerian românesc în luna septembrie 2025, iar fragmente de UAV au fost recuperate în apropiere de Tulcea în noiembrie 2025[4]. În plan politic, negocierile privind proiectul energetic Neptun Deep și deciderea traseelor Coridorului de Mijloc readuceau în atenția publică rolul strategic al României ca nod de conectivitate transcontinentală[5]. Totodată, documente strategice internaționale mai recente, cum ar fi Raportul Pentagonului privind puterea militară a Republicii Populare Chineze[6], și studiile unor think tank-uri prestigioase (precum CSIS, RAND și AEI) despre scenariile unei blocade chineze asupra Taiwanului converg analitic spre exemplificarea coerciției maritime sub pragul conflictului armat ca instrument preferat al puterilor revizioniste[7] [8] [9].

Prezentul articol își propune integrarea acestor fire analitice într-un cadru coerent, structurat în jurul a trei argumente principale:

- precedentul operațional stabilit prin utilizarea AI în operațiunea Maduro nu este izolat, ci reprezintă un precursor al integrării sistemice a inteligenței artificiale în arhitecturile de securitate – cu implicații (in)directe pentru postura maritimă a României în Marea Neagră;
- blocada și coerciția maritimă, analizate comparativ în teatrele Taiwan și Marea Neagră, configurează un arsenal de presiune sub pragul războiului sau Articolului 5 al NATO și față de care România prezintă vulnerabilități specifice, fiind nevoită să-și construiască și consolideze reziliența;
- cadrul teoretic oferit de cunoscutul politolog Edward Luttwak, privind logica paradoxală a strategiei, ne poate explica de ce investiția în conectivitate economică (TRIPP, BSSC, Neptun Deep, Constanța), deși generatoare de noi ținte strategice, rămâne singura cale sustenabilă de consolidare a securității pe termen lung[10].

Lecțiile extrase din conflictele armate actuale nu sunt noțiuni abstracte, ci conferă cadrului analitic propus o relevanță direct aplicabilă, prin articularea recomandărilor concrete pentru planificatorii apărării și decidenții politici români.

NOUL MEDIU OPERAȚIONAL ȘI CONVERGENȚA PROVOCĂRILOR MARITIME

Transformarea calculului de securitate în Marea Neagră

Invazia F.Ruse în Ucraina (februarie 2022) a reconfigurat radical mediul de securitate în bazinul Mării Negre. România, stat NATO de primă linie pe flancul sud-estic al Alianței, se confruntă cu un spectru de amenințări pe multiple dimensiuni: violări repetate ale spațiului aerian național de către drone rusești, mine marine derivate din teatrul ucrainean, amenințări directe la adresa infrastructurii energetice offshore (proiectul Neptun Deep) și perturbarea rutelor comerciale maritime critice pentru lanțurile europene de aprovizionare[11].

Strategia Națională de Apărare pentru 2025-2030 identifică explicit aceste amenințări, subliniind necesitatea cooperării consolidate cu Turcia și Bulgaria pentru protejarea infrastructurii

energetice și de telecomunicații[12]. Bugetul apărării în 2025 (2,24% din PIB, cu intenția de creștere la 2,5%) reflectă conștientizarea acestor provocări la nivel decizional, materializată în achiziții de aeronave F-16 și F-35, sisteme Patriot, dar mai ales prin pivotarea strategică spre sistemele fără pilot și anularea achizițiilor de submarine în favoarea vehiculelor autonome[13].

Convergența strategică China-Rusia ca factor structural

Un element definitoriu al noului mediu operațional, a cărui relevanță depășește teatrul regional al Mării Negre, este convergența operațională dintre strategiile coercitive ale F.Ruse și R.P. Chineze. Documentul *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2025* evidențiază modul în care ambele puteri utilizează o abordare de tipul „whole-of-government" pentru constrângerea adversarilor, combinând izolarea diplomatică, operațiunile informaționale, presiunile economice și acțiunile militare sub pragul conflictului armat. Exercițiile Joint Sword-2024 A/B ale Armatei Populare de Eliberare/ PLA (R.P. Chineză), cu peste 3.000 de violări ale zonei de apărare aeriană taiwaneze, integrând Garda de Coastă și miliția maritimă[14], oglindesc la nivel conceptual tacticile rusești din Marea Neagră – hărțuire sistematică, ambiguitate juridică și calibrare sub pragul de răspuns al NATO.

Convergența acestor metode nu este neapărat întâmplătoare. Atât R.P. Chineză, cât și F.Rusă percep amenințările prin grila defensivă în raport cu influența occidentală, justificând acțiunile hibride ca protecție a unui „excepționalism civilizațional". Această simetrie doctrinară explică paralelismul evident dintre blocada de facto a porturilor ucrainene în perioada anilor 2022-2025 și scenariile de carantinare a Taiwanului analizate de CSIS[15], în cadrul cărora ambii actori urmăresc impunerea costurilor economice maxime cu risc minim de escaladare formală. Potrivit German Marshall Fund of the United States, o invazie chineză directă este improbabilă deoarece ar implica pierderi estimate de 100.000 soldați ai PLA și un impact economic global de 2 până la 10 trilioane USD[16], confirmând predilecția marilor puteri revizioniste pentru scenarii și planuri de dominație instrumentate sub pragul războiului.

PRECEDENTUL OPERAȚIONAL ȘI INTELIGENȚA ARTIFICIALĂ ÎN OPERAȚIILE MILITARE CINETICE

Operațiunea Maduro și paradigma fuziunii multisursă

Utilizarea confirmată a modelului Claude în cadrul operațiunii din Venezuela introduce o distincție esențială față de utilizările anterioare ale Inteligenței Artificiale (IA) în mediile militare. Modelul nu a operat în cadrul funcțiilor administrative sau de planificare pre-misiune, ci a fost încorporat direct în fluxul decizional operațional pe durata angajamentului activ. Implementat prin Platforma AIP a Palantir Technologies pe rețelele clasificate IL6, Claude a sintetizat intelligence din spectrul SIGINT, HUMINT, OSINT și imagistică satelitară, furnizând suport analitic în timp real[17] [18] [19]. Acest fenomen reprezintă un salt calitativ față de utilizările anterioare, IA devenind agent operațional, nu doar instrument de planificare.

Arhitectura tehnică a „operațiunii Maduro" urmează paradigma *„fuziunii multi-sursă",* prin capacitatea integrării fluxurilor de informații din discipline sau ramuri de colectare fundamental diferite într-un produs analitic coerent și actualizat în timp real. Fără un strat de fuziune IA, datele generate de senzorii multipli rămân fragmentate și sub-exploatate, trimițându-ne la situația cu care se confruntă arhitectura de securitate maritimă a României, dispunând de o colecție valoroasă de platforme (drone V-BAT, Bayraktar TB2, MQ-9B SeaGuardian, Watchkeeper X, baterii costiere NSM, radare AIS), dar pe care le utilizează prin canale separate, fără integrare sistemică[20].

De la operații episodice la supraveghere persistentă

Totuși, diferența esențială între cazul Venezuela și realitatea Mării Negre rezidă din tempoul operațional. Operațiunea Maduro a fost

un angajament concentrat, limitat în timp – o problemă de procesare intensivă în *rafale* (burst processing). Securitatea Mării Negre impune o cerință fundamental diferită prin conștientizare situațională (situational awareness) persistentă, non-stop, pe un domeniu maritim vast, cu monitorizare continuă a activităților navale și aeriene rusești, protecția infrastructurii offshore și coordonare multinațională[21]. Un sistem de IA optimizat pentru suport de tip raid trebuie re-arhitecturat fundamental, trecând de la procesare în rafale la funcții analitice continue, alimentate de fluxuri de date în timp real.

Arhitectura de securitate maritimă pe cinci straturi propusă pentru România urmează această logică: stratul senzorial (V-BAT, SeaGuardian, radare costiere, AIS), stratul analitic AI (motor de fuziune multisursă cu Imagine Operațională Comună în timp real), stratul descurajării active prin sisteme autonome, stratul de apărare costieră asistată de AI și stratul cooperării regionale[22]. Această arhitectură demonstrează că principiile tehnologice validate operațional în Venezuela – fuziunea multisursă, suportul decizional în timp real și integrarea clasificată – sunt transferabile și scalabile la cerințele unui teatru maritim persistent.

Abordarea strategică a UE pentru Marea Neagră, din mai 2025, prevede înființarea Hub-ului European de Securitate Maritimă la Constanța[23], care ar reprezenta locul natural pentru implementarea unui strat unificat de ingestie și standardizare a datelor, conform standardelor STANAG, practic contrapartea instituțională a Platformei AIP Palantir în versiunea sa europeană.

BLOCADA CA INSTRUMENT DE COERCIȚIE SUB PRAGUL CONFLICTULUI ARMAT

Cadrul conceptual și lecțiile din Taiwan

Distincția conceptuală dintre „blocadă” și „carantină”, introdusă în lexicul strategic după Criza Rachetelor din Cuba (1962) și reactualizată de CSIS în contextul taiwanez, are implicații operaționale directe. *Blocada* este interpretată ca act de război în dreptul internațional și interzice accesul tuturor navelor într-o zonă delimitată, iar *carantina*, condusă de forțe de aplicare a legii, cum ar fi paza de coastă, nu constituie în sens formal un act de război, punând adversarul într-o poziție dificilă de răspuns[24]. Tocmai această ambiguitate juridică face din carantină instrumentul preferat, permițând impunerea unor costuri economice devastatoare, evitând simultan declanșarea unui răspuns militar colectiv.

Raportul elaborat de RAND Corporation (2022) privind implicațiile unei carantine coercitive aplicate Taiwanului de către Republica Populară Chineză evidențiază că obiectivul unei asemenea operațiuni nu este izolarea completă a insulei, ci demonstrarea suveranității de facto prin controlul spațiului aerian și maritim[25]. La rândul său, Raportul CSIS, din septembrie 2024, cartografiază scenariul concret: Beijingul ar putea impune „reguli vamale extinse” fără utilizarea termenului de „carantină” sau „blocadă”, solicitând declarații vamale prealabile tuturor navelor[26]. Aproximativ 90% dintre experții americani și 62% dintre cei taiwanezi consultați de CSIS sunt de acord că R.P. Chineză deține capabilitățile necesare pentru o carantină și doar 27% dintre aceștia consideră că ar putea executa o invazie amfibie[27]. Un alt raport, realizat de American Enterprise Institute/ AEI, argumentează că scenariul coerciției graduale, mult mai probabil decât invazie sau blocadă militară totală, a primit o atenție analitică insuficientă din partea planificatorilor occidentali[28].

Blocada rusă în Marea Neagră – mecanisme și contra-strategie

F.Rusă a implementat de facto o blocadă a porturilor ucrainene din Marea Neagră, începând cu invazia din februarie 2022, prin mecanisme care reflectă fidel logica carantinei din „zona gri”, prin poziționarea navelor de război, minarea rutelor comerciale, avertizări pentru navigația civilă și lovituri asupra infrastructurii portuare[29]. După retragerea din Inițiativa Cerealelor a Mării Negre (iulie 2023), Moscova a avertizat că navele îndreptate spre porturile ucrainene vor fi considerate „potențiale transportoare de marfă militară”[30]. Institutul Lieber de la West Point (SUA) a concluzionat că niciuna dintre acțiunile F.Ruse nu poate fi reconciliată conceptului tradițional de *blocadă navală* (potrivit dreptului războiului naval), dar efectele practice ale acestor acțiuni sunt comparabile cu o blocadă[31].

O lecție critică, direct transferabilă scenariului românesc, privește rolul pieței asigurărilor. RUSI (Royal United Services Institute), un cunoscut think-tank britanic, a subliniat că „efectul asigurărilor" a devenit probabil cea mai eficientă armă a blocadei. Simpla amenințare determină companiile de asigurări să majoreze dramatic primele sau să retragă complet acoperirea[32] (de exemplu, compania de asigurări Lloyd's a majorat primele pentru Marea Neagră cu 20-25% doar la debutul tensiunilor). Arma invizibilă operează identic în ambele teatre, confirmând că *blocada eficientă nu este o acțiune militară punctuală, ci un ecosistem de presiune care integrează amenințări militare, manipulare juridică, presiune economică indirectă și război informațional*.

Contra-strategia ucraineană a demonstrat că este posibilă spargerea blocadei fără o forță navală convențională. Dronele maritime (cost unitar sub 250.000 USD) au scufundat sau avariat nave de război rusești de miliarde de dolari, forțând retragerea Flotei Mării Negre a Federației Ruse din spațiul vestic al Mării Negre[33]. Coridorul umanitar costier, prin apele mai puțin adânci ale României și Bulgariei, unde submarinele ruse nu pot opera în proximitatea teritoriului NATO, a transformat o limită geografică în avantaj operațional. Portul Constanța a înregistrat niveluri record, devenind nod alternativ pentru exporturile de cereale ucrainene[34].

Factorul Montreux și specificul Mării Negre ca spațiu maritim semi-închis

Marea Neagră prezintă o caracteristică geostrategică fundamental diferită de Strâmtoarea Taiwan – este un spațiu maritim semi-închis, controlat de Turcia prin Convenția de la Montreux (din 1936). Această Convenție acordă Turciei dreptul de a reglementa tranzitul navelor de război, inclusiv închiderea strâmtorilor Bosfor și Dardanele în timpul unui conflict militar, limitând staționarea navelor statelor neriverane la maximum 21 de zile[35]. După invazia rusă din Ucraina, din 2022, Turcia a invocat Convenția pentru închiderea strâmtorilor și blocarea accesului navelor de război ale „puterilor beligerante", producând un efect dublu: F.Rusă nu și-a putut consolida Flota Mării Negre, dar și forțele navale NATO ale statelor neriverane sau extraregionale au fost private de capacitatea intervenției maritime în sprijinul Ucrainei[36].

Această arhitectură geostrategică reconfigurează calculul de securitate pentru România în moduri paradoxale, iar cadrul conceptual al lui Edward Luttwak contribuie semnificativ la clarificarea sa. Limitarea structurală impusă de Convenția de la Montreux, ca aparentă vulnerabilitate, prin interzicerea unei prezențe navale aliate substanțiale se transformă simultan într-o oportunitate, obligând statele costiere (România, Bulgaria și Turcia) să dezvolte capabilități autonome dintre cele mai eficiente în spații maritime restrânse, unde navele de suprafață mari reprezintă ținte vulnerabile.

LOGICA PARADOXALĂ A SECURITĂȚII EXTINSE A ROMÂNIEI PRIN LENTILA CONCEPTUALĂ LUTTWAK

Cele cinci paliere ale strategiei și tensiunile acestora

Edward Luttwak, în lucrarea sa fundamentală *Strategy: The Logic of War and Peace*, argumentează că întregul domeniu al strategiei este guvernat de o logică paradoxală, fundamental diferită de logica liniară aplicabilă în celelalte sfere ale vieții[37]. Succesul poate genera eșec prin supraextindere, victoria poate fi transformată în înfrângere, iar între cele cinci paliere strategice – tehnic, tactic, operațional, de teatru și mare strategie – nu există armonie naturală. În consecință, o decizie corectă la nivel tactic poate produce cel mai prost rezultat operațional.

Pe *palierul tehnic*, Marea Neagră oferă ilustrarea contemporană cea mai dramatică a paradoxului invocat de Luttwak. Dronele maritime ucrainene (cost unitar sub 250.000 USD) au scufundat sau avariat nave de război cu o valoare cumulată de miliarde de dolari, inclusiv crucișătorul Moskva. Inversiunea tehnică este completă, dar paradoxul operează și în sens invers. Minele derivate, o tehnologie specifică secolului XIX, rămân una dintre cele mai eficiente arme de interdicție, amenințând

proiectul cablului submarin pentru transport de energie și comunicații prin fibră optică din Marea Neagră (Black Sea Submarine Cable/ BSSC), precum și operațiunile Neptun Deep[38].

În cadrul *palierului operațional*, Luttwak distinge între războiul de uzură (care eșuează grațios, dar reușește cumulativ) și cel de manevră (care eșuează catastrofal, dar reușește cu resurse minime). Operațiunile din „zona gri", specifice carantinei graduale chineze, și blocada de facto rusă sunt operațiuni de uzură strategică care reușesc cumulativ. Pe de altă parte, contra-strategia ucraineană a scos în evidență oportunitatea manevrei operaționale, trecând de la forța navală convențională la drone maritime și la coridorul costier, transformând slăbiciunea structurală, respectiv absența marinei, în forță sau capabilitate[39].

Ecosistemul conectivității ca sursă dublă între putere și vulnerabilitate

Pe *palierul marii strategii*, Luttwak introduce conceptul de „suasiune armată" (armed suasion) – în traducere: utilizarea forțelor militare pentru influențarea comportamentului fără declanșarea unui conflict deschis[40]. Acest palier descrie perfect atât strategia imperială rusă în Marea Neagră, orientată spre subordonarea tuturor statelor costiere față de interesele Moscovei, pentru exercitarea dreptului de veto asupra opțiunilor acestora[41], cât și contra-strategia NATO prin descurajare extinsă.

Paradoxul central al „marii strategii" românești, dacă poate fi numită așa, derivă cu claritate prin cadrul lui Edward Luttwak, înțelegând următoarea relație: *cu cât România devine mai importantă din punct de vedere geoeconomic* (hub al coridorului Trump Route for International Peace and Prosperity/ TRIPP, terminal al The Black Sea Submarine Cable/ BSSC, nod logistic prin intermediul Portului Constanța, producător și furnizor energetic – Neptun Deep)*, cu atât devine o țintă mai atractivă pentru coerciția rusă, dar și un activ mai valoros pentru protecția occidentală.* Investiția în conectivitate este, simultan, atât sursa securității prin integrare în rețelele transcontinentale, cât și sursa vulnerabilității, prin crearea unor ținte de mare valoare. Rezolvarea paradoxului nu o reprezintă evitarea investiției, ci complementarea sa obligatorie cu descurajarea asimetrică[42].

TRIPP, BSSC ȘI ECOSISTEMUL DE CONECTIVITATE AL ROMÂNIEI

TRIPP ca braț occidental al Coridorului de Mijloc

În 8 august 2025, reuniunea trilaterală găzduită de președintele D.Trump la Casa Albă a generat Coridorul TRIPP (Trump Route for International Peace and Prosperity), o rută multimodală de 42-43 km prin sudul Armeniei (provincia Syunik), care conectează Azerbaidjanul continental cu enclava sa Nahicevan. Cadrul de implementare, publicat în 13 ianuarie 2026, prevede o companie de dezvoltare în cadrul căreia SUA dețin 74% din acțiuni pentru primul termen de 49 de ani, cu drepturi de dezvoltare exclusive pe 99 de ani[43]. Experții de la Atlantic Council evaluează că TRIPP poate deveni unul dintre cele mai semnificative rezultate de politică externă ale celui de-al doilea mandat Trump[44].

Valoarea reală a conectivității TRIPP devine evidentă ca braț occidental al Coridorului de Mijloc[45] (Middle Corridor/ Trans-Caspian International Transport Route). Înainte de 2022, peste 90% din traficul feroviar Europa-Extremul Orient tranzita Ruta Nordică prin Rusia. După 2022, transporturile prin Ruta Nordică au scăzut cu 40%, în timp ce volumele prin Coridorul de Mijloc au crescut cu peste 60% anual[46]. Comisia Europeană a publicat, în februarie 2026, un meta-studiu care estimează creșterea de patru ori a volumelor comerciale din 2022, cu o triplare previzionată până în 2030[47]. Coridorul de Mijloc se bifurcă spre vest, după traversarea Mării Caspice, spre ramura nordică, ce traversează Georgia și Marea Neagră, ajungând în Bulgaria, România și Ucraina, oferind portului Constanța potențialul transformării într-un veritabil nod și terminal european.

BSSC și Neptun Deep – dublă securitate și dublă vulnerabilitate

Proiectul cablului submarin al Mării Negre/ BSSC – 1.195 km. (1.100 km. submarin) de la Anaklia (Georgia) la Constanța, cu o capacitate de 1.000-1.500 MW și o linie de fibră optică paralelă

– transformă România dintr-un consumator net într-un hub de tranzit energetic, canalizând electricitate verde din Caucaz (cu potențial de 157 GW eolian offshore din Marea Caspică) către rețeaua europeană[48]. Inclus, în decembrie 2025, pe lista Proiectelor de Interes Comun ale UE și consolidat prin memorandumul semnat de Transelectrica și Georgian State Electrosystem, în februarie 2026[49], BSSC creează deopotrivă o nouă dimensiune a relevanței românești, dar și o nouă vulnerabilitate.

Incidentele din Marea Baltică (2023-2025) implicând nave rusești sau chinezești, suspectate de avarierea deliberată a cablurilor submarine (Newnew Polar Bear, Eagle S), și tăierile cablurilor din jurul Taiwanului (TPE Cable System și TPKM3) în 2025 constituie avertismente directe[50]. Cablul BSSC (1.195 km), conductele Neptun Deep și cablurile de telecomunicații din Marea Neagră se înscriu în tiparul vulnerabilității demonstrate din ambele teatre. Protecția simultană a acestor infrastructuri critice submarine creează nevoia convergentă ce justifică funcționalitatea unui sistem integrat de supraveghere subacvatică cu drone submarine, senzori pasivi și patrulare asistată de IA.

Sabotajul infrastructurii critice submarine de la Marea Baltică la Marea Neagră

Un vector de amenințare cu relevanță directă pentru România, specific convergenței celor două teatre, este sabotajul infrastructurii submarine. Incidentele din Marea Baltică cu nave rusești sau chinezești suspectate de tăierea deliberată a cablurilor energetice și de date, dar și din jurul Taiwanului, nu reprezintă anomalii ci un tipar (pattern) sistematic de testare a vulnerabilităților maritime[51]. În urma lecțiilor comune ale celor două teatre și în contextul conflictului ruso-ucrainean, sabotajul infrastructurii submarine devine un instrument predilect de coerciție hibridă pentru agresor, efectul fiind imediat și costisitor, atribuirea dificilă, iar pragul de răspuns destul de neclar.

Convergența dintre BSSC (1.195 km de conectivitate submarină între Anaklia și Constanța), platforma de extracție Neptun Deep și rețeaua cablurilor de telecomunicații submarine ale României generează acel profil concentrat de vulnerabilitate care impune răspunsuri concrete. Un sistem integrat de supraveghere subacvatică, combinând drone submarine (UUV), senzori pasivi de hidroacustică, patrulare asistată de IA și schimb de date în timp real cu aliații în cadrul Mine Countermeasures Task Group Black Sea (MCM), este instrumentul operațional corespunzător. Reprezentanții think-tank-ului Atlantic Council (Washington DC) sugerează, în mod explicit, că protecția infrastructurii energetice și de telecomunicații submarine trebuie tratată ca prioritate NATO de prim rang în Marea Neagră[52].

Convergența TRIPP – BSSC – Coridorul de Mijloc – Neptun Deep – Portul Constanța creează ceea ce estimările analitice ar putea defini ca „*ecuația românească*”, respectiv un ecosistem de conectivitate ce ar plasa România la intersecția proiectelor occidentale eurasiatice Est-Vest, pe ruta trans-caspică, și a unei axe Sud-Nord, prin Coridorul Grecia-Bulgaria-România-Republica Moldova-Ucraina (al cărei acord a fost semnat la Bruxelles în noiembrie 2025[53]). Din perspectiva paradoxului securității, această configurație geometrică generează atât relevanță strategică crescută pentru protecția investițiilor aliate considerate esențiale, dar și un potențial crescut de amenințare externă, considerând multitudinea țintelor de mare valoare.

Dimensiunea diplomatică de la nod logistic la actor strategic

Transformarea portului Constanța, cel de-al doilea port ca mărime din Marea Neagră – aflat la intersecția Coridorului IV Paneuropean, Coridorului Rin-Dunăre și Coridorului IX, în hub geostrategic creează o bază instituțională pentru exercitarea unei *diplomații pentru conectivitate activă.* România se află în poziția favorabilă de a propune o platformă de analiză comparativă NATO/ UE dedicată operațiunilor din „zona gri” specifice spațiilor maritime semi-închise, valorificând expertiza acumulată și poziția sa unică de „punte analitică” la înțelegerea dintre teatrul Mării Negre și cel a Indo-Pacificului. Deși ar putea părea o propunere voluntaristă, ea

reprezintă o nișă analitică reală. ***Niciun alt stat membru NATO nu combină experiența directă a presiunii rusești din Marea Neagră cu un ecosistem de conectivitate trans-continentală de tipul celui pe care România îl construiește.***

Vectorul american, consolidat prin coridorul TRIPP, și vectorul european, articulat prin Global Gateway, dar și strategia de conectivitate trans-caspică sunt complementare, auto-amplificându-se reciproc. Cu cât România devine mai importantă ca nod de conectivitate, cu atât interesele americane și europene pentru protecția României ar trebui să crească. Această logică de auto-consolidare a relevanței strategice este, în esență, rezolvarea practică a paradoxului lui Edward Luttwak de la nivelul *marii strategii*, tradus ca securitate prin indispensabilitate.

CADRUL INTEGRAT AL DESCURAJĂRII ADAPTIVE PENTRU ROMÂNIA

Modelul mixt „porcupine și hub" și convergența celor trei dimensiuni analitice

Sinteza celor trei dimensiuni analizate – *revoluția IA militare, arsenalul coercitiv sub pragul declanșării războiului (aplicat de puterile revizioniste) și logica paradoxală a geoeconomiei extinse* – generează un cadru prescriptiv care poate fi sintetizat în formula „porcupine și hub". Modelul „porcului spinos", validat de Center for Strategic and International Studies (CSIS)/ SUA și National Institute for Defense Studies (NIDS)/ Japonia în contextul taiwanez[54] [55], presupune ca agresiunea adversarului să devină prohibitiv de costisitoare prin investiție asimetrică (precum drone maritime, rachete costiere NSM, mine inteligente, sisteme de război electronic), iar modelul hub-ului înseamnă să devenim indispensabili în arhitectura de conectivitate trans-continentală, transformând interesul și dependența economică a aliaților în garanție de securitate pentru acest spațiu.

Rezolvarea paradoxului lui Luttwak privind marea strategie reprezintă exact această congruență. Conectivitatea economică generează relevanță și angajament aliat, descurajând agresiunea prin costuri politice, iar descurajarea asimetrică ridică exponențial costurile militare ale oricărei agresiuni externe. Niciuna dintre cele două nu poate asigura suficiență individual; împreună, ele generează ceea ce Luttwak numește „armonie artificială" între palierele strategice.

Arhitectura de securitate maritimă pe cinci straturi și integrarea IA

Cadrul operațional concret al descurajării adaptive în Marea Neagră occidentală s-ar putea articula pe cinci straturi integrate:

- un strat *senzorial* cuprinzător (V-BAT, Bayraktar TB2, SeaGuardian, Watchkeeper X, radare costiere, stații AIS, imagistică satelitară aliată);
- un motor *analitic de IA* (model de fuziune multisursă, Imagine Operațională Comună în timp real, detecție anomalii, modelare predictivă);
- un strat al *descurajării active* prin sisteme autonome (roiuri de drone maritime, cu navigare asistată de IA, reziliente la război electronic);
- un strat de *apărare costieră asistată de IA* (baterii NSM cu *pipeline* automatizat senzor-trăgător, integrare Patriot);
- un strat de *cooperare regională* (extinderea cadrului MCM tripartit cu Turcia și Bulgaria, partajare COP NATO, transfer de know-how din Ucraina).

Lacuna critică nu o reprezintă hardware-ul, deoarece senzorii se achiziționează, iar dronele se procură sau sunt manufacturate local. Marele neajuns constă în stratul analitic al Inteligenței Artificiale care transformă o colecție de capabilități individuale într-un sistem de securitate integrat și inteligent. Fără stratul II (motorul analitic), investițiile în straturile I, III, IV rămân fragmentate. Hub-ul European de Securitate Maritimă propus la Constanța, prin Abordarea Strategică a Uniunii Europene pentru Marea Neagră[56], poate reprezenta infrastructura instituțională pentru găzduirea acestui strat integrator.

***Reziliența* anti-blocadă și adresarea armei invizibile**

Lecția cea mai contraintuitivă, dar poate cea mai importantă pentru planificatorii apărării, este

conectată invariabil la piața asigurărilor maritime – „arma invizibilă" a blocadei de facto. Guvernele occidentale au intervenit ca reasiguratori de ultimă instanță în „războiul petrolului" din Golful Persic (1980), instrument care a menținut navigația comercială în condițiile tensiunilor militare. Un mecanism similar UE/ NATO pentru Marea Neagră ar anula vectorul de presiune indirect, soluție sugerată în urma analizei celor două teatre[57].

Celelalte recomandări pentru reziliență și anti-blocadă derivă din analiza comparativă Taiwan – Marea Neagră. Printre recomandări putem identifica: consolidarea coridorului costier NATO ca rută permanentă instituționalizată, extinderea Task Force-ului MCM Marea Neagră cu capabilități autonome de deminare și dezvoltarea capacității de contra-blocadă asimetrică după modelul ucrainean cu drone maritime și rachete NSM costiere.

Guvernanța Inteligenței Artificiale și capitalul uman

Implementarea IA în operațiile militare ridică întrebări de guvernanță care nu pot fi soluționate post-eveniment. Tensiunile post-operaționale dintre compania Anthropic și Departamentul de Război al SUA au ridicat întrebări privind utilizarea instrumentului de IA Claude. Conducerea companiei a luat în considerare anularea contractului de 200 milioane USD, iar șeful echipei de cercetare pentru măsuri de siguranță a demisionat cu un avertisment criptic[58], admițând că nici cei mai avansați actori nu au rezolvat pe deplin această problemă. România ar trebui să stabilească proactiv un cadru național de guvernanță a IA pentru apărare, ancorat în controlul uman semnificativ asupra deciziilor letale, transparență și auditarea algoritmilor în mediul clasificat și un cadru juridic clar pentru operaționalizarea sistemelor autonome.

Provocarea capitalului uman este la fel de critică. Nicio arhitectură tehnologică nu funcționează fără operatori și decidenți capabili să o utilizeze eficient. Integrarea alfabetizării în IA în curricula studiilor de securitate și științelor militare nu mai este opțională, fiind necesară o platformă de formare a specialiștilor noilor generații, cu ancorare în perspectivele analitice ale acestor nevoi.

Dimensiunea doctrinară – de la capabilități la sistem

Experiența ucraineană din Marea Neagră, probabil cel mai dens laborator de inovație militară contemporană sub presiunea conflictului direct, oferă lecții doctrinare care transcend specificul teatrului de operații. Ucraina nu a dispus inițial de o doctrină articulată pentru utilizarea dronelor maritime; aceasta a fost construită iterativ, în condiții de luptă, prin feedback rapid și adaptare. Viteza de adaptare doctrinară a depășit cu mult toate ciclurile formale de achiziție și proces doctrinar ale NATO[59]. Această lecție despre valoarea structurilor organizaționale cu ciclu scurt de feedback și autoritate decizională descentralizată este direct aplicabilă contextului românesc.

Instituirea unui Centru de Integrare a Sistemelor Autonome în relație permanentă de transfer tehnologic cu operatorii ucraineni ar permite României să capitalizeze această experiență operațională, transformând know-how-ul de luptă în doctrină sistematizată și capabilități industriale proprii. O fabrică de drone, dezvoltată în parteneriat cu Ucraina prin mecanismul SAFE[60], poate oferi infrastructura concretă pentru această viziune.

La nivelul interoperabilității, extinderea acordului tripartit MCM cu Turcia și Bulgaria, semnat în ianuarie 2024, într-un acord de partajare a *Conştientizării Domeniului Maritim* la nivel NATO SECRET, cu prevederi pentru participarea Ucrainei ca partener asociat, ar crea prima arhitectură regională de securitate maritimă bazată pe schimb de date în timp real în Marea Neagră[61]. Această arhitectură ar fi, în esență, contrapartea regională a imaginii operaționale comune propuse la nivel național – un angrenaj de sisteme care amplifică eficacitatea fiecărui actor individual.

Scenariul integrat de amenințare pentru „zona gri" în Marea Neagră

O analiză responsabilă a scenariilor trebuie să descrie explicit tipologia amenințărilor față de care descurajarea adaptivă este proiectată.

Convergența dintre lecțiile blocadei rusești în Marea Neagră, doctrina chineză a Armatei de Eliberare a Poporului[62] și campaniile sistematice de destabilizare sub pragul războiului sau sub pragul activării Articolului 5 al NATO, permit conturarea unui scenariu credibil de zonă gri pentru România.

Scenariul de amenințare integrat combină mine „accidentale" în apropierea rutelor comerciale și a platformei Neptun Deep, fiind totodată mecanismul de interdicție cel mai dificil de atribuit și cel mai costisitor de contracarat, alături de incursiuni repetate ale dronelor în spațiul aerian pentru epuizarea sistemelor de apărare și colectare de date SIGINT, amenințări la adresa navigației comerciale prin mesaje ambigue care activează „efectul asigurărilor" prin creșterea primelor de asigurare și retragerea automată a acoperirii de risc în caz de război, atacuri cibernetice asupra sistemelor de control a infrastructurii portuare și energetice și presiune informațională care contestă legitimitatea investițiilor și viabilitatea alianțelor României. Fiecare element individual este instrumentat sub pragul Articolului 5 al NATO, iar efectul cumulativ poate fi echivalentul unei blocade parțiale.

Cadrul de răspuns, cu protocoale clare pentru fiecare treaptă a nivelului de escaladare, trebuie definit și agreat în avans cu aliații, astfel încât decizia să nu fie marcată de incertitudine în momentul acțiunii. Acesta reprezintă unul dintre instrumentele doctrinare cel mai frecvent recomandate în literatura de specialitate examinată. NIDS Japonia subliniază, în contextul lecțiilor din Ucraina aplicate scenariului taiwanez, că „*deterrence by denial*" funcționează numai dacă adversarul are certitudinea că răspunsul se va produce automat, fără deliberări prelungite[63].

SPRE O STRATEGIE NAȚIONALĂ DE DESCURAJARE ADAPTIVĂ

În prezentul articol am propus un cadru analitic integrat, construit pe trei piloni complementari: *precedentul operațional al IA* (operațiunea Maduro), *arsenalul coercitiv sub pragul războiului* (blocada și carantina comparativă Taiwan - Marea Neagră) și *logica paradoxală a securității extinse a României* (cadrul conceptual al lui Edward Luttwak aplicat ecosistemului de conectivitate TRIPP – BSSC – Portul Constanța – Neptun Deep). Convergența celor trei dimensiuni analitice articulează o concluzie care depășește suma componentelor. *România se confruntă cu un set de provocări care nu necesită răspunsuri sectoriale, ci o strategie națională de descurajare adaptivă integrată.*

Lecțiile din conflictele actuale sunt evidente și acționabile:

1 Integrarea IA în operațiile militare nu sugerează un scenariu viitor, ci o realitate operațională demonstrată care impune investiție imediată în stratul analitic și capitalul uman capabil să-l opereze.

2 Blocada eficientă nu este un act militar punctual, ci un ecosistem de presiune care operează simultan prin intermediul minelor, sabotajelor, amenințărilor, piața asigurărilor, operații cyber și dezinformare, iar contra-strategia trebuie adresată simultan tuturor acestor dimensiuni.

3 Geoeconomia nu este separată de securitate, ci parte integrantă a acesteia. România are oportunitatea unică de a transforma un ecosistem de conectivitate extinsă (TRIPP, BSSC, Constanța, Neptun Deep) în garanție de securitate, cu condiția ca investiția economică să fie însoțită de descurajare asimetrică.

Adaptarea strategică centrală presupune descurajarea prin transparență, respectiv transformarea Mării Negre occidentale într-un spațiu complet monitorizat și capabilități de răspuns credibile, încât costul oricărei acțiuni agresive să devină prohibitiv. Această strategie nu este una de confruntare, ci de *descurajare prin conştientizare demonstrată*. Acest concept este validat simultan de precedentul operațional american în Venezuela și lecțiile inovației asimetrice ucrainene în teatrul Mării Negre.

REFERINȚE

1. AYDIN Mustafa, Aydintaşbaş Asli, *Bridging the Bosphorus: How Europe and Turkey can turn tiffs into tactics in the Black Sea*, Policy Brief, European Council on Foreign Relations, 18.03.2025, 20 p.; https://ecfr.eu/publication/bridging-the-bosphorus-how-europe-and-turkey-can-turn-tiffs-into-tactics-in-the-black-sea/
2. BERMAN Noah, Mariel Ferragamo, Sabine Baumgartner, ”How Ukraine Overcame Russia’s Grain Blockade”, Council on Foreign Relations, 27.02.2024; https://www.cfr.org/photo-essay/how-ukraine-overcame-russias-grain-blockade.
3. BLUMENTHAL Dan, Frederick W. Kagan, Jonathan Baumel, Cindy Chen, Francis de Beixedon, Logan Rank, Alexis Turek, *From Coercion to Capitulation: How China Can Take Taiwan Without a War*, Report, American Enterprise Institute, 13 Mai 2024, 111 p.; https://www.aei.org/research-products/report/from-coercion-to-capitulation-how-china-can-take-taiwan-without-a-war/
4. CALUS Kamil, Adam Michalski, Jan Nowinowski, Jacek Tarocinski, ”Romania, Bulgaria and Turkey in the Black Sea Region: Increased Cooperation?”, Centre for Eastern Studies, *OSW Commentary,* nr. 676, 26.06.2025, 8 p.
5. DALY J. K. John, ”Referee and Goalkeeper of the Turkish Straits: The Relevance and Strategic Implications of the Montreux Convention for Conflict in the Black Sea”, Jamestown Foundation, 05.10.2022; https://jamestown.org/referee-and-goalkeeper-of-the-turkish-straits-the-history-relevance-and-strategic-implications-of-the-montreux-convention-for-conflict-in-the-black-sea/
6. D`ANIERI Andrew, Joseph Epstein, ”How Trump’s “TRIPP” Triumph Can Advance US Interests in the South Caucasus”, *Dispatches*, Atlantic Council, 20.01.2026; https://www.atlanticcouncil.org/dispatches/how-trumps-tripp-triumph-can-advance-us-interests-in-the-south-caucasus/
7. DESAI Suyash, ”Forceful Taiwan Reunification: China's Targeted Military and Civilian-Military Measures”, Foreign Policy Research Institute, 11 martie 2025; fpri.org/article/2025/03/forceful-taiwan-reunification-chinas-targeted-military-and-civilian-military-measures/
8. DUPUY C. Arnold, ”How NATO and its partners should respond to Russia’s militarization of the Wider Black Sea Region”, TurkeySource, Atlantic Council, 19.12.2025; https://www.atlanticcouncil.org/blogs/turkeysource/how-nato-and-its-partners-should-respond-to-russias-militarization-of-the-wider-black-sea-region/
9. GLASSER S. Bonnie (editor), *If China Attacks Taiwan. The Consequences for China of ”Minor Conflict” and ”Major War” Scenarios,* The German Marshall Fund of the United States, Decembrie 2025, 61 p.; https://www.gmfus.org/news/if-china-attacks-taiwan.
10. GRAZIER Dan, James Siebens, MacKenna Rawlins, *Rethinking the Threat: Why China is Unlikely to Invade Taiwan*, Stimson Center, Report, August 2025, 30 p.
11. HAMILTON S. Daniel, Angela Stent, ”Russia’s Imperial Black Sea Strategy: Maritime Power and the Quest for Regional Dominance”, *Foreign Affairs*, 19.08.2025; https://www.foreignaffairs.com/georgia/russias-imperial-black-sea-strategy.
12. HASANOVA Tamilla, ”TRIPP-Middle Corridor alliance reshapes Eurasian trade map”, caliber.az, 12.02.2026; caliber.az/en/post/tripp-middle-corridor-alliance-reshapes-eurasian-trade-map.
13. KAUSHAL Sidharth, ”How Can NATO Overcome Russia’s Black Sea Blockade?”, Royal United Services Institute, Londra, 11.08.2026; https://www.rusi.orghttps://www.rusi.org.
14. KIKUCHI Shigeo, Yasuyuki Sugiura (eds.), *War with New and Old Characteristics. Lessons from the Russo-Ukrainian War and*

Prospects for the U.S.–China Confrontation, National Institute for Defense Studies (NIDS), Tokyo, March 2025; https://www.nids.mod.go.jp/english/publication/perspectives/pdf/2025/12_e2025-all.pdf.

15. LAWLER Dave, Maria Curi, ”Pentagon Used Anthropic’s Claude during Maduro Raid”, *Axios*, 14.02.2026; https://www.axios.com/2026/02/13/anthropic-claude-maduro-raid-pentagon.
16. LIN Bonny, Brian Hart, Matthew P. Funaiole, Samantha Lu, Truly Tinsley, *How China Could Quarantine Taiwan: Mapping Out Two Possible Scenarios*, Center for Strategic and International Studies, CSIS Briefs, June 2024, 11 p.; https://www.csis.org/analysis/how-china-could-quarantine-taiwan-mapping-out-two-possible-scenarios.
17. LIN Bonny, Brian Hart, Matthew P. Funaiole, Samantha Lu, Truly Tinsley, *How China Could Blockade Taiwan*, Center for Strategic and International Studies, China Power Series, 22.08.2024; features.csis.org/chinapower/china-blockade-taiwan/
18. LUTTWAK Edward, *Strategy: The Logic of War and Peace*, Harvard University Press, 2001.
19. MARTIN Bradley, Kristen Gunness, Paul DeLuca, Melissa Shostak, *Implications of a Coercive Quarantine of Taiwan by the People’s Republic of China*, RAND Corporation, Washington DC, 2022; https://www.rand.org/pubs/research_reports/RRA1279-1.html.
20. NATE Silviu, ”Joint Communication on the EU Strategic Approach to the Black Sea”, Text, European Commission - *Have Your Say, Feedback from the Global Studies Center*, 5 May 2025; https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14623-Joint-Communication-on-the-EU-strategic-approach-to-the-Black-Sea/F3541060-en.
21. NATE Silviu, James Jay Carafano, ”The West Should Welcome the Middle Corridor”, *The National Interest*, The Center for the National Interest, 01.10.2022; https://nationalinterest.org/feature/west-should-welcome-middle-corridor-205085.
22. PEDROZO (Pete) Raul, ”Russia-Ukraine War at Sea: Naval Blockades, Visit and Search, and Targeting War-Sustaining Objects”, Lieber Institute, West Point, 25.08.2023; https://lieber.westpoint.edu/russia-ukraine-war-naval-blockades-visit-search-targeting-war-sustaining-objects/
23. PETERS Robert, Wilson Beaver, *Defending Taiwan from an Invasion: Next Steps*, Backgrounder, nr. 3943, 17 Decembrie 2025, The Heritage Foundation, 9 p.
24. QIU Winston, ”Romania and Georgia Advance Black Sea Submarine Cable Project with New MoU”, Submarine Cable Networks, 05.02.2025; https://www.submarinenetworks.com/en/systems/asia-europe-africa/bssc/romania-and-georgia-advance-black-sea-submarine-cable-project-with-new-mou.
25. RAMKUMAR Amrith, Keach Hagey, Vera Bergengruen, ”Exclusive| Pentagon Used Anthropic’s Claude in Maduro Venezuela Raid”, Tech, *Wall Street Journal*, 13.02.2026; https://www.wsj.com/politics/national-security/pentagon-used-anthropics-claude-in-maduro-venezuela-raid-583aff17
26. SINKEWICZ Michael, ”AI Tool Claude Helped Capture Venezuelan Dictator Maduro in US Military Raid Operation: Report”, *Fox News*, 13.02.2026; https://www.foxnews.com/us/ai-tool-claude-helped-capture-venezuelan-dictator-maduro-us-military-raid-operation-report.
27. VERES Andrei, ”Romania’s Emerging Drone Industry: Laying the Foundation for the EU Drone Wall”, The Saratoga Foundation, 09.12.2025; https://www.saratoga-foundation.org/p/romanias-emerging-drone-industry.
28. YULIANG Zhang, Zhanyi Xue, *The Science of Campaigns*, Publisher of PLA National Defense University, Beijing, 2006.
29. *** Președinția României, *Strategia Națională de Apărare a Țării pentru perioada 2025-2030,* 43 p.; https://www.presidency.ro/ro/media/csat/strategia-nationala-de-aparare-

a-tarii-pentru-perioada-2025-2030

30. *** ”Romania Finds Drone Fragments after Russian Strikes on Ukrainian Ports”, *Euronews*, 11.11.2025; https://www.euronews.com/2025/11/11/nato-member-romania-finds-drone-fragments-after-russian-strikes-on-ukrainian-ports.
31. *** U.S. Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2025*, 23.12.2025, 95 p.; http://media.defense.gov/2025/Dec/23/2003849070/-1/-1/1/ANNUAL-REPORT-TO-CONGRESS-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2025.PDF.
32. *** U.S. Department of State, *Joint Statement on the Publication of the U.S.-Armenia Implementation Framework for the Trump Route for International Peace and Prosperity (TRIPP)*, Office of the Spokesperson, 13 Ianuarie 2026.
33. *** ”Romania's Defence Strategy Focuses on Black Sea Risks”, *Modern Diplomacy*, 12.11.2025; https://moderndiplomacy.eu/2025/11/12/romanias-defence-strategy-focuses-on-black-sea-risks/
34. *** *The Multi-Domain Deadlock in the Context of Romania and the Black Sea,* Maritime Security Forum, 09 Februarie 2026; https://www.forumulsecuritatiimaritime.ro/the-multi-domain-deadlock-in-the-context-of-romania-and-the-black-sea.
35. *** ”EU Strategic Approach to the Black Sea Region”, European External Action Service, European Union; https://www.eeas.europa.eu/eeas/eu-strategic-approach-black-sea-region_en.
36. *** EU4Digital, ”Meta Study - Advancing a Cross-Regional Connectivity Agenda with Central Asia, Turkiye and South Caucasus”, Enlargement and Eastern Neighbourhood, European Commission, 06.02.2025; https://enlargement.ec.europa.eu/meta-study-advancing-cross-regional-connectivity-agenda-en.
37. *** Conflict in Focus, *Maritime Domain Lessons from Russia-Ukraine,* Event Transcript, Center for Strategic and International Studies, 27 Februarie 2025, 23 p.; https://www.csis.org/analysis/maritime-domain-lessons-russia-ukraine-conflict-focus.

[1] Dave Lawler, Maria Curi, ”Pentagon Used Anthropic's Claude during Maduro Raid”, *Axios*, 14.02.2026; https://www.axios.com/2026/02/13/anthropic-claude-maduro-raid-pentagon, accesat la 14.02.2026.

[2] Amrith Ramkumar, Keach Hagey, Vera Bergengruen, ”Exclusive| Pentagon Used Anthropic's Claude in Maduro Venezuela Raid”, Tech, *Wall Street Journal*, 13.02.2026; https://www.wsj.com/politics/national-security/pentagon-used-anthropics-claude-in-maduro-venezuela-raid-583aff17, accesat la 13.02.2026.

[3] Michael Sinkewicz, ”AI Tool Claude Helped Capture Venezuelan Dictator Maduro in US Military Raid Operation: Report”, *Fox News*, 13.02.2026; https://www.foxnews.com/us/ai-tool-claude-helped-capture-venezuelan-dictator-maduro-us-military-raid-operation-report, accesat la13.02.2026.

[4] *** ”Romania Finds Drone Fragments after Russian Strikes on Ukrainian Ports”, *Euronews*, 11.11.2025; https://www.euronews.com/2025/11/11/nato-member-romania-finds-drone-fragments-after-russian-strikes-on-ukrainian-ports, accesat la 15.01.2026.

[5] Andrew D`Anieri, Joseph Epstein, ”How Trump's “TRIPP” Triumph Can Advance US Interests in the South Caucasus”, Dispatches, Atlantic Council; https://www.atlanticcouncil.org/dispatches/how-trumps-tripp-triumph-can-advance-us-interests-in-the-south-caucasus/, accesat la12.02.2026.

[6] U.S. Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2025*, 23.12.2025, 95 p.; http://media.defense.gov/2025/Dec/23/2003849070/-1/-1/1/ANNUAL-REPORT-TO-CONGRESS-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2025.PDF, accesat la 27.12.2025.

[7] Bradley Martin and others, *Implications of a Coercive Quarantine of Taiwan by the People's Republic of China*, RAND Corporation, 2022; https://www.rand.org/pubs/research_reports/RRA1279-1.html, accesat la 19.02.2026.

[8] Bonny Lin, Brian Hart, Matthew P. Funaiole, Samantha Lu, Truly Tinsley, *How China Could Quarantine Taiwan: Mapping Out Two Possible Scenarios*, CSIS Briefs, June 2024, 11 p.; https://www.csis.org/analysis/how-china-could-quarantine-taiwan-mapping-out-two-possible-scenarios; accesat la 02.02 2026.

[9] Dan Blumenthal, Frederick W. Kagan, Jonathan Baumel, Cindy Chen, Francis de Beixedon, Logan Rank, Alexis Turek, "From Coercion to Capitulation: How China Can Take Taiwan Without a War", *American Enterprise Institute/AEI*; https://www.aei.org/research-products/report/from-coercion-to-capitulation-how-china-can-take-taiwan-without-a-war/, accesat la 30.01.2026.

[10] Edward Luttwak, *Strategy: The Logic of War and Peace*, Harvard University Press, 2001.

[11] *** "Romania's Defence Strategy Focuses on Black Sea Risks", *Modern Diplomacy*; https://moderndiplomacy.eu/2025/11/12/romanias-defence-strategy-focuses-on-black-sea-risks/, accesat la 15.02.2026.

[12] Președinția României, *Strategia Națională de Apărare a Țării pentru perioada 2025-2030*, 26.11.2025, 43 p.; https://www.presidency.ro/ro/media/csat/strategia-nationala-de-aparare-a-tarii-pentru-perioada-2025-2030, accesat la 11.02.2026.

[13] Andrei Veres, "Romania's Emerging Drone Industry: Laying the Foundation for the EU Drone Wall", The Saratoga Foundation, 09.12.2025; https://www.saratoga-foundation.org/p/romanias-emerging-drone-industry, accesat la 18.01.2026.

[14] U.S. Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2025*.

[15] *Op. cit.*- "How China Could Quarantine Taiwan: Mapping Out Two Possible Scenarios".

[16] Bonnie S. Glasser (editor), *If China Attacks Taiwan. The Consequences for China of "Minor Conflict" and "Major War" Scenarios,* The German Marshall Fund of the United States, Decembrie 2025, 61 p.; https://www.gmfus.org/news/if-china-attacks-taiwan, accesat la 12 Februarie 2026.

[17] Dave Lawler, Maria Curi, *Op.cit.*

[18] Amrith Ramkumar, Keach Hagey, Vera Bergengruen, *Op.cit.*

[19] Michael Sinkewicz, *Op.cit.*

[20] *** *The Multi-Domain Deadlock in the Context of Romania and the Black Sea,* Maritime Security Forum, 09 Februarie 2026; https://www.forumulsecuritatiimaritime.ro/the-multi-domain-deadlock-in-the-context-of-romania-and-the-black-sea/, accesat la 09.02.2026.

[21] *Ibidem*.

[22] *Ibidem.*

[23] *** "EU Strategic Approach to the Black Sea Region", European External Action Service; https://www.eeas.europa.eu/eeas/eu-strategic-approach-black-sea-region_en, accesat la 03.02.2026.

[24] Bonny Lin, Brian Hart, Matthew P. Funaiole, Samantha Lu, Truly Tinsley, *Op.cit*.

[25] Bradley Martin and others, *Op.cit*

[26] Bonny Lin, Brian Hart, Matthew P. Funaiole, Samantha Lu, Truly Tinsley, *Op.cit*.

[27] *Ibidem*.

[28] Dan Blumenthal, Frederick W. Kagan, Jonathan Baumel, Cindy Chen, Francis de Beixedon, Logan Rank, Alexis Turek, *Op. cit.*

[29] Raul (Pete) Pedrozo, "Russia-Ukraine War at Sea: Naval Blockades, Visit and Search, and Targeting War-Sustaining Objects", Lieber Institute, West Point, 25.08.2023; https://lieber.westpoint.edu/russia-ukraine-war-naval-blockades-visit-search-targeting-war-sustaining-objects/, accesat la 08.01.2026.

[30] *Ibidem*.

[31] *Ibidem*.

[32] Sidharth Kaushal, "How Can NATO Overcome Russia's Black Sea Blockade?", Royal United Services Institute, 11.08.2026; https://www.rusi.orghttps://www.rusi.org, accesat la 07.02.2026.

[33] Noah Berman, Mariel Ferragamo, Sabine Baumgartner, "How Ukraine Overcame Russia's Grain Blockade", Council on Foreign Relations, 27.02.2024; https://www.cfr.org/photo-essay/how-ukraine-overcame-russias-grain-blockade, accesat la 18.01.2026.

[34] *** *The Multi-Domain Deadlock in the Context of Romania and the Black Sea,* Maritime Security Forum.

[35] John J. K. Daly, "Referee and Goalkeeper of the Turkish Straits: The Relevance and Strategic Implications of the Montreux Convention for Conflict in the Black Sea", Jamestown Foundation, 05.10.2022; https://jamestown.org/referee-and-goalkeeper-of-the-turkish-straits-the-history-relevance-and-strategic-implications-of-the-montreux-convention-for-conflict-in-the-black-sea/, accesat la 03.02.2026.

[36] Mustafa Aydin, Aydintaşbaş Asli, *Bridging the Bosphorus: How Europe and Turkey can turn tiffs into tactics in the Black Sea*, Policy Brief, European Council on Foreign Relations, 18.03.2025, 20 p.; https://ecfr.eu/publication/bridging-the-bosphorus-how-europe-and-turkey-can-turn-tiffs-into-tactics-in-the-black-sea/, accesat la 11.01.2026.

[37] Edward N. Luttwak, *Op.cit*.

[38] *Ibidem*.

[39] Noah Berman, Mariel Ferragamo, Sabine Baumgartner, *Op.cit.*.

[40] Edward N. Luttwak, *Op.cit*.

[41] Daniel S. Hamilton, Angela Stent, ”Russia’s Imperial Black Sea Strategy”, *Foreign Affairs*, 19.08.2025; https://www.foreignaffairs.com/georgia/russias-imperial-black-sea-strategy, accesat la 07.01.2026.

[42] Silviu Nate, ”Joint Communication on the EU Strategic Approach to the Black Sea”, Text, European Commission - *Have Your Say, Feedback from the Global Studies Center*, 5 May 2025; https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14623-Joint-Communication-on-the-EU-strategic-approach-to-the-Black-Sea/F3541060_en, accesat la 03.01.2026.

[43] United States Department of State, *Joint Statement on the Publication of the U.S.-Armenia Implementation Framework for the Trump Route for International Peace and Prosperity (TRIPP)*, Office of the Spokesperson, Press Releases, 13.01.2026; https://www.state.gov/releases/office-of-the-spokesperson/2026/01/joint-statement-on-the-publication-of-the-u-s-armenia-implementation-framework-for-the-trump-route-for-international-peace-and-prosperity-tripp/, accesat la 12.02.2026.

[44] Andrew d`Anieri, Joseph Epstein, *Op.cit.*

[45] Silviu Nate, James Jay Carafano, ”The West Should Welcome the Middle Corridor”, *The National Interest*, The Center for the National Interest, 01.10.2022; https://nationalinterest.org/feature/west-should-welcome-middle-corridor-205085, accesat la 29.12.2025.

[46] EU4Digital, ”Meta Study - Advancing a Cross-Regional Connectivity Agenda with Central asia, Turkiye and South Caucasus”, Enlargement and Eastern Neighbourhood, European Commission, 06.02.2025; https://enlargement.ec.europa.eu/meta-study-advancing-cross-regional-connectivity-agenda_en, accesat la 10.02.2026.

[47] *Ibidem*.

[48] Winston Qiu, ”Romania and Georgia Advance Black Sea Submarine Cable Project with New MoU”, Submarine Cable Networks, 05.02.2025; https://www.submarinenetworks.com/en/systems/asia-europe-africa/bssc/romania-and-georgia-advance-black-sea-submarine-cable-project-with-new-mou, accesat la 05.02.2026.

[49] *Ibidem*.

[50] *** Conflict in Focus, *Maritime Domain Lessons from Russia-Ukraine,* Event Transcript, Center for Strategic and International Studies, 27 Februarie 2025, 23 p.; https://www.csis.org/analysis/maritime-domain-lessons-russia-ukraine-conflict-focus, accesat la 12.02.2026.

[51] *Ibidem*.

[52] Arnold C. Dupuy, ”How NATO and its partners should respond to Russia’s militarization of the Wider Black Sea Region”, TurkeySource, Atlantic Council, 19.12.2025; https://www.atlanticcouncil.org/blogs/turkeysource/how-nato-and-its-partners-should-respond-to-russias-militarization-of-the-wider-black-sea-region/, accesat la 19.01.2026.

[53] *** *The Multi-Domain Deadlock in the Context of Romania and the Black Sea,* Maritime Security Forum.

[54] Bonny Lin, Brian Hart, Matthew P. Funaiole, Samantha Lu, Truly Tinsley, *Op.cit.*

[55] Takayuki Igarashi, ”Taiwan's Military Strategy and Preparations for Defense Operations. Strengthening Resilience against a Possible Chinese Invasion”, p. 89-146, în Shigeo Kikuchi, Yasuyuki Sugiura (eds.), *War with New and Old Characteristics. Lessons from the Russo-Ukrainian War and Prospects for the U.S.–China Confrontation*, National Institute for Defense Studies (NIDS), Tokyo, March 2025; https://www.nids.mod.go.jp/english/publication/perspectives/pdf/2025/12_e2025_all.pdf., accesat la 12.12.2025.

[56] *** ”EU Strategic Approach to the Black Sea Region”, European External Action Service

[57] Sidharth Kaushal, *Op.cit*.

[58] Dave Lawler, Maria Curi, *Op.cit*.

[59] Noah Berman, Mariel Ferragamo, Sabine Baumgartner, *Op.cit*.

[60] *** ”Romania Wants to Build UAV Manufacturing Plant Together With Ukraine”, *Defense Express*, 25.09.2025;https://en.defence-ua.com/news/romania_wants_to_build_uav_manufacturing_plant_together_with_ukraine-15938.html, accesat la 12 Februarie 2026.

[61] Kamil Calus, Adam Michalski, Jan Nowinowski, Jacek Tarocinski, ”Romania, Bulgaria and Turkey in the Black Sea Region: Increased Cooperation?”, Centre for Eastern Studies, *OSW Commentary,* nr. 676, 26.06.2025, 8 p.; https://www.osw.waw.pl/en/publikacje/osw-commentary/2025-06-26/romania-bulgaria-and-turkey-black-sea-region-increased, accesat la 20 decembrie 2025.

[62] Zhang Yuliang, Zhanyi Xue, *The Science of Campaigns*, Publisher of PLA National Defense University, Beijing, 2006.

[63] Takayuki Igarashi, *Op.cit*.

RĂZBOIUL CU SPECTRU LARG ȘI NEVOIA PLANIFICĂRII STRATEGICE INTEGRATE. CAZURILE SPIDER WEB ȘI BORACAY

Iulian CHIFU*

Abstract

Hybrid warfare has evolved lately in a more complex combination of the full spectrum warfare, using multiple orchestrated instruments from several spectrums of the security complex in order to achieve military and security objectives. Defending and deterring combined threats in a full spectrum warfare involve not only national and societal resilience, but an integrated strategic planning tool to comprehend and react timely to such threats.

The abuses of individuals regarding their legitimate rights and liberties are becoming ingredients of choice in such offensive full spectrum warfare planning. The cases of Spider Web and Boracay operations involved both conventional and hybrid instruments – criminality, corruption, cheating sanctions, multiple attacks on security and safety, maritime law breaches and so on, and the case of the coffin graffiti marked "French soldier in Ukraine" in Paris is adding to the complexity of the issue.

Keywords: *full spectrum warfare; integrated strategic planning; resilience; hybrid threats.*

INTRODUCERE ȘI METODOLOGIE

Studiul nostru pornește de la evaluarea operațiunilor și războaielor de secol 21 și a modului în care se dezvoltă acestea. Am ales, astfel, războiul de 44 de zile din Nagorno-Karabakh (2020) și operațiunea specială de o zi, din 2023, care a dus în final și la căderea Stepanakert-ului/Hankendi[1], fără să uităm operațiunea de blocare a coridorului Lachin realizată de „societatea civilă" ecologistă[2]. Apoi am evaluat complexitatea operațiunilor din războiul din Gaza de după operațiunea teroristă din 7 octombrie 2023 a Hamas în sudul Israelului[3], cu numeroase acțiuni la zi. În fine, am abordat agresiunea rusă împotriva Ucrainei, de la operațiunea hibridă clasică a „omuleților verzi" și pseudo-referendumul din Crimeea (2014) până la războiul pe scară largă, de mare intensitate, pe

* ***Președintele Centrului pentru Prevenirea Conflictelor și Early Warning, profesor universitar doctor la Universitatea Națională de Apărare „Carol I", profesor asociat la SNSPA București. A fost consilier prezidențial 2011-2014 și consilier de stat al prim-ministrului 2021-2023.***

termen lung al Rusiei în Ucraina[4], declanșat la 24 februarie 2022. Am adăugat un set de operațiuni desfășurate de Moscova în Europa, sub radar, de la sabotaje la război cognitiv-informațional, utilizate în runde repetate de alegeri, și ne-am întrebat ce lipsește? De ce nu am putut preveni aceste agresiuni?

Dacă resursele, cunoașterea și pregătirea personalului pentru prevenirea crizelor sunt prezente, iar reziliența societală este la un nivel înalt, ce componente structurale nu sunt folosite eficient, ce instrumente instituționale sau de expertiză lipsesc sau ce ne mai lipsește la nivelul infrastructurii și cunoașterii pentru a putea preveni atacurile războiului cu spectru larg. Ce piese lipsesc din angrenaj, ce componente ale structurii instituționale nu funcționează eficient sau unde sunt unghiurile moarte/ „punctele oarbe" pe care nu le sesizăm? De aici vine și prima noastră întrebare de cercetare: ***de ce aceste atacuri nu au putut fi prevenite?***

Am utilizat pe larg, în acest cadru de analiză, conceptul de război cu spectru larg - *full spectrum warfare*, pe care l-am studiat și căruia i-am dat o definiție operațională, însemnând utilizarea mai multor mijloace militare și non-militare, integrate, orchestrate și coordonate de către o comandă unică și dirijate spre a atinge un obiectiv politic clar[5]. Nu este un concept nou, dar am arătat fundamentele sale. Astfel, Statele Unite definesc dominația cu spectru larg drept controlul asupra tuturor domeniilor – de la cel naval la spațiul aerian, pentru ocuparea completă și controlul teritoriului, apelor, spațiului exterior, spațiului cibernetic și chiar spațiului psihologic[6], obiectivul final fiind preponderența pe întregul spectru al războiului, în conflicte convenționale sau războaie neregulate/ iregulare[7]. De exemplu, fostul Secretar al Pentagonului, Donald Rumsfeld, a solicitat la începutul mandatului său o strategie pentru a confrunta, în același timp, un întreg spectru de amenințări și nu doar un adversar particular de un anumit tip, planificând victoria pe întregul spectru al unui posibil conflict[8].

Tot în zona multidomeniu plasează și Australia apărarea cu spectru larg – *full spectrum*. Aceasta este destinată să determine protecția împotriva amenințărilor militare care provin din spațiul cibernetic sau spațiul exterior, ca și din spațiul terestru, aerian și maritim[9]. F.Rusă, chiar dacă nu a teoretizat, a aplicat conflictul cu spectru larg (*full spectrum conflict*), înțelegând, însă, prin acest concept patru spectre distincte – militar, informațional, economic și energetic, precum și operațiuni de influență politică[10]. Iar reacția la agresiunile cu spectru larg trebuie să aibă în atenție această definiție și modul în care este aplicată de virtualul agresor.

Cum F.Rusă a înțeles nevoia comenzii unice pentru integrarea elementelor provenind din diverse spectre pentru atacul de această factură[11], așa și R.P. Chineză identifică această nevoie atunci când se referă la abordarea „Celor Trei Războaie"[12]. Potrivit unui raport al Pentagonului, abordarea „celor trei războaie" ale Chinei este o provocare pentru Statele Unite deoarece este „un concept executat de către o structură (Departamentul Politic General) care nu are un corespondent în armata americană"[13]. Fără o asemenea instituționalizare sau un mandat politic, precum și fără măcar o înțelegere filosofică asupra faptului că războiul operează într-o formă coordonată în spațiul militar și civil, coordonarea occidentală pentru un răspuns la războiul cu spectru larg devine complicată[14].

În urma analizării acestor elemente, am ajuns la definiția operațională pe care o utilizăm pentru războiul cu spectru larg: o colecție largă de mijloace militare și non-militare, utilizate de actori statali sau non-statali, în cadrul unei operațiuni planificate integrat și coordonat, cu obiectivul de a dezvolta o acțiune surpriză și a crea un avantaj strategic printr-o serie neașteptată de evenimente (benigne și legale sau maligne și ilegale, deopotrivă), implicând agresiunea și violența[15]. Raționalizarea epistemologică a păstrat în definiție abordarea coordonată și integrată, surpriza, instrumentele multiple din spectrul larg, în realizarea atacului cu spectru larg.

Am folosit în această parte a analizei noastre studiul enciclopedic și epistemologic, studiile empirice, abordarea cognitiv-instituțională și metoda polieuristică, ca și „teoria celor trei războaie" dezvoltată de experții chinezi.

Rezultatul a fost identificarea a trei componente distincte: nuclear – rămas cu precădere la nivel retoric și folosit în atacuri de natură cognitiv-informațională; convențional – la toate nivelurile; hibrid – cu toate componentele militare, instituționale și civile. Analiza noastră empirică a mai descoperit o componentă, cea de-a patra, pe care o adăugăm aici pentru a complini, la acest moment, războiul cu spectru larg: rolul persoanelor individuale care își exercită drepturile legitime și legale, ca și libertățile lor, dar abuzând de acestea prin combinarea lor, cu voie sau fără consimțământul propriu, în planificarea operațiunilor strategice integrate ale războiului cu spectru larg. Cu atât mai dificil este de separat și distins linia fină dintre obișnuințe, recursul legitim la drepturi individuale și elementele de abuz și participarea la agresiune.

Cea de-a doua întrebare de cercetare este ***dacă războiul cu spectru larg a fost o soluție identificată ad-hoc, una planificată sau o improvizație testată, care s-a dovedit relevantă pentru tipul de atac cu spectrul larg desfășurat***. Desigur, un răspuns final complet este greu de decelat, dar aplicarea acestui model la cazurile particulare Boracay și Spider Web ne oferă un set de răspunsuri, alături de alte cazuri desfășurate la nivel european – precum recrutarea prin intermediul Internetului, formule de constrângere și radicalizare împrumutate din panoplia ISIS/ Statul Islamic, sau recrutarea pe bază strict financiară (cazul grafitti-urilor din Franța). Dacă la început primele au fost întâmplări, improvizații sau teste, astăzi operațiunile au fost pe deplin planificate în agresiunile cu spectru larg. Avem și un răspuns parțial în aceste cazuri și privitor la participarea individuală: aceasta este planificată și orchestrată de agresor, indiferent care este mecanismul sau motivația cetățenilor care participă vinovat sau sunt exploatați în orb.

De aici am decelat și cea de-a treia întrebare de cercetare: ***cum putem preveni, anticipa sau combate asemenea atacuri cu spectru larg?*** Iar răspunsul nu este absolut nou, l-am văzut în Raportul Comisiei 11.09 din SUA în urma atacurilor teroriste de la Word Trade Center[16] - atunci când, urmare a incapacității de a integra informația venind de la 99 de agenții independente ale guvernului SUA, a fost creat DHS/ Department of Homeland Security. Astfel, vidul de integrare și coordonare în materie de evaluare și soluții, de analiză, a fost compensat prin crearea instituției responsabile cu aceste elemente.

Și Guvernul german a trecut prin aceleași procese de evaluare și a ajuns la ideea înființării Consiliului Național de Securitate, în subordinea Cancelariei federale[17]. Documentul menționează scopul „de a forma un pod între departamente pentru ca să aducă împreună teme largi și cunoștințe și expertiza provenind de la politicile de securitate interne, externe, economice și digitale. Pe baza cuprinzătoare creată, Guvernul Federal poate lua deciziile necesare în interesul securității”[18]. Cele trei atribuții principale vizează supravegherea comprehensivă (integrată, combinată, de informație și cunoaștere) a situației de securitate, realizarea planificării strategice și abordărilor prospective (*foresight*) și, respectiv, întărirea rezilienței Germaniei.

CAZUL BORACAY

Un caz tipic de planificare a unei agresiuni cu spectru larg îl reprezintă „cazul Boracay”. Este vorba despre un vas reținut de Franța în largul coastelor sale, cu căpitanul arestat și adus în instanță pentru că nu a răspuns solicitărilor poliției legate de infracțiuni la legile navale. Premierul francez, Sebastien Lecornu, a subliniat că vasul face parte din „flota din umbră” utilizată de către Rusia pentru a evita restricțiile de vânzare de petrol și plafonarea prețului prin sancțiunile europene[19]. Nava Boracay, care pretindea că are pavilionul statului Benin, este legată de zborurile de drone deasupra Danemarcei, parte a violărilor spațiului aerian și blocării aeroporturilor europene, supravegherii și filmării bazelor militare și a infrastructurii critice în Danemarca

și Germania, violări și agresiuni pentru care europenii au acuzat Moscova, în timp ce Rusia a negat orice responsabilitate pe motive de lipsă a probei absolute a atribuirii[20].

Potrivit procurorilor francezi, vasul Boracay era „considerat un vas neînregistrat potrivit legilor internaționale" (acesta schimbase mai multe pavilioane, proprietari și armatori în timpul curselor) și ducea o încărcătură mare de petrol din Rusia în India. Căpitanul și membrii echipajului, arestați împreună cu el, erau cetățeni chinezi, cu toții întrând într-o investigație formală și fiind chemați în instanță în februarie anul acesta[21]. Nava se afla în largul coastelor Danemarcei atunci când drone neidentificate au determinat închiderea mai multor aeroporturi, dar și a siturilor militare din Peninsula Jutland[22]. Tancul petrolier este suspectat că a fost platforma de lansare a dronelor, incident care a avut loc chiar înaintea summitului liderilor UE de la Copenhaga[23].

Arestarea și urcarea la bordul tancului petrolier a marinei franceze în largul portului Saint Nazare, la 25 septembrie 2025, creează un precedent.[24] Navei i s-a atribuit responsabilitatea participării la operațiunile hibride ruse[25, 26]. Evaluările au arătat că măcar o parte a dronelor a fost lansată de pe navă[27], iar incursiunile dronelor au fost identificate în spațiile danez și norvegian. Anterior, Germania a reclamat, alături de alte state, astfel de incidente[28, 29]. Asemenea incidente ciudate, implicând nave ale flotei din umbră, conduse de căpitani de naționalitate chineză, au fost înregistrate în Marea Baltică, fiind vorba despre acțiuni de sabotaj a cablurilor de comunicații digitale și a unor conducte care au fost tăiate prin procedeul lăsării ancorei la fund și a navigării prin agățarea, târârea și ruperea infrastructurii critice plasate pe fundul mării[30].

Analiza acestui caz arată foarte clar premeditarea și planificarea unor acțiuni aferente unui spectru larg, nu numai de natură hibridă, care implică cartografierea fundului Mării Baltice pentru pregătirea operațiunilor de sabotaj ulterioare, nave civile neînregistrate legal, dotate cu senzori militari și personal militar îmbrăcat civil care efectuează acțiuni de *intelligence*, ascultarea comunicațiilor militare, culegere de informații despre liniile de furnizare a capabilităților și muniției, evaluarea gradului de pregătire a unor state prin testarea reacțiilor, campanii de zboruri neautorizate cu drone, toate fiind greu de contracarat și de atribuit[31, 32]. Planificarea integrată a agresiunilor este evidentă, așa cum lipsa de reacție este determinată de combinarea diferitelor elemente pentru care statele au instituții diverse de răspuns, care nu sunt coordonate și integrate.

OPERAȚIUNEA SPYDER WEB

Este binecunoscută operațiunea specială a serviciilor de *intelligence* ucrainene prin care a fost distrusă o treime din flota strategică aeriană rusă amplasată adânc în teritoriul rus. După o planificare de 18 luni, au fost atacate patru aerodromuri, cu 117 drone transportate în camioane, în lăzi de lemn, cu documente ce indicau transportul de mobilă, fiind distruse sau avariate grav 40 de avioane de diferite tipuri (A-50, Tu-95 și TU-22M[33]), reprezentând 34% din flota aeriană care asigură lansarea rachetelor nucleare strategice ruse. Unele dintre bazele vizate, Olenya (Murmansk), Diaghilevo (Ryazan), Belaya (Irkutsk) și Ivanovo (Oblastul Ivanovo), se află la peste 4000 km de frontiera Ucrainei.

Operațiunea a utilizat elemente ale războiului cu spectru larg, conținând componente de contrabandă, corupție, atac informațional hibrid și convențional, distrugerea dronelor, dar și exercitarea liberă a unor drepturi individuale ale șoferilor de camion – dreptul la muncă – și al companiilor de transport, legate de drepturile lor comerciale și economice[34]. Toate persoanele implicate au părăsit teritoriul Rusiei fără a fi interceptate[35]. Operațiunea a fost planificată integrat și realizată de SBU, serviciul special de informații interne al Ucrainei, împreună cu colaboratori militari[36]. Ofițerii de *intelligence* care au identificat și pregătit zonele de lansare au fost și ei exfiltrați înainte ca atacul să înceapă.[37]

În cadrul operațiunii Spider Web a fost utilizată o combinație de control uman al dronelor și elemente de autonomie cu funcționalitate asistată de Inteligența Artificială, în faza finală a zborului și lovirii. Dronele de tip FPV utilizate au fost controlate prin intermediul rețelelor de telecomunicații/ telefonie mobile ruse 4G și LTE și au beneficiat de transmisiune video în timp real către comanda și controlul din Ucraina și input-uri de comandă venite de la distanță mare, din afara teritoriului Rusiei. Nu a fost nevoie de operatori sau persoane care să asigure comanda la sol din apropiere. Operațiunea a fost una cu cost redus, cu funcția de operare extrasă din surse deschise și disponibilă comercial, costul dronelor fiind între 600 și 1000 de dolari. Atacul a beneficiat de lipsa totală de apărare sau contra măsuri anti-UAV din partea Rusiei la acele aeroporturi, considerate sigure, o infrastructură strategică de mare valoare, cu un grad de vulnerabilitate extrem de mare[38] [39], într-un teritoriu considerat de neatins de capabilitățile ucrainene[40]. Atacul a constituit un punct de cotitură psihologic care a marcat maturitatea doctrinară a Kievului pe linia țintirii susținute de *intelligence*, a agilității tehnologice și structurii de comandă flexibile, care a compensat inferioritatea numerică[41].

Lovitura poate să fi influențat postura nucleară a Rusiei, fiind considerată un Pearl Harbor al Moscovei chiar de către media oficială rusă. Impactul pe dimensiunea cognitiv-informațională care a urmat a fost devastator pentru Rusia și a generat reasigurări, încredere și unitate la nivelul publicului ucrainean. Creativitatea, inovația și încrederea, la care adăugăm cutezanța, au rescris regulile războiului prin operațiunea cu spectru larg de un asemenea impact.[42] După atac, șiruri lungi de camioane controlate de poliție au apărut în filmări video în întreaga Rusie, dar e imposibil de verificat fiecare transport sau container privind prezența dronelor[43]. În noile condiții de război nu totul poate fi protejat, iar prioritizarea creează probleme majore. Investiția trebuie făcută în *intelligence* și descurajare, mai degrabă, până la un atac ostil care nu mai poate fi oprit[44]. De aceea, vorbim despre necesitatea unei planificări integrate a apărării, care să țină cont de toți senzorii și semnalele care vin pe diferitele spectre ale activității militare și civile și care pot oferi elementele necesare prevenirii atacurilor.

UTILIZAREA DREPTURILOR INDIVIDUALE ALE OMULUI – ABUZ DE DREPT AL CETĂȚENILOR MOTIVAȚI SAU „EXPLOATARE ÎN ORB”

Cetățenii sunt liberi să-și utilizeze și exercite drepturile fundamentale în orice stat care le respectă. Atunci când ei sunt angajați direct – cu mijlocire financiară sau din diverse motivații – pentru a abuza de aceste drepturi, iar activitatea lor, consimțită sau nu, se combină cu alte elemente ale războiului cu spectru larg și determină o agresiune împotriva unui inamic, rezultatul antrenează răspunderea celui în cauză. Am folosit aici drept caz școală și exemplu relevant cazul grafitti-urilor, cu un coșciug pe care scria „Soldat francez în Ucraina”, apărute pe clădiri din Paris, la 18 iunie 2024. Trei cetățeni ai R.Moldova au fost arestați apoi la Paris, fiind identificați ca autori ai acelor grafitti. Poliția franceză a subliniat că, în spatele celor trei, este prezumată interferența unui terț actor străin (Rusia), în timp ce ministrul Afacerilor Externe de la Chișinău, Mihai Popșoi, a condamnat pe Twitter autorii și a notat că incidentul este „parte a tacticilor hibride care sunt menite să afecteze imaginea internațională a statului”. R.Moldova a anunțat colaborarea cu partea franceză pentru a identifica toți responsabilii și a-i aduce în fața legii[45].

La 1 iunie 2024, cinci sicrie au fost plasate în imediata apropiere a Turnului Eiffel. Trei suspecți au fost luați în custodie în legătură cu incidentul: un adolescent ucrainean, un cetățean german și unul bulgar. Un presupus grup artistic „Mirya” – Pace a anunțat, apoi, că era autorul protestului care se dorea un apel la pace. În același șir de acțiuni, cetățeni bulgari au fost suspectați că au pictat mâini roșii pe memorialul Shoah, act de vandalism la adresa memorialului Holocaustului din Paris, la 14 mai 2024[46].

Doi dintre cetățenii R.Moldova arestați au fost acuzați, la 22 iunie 2024, de către procurorii

francezi, de distrugere de proprietate și participare la acțiuni destinate „a demoraliza armata și a afecta apărarea națională pe timp de pace”[47]. Cei trei cetățeni au fost plătiți cu câte 100 de dolari pentru a picta grafitti-ul. Tot coșciuge, de data aceasta în formă de avioane Mirage franceze, au fost descoperite în trei districte franceze, cu mesajul „Mirage pentru Ucraina”. Același mesaj a fost găsit și pe clădirea Agenției France-Presse. Mesajele făceau referire la anunțul din iunie 2024 al președintelui francez, Emmanuel Macron, de trimitere a avioanelor de luptă Mirage-2000 în Ucraina și antrenarea piloților ucraineni pentru a le pilota.

În final, patru indivizi, dintre care trei cetățeni ai R.Moldova, suspecți de acțiunile petrecute între 18 și 20 iunie 2024, urmau să fie aduși în fața instanței la 23 februarie 2026. Doi au lucrat la imprimarea grafitti-urilor, unul stătea de pază, iar al patrulea este cel care a plătit și a dat indicațiile pentru grafitti, fiind un susținător al oligarhului pro-rus din R.Moldova, Ilan Shor, refugiat la Moscova[48].

CONCLUZII

Am prezentat, în acest articol, un număr de modalități de planificare și executare a operațiunilor agresive la adresa unui stat țintă, care includ exercitarea prin abuz a drepturilor individuale (dreptul la liberă exprimare, dreptul la protest etc.), combinată cu celelalte instrumente de natură hibridă (criminalitate organizată, sabotaj, spălare de bani, subversiune, spionaj, atac convențional cu drone), fapt care determină o agresiune pe formatul cu spectru larg la adresa unui stat.

La prima întrebare de cercetare răspunsul este că cel agresat nu a avut capacitatea de a preveni atacul pentru că instrumentarul pentru fiecare element al spectrului este separat și nu există o formulă integrată a unei asemenea planificări a apărării. Când la suma de instrumente se adaugă și recrutarea (aleatoare) de persoane civile, convinse sau plătite să execute acțiuni ce par benigne sau de protest (ca efect al exercitării propriilor drepturi), capacitatea de prevenție este și mai dificilă.

În privința celei de-a doua întrebări de cercetare, răspunsul este parțial și se referă la faptul că, dacă la origine operațiunile cu spectru larg au apărut din întâmplare sau prin improvizații ad-hoc, urmare a nevoii de a compensa lipsuri în planificare și acțiune, cu certitudine în cazurile prezentate avem de-a face cu operațiuni planificate integrat din start. De unde răspunsul la cea de a treia întrebare de cercetare, care presupune că soluția de contracarare și prevenire a unui asemenea atac este o planificare integrată a apărării, care să cuprindă instrumentar militar și civil din toate spectrele.

Limitele cercetării sunt date de faptul că nu am ajuns la abordarea și detalierea componentei cognitiv-instituționale, respectiv o analiză care să determine unde și cine ar trebui să realizeze această planificare integrată și la ce nivel ar trebui aceasta plasată. Astfel, în mod tradițional, componenta militară vizează crizele de natură militară, iar Ministerul de Interne și Departamentul său de Urgențe Civile se ocupă de celelalte elemente relevante ale spectrului, fără a evita să includem aici numeroase alte instituții cu propriile lor atribuții. O variantă de planificare integrată ar trebui plasată la un nivel superior, fie la nivelul Guvernului, dacă responsabilitățile de securitate și apărare revin Executivului, în monarhii constituționale și republicile parlamentare, sau la nivelul Președintelui, în republicile prezidențiale. Soluțiile de tip Consiliul Național de Securitate în subordinea Președintelui, cazul SUA, sau al Cancelariei, cazul german, ar trebui identificate ca formule ce se pot extinde și împrumuta, desigur și în funcție de analiza constituțională aferentă.

BIBLIOGRAFIE

1. ABDYRAEVA Cholpon, *The Use of Cyberspace in the Context of Hybrid Warfare. Means, Challenges and Trends,* Austrian Institute for International Affairs, Working Paper, nr. 107, Iunie 2020, 36 p.; https://www.oiip.ac.at/cms/media/working-paper-107-cyberspace-in-the-context-of-hybrid-warfare.pdf.
2. BAGO Katja, *Ukraine's Operation Spider's Web is a game-changer for modern drone warfare. NATO should pay attention*, 17 July 2025; https://www.chathamhouse.org/2025/06/ukraines-operation-spiders-web-game changer-modern-drone-warfare-nato-should-pay-attention.
3. BALMFORTH Tom, Hunder Max, "To attack Russian air bases, Ukrainian spies hid drones in wooden sheds", *Reuters*, June 1, 2025; https://shorturl.at/JXeHE.
4. BONDAR Kateryna, *How Ukraine's Operation "Spider's Web" Redefines Asymmetric Warfare*, CSIS, 2 June 2025; https://www.csis.org/analysis/how-ukraines-spider-web-operation-redefines-asymmetric-warfare.
5. CAULCUTT Clea, "French military arrests 2 crew on suspected Russian shadow fleet vessel", *Politico*, 2 October 2025, https://www.politico.eu/article/french-military-arrests-crew-russian-shadow-fleet-vessel-boracay/.
6. CHIARELLI W. Peter, Patrick R. Michaelis, "Winning the Peace. The Requirement for Full-Spectrum Operations", *Military Review*, vol. LXXXV, nr. 4, 2025, Army University Press; https://www.armyupress.army.mil/Journals/Military-Review/ English-Edition-Archives/COIN-Reader-1/Chiarelli-JA-2005/.
7. CHIFU Iulian, Drăgan Iulian Mihaela, "Polarization and radicalization as identity dynamics in a fluid environment. The case of the explosion at Al Ahli Hospital in Gaza", *Security Science Journal*, vol. 5, nr. 1, 2024, pp. 7-21.
8. CHIFU Iulian, Grigore Cosmin, "Full-spectrum warfare. From broadening the instruments to thinking the unthinkable", *Romanian Military Thinking*, nr. 2, 2025, pp. 10-35.
9. CHIFU Iulian, "Lege, etică și legitimitate vizând proporționalitatea în război. Cazul Gaza", *Infosfera*, vol. XVI, nr. 1, 2024, pp. 5-19.
10. CHIFU Iulian, „Relativizarea etică a dreptului de a ucide legal ca răzbunare, sancționare a trădării și represiune. Cazul Ismail Hanyieh", *Infosfera*, vol. XVI, nr. 4, 2024, pp. 11-21.
11. CHIFU Iulian, "Resilience, societal security and the intangible aspects of war. Ukraine's lessons learned", *Romanian Military Thinking*, nr. 1, 2024, pp. 14-25.
12. CONSTANT Méheut, Ivan Nechepurenko, Nataliya Vasilyeva, "Ukraine and Russia Met for 2nd Round of Talks as Attacks Escalate", *The New York Times*, June 2, 2025; https://shorturl.at/YiQT6.
13. CULVERWELL Dominic, "Moldovan citizens detained over graffiti warning against sending French soldiers to Ukraine", *kyivindependent*, 10 June 2024; https://kyivindependent.com/moldovan-citizens-detained-over-graffiti-depicting-dead-french-soldiers-in-ukraine/.
14. DUPONT Alan, *Full spectrum defence: Re-thinking the fundamentals of Australian defence strategy,* Lowy Institute, March 2015, 16 p.; http://www.jstor.com/stable/resrep10131.
15. GOZZI Laura, BBC Verify, "How Ukraine carried out daring 'Spider Web' attack on Russian bombers", *BBC*, 2 June 2025; https://www.bbc.com/news/articles/cq69qnvj6nlo.
16. HALPER Stefan (ed.), "China: The Three Warfares", Report for the Director of Office of Net Assessment, Office of the Secretary of Defense, DoD, May 2013, 565 p.
17. JONSSON Oscar, Robert Seely, "Russian Full-Spectrum Conflict: An Appraisal After Ukraine", *The Journal of Slavic Military Studies*, vol. 28, nr. 1, 2015, pp. 1-22.
18. KULLAB Samya, "A surprise drone attack on airfields across Russia encapsulates Ukraine's wartime strategy", *Associated Press*, 2 June 2025; https://apnews.com/article/what-to-know-ukraine-drone-attack-russia-bombers-

2d01b23341e2289882760b9f121431d4,
19. LISOVA Anastasia, *Three Moldovans to be tried in France for graffiti with coffins of "French soldiers in Ukraine"*, Liga.net, 9 octombrie 2025; https://news.liga.net/en/politics/news/three-moldovans-to-be-tried-in-france-for-graffiti-with-coffins-of-french-soldiers-in-ukraine.
20. MAGAKYIAN Simon, "How Azerbaijan Weaponized Environmentalism to Justify Ethnic Cleansing", *Time*, 22 february 2023; https://time.com/6257467/armenia-azerbaijan-nagorno-karabakh-lachin-environment-icj/
21. REICHBORN-KJENNERUD Erik, Cullen Patrick, *What is Hybrid Warfare?*, Norwegian Institute for International Affairs (NUPI), Policy Brief, nr. 1, 2016, 4 p.; http://www.jstor.com/stable/resrep07978.
22. RUMSFELD H. Donald, *Guidance and Terms of Reference for the 2001 Quadrennial Defense Review,* Department of Defense, 2001, June 22, 22 p.; https://www.comw.org/qdr/qdrguidance.pdf.
23. RYAN Maria, "'Full spectrum dominance': Donald Rumsfeld, the Department of Defense, and US irregular warfare strategy, 2001–2008", *Small Wars & Insurgencies*, vol. 25, nr. 1, 2014, pp. 41-68.
24. SCHOFIELD Hugh, Kupemba Danai Nesta, "French troops board oil tanker linked to Russian 'shadow fleet'", *BBC*, 1 October 2025; https://www.bbc.com/news/articles/cx2j1gynjddo.
25. SEIBT Sebastian, "Drones, sabotage, surveillance Moscow's hybrid warfare takes to the high seas", *France 24*, 03.10.2025; https://www.france24.com/en/europe/20251003-drones-sabotage-surveillance-moscow-s-hybrid-warfare-takes-to-the-high-seas.
26. SHAW G. Ian, *Predator Empire. Drone warfare and full spectrum dominance.* University of Minnesota Press, 2016.
27. SIMONS Greg, Chifu Iulian, "Realist and Constructivist Interpretations and Representations of the Second Nagorno-Karabakh War: As an Event and as a Process", *Journalism and Media*, vol. 6, nr. 1, 2025.
28. VAKULINA Sasha, "'Operation Spiderweb': How Ukraine destroyed over a third of Russian bombers," *Euronews*, June 1, 2025; https://shorturl.at/6nGz2.
29. *** Trends Research & Advisory, Strategic Studies Department, *Significance and Implications of Ukraine's Operation Spiderweb*, 3 June 2025; https://trendsresearch.org/insight/significance-and-implications-of-ukraines-operation-spiderweb/.
30. *** UNHR, *UN experts urge Azerbaijan to lift Lachin corridor blockade and end humanitarian crisis in Nagorno-Karabakh*, 7 August 2023; https://www.ohchr.org/en/press-releases/2023/08/un-experts-urge-azerbaijan-lift-lachin-corridor-blockade-and-end.
31. *** Financial Times, *France detains captain of oil tanker after Denmark drone incursions*, 2 October 2025; https://www.ft.com/content/575db002-5cb0-42cf-b116-8688558cc81f.
32. *** German Federal Chancellery, *Germany gets a National Security Council*, 27 august 2025; https://www.bundesregierung.de/breg-en/news/cabinet-security-council-2381754.
33. *** "Russian Offensive Campaign Assessment", Institute for the Study of War, June 2, 2025; https://shorturl.at/MbeB6.
34. *** Joint Chiefs of Staff, *National Military Strategy*, U.S. Department of Defense, martie 2004.
35. *** Le Monde, *France: Two Moldovans charged over coffin graffiti in Paris*, Le Monde, 22 iunie 2024; https://www.lemonde.fr/en/france/article/2024/06/22/france-two-moldovans-charged-over-coffin-graffiti-in-paris_6675480_7.html.
36. *** National Commission on Terrorist Attacks upon the United States, *9/11 Commission Report*, 2002, https://govinfo.library.unt.edu/911/report/911Report.pdf.
37. *** RFI, *Russian 'shadow fleet' ship detained by French navy resumes voyage*, RFI, 3 October 2025, https://www.rfi.fr/en/international/20251003-russian-shadow-fleet-ship-detained-by-french-navy-resumes-voyage-boracay.

[1] Greg Simons, Iulian Chifu, ”Realist and Constructivist Interpretations and Representations of the Second Nagorno-Karabakh War: As an Event and as a Process”, *Journalism and Media*, vol. 6, nr. 1, 2025.

[2] Simon Magakyian, ”How Azerbaijan Weaponized Environmentalism to Justify Ethnic Cleansing”, *Time*, 22 february 2023, https://time.com/6257467/armenia-azerbaijan-nagorno-karabakh-lachin-environment-icj/; UNHR, ”UN experts urge Azerbaijan to lift Lachin corridor blockade and end humanitarian crisis in Nagorno-Karabakh”, *UNHR*, 7 August 2023, https://www.ohchr.org/en/press-releases/2023/08/un-experts-urge-azerbaijan-lift-lachin-corridor-blockade-and-end.

[3] Iulian Chifu, ”Lege, etică și legitimitate vizând proporționalitatea în război. Cazul Gaza”, *Infosfera*, vol. XVI, nr. 1, 2024, pp. 5-19; Iulian Chifu Iulian, Mihaela Drăgan, ”Polarization and radicalization as identity dynamics in a fluid environment. The case of the explosion at Al Ahli Hospital in Gaza”, *Security Science Journal*, vol. 5, nr. 1, 2024, pp. 7-21; Iulian Chifu, „Relativizarea etică a dreptului de a ucide legal ca răzbunare, sancționare a trădării și represiune. Cazul Ismail Hanyieh”, *Infosfera*, vol. XVI, nr. 4, 2024, pp. 11-21.

[4] Iulian Chifu, ”Resilience, societal security and the intangible aspects of war. Ukraine’s lessons learned”, *Romanian Military Thinking*, nr. 1, 2024, pp. 14-25.

[5] Iulian Chifu, Cosmin Grigore, ”Full-spectrum warfare. From broadening the instruments to thinking the unthinkable”, *Romanian Military Thinking*, nr. 2, 2025, pp. 10-35; Cholpon Abdyraeva, *The Use of Cyberspace in the Context of Hybrid Warfare. Means, Challenges and Trends,* Austrian Institute for International Affairs, Working Paper, nr. 107, Iunie 2020, 36 p., https://www.oiip.ac.at/cms/media/working-paper-107-cyberspace-in-the-context-of-hybrid-warfare.pdf; Alan Dupont, *Full spectrum defence: Re-thinking the fundamentals of Australian defence strategy,* Lowy Institute, March 2015, 16 p., http://www.jstor.com/stable/resrep10131; Oscar Jonsson, Robert Seely, ”Russian Full-Spectrum Conflict: An Appraisal After Ukraine”, *The Journal of Slavic Military Studies*, vol. 28, nr. 1, 2015, pp. 1-22.

[6] Ian G. R. Shaw, *Predator Empire. Drone Warfare and Full Spectrum Dominance,* University of Minnesota Press, 2016.

[7] *** Joint Chiefs of Staff, *National Military Strategy*, martie 2004; Peter W. Chiarelli, Patrick R. Michaelis, ”Winning the Peace. The Requirement for Full-Spectrum Operations”, *Military Review*, vol. LXXXV, nr. 4, 2025, Army University Press, pp. 13-26, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/COIN-Reader-1/Chiarelli-JA-2005/; Maria Ryan, ”‘Full spectrum dominance’: Donald Rumsfeld, the Department of Defense, and US irregular warfare strategy, 2001–2008”, *Small Wars & Insurgencies*, vol. 25, nr. 1, 2014, pp. 41-68.

[8] Donald H. Rumsfeld, *Guidance and Terms of Reference for the 2001 Quadrennial Defense Review,* Department of Defense, 2001, June 22, 22 p., https://www.comw.org/qdr/qdrguidance.pdf.

[9] Alan Dupont, *Op.cit*.

[10] Oscar Jonsson, Robert Seely, *Op.cit.*

[11] *Ibidem*.

[12] Erik Reichborn-Kjennerud, Patrick Cullen, *What is Hybrid Warfare?*, Norwegian Institute for International Affairs (NUPI), Policy Brief, nr. 1, 2016, 4 p., http://www.jstor.com/stable/resrep07978.

[13] Stefan Halper (ed.), “China: The Three Warfares”, Report for the Director of Office of Net Assessment, Office of the Secretary of Defense, DoD, May 2013, 565 p.

[14] Erik Reichborn-Kjennerud, Patrick Cullen, *Op.cit.*

[15] Iulian Chifu, Cosmin Grigore, *Op.cit.*

[16] National Commission on Terrorist Attacks upon the United States, *9/11 Commission Report*, 2002, https://govinfo.library.unt.edu/911/report/911Report.pdf.

[17] German Federal Chancellery, *Germany gets a National Security Council*, 27 august 2025, https://www.bundesregierung.de/breg-en/news/cabinet-security-council-2381754.

[18] *Idem*.

[19] Financial Times, *France detains captain of oil tanker after Denmark drone incursions*, 2 October 2025, https://www.ft.com/content/575db002-5cb0-42cf-b116-8688558cc81f.

[20] Radio France International, *Russian 'shadow fleet' ship detained by French navy resumes voyage*, RFI, 3 October 2025, https://www.rfi.fr/en/international/20251003-russian-shadow-fleet-ship-detained-by-french-navy-resumes-voyage-boracay.

[21] Financial Times, *Op.cit.*

[22] Hugh Schofield, Danai Nesta Kupemba, ”French troops board oil tanker linked to Russian 'shadow fleet'”*, BBC*, 1 October 2025, https://www.bbc.com/news/articles/cx2j1gynjddo.

[23] Clea Caulcutt, ”French military arrests 2 crew on suspected Russian shadow fleet vessel”, *Politico*, 2 October 2025, https://www.politico.eu/article/french-military-arrests-crew-russian-shadow-fleet-vessel-boracay/

[24] Sebastian Seibt, ”Drones, sabotage, surveillance: Moscow’s hybrid warfare takes to the high seas”*, France 24*, 3.10.2025, https://www.france24.com/en/europe/20251003-drones-sabotage-surveillance-moscow-s-hybrid-warfare-takes-to-the-high-seas.

[25] *Idem.*

[26] Financial Times, *Op.cit.*

[27] *Idem.*
[28] Sebastian Seibt, *Op.cit.*
[29] Financial Times, *Op.cit.*
[30] *Ibidem.*
[31] Sebastian Seibt, *Op.cit.*
[32] *Ibidem*.
[33] Samya Kullab, ”A surprise drone attack on airfields across Russia encapsulates Ukraine’s wartime strategy”, *Associated Press*, 2 June 2025, https://apnews.com/article/what-to-know-ukraine-drone-attack-russia-bombers-2d01b23341e2289882760b9f121431d4,
[34] Laura Gozzi & BBC Verify, ”How Ukraine carried out daring 'Spider Web' attack on Russian bombers”, *BBC*, 2 June 2025, https://www.bbc.com/news/articles/cq69qnvj6nlo.
[35] Kateryna Bondar, *How Ukraine’s Operation “Spider’s Web” Redefines Asymmetric Warfare*, CSIS, 2 June 2025, https://www.csis.org/analysis/how-ukraines-spider-web-operation-redefines-asymmetric-warfare.
[36] Tom Balmforth, Max Hunder, “To attack Russian air bases, Ukrainian spies hid drones in wooden sheds”, *Reuters*, June 1, 2025, https://shorturl.at/JXeHE.
[37] Trends Research & Advisory, Strategic Studies Department, *Significance and Implications of Ukraine’s Operation Spiderweb*, 3 June 2025; https://trendsresearch.org/insight/significance-and-implications-of-ukraines-operation-spiderweb/.
[38] Kateryna Bondar, *Op. cit.*
[39] “Russian Offensive Campaign Assessment,” Institute for the Study of War, June 2, 2025, https://shorturl.at/MbeB6.
[40] Constant Méheut, Ivan Nechepurenko, Nataliya Vasilyeva, “Ukraine and Russia Met for 2nd Round of Talks as Attacks Escalate”, *The New York Times*, June 2, 2025, https://shorturl.at/YiQT6.
[41] Trends Research & Advisory, Strategic Studies Department, *Op. cit.*
[42] Sasha Vakulina, “’Operation Spiderweb’: How Ukraine destroyed over a third of Russian bombers”, *Euronews*, June 1, 2025, https://shorturl.at/6nGz2.
[43] Katja Bago, *Ukraine’s Operation Spider’s Web is a game-changer for modern drone warfare. NATO should pay attention*, 17 July 2025; https://www.chathamhouse.org/2025/06/ukraines-operation-spiders-web-game-changer-modern-drone-warfare-nato-should-pay-attention.
[44] *Ibidem*.
[45] Dominic Culverwell, ”Moldovan citizens detained over graffiti warning against sending French soldiers to Ukraine”, *kyivindependent*, 10 June 2024; https://kyivindependent.com/moldovan-citizens-detained-over-graffiti-depicting-dead-french-soldiers-in-ukraine/.
[46] *Idem*.
[47] ***, ”France: Two Moldovans charged over coffin graffiti in Paris”, *Le Monde*, 22 iunie 2024; https://www.lemonde.fr/en/france/article/2024/06/22/france-two-moldovans-charged-over-coffin-graffiti-in-paris_6675480_7.html.
[48] Anastasia Lisova, *Three Moldovans to be tried in France for graffiti with coffins of "French soldiers in Ukraine"*, Liga.net, 9 octombrie 2025; https://news.liga.net/en/politics/news/three-moldovans-to-be-tried-in-france-for-graffiti-with-coffins-of-french-soldiers-in-ukraine.

DIPLOMAȚIA CULTURALĂ A TURCIEI - ÎNTRE PRAGMATISM KEMALIST, PANTURCISM ȘI NEO-OTOMANISM

Isabela ANCUȚ*

Abstract

Elements regarding national identity, culture, religion or ethnicity play an essential role in defining the concept of cultural diplomacy. At a practical level, cultural diplomacy plays an essential role in the implementation of foreign policy, being a useful tool in achieving state interests and contributing to the creation of favorable conditions for the fulfillment of a state`s foreign policy objectives.

As for Turkiye, cultural diplomacy has succeeded in creating the image of a modern Islamic state, a promoter of humanitarian diplomacy, a state that wants "zero problems with its neighbors" and that can mediate the negociation of international agreements in order to establish peace at regional level.

Keywords**:** *cultural diplomacy; international relations; soft power; pan-Turkism; neo-otomanism.*

DIPLOMAȚIA CULTURALĂ

Conceptul de „diplomație culturală" pare ușor de definit, însă realitatea reprezintă tocmai contrariul acestei afirmații. În ultimele decenii acest concept a „îmbrăcat" numeroase forme, definițiile variind în funcție de țara de origine, de istoria și caracteristicile sale naționale, de interesele strategice ale acesteia și chiar de orientările geopolitice și geostrategice ale specialiștilor care au enunțat definiția. Unul dintre cei mai cunoscuți specialiști din domeniu, Milton C. Cummings Jr., definea diplomația culturală drept „schimbul de idei, informații, artă și alte aspecte ale culturii între națiuni și popoarele acestora, cu scopul de a iniția înțelegerea reciprocă"[1]. La nivel practic, importanța conceptului a fost determinată de evoluțiile geopolitice și geostrategice de pe scena internațională, acesta având un alt efect pe timpul existenței bipolarității din perioada Războiului Rece în comparație cu efectele contemporane, influențate de existența unei multitudini de actori statali și non-statali a căror putere se poate aprecia a fi de importanță egală.

Factorii care privesc identitatea națională, cultura, religia sau etnia joacă un rol esențial în definirea conceptului de diplomație culturală[2].

****Doctor în Științe Militare și Informații.***

Achiesăm la afirmațiile potrivit cărora „într-o lume tot mai mult interconectată, nu ne mai putem gândi la cultură ca fiind *subordonată* politicii. În schimb ne putem gândi la cultură ca fiind cea care *furnizează contextul operațional* pentru politică”[3], aceste opinii contribuind la consolidarea ideii de *soft power* promovată de Joseph S. Nye[4]. În fapt, dacă analizăm definițiile clasice ale conceptului și ceea ce J. Nye definește drept *soft power* vom identifica o idee centrală comună, respectiv faptul că „scopul este de a forma o mentalitate colectivă într-o comunitate externă, care să reproducă modalitățile de existență și funcționalitate ale statului care acționează”, cât mai aproape de realitatea acestuia[5]. Ca exemplu al complexității procesului de definire a conceptului, menționăm că, utilizând ca termen de căutare sintagma „diplomație publică”, unii specialiști brazilieni[6] au găsit, la nivel național, peste 468 de înregistrări. Iar conex definirii acestui concept au identificat peste 1031 înregistrări pentru termenul de „soft power” și 156 pentru „diplomația publică”.

Globalizarea a facilitat diversificarea instrumentelor diplomației culturale, crescând ritmul cu care au apărut (printr-un proces de copiere/ reproducere) o multitudine de organisme private cu rol similar, dacă nu chiar identic, cu cel îndeplinit de către unele instituții și organisme oficiale/ statale specifice domeniului[7]. Astfel, în anul 1965, decanul Școlii de Drept și Diplomație din cadrul Universității Tufts, Edmund Gullion, a înființat *Centrul de diplomație publică Edward R. Murrow*, prin care promova o serie de programe, finanțate de guvern, al căror scop consta în influențarea opiniei publice străine. Prin urmare, se poate afirma că diplomația a devenit și un mijloc de manipulare ideologică foarte eficientă pentru unii lideri regionali sau internaționali, atunci când au dorit să se impună sau să-și consolideze *statu-quo*-ul pe scena internațională[8]. Această idee a fost acceptată și de Gifford D. Malone, care afirma că se pot influența cetățenii unui stat astfel încât să accepte și să promoveze, mai departe, o atitudine pozitivă față de un terț stat[9], iar Jian Wang sublinia că diplomația publică „poate face posibil procesul de transformare a reputației unui stat într-un mod care să-i determine poziția pe scena internațională. Reputația își are rădăcina în opinia publică și, astfel, indică dacă statul are mandat pentru inițiativele sale”[10].

Alături de aspectele pozitive generate de *diplomația culturală* au apărut și aspecte discutabile, precum utilizarea sa pentru atenuarea percepției negative create de către anumiți actori internaționali și/ sau clase conducătoare/ lideri de state, diplomația culturală devenind unul dintre cele mai eficiente instrumente de manipulare[11]. Poate cel ușor exemplu în acest sens ar fi diplomația sportului (baschet) practicată de Coreea de Nord sau, pe timpul Războiului Rece, diplomația bazată pe promovarea baletului la nivel internațional de către liderii de la Kremlin.

Contemporaneitatea ne-a demonstrat că diplomația culturală utilizată de actorii non-statali a complicat așa-numita „diplomație reală”, în sensul că dacă un actor statal (sau un actor statal terț) se implică și oferă susținere unui actor non-statal pentru atingerea scopurilor proprii, atunci acest demers va influența, pe termen lung, politica și diplomația actorului statal. Situația a fost și este evidentă în cazul actorilor implicați în crizele din Orientul Mijlociu Extins. Din păcate, lupta pentru putere, pentru reala putere, este în plină desfășurare, iar diplomația culturală este instrumentul ideal prin care se poate susține expansiunea și exploatarea de noi teritorii sau se testează legătura cu trecutul, cu identitatea națională, cu religia[12]. Demersul nu reprezintă o idee nouă, iar istoria ne demonstrează faptul foarte simplu, cu exemple precum Franța și a sa politică de promovare a francofoniei, Germania și politicile sale de reîntregire a Marii Germanii sau Marea Britanie și vastul său imperiu.

Dezvoltarea tehnologică, creșterea economică, accentuarea clivajelor între clasele sociale și/ sau diverse minorități etnice/ religioase sunt factori care au potențat dezvoltarea conceptului de diplomație culturală. Turcia reprezintă un exemplu elocvent și de succes în ceea ce privește câștigarea de noi oportunități comerciale și piețe de desfacere, de proiectare a intereselor sale strategice de lungă durată în zonele considerate de interes pentru conducerea de la Ankara și nu numai. Aceste proiecții externe

își regăsesc imaginea și în succesele parțiale sau totale înregistrate pe plan intern. Chiar dacă direcțiile de politică externă ale Turciei permit interpretări diverse, diplomația sa culturală și strategiile acesteia au reușit schimbarea percepției la nivel internațional, au permis crearea de noi alianțe (unele chiar surprinzătoare) și implementarea, la începutul secolului XXI a așa-numitei politici externe de „zero probleme cu vecinii".

DIPLOMAȚIA CULTURALĂ A TURCIEI

Turcia este un actor regional semnificativ, un jucător strategic important pe scena internațională, iar actuala conducere de la Ankara nu numai că dorește să-și consolideze importanța, dar aspiră la un rol și mai important alături de „greii" lumii. Politica externă turcă a început să se manifeste și în regiuni îndepărtate de sfera sa de interese (precum Balcanii), cum ar fi Orientul Mijlociu Extins, Asia-Pacific, America Latină și Europa de Nord, iar diplomația culturală turcă are ca scop principal promovarea influenței Turciei în regiuni de interes strategic, inclusiv prin diminuarea/ eliminarea percepțiilor negative legate de istoria expansiunii Imperiului Otoman din secolele trecute[13]. În prezent, acest tip de diplomație a reușit să creeze imaginea unui stat islamic modern, în comparație cu alte state musulmane, un promotor al diplomației sănătății, umanității și educației superioare și academice de nivel mondial, un stat care dorește „zero probleme cu vecinii" și care poate mijloci negocierea de acorduri internaționale în vederea instaurării păcii. Esența acestor acțiuni vine din ideologia neo-otomanismului, promovată de către fostul ministru turc de externe, Ahmet Davutoglu[14], care, în lucrarea sa „Profunzimi Strategice"[15], arăta că diplomația culturală a Turciei ar trebui să joace un rol esențial în realizarea imaginii unui stat modern, unde regiunea Anatoliei ar putea reprezenta puntea dintre Europa, Africa și Asia, iar „interesele geopolitice ale Ankarei trebuie urmărite printr-o profunzime strategică ce se întinde pe trei continente"[16].

Ideea nu a fost o noutate (și fostul președinte turc Turgut Özal o susținea), deoarece, în alte forme, a fost promovată și pe timpul Războiului Rece. Treptat, s-a constituit o imensă rețea de instituții statale și private al cărei scop unic constă în promovarea acestei diplomații culturale. Poate cea mai cunoscută rămâne Direcția pentru Afaceri Religioase în Străinătate (*Diyanet*), care gestionează (cel puțin financiar) peste 2000 de moschei aflate în statele europene (chiar și în statele baltice), latino-americane și africane, promovând educația religioasă islamică. Acțiunile unor astfel de instituții de stat au fost dublate de acțiunile unor organizații regionale și/ sau internaționale precum Consiliul Islamic Eurasia, Consiliul Islamic al Țărilor Balcanice, Summit-ul Liderilor Religioși Africani, Summit-ul Musulman al țărilor din America Latină[17]. Liderii de la Ankara sunt conștienți că dacă statul turc va reuși să-și legitimeze puterea și acțiunile în fața altor state prin instrumente de tip soft power, va întâmpina o rezistență mai mică (sau chiar deloc) atunci când va dori să implementeze politicile privind realizarea intereselor sale strategice. Și cel mai facil instrument aflat la îndemâna sa este cel cultural, în ansamblul său.

După criza financiară internațională din 2007-2009, au apărut, la nivel global, idei privind nevoia unei noi ordini mondiale, clivaje la nivelul societăților naționale și între vechile alianțe, ciocniri între actorii statali și cei non-statali, totul ducând spre necesitatea declanșării unui proces de transformare. Și Turcia a decis că este necesar un proces de transformare internă, ceea ce i-a și adus noi deschideri către noi centre de putere. Schimbarea dinamicii interne în Turcia a generat schimbări de percepție despre acest stat în Europa, Americi, Orientul Mijlociu, Africa și Asia.

Schimbările de percepții din exterior au forțat Ankara să genereze noi strategii de abordare în politica sa externă, inclusiv în domeniul diplomației culturale[18]. Specialiștii turci[19] din domeniu au considerat că schimbările din politica externă turcă „nu pot fi limitate la transformările unor aspecte de tip ideologic și nici de unele anxietăți de tip Realpolitik"[20]. Diplomația

culturală/ diplomația publică (soft power-ul turc) s-a manifestat în plen după 2010, dar într-un mod specific Turciei deoarece potențialul acesteia este, în mod semnificativ, ancorat în experiența sa culturală și istorică. Moștenirea Imperiului Otoman pare a reînvia, deși unii specialiști turci[21] nu o consideră parte a unei noi ideologii – neo-otomanismul. Cu alte cuvinte, transformarea Turciei într-un nucleu de influență pentru Balcani și Orientul Mijlociu Extins va depinde mereu de abilitatea sa de a păstra un echilibru perfect între *libertate* și *securitate* chiar în timpul proceselor de afirmare a intereselor în diferite regiuni strategice.

Statutul de mediator, de pacifist, de stat cu o strategie de apărare și izolat de conflicte externe, însușit de Turcia lui R.T. Erdoğan, este o nouă realitate în plan practic. Turcia este parte foarte activă a dinamicii politice și strategice din Balcani, Orientul Mijlociu Extins și Caucaz. În același timp, este binecunoscut faptul că elitele intelectuale turce acționează pentru consolidarea sentimentului identitar de apartenență a comunităților musulmane (cu precădere din Bosnia **și** Herțegovina), având o puternică filiație islamică și legături strânse pe planul culturii, respectiv în tradițiile religioase din Anatolia. Cu alte cuvinte, manifestarea intereselor Turciei (de actor regional) în Bosnia și Herțegovina, Macedonia de Nord și Albania se face simțită prin orchestrarea unei reale strategii cu instrumente de politică externă, respectiv de diplomație culturală și de oportunități economice, fundamentate pe afinitatea culturală și spirituală.

Acțiunile de diplomație publică ale unor instituții precum TIKA (*Turkish International Cooperation and Development Agency*), Kizilay (*The Turkish Red Crescent*), Ministerul Turismului și Culturii, Ministerul de Externe, ale diverselor televiziuni, ale Fundației Yunus Emre, ale Oficiului de Diplomație Publică etc. sunt extrem de cunoscute datorită intensității acestora. Dovezile extrem de vizibile ale diplomației culturale turcești se concretizează și în instituțiile și organizațiile înființate pentru diaspora turcă, în cele peste 200 de universități și institute înființate cu scopul de „a populariza arta și cultura turcă către publicul străin, predarea limbii turce și furnizarea de informații despre trecutul istoric otoman și atragerea de simpatizanți pentru spiritualitatea islamică (..), respectiv exportul unei imagini pozitive a Turciei în lume”[22].

AVANTAJELE ȘI DEZAVANTAJELE DIPLOMAȚIEI CULTURALE ALE TURCIEI

Unele probleme întâmpinate de Turcia în dezvoltarea sa la nivel intern își găsesc originile într-o acțiune externă, respectiv în momentul încetării existenței Imperiului Otoman, consfințit de Tratatul de la Sèvres (10 august 1920)[23]. Realizând un salt în timp, intrarea în Uniunea Europeană și beneficiile economice ce derivă din aceasta, modernizarea și globalizarea, pot fi extrem de atractive pentru societatea turcă, dar sunt dublate de teama indusă de posibilele efecte care ar putea fi generate de un „nou Tratat Sèvres”, așa cum menționează chiar președintele R.T. Erdoğan în discursurile sale.

Pornind de la necesitatea unui balans între riscuri și oportunități, liderii turci au considerat, cel mai probabil, că afirmarea poziției geostrategice pe scena internațională trebuie corelată cu o imagine „bună”, redimensionând toate fațetele diplomației turce, în ansamblu. Pe de altă parte, dacă este să luăm în considerare opiniile expertului Darko Tanasković[24], influența tezelor „neo-otomaniste” se bazează pe un „amalgam ideologic de Islamism, (Pan)Turcism și Imperialism Otoman”, amalgam susținut de promovarea activă (la nivelul diplomației culturale) a aspectelor istorice și geografice specifice în fostele teritorii ale Imperiului Otoman. Kemalismul (doctrina eurasianistă a lui Mustafa Kemal Attatürk) și orientarea sa pro-occidentală nu pot dispare, ci se „strecoară” discret în discursul lui R.T. Erdoğan, alături de ideile de neo-otomanism, președintele turc realizând un echilibru între conștientizarea trecutului istoric, care generează profunzimea strategică, și acțiunile care depășesc sferele clasice de influență ale Turciei și care creează profunzimea istorică, precum reactivarea relațiilor cu minoritățile turcești din fostele provincii otomane (din Balcani,

Orientul Mijlociu, Caucaz). Un echilibru identic îl „joacă" președintele turc și atunci când vorbim de secularismul kemalist și Islamul tradiționalist, în acest aspect R.T. Erdoğan acționând fabulos, conform unei idei mai vechi (cea a fostului președinte T. Özal), demonstrând că libertatea religioasă poate exista chiar și în prezența unei democrații de tip occidental, responsabilitatea socială promovată de islamiști fiind adoptată de către clasa laică modernă, și amândouă susținând mândria națională turcă.

La nivel regional, viziunea lui Erdoğan s-a manifestat prin „atipicitatea" alianțelor încheiate la nivel bi- și multilateral, Turcia reușind să „provoace" unele reguli și percepții stabilite după Războiul Rece, contestând acele politici care i-ar putea afecta interesele. Turcia dorește să aibă suficientă putere pentru a influența balanța de putere dintre SUA și Rusia, precum și dreptul de a decide cu cine încheie alianțe, bazându-se pe experiența sa istorică, în condițiile în care Eurasia a fost (și este) un spațiu de confluență a direcțiilor de dominație culturală, istorică, politică și economică ale Occidentului, civilizațiilor asiatice și lumii arabe.

În ultimele decenii, Turcia a urmărit să joace un rol mai important în Libia, Siria și Azerbaidjan, în Marea Egee și Europa, fiind totodată deschisă către o cooperare oportunistă, dar eficientă, cu Iranul[25]. La nivel practic, eurasianismul turc, în special prin statutul de membru al NATO, este un atu al Turciei în relațiile cu F.Rusă. R.P. Chineză și Iran, cu precădere prin prisma tensiunilor pe care le induce în interiorul acestui triunghi[26]. Ca și restul statelor, Turcia rămâne foarte pragmatică în urmărirea intereselor strategice în cadrul sistemului internațional. Pentru liderii de la Ankara mai există un punct de interes, care le aduce multe avantaje în relațiile cu actorii de pe scena internațională – Balcanii de Vest. Acest spațiu oferă cel mai elocvent exemplu de diplomație publică (spre deosebire de restul zonelor unde a intervenit elementul de hard power), acțiunile culturale și financiar-bancare economice finanțate de către Turcia demonstrând preocuparea deosebită a acesteia pentru consolidarea amprentei identitare turcice în regiune, preocupare care excede retorica caracteristică neo-otomanismului.

Astfel, în prima parte a secolului XXI, Turcia a încercat să realizeze un echilibru între trei atitudini: „să fie cooperantă pentru a prospera ca și Occidentul, să se teamă de Occident ca urmare a Sindromului Sèvres și/ sau să adopte o atitudine superioară, neo-imperialistă în relația cu Occidentul"[27]. În acest context, pendularea Administrației Erdoğan între ideologiile strategice pan-turcice, panislamiste și neo-otomaniste ar putea genera atât oportunități, cât și provocări pentru viitoarea politică externă a statului turc, inclusiv din perspectiva diplomației culturale.

BIBLIOGRAFIE

1. ARNDT T. Richard, *The First Resort of Kings. American Cultural Diplomacy in the Twentieth Century,* Potomac Books Inc., Washington, D.C., 2006.
2. BOUND Kirsten, Briggs Rachel, Holden John, Jones Samuel, *Culture is a central component of international relations. It's time to unlock its full potential* ..., Ed. Demos, Londra, 2007.
3. CLARKE David, "Cultural diplomacy", *Oxford Research Encyclopedia of International Studies,* Oxford University Press, 2020, http://doi.org/10.1093/acrefore/9780190846626.013, republicat în ORCA, Cardiff University's institutional repository: http://orca.cardiff.ac.uk/id/eprint/133791/
4. CONSTANTIN-BERCEAN Ioana, *Pentru cine bat clopotele? China, Rusia Iran* și *Turcia – modelul eurasiatic al aliațelor de necessitate*, LARICS, 28.09.2022, https://larics.ro/pentru-cine-bat-clopotele-china-rusia-iran-si-turcia-modelul-eurasiatic-al-aliantelor-denecesitate/.
5. CULL J. Nicholas, "Public diplomacy: Taxonomies and Histories", *The Annals of the American Academy of Political and Social Science*, nr. 616 (1), 2008, pp. 31-54.
6. CUMMINGS C. Milton, *Cultural Diplomacy and the United State Government: a Survey*, Center for Arts and Culture, 2003.
7. DAVUTOGLU Ahmet, *Stratejik Derinlik*, Ed. Kure Yayinlari, 2009, 584 p.
8. FREDERIC H. Howard, *Global communication and international relations*, Belmont CA, Wadsworth, 1993, 306 p.
9. GILBOA Eytan, "Diplomacy in the media age: Three models of uses and effect", *Diplomacy & Statecraft*, vol. 12, nr. 2, 2001, pp. 1-28.
10. GRAHAM Sarah Ellen, *Culture and Propaganda. The Progressive Origins of American Public Diplomacy, 1936-1953*, Ashgate, 2015.
11. GROSOIU Gabriel-Sorin, *„Sultanul" Erdoğan* în *Balcanii de Vest. Neo-otomanism* și *pragmatism*, LARICS, 28.09.2022.
12. GUMENYUK Tatyana, Frotveit Maryna, Bondar Ihor, Horban Yurii, Karakoz Olena, "Cultural Diplomacy in Modern International Relations: The Influence of Digitalization", *Journal of Theoretical and Applied Information Technology*, vol. 99, nr. 7, 2021, Little Lion Scientific, 15.04.2021, accesat la www.jatit.org.
13. HLIHOR Constantin, *România și șocurile geopolitice ale Războiului Rece (1980-1991)*, Ed. Institutului Revoluției Române din Decembrie 1989, București, 2016.
14. HLIHOR Ecaterina, "Ideologie și diplomație publică: neo-otomanismul turc", *Gândirea Militară Românească*, nr. 4, 2023, pp. 336-349.
15. HLIHOR Ecaterina, *Diplomația publică în politica internațională*, Ed. Universității Naționale de Apărare „Carol I", 2017.
16. KALIN Ibrahim, "Soft Power and Public Diplomacy in Turkey", *Percepțions: Journal of International Affairs*, Center for Strategic Research, vol. XVI, nr. 3, 2011, pp. 5-23, http://dergipark.org.tr/download/article-file/816442.
17. KALIN Ibrahim, "Debating Turkey in the Middle East: The Dawn of a New Geopolitical Imagination", *Insight Turkey*, vol. 11, nr. 1, 2009, pp. 83-96.
18. KURLANTZICK Joshua, *Charm offensive: how China's soft power is transforming the world*, Yale University Press, 2007.
19. LEONARD Mark, Catherine Stead, Conrad Smewing, *Public Diplomacy,* Foreign Policy Centre, Londra, 2002.
20. MALONE D. Gifford, *Political Advocacy and Cultural Communication: Organizing the Nation's Public Diplomacy*, vol. 11, University Press of America, Boston, 1988, 162 p.
21. MASSARA Gaetano, *Turkey`s imperial ambitions between dreams and reality*, Aspenia online. International analysis and commnetary, Aspen Institute Italia, 2022, http://aspeniaonline.it/turkeys-imperial-ambitions-between-dreams-and-reality/
22. NYE S. Joseph, *Soft Power. The means to*

succeed in world politics, Public Affairs, New York, 2004.
23. NYE S. Joseph, *The Future of Powe*r, New York, Public Affairs, 2011.
24. PAJTINKA Erik, ”Cultural Diplomacy in Theory and Practice of Contemporary International Relations”, *Politické vedy/ Studies*, vol. 12, nr. 4, 2014, pp. 95-108.
25. ROTARU Veronica, ”Mecanisme și practici contemporane de cooperare a Republicii Moldova în contextul diplomației culturale”*,* în vol. *Știința politică și societatea în schimbare,* Chișinău, 2015, 667 p.
26. SIGNITZER H. Benno, ”Public Relations and Public Diplomacy: Some Conceptual Explorations”, în *Public Relations Research. European and International Perspectives and Innovations* (Ansgar Zerfass, Betteke Ruler, Krishnamurthy Sriramesh eds.), VS Verlag fur Sozialwissenchaften, Wiesbaden, 2008.
27. SCHNEIDER P. Cynthia, *Culture Communicates: US Diplomacy that Works*, Discussion Paper in Diplomacy, Netherlands Institute of International Relations ”Clingendael”, nr. 24, 2004.
28. SCHULTZ P. George, *Diplomacy in the Information Age*, Virtual Diplomacy Conference, United States Institute of Peace, Washington D.C., 01.04.1997.
29. SNOW Nancy și Nicholas J. Cull (coord.), *The Oxford Handbook of Modern Diplomac*y, Oxford University Press, 2020.
30. ZANELLA Koehler Cristine, Edson José Neves Junior, Livia Ribeiro da Silva, ”Cultural Diplomacy and Soft Power: Critical Analysis and Methodological Application”, *Revista Brasiliera de Politica Internacional/RBPI*, 05.07.2024, 18 p., http://www.scielo.br/rbpi.
31. ZAMORANO Mariano Martin, ”Reframing Cultural Diplomacy: The Instrumentalization of Culture under The Soft Power Theory”, *Culture Unbound. Journal of Current Culture Research*, vol. 8, 2010, Linköping University Electronic Press, http://www.cultureunbound.ep.liu.se
32. WANG Jian, ”Managing international reputation and international relations in the global era: Public diplomacy revisited”, *Public Relations Review*, vol. 32, nr. 2, 2006, pp. 91-96.
33. WYSZOMIRSKI J. Margaret, Burgess Christopher, Peila Catherine, *International Cultural Relations: A Multi-Country Comparison*, Center for Art and Culture, Ohio, USA, 2003.

[1] Milton C. Cummings Jr., *Cultural Diplomacy and the United States Government: A Surve*y, Washington D.C., Center for Arts and Culture, 2003, p.1.

[2] Mark Leonard, *Public Diplomacy,* Foreign Policy Centre, Londra, 2002.

[3] Kirsten Bound, Rachel Briggs, John Holden, Samuel Jones, *Culture is a central component of international relations. It's time to unlock its full potential* ..., Cultural Diplomacy, Demos, Londra, 2007, p. 20.

[4] Joseph S. Nye, *Soft Power*. *The means to succeed in world politics,* Public Affairs, New York, 2004; Idem., *The Future of Power,* New York, Public Affairs, 2011, pp. 20-21.

[5] *Idem.*

[6] Cristine Koehler Zanella, Edson José Neves Junior, Livia Ribeiro da Silva, "Cultural Diplomacy and Soft Power: critical analysis and methodological application", *Revista Brasiliera de Politica Internacional/RBPI*, 05.07.2024, http://www.scielo.br/rbpi.

[7] Mariano Martin Zamorano, "Reframing Cultural Diplomacy: The Instrumentalization of Culture under the Soft Power Theory", *Culture Unbound. Journal of Current Culture Research*, vol. 8, nr. 2, 2016, Linköping University Electronic Press, pp. 165-186, http://www.cultureunbound.ep.liu.se; *apud.* Margaret J. Wyszomirski, Christopher Burgess, Catherine Peila, *International Cultural Relations: A Multi-Country Comparison*, Cultural Diplomacy Research Series, Center for Art and Culture, Ohio, USA, 2003.

[8] Veronica Rotaru, "Mecanisme și practici contemporane de cooperare a Republicii Moldova în contextul diplomației culturale", în vol. *Știința politică și societatea în schimbare,* Chișinău, 2015, pp. 499-505, accesat la adresa http://ibn.idsi.md/sites/default/files/imag_file/499-505 0.pdf.

[9] Gifford D. Malone, *Political Advocacy and Cultural Communication: Organizing the Nation's Public Diplomacy*, vol. 11, University Press of America, Boston, 1988, p. 1.

[10] Jian Wang, "Managing international reputation and international relations in the global era: Public diplomacy revisited", *Public Relations Review*, vol. 32, nr. 2, 2006, p. 92.

[11] David Clarke, *Cultural diplomacy*, Oxford Research Encyclopedias: International Studies, Oxford University Press, 2020, 51 p., http://doi.org/10.1093/acrefore/9780190846626.013, republicat în ORCA, Cardiff University's Institutional Repository, http://orca.cardiff.ac.uk/id/eprint/133791/; apud. Patricia M. Goff, "Cultural diplomacy", în Nancy Snow și Nicholas J. Cull (coord.), *The Oxford Handbook of Modern Diplomacy*, Oxford University Press, 2020, pp. 30-37; a se vedea și Joshua Kurlantzick, *Charm Offensive: How China's Soft Power Is Transforming the World*, Yale University Press, 2007.

[12] Constantin Hlihor, *România și șocurile geopolitice ale Războiului Rece (1980-1991)*, Ed. Institutului Revoluției Române din Decembrie 1989, București, 2016; Ecaterina Hlihor, *Diplomația publică în politica internațională*, Ed. Universității Naționale de Apărare „Carol I", 2017; Ecaterina Hlihor, "Ideologie și diplomație publică: neo-otomanismul turc", *Gândirea Militară Românească*, nr. 4, 2023, pp. 336-349.

[13] Ibrahim Kalin, "Soft Power and Public Diplomacy in Turkey", *Percepțions: Journal of International Affairs*, Center for Strategic Research, vol. XVI, nr. 3, 2011, pp. 5-23, http://dergipark.org.tr/download/article-file/816442.

[14] Ministru de externe al Turciei în perioada 2009-2014.

[15] *Stratejik Derinlik*, 2001.

[16] Gaetano Massara, *Turkey`s imperial ambitions between dreams and reality*, Aspenia, 2022, http://aspeniaonline.it/turkeys-imperial-ambitions-between-dreams-and-reality/

[17] Ecaterina Hlihor, „Ideologie și diplomație publică: neo-otomanismul turc", *Gândirea Militară Românească*, nr. 4, 2023, pp. 336-349.

[18] Ibrahim Kalin, "Turkey and the Middle East: Ideology or Geopolitics", *Private View*, nr. 13, 2008, pp. 26-35.

[19] *Idem*., "Debating Turkey in the Middle East: The Dawn of a New Geopolitical Imagination", *Insight Turkey*, vol. 11, nr. 1, 2009, pp. 83-96; a se vedea și "US - Turkish Relations under Obama: Promise, Challenge and Opportunity in the 21st Century", *Journal of Balkan and Near East Studies*, vol. 12, nr. 1, 2010, pp. 93-108.

[20] *Ibidem.*

[21] *Ibidem.*

[22] Ecaterina Hlihor, *Ideologie și diplomație publică: neo-otomanismul turc*, Universitatea Națională de Apărare „Carol I", București, 2023.

[23] Matei Blănaru, *Sondaje – ce cred turcii într-adevăr despre Occident? Între dorința de prosperitate, complexul de superioritate și teama din sindromul Sèvres,* LARICS, 07.08.2023, București.

[24] Darko Tanasković, *From neo-ottomanism to Erdoganism: a doctrine and foreign policy of Turkey,* Association of Non-Governmental Organisations of Southeast Europe CIVIS, Belgrad, 2016; citat de Blănaru Matei, *Geopolitica Turciei lui Erdoğan*, LARICS, 26.12.2023.

[25] Gabriel-Sorin Grosoiu, *„Sultanul" Erdoğan în Balcanii de Vest. Neo-otomanism și pragmatism*, LARICS, 28.09.2022, https://larics.ro/sultanul-erdogan-in-balcanii-de-vest-neo-otomanism-si-pragmatism/, accesat la 02.02.2026.

[26] Ioana Constantin-Bercean, *Pentru cine bat clopotele?. China, Rusia Iran și Turcia – modelul eurasiatic al alianțelor de necesitate*, LARICS, 28.09.2022, https://larics.ro/pentru-cine-bat-clopotele-china-rusia-iran-si-turcia-modelul-eurasiatic-al-aliantelor-denecesitate/, accesat la 29.01.2026.

[27] *Ibidem.*

IMPACTUL CLIMATULUI GEOPOLITIC GENERAT DE F.RUSĂ ASUPRA ACTIVITĂȚILOR DE INTELLIGENCE ÎN EUROPA

Eugen-Nicolae BOGOVICI*

Motto:

„In the age of information, ignorance is a choice, and knowledge is a weapon."
Alvin TOFFLER

Abstract

The geopolitical climate shaped by the Russian Federation has transformed the operational environment of European intelligence and counterintelligence services. Strategic competition now unfolds predominantly below the threshold of open armed conflict, where intelligence operations, cyber capabilities, and information warfare function as primary instruments of state power. Within this environment, the protection of national decision-making autonomy and institutional resilience has become a main security imperative.

Russian strategy integrates hybrid instruments—including clandestine intelligence collection, influence networks, economic leverage, cyber intrusions, and coordinated narrative amplification—designed to exploit structural vulnerabilities inherent in open democratic systems. The informational and cognitive domain has emerged as a decisive arena, where perceptions, legitimacy, and societal cohesion are systematically targeted. Operations are calibrated to erode trust in institutions, polarize public discourse, and shape strategic outcomes without triggering conventional military confrontation.

The transformation of the European security architecture since 2014 has reinforced the relevance of counterintelligence as a systemic function extending beyond classical counter-espionage. Contemporary counterintelligence encompasses the protection of classified information, the safeguarding of strategic communications, and the defense of the decision-making process against infiltration, manipulation, and cognitive distortion. Institutional penetration may occur through diplomatic cover, economic entanglement, academic or media front structures, and indirect influence mechanisms, requiring comprehensive and legally grounded preventive frameworks.

Sustainable resilience depends on anticipatory governance, interinstitutional cooperation, reduction of strategic dependencies, and societal robustness against manipulation. Over the 2026–2035 horizon, hybrid competition in the Black Sea region is expected to remain structurally embedded, requiring adaptive security architectures capable of protecting democratic legitimacy and sovereign strategic choice.

Keywords: *strategic competition; hybrid threats; intelligence; counterintelligence; information warfare; cognitive domain; critical infrastructure protection; Black Sea security; decision-making resilience.*

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

CLIMATUL GEOPOLITIC CONTEMPORAN ȘI ROLUL F.RUSE

Federația Rusă ca actor revizionist în spațiul euroatlantic

În contextul evoluțiilor geopolitice din ultima perioadă, F.Rusă s-a manifestat tot mai clar ca un actor revizionist în arhitectura de securitate euroatlantică, contestând ordinea internațională. În percepția și practica factorilor decizionali europeni, F.Rusă întrunește mai multe elemente definitorii ale strategiei revizioniste, ceea ce a determinat o reevaluare amplă a conceptelor tradiționale de securitate colectivă și a instrumentelor de răspuns ale UE și NATO. Intensificarea acțiunilor hibride denotă continuitate doctrinară și operațională: de la instrumentele clasice ale spionajului și influenței până la noile tactici care exploatează vulnerabilitățile digitale și mediile informaționale ale societăților democratice.

Totodată, acest caracter revizionist al politicii externe ruse nu se reflectă doar prin intensitatea operațiunilor hibride, ci și prin modul în care aceste operațiuni vizează structurile aflate la guvernare, prin interferarea în derularea proceselor electorale și prin afectarea coeziunii sociale a statelor membre UE. Acțiunile Moscovei urmăresc fragmentarea societăților occidentale și exploatarea polarizării interne pentru crearea de discrepanțe sociale, astfel încât să favorizeze erodarea încrederii în sistemul democratic.

Zona gri și competiția sub pragul conflictului armat

Evoluția mediului de securitate european evidențiază o tendință accentuată de mutare a confruntării geopolitice în așa-numita „zonă gri”, un spațiu operațional aflat între pace și război, caracterizat prin acțiuni deliberate desfășurate sub pragul confruntării armate convenționale. În acest cadru, competiția dintre state nu mai este definită exclusiv prin utilizarea forțelor armate, ci prin ansamblul de instrumente non-cinetice menite să producă efecte strategice semnificative fără declanșarea mecanismelor clasice de răspuns.

În acest context, competiția sub pragul conflictului armat devine un adevărat test al capacității statelor de a anticipa, detecta și, mai ales, de a gestiona amenințările care nu urmăresc o victorie rapidă, ci obținerea unui avantaj strategic gradual. Această zonă gri nu reprezintă o etapă tranzitorie spre conflict, ci o formă distinctă și durabilă de confruntare, cu implicații directe asupra modului în care este concepută și implementată securitatea europeană la momentul actual.

Dimensiunea informațională a confruntării geopolitice

Dimensiunea informațională a devenit un spațiu distinct al competiției strategice, cu relevanță comparabilă domeniilor terestru, aerian, maritim. Spre deosebire de acestea, componenta informațională nu are delimitare geografică, nu este reglementată unitar și nu presupune o separație clară între actorii statali și non-statali. Această caracteristică o transformă într-un domeniu favorabil confruntărilor indirecte, unde influența, percepția și controlul au impact strategic fără utilizarea forțelor armate.

Confruntarea informațională se manifestă prin competiția pentru controlul agendei publice, al interpretării evenimentelor și al cadrului cognitiv în care deciziile politico-sociale sunt luate. În acest sens, informația nu mai este doar un canal al comunicării, ci și cea mai importantă resursă strategică, utilizată pentru modelarea comportamentală, inducerea confuziei sau alterarea raportului dintre realitate și percepție. Obiectivul nu este întotdeauna convingerea totală a publicului-țintă, ci fragmentarea acestuia, diminuarea consensului unitar și pierderea încrederii față de autoritățile naționale.

METODELE DE INTELLIGENCE UTILIZATE DE F.RUSĂ ÎN CONTEXT EUROPEAN

Intelligence-ul ca instrument strategic al politicii externe ruse

În arhitectura de putere a F.Ruse, *Intelligence-ul* ocupă o poziție structurală centrală, depășind funcția tradițională de sprijin informativ pentru

decizia politică și asumând rolul unui instrument activ al proiecției în mediul extern. Politica externă rusă contemporană nu poate fi înțeleasă în absența acestui pilon central informativ, întrucât serviciile de informații sunt integrate organic în mecanismele de formulare, implementare și ajustare a obiectivelor strategice statale. Această integrare reflectă o concepție asupra puterii în care cunoașterea, influența și controlul mediului extern sunt considerate resurse strategice superioare sau cel puțin echivalente cu resursele forței militare convenționale.

În același timp, intelligence-ul rus îndeplinește o funcție operațională, în sensul în care participă direct la implementarea obiectivelor de politică externă. Această dimensiune activă se distinge prin asumarea unor roluri care în alte sisteme politice ar fi rezervate diplomației sau altor instrumente de stat. Activitatea informativă externă este concepută ca un mijloc legitim de influențare a proceselor politice, economice și informaționale din afara granițelor naționale, fără a fi necesară o delimitare rigidă între acțiune și culegere. Această abordare conferă Moscovei o flexibilitate strategică sporită, permițând adaptarea rapidă a instrumentelor utilizate în funcție de reacțiile survenite în mediul extern.

În aceeași sferă, liderii de la Kremlin utilizează avantajele asimetrice oferite de activitatea informativă pentru a echilibra raporturile de putere. Accesul la informații clasificate, capacitatea de a anticipa decizii și de a influența indirect comportamentul altor actori permit F.Ruse să exercite o influență disproporționată față de resursele sale materiale. Astfel, intelligence-ul devine un multiplicator de putere, capabil să extindă aria de manevră strategică a statului rus.

Structurile informative sunt calibrate pentru a opera într-un spectru larg de medii politice și culturale, exploatând particularitățile locale și diferențele de reglementare. Această capacitate de adaptare este susținută de o cultură organizațională care valorizează inițiativa, creativitatea operațională și capacitatea de a acționa în condiții de ambiguitate. Rezultatul este un sistem informativ capabil să răspundă rapid la schimbările contextuale și să își recalibreze metodele fără a-și pierde coerența strategică.

Un rol distinct îl joacă gestionarea percepției externe. Din această perspectivă, serviciile ruse de informații contribuie la menținerea unui grad ridicat de incertitudine cu privire la intențiile și capabilitățile F.Ruse. Ambiguitatea strategică este utilizată ca instrument de influență, complicând evaluările adversarilor și reducând predictibilitatea reacțiilor acestora. În acest sens, intelligence-ul nu urmărește doar obținerea de informații, ci și controlul modului în care informațiile despre spațiul rus sunt interpretate și utilizate în mediul internațional.

Componenta HUMINT rămâne un pilon esențial al sistemului informativ rus, fiind utilizată atât pentru obținerea de informații clasificate, cât și pentru cultivarea unor relații de influență pe termen lung. Practica rusească privilegiază infiltrarea discretă în cercuri academice, economice, diplomatice și politice, unde pot fi identificate vulnerabilități sau oportunități de exploatare. Particularitatea modelului rus constă în cultivarea relațiilor de lungă durată, uneori pe parcursul a zeci de ani, fără presiunea obținerii imediate de informații clasificate. Accentul cade pe poziționarea surselor în noduri decizionale sau în proximitatea acestora. În spațiul european, numeroase cazuri de expulzare a diplomaților acreditați s-au fundamentat pe suspiciuni de activități HUMINT desfășurate sub acoperire diplomatică.

Componenta SIGINT (Signals Intelligence) este structurată pentru a exploata comunicațiile electronice, fluxurile de date și infrastructura de telecomunicații. F.Rusă dispune de capacități consolidate în domeniul interceptării comunicațiilor prin mijloace terestre, aeriene, navale și spațiale.

CYBERINT (Cyber Intelligence) reprezintă una dintre cele mai dinamice componente ale arhitecturii informative ruse. Spre deosebire de SIGINT, care presupune interceptare pasivă, CYBINT implică penetrare activă a sistemelor informatice, exfiltrare de date și, în anumite cazuri, sabotaj digital.

OSINT și exploatarea mediului informațional deschis: dimensiunea informațional-cognitivă

În paradigma contemporană, axată pe competiția strategică, OSINT nu mai reprezintă doar o disciplină auxiliară de colectare a datelor din surse deschise, ci un instrument central în modelarea mediului cognitiv al societăților vizate. În cazul F.Ruse, exploatarea mediului informațional deschis depășește logica pasivă a monitorizării și devine un proces activ de cartografiere, calibrare și influențare a spațiului perceptiv colectiv.

Dimensiunea cognitivă nu este limitată la raționalitate. OSINT-ul rusesc acordă o atenție deosebită componentei emoționale a discursului public. Analiza tonalității (sentiment analysis) este utilizată pentru a identifica, în principal, temele generatoare de anxietate colectivă axate pe subiecte care produc indignare sau frustrare prin utilizarea evenimentelor cu potențial de radicalizare discursivă. Exploatarea vectorilor afectivi permite ajustarea fină a mesajelor, astfel încât acestea să rezoneze cu predispozițiile emoționale existente. Scopul nu este neapărat persuasiunea directă, ci amplificarea reacțiilor deja prezente în spațiul public, favorizând auto-polarizarea și consolidarea bulelor informaționale.

Această abordare presupune o înțelegere sofisticată a psihologiei colective și a mecanismelor de viralizare digitală. În mediul online, conținutul care provoacă reacții emoționale puternice are o probabilitate mai mare de distribuire, ceea ce amplifică organic mesajele calibrate corespunzător. Dimensiunea cognitivă urmărește, în esență, modificarea relației dintre cetățean și instituțiile statului. Prin amplificarea contradicțiilor, evidențierea incoerențelor sau promovarea interpretărilor alternative, mediul informațional poate fi fragmentat. Astfel, nu este necesară convingerea majorității, ci este suficientă diminuarea consensului și creșterea incertitudinii. Într-o societate democratică, unde legitimitatea deciziei politice depinde de încredere și participare informată, fragmentarea cognitivă poate avea efecte structurale.

IMPACTUL ACTIVITĂȚILOR DE INTELLIGENCE RUSE ASUPRA ARHITECTURII DE SECURITATE EUROPENE

Activitățile de intelligence și influență asociate F.Ruse nu produc doar efecte punctuale, ci generează consecințe structurale asupra arhitecturii de securitate europene. Impactul lor se manifestă la nivel doctrinar, instituțional, legislativ și operațional, determinând o recalibrare a priorităților serviciilor occidentale și o redefinire a conceptului de securitate națională în spațiul euroatlantic.

Una dintre cele mai semnificative consecințe structurale a fost abandonarea progresivă a paradigmei post-Război Rece, centrată pe managementul crizelor externe și combaterea terorismului, în favoarea revenirii la logica competiției între mari puteri. Intelligence-ul rus, prin caracterul său persistent și multidimensional, a determinat serviciile europene să acorde prioritate sporită contraspionajului și protecției infrastructurii critice. Această reorientare a fost reflectată în documente strategice adoptate după 2014 și consolidate ulterior după 2022, când competiția informațională și cibernetică a fost recunoscută explicit drept componentă a securității colective.

Un indicator concret al reacției occidentale îl constituie valul de expulzări coordonate ale diplomaților ruși suspectați de activități informative. După declanșarea conflictului din Ucraina, statele membre ale UE au adoptat măsuri fără precedent, reducând semnificativ prezența oficială rusă pe teritoriul lor. Aceste măsuri au avut un dublu efect: diminuarea capacității HUMINT sub acoperire diplomatică și transmiterea unui semnal de descurajare strategică. Totuși, experiența operațională indică faptul că astfel de măsuri determină adaptarea, nu abandonarea activităților informative.

Reorientarea priorităților de intelligence în fața amenințărilor ruse

Reconfigurarea mediului de securitate european în ultimul deceniu a impus o transformare profundă a priorităților serviciilor

de informații occidentale. Dacă perioada post-Război Rece a fost dominată de operațiuni de stabilizare externă, combaterea terorismului și gestionarea amenințărilor asimetrice non-statale, dinamica generată de F.Rusă a readus în prim-plan competiția interstatală, spionajul strategic și confruntarea informațională multidomeniu.

În plan doctrinar, prima transformare majoră a constat în revenirea la paradigma „great power competition". Serviciile de intelligence au fost nevoite să își recalibreze analiza strategică de la amenințări difuze și fragmentate către un adversar statal cu capabilități integrate – convenționale, cibernetice, informaționale și clandestine. Această schimbare a presupus creșterea ponderii analizei geopolitice clasice, revitalizarea competențelor de contraspionaj strategic și dezvoltarea evaluărilor predictive pe termen lung.

În multe state europene, resursele anterior dedicate predominant combaterii radicalizării sau terorismului au fost redistribuite către monitorizarea activităților ruse, inclusiv a rețelelor de influență, penetrării economice și operațiunilor cibernetice persistente. În acest context, anticiparea nu mai este limitată la mobilizări militare vizibile, ci include indicatori subtili: activitate informațională intensificată, schimbări în discursul strategic oficial, repoziționări economice sau diplomatice. Reorientarea priorităților a adus în prim-plan protecția infrastructurii critice – energetică, digitală, financiară și logistică, astfel încât serviciile de intelligence au devenit actori centrali în evaluarea riscurilor asociate investițiilor externe, achizițiilor tehnologice și dependențelor strategice.

Un element distinct al reacției occidentale îl reprezintă menținerea echilibrului între eficiență operațională și respectarea cadrului legal. Spre deosebire de modelul autoritar, serviciile europene operează sub control parlamentar și jurisdicțional strict. Pe de altă parte, statele din proximitatea F.Ruse, inclusiv România, Polonia și statele baltice, au adoptat o abordare mai proactivă: pentru aceste state, amenințarea nu este teoretică, ci geografic și istoric contextualizată.

Transformarea mediului strategic, generată de competiția cu F.Rusă, a impus nu doar reorientarea priorităților, ci și o reformă profundă a modului în care serviciile occidentale analizează informația. Volumul de date, viteza circulației informaționale și caracterul multi-domeniu al amenințărilor au determinat o trecere de la analiza predominant reactivă la un model anticipativ, susținut tehnologic și metodologic. Această evoluție presupune integrarea *big data,* a inteligenței artificiale, a tehnicilor analitice structurate și a modelării predictive într-un ecosistem analitic coerent.

Integrarea AI în intelligence nu înlocuiește analistul uman, ci îi amplifică capacitatea. Modelele de *machine learning* sunt utilizate pentru clasificarea automată a volumelor mari de documente, recunoaștere facială și de obiect în imagini satelitare, detectarea campaniilor coordonate online și predicția probabilistică a scenariilor geopolitice. În analiza comportamentului F.Ruse, aceste metode sunt esențiale pentru a evita proiecția propriilor valori asupra unui actor strategic diferit. De exemplu, analiza scenariilor permite explorarea unor opțiuni considerate anterior improbabile, dar coerente din perspectiva doctrinară rusă.

Având în vedere că fluxul de date este continuu, nu episodic, iar în multe situații sistemele colectează volume de informații imposibil de procesat exclusiv uman, pentru statele de pe flancul estic, inclusiv România, cooperarea aliată a devenit o componentă esențială a securității informaționale.

CONTRAINFORMAȚIILE CA ELEMENT ESENȚIAL AL SECURITĂȚII NAȚIONALE

În arhitectura contemporană de securitate, contrainformațiile nu mai reprezintă o funcție auxiliară a aparatului de intelligence, ci un pilon central al protecției statului. În competiția strategică actuală, în care F.Rusă utilizează instrumente clandestine multidimensionale – HUMINT, influență, operațiuni cibernetice, presiune economică – vulnerabilitățile interne

devin principalele puncte de exploatare. În acest context, contrainformațiile sunt mecanismul prin care statul își protejează suveranitatea decizională, integritatea instituțională și reziliența sistemică.

Una dintre cele mai importante funcții ale contrainformațiilor este protecția procesului decizional strategic. În competiția contemporană, obiectivul unui adversar nu este neapărat obținerea unor documente clasificate punctuale, ci influențarea deciziilor politice și militare. Aceasta poate fi realizată prin infiltrarea în cercurile înalte decizionale, manipularea percepției publice și exploatarea vulnerabilităților personale ale decidenților. Contrainformațiile acționează pentru a preveni astfel de penetrări prin verificări de securitate aprofundate: monitorizarea contactelor externe sensibile, evaluarea vulnerabilităților individuale și protecția comunicațiilor oficiale. Suveranitatea decizională devine astfel obiectiv strategic prioritar.

Protecția presupune cooperare între serviciile de intelligence și operatorii privați, iar domeniile prioritare includ infrastructura energetică, rețelele de telecomunicații, infrastructura financiară, transportul strategic și infrastructura digitală. Evaluările de risc trebuie să fie continue, iar schimbul de informații între stat și sectorul privat este esențial.

Una dintre cele mai complexe provocări este amenințarea internă. Persoanele cu acces legitim la informații pot deveni vulnerabile la MICE (Money, Ideology, Coercion/Compromise, and Ego), iar educația de securitate și formarea continuă, de exemplu, reduc vulnerabilitățile exploatabile. Eficiența contrainformațiilor depinde și de cultura instituțională: personalul din instituții publice și private trebuie să înțeleagă riscurile și să manifeste vigilență constantă.

Pe lângă rolul defensiv, contrainformațiile au și rol de descurajare. Expunerea agenților, atribuirea publică a operațiunilor și coordonarea sancțiunilor cresc costul activităților clandestine. În competiția strategică contemporană, penetrarea instituțională nu urmărește exclusiv obținerea de informații clasificate, ci exploatarea vulnerabilităților sistemice pentru influențarea deciziilor, blocarea unor politici sau modelarea mediului strategic intern. În condițiile în care recrutarea directă clasică este adesea înlocuită de forme mai subtile, prin relații academice sau culturale prelungite, colaborări economice, implicare în proiecte internaționale și parteneriate profesionale, delimitarea dintre interacțiune legitimă și exploatare clandestină devine mai dificilă. Din acest punct de vedere, prevenirea penetrării devine funcție centrală a contrainformațiilor moderne.

Una dintre cele mai cunoscute forme de prezență operațională este utilizarea acoperirii diplomatice. Convențiile internaționale oferă imunitate și libertate de mișcare personalului diplomatic, ceea ce creează un cadru exploatabil. Caracteristicile acestui tip de acoperire includ statut oficial recunoscut, acces la mediul politic și instituțional, posibilitatea organizării de evenimente oficiale și comunicații protejate prin canale diplomatice. Dincolo de acoperirea oficială, arhitectura operațională include și infrastructuri paravan (companii comerciale, organizații culturale, entități media, fundații sau ONG-uri, structuri academice, institute de cercetare), iar contrainformațiile trebuie să distingă între activitate legitimă și instrumentalizare strategică, fără a afecta libertățile civile sau mediul academic.

Un vector tot mai relevant este cel economic, cu atât mai mult cu cât investițiile în sectoare sensibile pot genera dependențe strategice. Pe de altă parte, penetrarea economică nu presupune neapărat ilegalitate, ci exploatarea cadrului deschis al economiilor occidentale.

Protecția informațiilor clasificate și a procesului decizional

În competiția strategică actuală, protecția informațiilor clasificate nu este doar o problemă administrativă, ci o condiție fundamentală a suveranității statului. Informația strategică – planuri militare, evaluări de intelligence, poziții de negociere, capabilități tehnologice – reprezintă nucleul puterii decizionale. Compromiterea acesteia afectează nu doar securitatea operațională, ci însăși capacitatea statului de a acționa autonom.

Contracararea operațiunilor de influență și a amenințărilor hibride

Operațiunile de influență și amenințările hibride reprezintă forma dominantă de confruntare strategică în spațiul european post-2014.

Ele sunt concepute pentru a exploata deschiderea sistemelor democratice, interdependența economică și vulnerabilitățile informaționale, fără a depăși pragul conflictului armat convențional. În acest context, contracararea nu mai este exclusiv responsabilitatea serviciilor de informații, ci presupune un efort integrat – instituțional, legislativ, societal și aliat.

După anexarea Crimeei, în 2014, comunitatea euroatlantică a accelerat conceptualizarea acestui tip de confruntare. În cadrul NATO s-a dezvoltat „*comprehensive approach*", iar la nivelul Uniunii Europene au fost create mecanisme dedicate combaterii ingerințelor externe.

Contracararea eficientă se bazează pe cinci piloni:

- ✓ *Identificarea timpurie* – implică monitorizarea ecosistemelor media, analiză de rețea a amplificării narative, corelarea indicatorilor cibernetici cu evenimente politice și schimb de informații între statele membre. De exemplu, în timpul pandemiei COVID-19, mai multe state europene au identificat campanii coordonate care promovau narațiuni privind „ineficiența UE" sau „superioritatea modelelor autoritare". Un element central, în ultimii ani, a fost creșterea frecvenței atribuirilor publice, exemplificate prin atribuirea atacului cibernetic asupra Bundestagului german (2015) către actori asociați GRU, atribuirea atacului cibernetic SolarWinds către structuri ruse, expulzările coordonate de diplomați ruși după cazul Skripal (2018).
- ✓ *Atribuirea publică* – reduce plauzibilitatea negării, consolidează coeziunea aliată și crește costul reputațional și diplomatic al acțiunilor ostile.
- ✓ *Comunicarea strategică* – este complementară contrainformațiilor/ nu este propagandă, ci comunicare bazată pe transparență și fapte verificabile. În cadrul NATO funcționează structuri dedicate StratCom, iar la nivelul UE există East StratCom Task Force, care monitorizează și demontează narațiuni false (ex.: campaniile privind presupusa „militarizare agresivă a României" în contextul consolidării prezenței aliate au fost contracarate prin comunicare oficială transparentă privind caracterul defensiv al măsurilor). De asemenea, alegerile reprezintă ținte prioritare pentru operațiuni de influență.
- ✓ *Mecanismele de contracarare* – includ monitorizarea finanțărilor politice externe, protecția infrastructurii IT electorale, colaborarea cu platformele digitale și transparență privind campaniile sponsorizate, exemplificate prin interferențele identificate în alegerile prezidențiale din SUA (2016), campanii de dezinformare în timpul alegerilor europene, tentative de influență în procese electorale din state baltice și Europa Centrală.
- ✓ Cea mai eficientă apărare împotriva influenței este *reziliența societală*. Statele baltice sunt adesea citate ca exemplu de reziliență consolidată prin educație strategică și reacție rapidă la dezinformare.

CONSOLIDAREA REZILIENȚEI ROMÂNIEI ÎN CONTEXTUL COMPETIȚIEI INFORMAȚIONALE GENERATE DE F.RUSĂ

Poziționarea României pe flancul estic al NATO, proximitatea față de Marea Neagră și relevanța infrastructurii sale energetice și logistice transformă statul român într-un actor strategic de primă linie. Această poziție generează atât oportunități geopolitice, cât și vulnerabilități exploatabile în competiția multidomeniu cu F.Rusă.

În acest context, consolidarea rezilienței nu poate fi tratată ca reacție punctuală, ci ca proces structural, pe termen lung, care implică instituții, societate, sector privat și parteneri aliați:

- un prim pilon este reprezentat de coordonarea instituțională, cu atât mai mult cu cât amenințările hibride sunt transversale și nu respectă delimitări administrative;
- integrarea între dimensiunea de intelligence și cea de comunicare strategică este esențială pentru reacții rapide la campanii

de influență;
- Marea Neagră reprezintă un spațiu de competiție strategică intensificată/ pentru România, vulnerabilitățile includ infrastructura portuară (Constanța), terminalele energetice, cablurile submarine de comunicații, exploatările offshore de gaze și infrastructura militară aliată;
- sabotajele asupra infrastructurii energetice europene, din ultimii ani, au demonstrat că infrastructura critică este o țintă prioritară în competiția hibridă;
- o vulnerabilitate exploatabilă este dependența economică sau tehnologică excesivă de furnizori din state ostile/ prin urmare, mecanismele de screening al investițiilor străine, armonizate cu politicile Uniunii Europene, sunt un instrument esențial de prevenție.

ANALIZA CRITICĂ A COMPETIȚIEI INFORMAȚIONALE

Confruntarea informațională contemporană nu poate fi înțeleasă în totalitate dacă este analizată fragmentar, pe paliere separate - tehnologic, juridic, social sau militar. În realitate, competiția strategică desfășurată sub pragul conflictului armat este un conflict integrat, în care dimensiunea economică susține infrastructura, cadrul normativ determină reacțiile, factorul uman constituie centrul de greutate din punct de vedere operațional, iar instrumentul militar oferă fundalul descurajării amenințărilor și aduce stabilitatea. Interacțiunea dintre aceste componente definește arhitectura reală a confruntării hibride din spațiul euro-atlantic.

Dimensiunea economico - tehnologică reprezintă fundamentul material al competiției informaționale. Interdependențele comerciale, investițiile în infrastructuri critice și integrarea tehnologiilor digitale în procesele industriale au creat un mediu în care vulnerabilitățile au ieșit din sfera militară și au intrat în spectrul extins. Controlul sau afectarea infrastructurii energetice, a rețelelor de transport, a sistemelor de comunicații și a centrelor de date ar putea genera efecte strategice fără aplicarea forțelor kinetice.

Automatizarea influenței prin utilizarea AI și a analizelor big data amplifică această dinamică. Capacitatea de segmentare a audiențelor, de a adapta mesaje în funcție de profiluri psihologice și de a evalua reacțiile în timp real transformă operațiunile informaționale într-un proces scalabil și sofisticat. Narativele nu sunt diseminate uniform, ci calibrate pentru a activa predispoziții cognitive specifice cu scopul polarizării și erodării încrederii inter-instituționale.

În context, cadrul juridic devine atât un instrument de protecție, cât și o vulnerabilitate exploatabilă. Ambiguitatea normativă a operațiunilor desfășurate sub pragul agresiunii convenționale permite actorilor revizioniști să evite asumarea formală a responsabilității. Manipularea informațională și finanțarea indirectă a entităților sau campaniilor de influență coordonate ating nivelul agresiunilor clasice, însă pot afecta substanțial autonomia decizională și stabilitatea internă. Democrațiile sunt constrânse să răspundă în limitele statului de drept, aspect ce presupune proporționalitate, transparență și control jurisdicțional. Echilibrul dintre protecția securității naționale și garantarea libertății de exprimare este foarte delicat. Reglementarea conținutului online sau restricționarea unor canale asociate propagandei externe trebuie calibrate astfel încât să nu submineze valorile democratice pe care încearcă să le apere.

Operațiunile informaționale moderne exploatează vulnerabilitățile cognitive inerente: tendința de confirmare a convingerilor preexistente, reacțiile emoționale la conținut polarizant, preferința pentru narațiuni simple într-un mediu vast și complex. O societate polarizată devine una mai puțin capabilă să susțină politici strategice coerente, iar presiunea mediatică poate influența indirect procesul decizional. Educația media, alfabetizarea digitală și conștientizarea riscurilor asociate ingerinței externe constituie mecanisme preventive care reduc eficiența manipulării. Dimensiunea umană nu este doar o vulnerabilitate, ci și o resursă: coeziunea socială, încrederea instituțională și profesionalismul

reprezintă barierele naturale împotriva ingerinței.

Dimensiunea strategic-militară oferă fundalul stabilității în ambiguitatea actuală. Intelligence-ul nu mai funcționează exclusiv ca instrument de avertizare, ci ca element integrat al descurajării, furnizând baza de date pentru decizii calibrate, evitând escaladarea neintenționată. Superioritatea informațională devine astfel condiția primordială a stabilității.

Pentru România, această arhitectură integrată are implicații directe. Reziliența economică, solidaritatea cadrului normativ, cultura de securitate a societății și integrarea în mecanismele aliate de intelligence constituie componentele interdependente securității naționale. În ansamblu, confruntarea hibridă contemporană nu este un episod, ci o stare structurală a competiției dintre modele politice și viziuni strategice diferite. Economia, tehnologia, norma juridică, factorul uman și instrumentul militar nu acționează izolat, ci formează o rețea de interdependențe care definește câmpul de luptă informațional.

BIBLIOGRAFIE

1. AHMAD Atif, Jeb Webb, Kevin C. Desouza, James Boorman, ”Strategically-Motivated Advanced Persistent Threat: Definition, Process, Tactics and a Disinformation Model of Counterattack”, *Computers & Security*, vol. 86, 2019, pp. 402-418; https://semanticscholar.org/reader/469473b9ab191656fb6be7162c9e09a181a4165c
2. BITTMAN Ladislav, *The KGB and Soviet Disinformation: An Insider`s View*, Pergamon Brassey`s, 1985, 216 p.
3. BYMAN Daniel, ”NATO and Countering Hybrid Warfare”, *Commentary*, Center for Strategic and International Studies, Washington DC, 12.07.2024; https://csis.org/analysis/nato-and-countering-hybrid-warfare.
4. DUGHIN Aleksandr, *Bazele geopoliticii și viitorul geopolitic al Rusiei*, Editura Eurasiatica.ro, București, 2011, 446 p.
5. FATHAIGH O. Ronan, Tom Dobber, Frederik Zuiderveen Borgesius, james Shires, ”Microtargeted propaganda by foreign actors: An interdisciplinary exploration”, *Maastricht Journal of European and Comparative Law*, vol. 28, nr. 6, 2021, pp. 856-877;
6. GALEOTTI Mark, *The Weaponisation of Everything: A Field Guide to the New Way of War*, Yale University Press, 2022, 248 p.
7. GILES Keir*, Moscow Rules: What Drives Russia to Confront the West,* Brookings Institution Press, 2019, 257 p.
8. KOTT Alexander et al., *Toward Intelligent Autonomous Agents for Cyber Defence: Report of the 2017 Workshop by the North Atlantic Treaty Organization Research Group IST-152-RTG,* ARL-SR-0395, US Army Research Laboratory, April 2018, 40 p.
9. MAZARR J. Michael et al., *Hostile Social Manipulation. Present Realities and Emerging Trends*, RAND Corporation, Santa Monica, California, 2019, 282 p.
10. NIETZMAN Lotte, Peter Schrijver, ”Communicating the Russian Threat: Intelligence Agencies` Public Messaging in Europe”, *National Security and the Future*, vol. 26. nr. 2, Zagreb, 2025.
11. PACEPA Ion Mihai, Ronald J. Rychlak, *Dezinformarea,* Editura Humanitas, București, 2015, 468 p.
12. RENZ Betina, *Russia`s Military Revival*, Polity Press, 2018, 240 p.
13. RID Thomas, *Active Measures: The Secret History of Disinformation and Political Warfare,* Farrar, Straus & Giroux, 2020, 528 p.
14. WATLING Jack, Olexandr V. Danylyuk, Nick Reynolds, *The Threat from Russia`s Unconventional Warfare Beyond Ukraine, 2022*-2024, Special Report, Royal United Services Institute, London, 2024*,* 35 p.
15. *** „Hybrid threats/ Russia. Statement by the High representative on behalf of the EU condemning Russia’s persistent hybrid campaigns”, Consiliul UE (iulie 2025); https://www.consilium.europa.eu.
16. *** „Hybrid threats”. Politici ale Consiliului UE despre amenințările hibride și răspunsul UE; https://www.consilium.europa.eu.
17. *** „Russia’s hybrid activities: EU sanctions”, Consiliul UE (octombrie 2024) - cadrul legal și sancțiunile adoptate pentru contracararea amenințărilor rusești; https://www.consilium.europa.eu.
18. *** „Hybrid threats”. Politici și definiții ale Consiliului UE privind amenințările hibride ale Rusiei; https://www.consilium.europa.eu.
19. *** „Activitățile hibride ale Rusiei: sancțiuni ale UE”, Consiliul UE; https://www.consilium.europa.eu.

FOLOSIREA INSTRUMENTELOR DE INFORMAȚII MILITARE ȘI COMANDA PRIN MISIUNE ÎN RĂZBOIUL DIN UCRAINA

Radu PRIOTEASA*
Tudorel Niculai LEHACI**

Abstract

Beyond the brutality of the conflict that bursted close to the Romanian border in 2022, we think that there are numerous aspects that can be studied and integrated in the training, and, at large, in the way of carrying a war. From denying the possibility of an invasion, present in the Kiev elite (and not only) before the attack of Russian Federation, all the way to the improbability of Ukraine's military resistance against a much stronger opponent, these are as many reasons to initiate a deep study in order to identify ways of enhancing the training level of our own army. We stopped, within this article, at two essential components, mission command and military intelligence. We have tried ito identify, based on OSINT examples, new ways of warfighting, in accordance with the two components.

Keywords: *mission command; military intelligence; Ukraine; Russian Federation.*

INTRODUCERE

Războiul ruso-ucrainean, debutând la scară largă în 24 februarie 2022, reprezintă cel mai sângeros conflict pe care l-a văzut Europa de la sfârșitul celui de-al Doilea Război Mondial încoace. Războiul a modelat noua realitate în care au trăit societățile europene în ultimii 4 ani, în toate sferele vieții publice: politică, socială, economică, culturală etc. Pentru sistemul militar, cel puțin pentru armatele occidentale, a reprezentat, printre altele, o schimbare de paradigmă: o trecere sau, mai degrabă, o reîntoarcere de la pregătiri/participări la conflicte asimetrice către un război clasic, desfășurat cu armate de masă, cu artilerie și NBC, cu procese de planificare și state majore de brigadă sau divizie, cu dezinformare și acțiuni asimetrice, cu inovații tehnologice și utilizarea noilor tehnologii disruptive.

Ne aflăm într-un punct de inflexiune strategică care ne modelează istoria pentru următorii zeci de ani, iar în mijlocul acestei paradigme de dezvoltare societală se găsește sistemul militar.

**Student doctorand la Universitatea Națională de Apărare „Carol I".*
***Prof. univ. dr. la Universitatea Națională de Apărare „Carol I".*

O gamă largă de lecții identificate și pe cale de a fi învățate se evidențiază deja în programe de înzestrare, modificări doctrinare sau noi tactici, tehnici și proceduri implementate la nivelul Armatei României și, într-un plan general, la cel al forțelor armate ale statelor NATO. Principiul machiavellian care susține că legile bune și armatele puternice constituie baza unui stat este mai actual ca niciodată.

Războiul ruso-ucrainean constituie baza restructurării sistemului militar actual, iar lecțiile acestuia în narativul despre conflict, arta operațională, informații, sprijin cu foc, comanda prin misiune, conducerea forțelor/ leadership, logistică, manevră, protecția personalului, sprijin medical, operații navale/ aeriene și multe altele vor sprijini viziunea națională asupra felului în care vor arăta forțele armate române peste 5, 10 sau 20 de ani.

În acest articol ne vom concentra asupra a două aspecte, pe care le considerăm de interes a fi investigate mai profund, și anume aplicarea conceptului de ***„comandă prin misiune”*** (*mission command*) și ***evoluția informațiilor militare,*** în contextul războiului din Ucraina. Ambele și-au dovedit utilitatea, ca să folosim un termen neutru, în principal pentru forțele armate ucrainene. Vom încerca, pe parcursul acestui articol, să subliniem importanța factorilor care au asigurat adaptabilitatea și succesul forțelor în implementarea principiilor de mai sus și, totodată, vom argumenta necesitatea preluării bunelor practice la nivelul armatei noastre.

COMANDA PRIN MISIUNE – O ISTORIE CÂT VECHIMEA RĂZBOIULUI

Conceptul de „***comandă prin misiune***” își are rădăcinile în abordările generalilor prusaci Johann David von Scharnhorst, August Graf Neidhardt von Gneisenau și Carl von Clausewitz. În urma înfrângerii prusace în bătăliile de la Jena și Auerstedt (1806), comandanţii prusaci au iniţiat o revizuire totală a doctrinei militare și, în 1837, au actualizat regulamentele de luptă prusace. Elementul central aflat la rădăcina acestei revizii s-a bazat pe constatarea că „francezii au impus un ritm rapid al acţiunilor prin comunicarea rapidă a intențiilor și argumentelor lui Napoleon. Poate cel mai important, exercițiul inițiativei de către ofițerii cu grade inferioare a fost tolerat ... iar rezultatul fiind un tempo operațional care i-a lăsat pe prusaci nedumeriți”.

Pe baza acestor constatări, prusacii au adăugat la propriul regulament de luptă că „dacă executarea unui ordin este imposibilă, un ofițer ar trebui să caute să acționeze în conformitate cu intenția din spatele acestui ordin”, iar greșelile erau „preferabile ezitării pentru a permite o acțiune decisivă și îndrăzneață[1]”.

Mai departe asistăm la o descentralizare sau, din contră, la o centralizare a comenzii, în toate conflagraţiile care vor urma, până când succesele iniţiale ale Wehrmacht-ului şi-au găsit rădăcinile în implementarea „Auftragstaktik”. Generalul german Erich von Manstein, în memoriile sale intitulate *Victorii pierdute*, încerca, într-un mod destul de neconvingător, să argumenteze dezastrul încercuirii Armatei 6 Germane la Stalingrad: astfel, în cadrul argumentaţiei sale, acesta prezenta nucleul funcţiunii de comandă şi control a armatei germane – „ne-am ghidat acţiunile după principiile germane binecunoscute ale comenzii: 1. conducerea operaţiilor militare într-un mod flexibil şi inovator. 2. încurajarea iniţiativei şi libertăţii de acţiune a comandanţilor subordonaţi. Libertatea de acţiune a comandanţilor subordonaţi a constituit întotdeauna un avantaj pentru sistemul de comandă şi control german. Primeau o misiune şi era treaba lor cum să o îndeplinească.”

Comanda prin misiune reprezintă, prin urmare, un concept pe cât de vechi[2], pe atât de redescoperit cu fiecare generaţie sau nou tip de război. Strategi şi gânditori militari, de la Sun Tzî la Napoleon și de la Pericle la generalul Joffre, au subliniat importanţa „împuternicirii” subordonaţilor, a descentralizării deciziei, precum și avantajele inițiativei la nivel tactic pe câmpul de luptă. Există nenumărate exemple de victorii, pentru că, da, victoria este obiectivul acţiunii militare, de la Termopile la Posada, chiar şi Stalingrad, unde descentralizarea comenzii şi iniţiativa disciplinată au dus la victorii răsunătoare.

Implementarea conceputului, dincolo de situațiile individuale când a fost dată drept exemplu, a prins formă, în epoca contemporană, în sistemul militar american, prin impunerea sa ca fundament doctrinar odată cu publicarea Manualului 6-0 (FM 6-0)[3] în anul 2003. Principiile conceptului „*comanda prin misiune/ mission command*", așa cum sunt prezentate în cadrul Doctrinei Forțelor Terestre ale SUA 6-0 (Army Doctrine Publication 6-0) sunt: „competența, încrederea reciprocă, înțelegerea mediului operațional, intenția comandantului, ordinele misiunii, inițiativa disciplinată și acceptarea riscului – acestea fac posibilă relaționarea între lideri, împuternicirea subordonaților cu atributele luării deciziei și execuția descentralizată a misiunii"[4].

Aceste principii sunt strâns interconectate și constituie baza implementării conceptului la nivelul tuturor structurilor. Cu toate că, la prima vedere, par mai degrabă o serie de atribute a căror implementare și cuantificare sunt dificile, apreciem că, la fel ca orice alte calități mai „măsurabile" din sistemul militar, odată cu repetarea conceptelor, în mediul de instruire, vine și cuantificarea. Dacă majoritatea atributelor prezentate mai sus sunt intuitive, într-o mare măsură, cu grad ridicat de generalitate pentru o paletă largă de activități, nu același lucru îl putem spune și despre acceptarea riscului. Comandanții, la toate eșaloanele, trebuie să definească și să comunice nivelul de risc acceptat, iar riscul este parte integrantă a operațiilor militare și se află într-o relație aproape simbiotică cu responsabilitatea. Astfel, comandanții trebuie să-și dezvolte capacitatea de a evalua situațiile punctual, încât raportul între riscuri și beneficii să fie cântărit în contextul nivelului beneficiilor versus probabilitatea și gravitatea riscurilor.

Cu toate aceste, implementarea conceptului „comenzii prin misiune/ mission command" s-a dovedit a fi provocatoare, fiind identificați[5] următorii factori care contribuie la aceasta:

- îngrijorări din partea comandanților cu privire la potențialele greșeli comise de subordonați;
- riscuri la adresa carierei liderilor din cauza acestor greșeli;
- lipsa controlului potențează starea de neliniște a liderilor militari.

În vederea implementării conceptului la nivelul structurii de forțe, am identificat câteva bune practici care pot sprijini comandanții de pe toate treptele ierarhice, astfel:

a) asumarea conștientă a implementării conceptului la nivelul structurii/unității: pasul esențial pentru implementarea conceptului este o asumare conștientă a liderului pentru implementare/ acest lucru poate surveni în urma unui process de reflecție personală, în urma unui proces de planificare cu cei responsabili sau chiar în urma unui moment de tip „evrika", după lecturarea unui material de interes pe această temă.
b) folosirea terminologiei adecvate implementării conceptului: următorul pas logic este implementarea vocabularului corespunzător în activitatea zilnică, începând cu cele mai simple ordine formulate pentru rezolvarea aspectelor zilnice ale rutinei operaționale, continuând cu implementarea în documentele scrise (ex.: răspunsuri la solicitările eșalonului superior, dări de seamă, evaluări anuale etc.) și chiar introducerea în jargonul/ povestirile/ etosul unității.
c) utilizarea unor viniete/ situații progresive în instruirea forțelor, care să contribuie la implementarea conceptului, într-un mediu controlat, cu riscuri reduse.

COMANDA PRIN MISIUNE – IMPLEMENTAREA CONCEPTULUI ÎN RĂZBOIUL RUSO-UCRAINEAN

În vederea înțelegerii drumului pe care l-au urmat forțele armate ucrainene pentru implementarea comenzii prin misiune este necesară prezentarea unor condiții inițiale[6], contextuale, referitoare la situația generică a armatei, la începutul anilor 2000 (și, cu siguranță și ulterior), și anume:

- implementarea conceptului a fost parte componentă a efortului de modernizare a

forțelor armate, ulterior anexării Crimeei de către Federația Rusă în anul 2014;
- stilul sovietic preexistent în toate domeniile vieții militare, cu precădere în experiența/ expertiza comenzii, a frânat implementarea conceptului;
- datorită interconexării acestui concept cu cultura populară, schimbarea a fost dificilă;
- lipsa investițiilor, instruirea militară (caracterizată ca neavând vreo strategie) și o puternică mentalitate sovietică au influențat adoptarea acestui stil de conducere.

Aceste condiții au fost similare, într-un grad mai mare sau mai redus, tuturor forțelor armate aparținând statelor din fostul lagăr comunist; cu toate acestea, ar fi nedrept să atribuim caracteristici generale, tipice sistemului militar, în general, ca rigiditatea sau controlul excesiv, doar unor forțe armate din Estul Europei.

Înțelegând nevoia de modernizare și identificând NATO ca fiind un partener viabil în această schimbare, conducerea Ucrainei a solicitat sprijinul Alianței, și, în anul 2021, forțele armate ale Ucrainei au fost încorporate în Programul NATO de Dezvoltare a Educației în Domeniul Apărării (*NATO Defense Enhancement Education Programme*). Anexarea Crimeei și, subsecvent, deschiderea unui nou front în estul țării, au constituit provocări suplimentare pentru reformarea sistemului militar ucrainean, dar, în același timp, și o confirmare a nevoii de modernizare.

Principalele caracteristici ale comenzii prin misiune au fost confirmate și implementate în conflictul din Ucraina, astfel:
- succesele inițiale ale forțelor armate ucrainene, materializate prin recâștigarea teritoriilor cucerite inițial de forțele ruse au fost creditate[7], de către fostul ministru al apărării, Oleksyi Reznikov, ca fiind datorate abilităților de luare a deciziei, la toate nivelurile de comandă, aceasta ducând la reacții de răspuns mai rapide ca ale rușilor;
- evaluarea realizată de *Royal United Services Institute/ RUSI*, cu privire la performanțele forțelor armate ucrainene la începutul războiului, a arătat că „acestea au fost competitive în acțiunile desfășurate împotriva adversarului nu datorită superiorității echipamentului, ci pentru că erau adaptabile - în mod special la nivel tactic - și au inovat într-un ritm rapid în acele domenii în care rușii erau vulnerabili”[8];

Cu toate acestea, forțele ucrainene sunt tributare unui stil de comandă adânc înrădăcinat în cultura sovietică, după cum a reieșit dintr-o cercetare efectuată de o echipă de experți militari occidentali. Dincolo de aspectele de rezistență la schimbare prezentate anterior, concluziile[9] misiunii, la nivel tactic, vorbesc de la sine: „*… dacă ofițerii cu grad inferior ar avea autoritatea de a exploata oportunitățile care apar, desfășurând atacuri coordonate ale infanteriei și vehiculelor blindate, sprijinite de baraje ale artileriei ghidate, scurte dar punctuale, aceasta ar reduce în mod drastic cantitatea de muniție folosită*”.

Existența unui sistem strict de comandă și control la nivelul forțelor armate ale Federației Ruse poate fi una dintre cauzele eșecului în atingerea obiectivelor, cât și a provocărilor operaționale. Sistemul de comandă și control a înrădăcinat o subordonare aproape oarbă pe lanțul ierarhic, o atitudine strictă de îndeplinire a ordinelor primite, chiar în condițiile în care este evident că situațiile inițiale care au conturat acțiunea s-au schimbat fundamental; chiar și în aceste condiții, comandanții ruși mențin ordinul inițial, dacă nu primesc un alt ordin care îl contramandează. Rușii au recunoscut în aceasta o slăbiciune, inclusiv ca parte a unui sistem C2 robust, una dintre măsurile luate de aceștia fiind trimiterea ofițerilor cu grade superioare (inclusiv generali) pe linia frontului, rezultatul fiind uciderea unui număr important de generali ruși de către ucraineni.

Unele considerații privitoare la implementarea conceptului

Acceptarea riscului

Nicio forță armată nu este imună la constrângerile identificate atât la nivelul forțelor armate ucrainene, cât și al celor ruse, în mod special la cele privitoare la aversiunea comandanților față de risc. Factorii identificați anterior de Burton L. Brender (teama ca subordonații să

greșească, disconfortul superiorilor în contextul sentimentului de pierdere a controlului și angoasele referitoare la efectele asupra carierei personale în situația unor posibile greșeli) sunt general valabili și necesită o atenție deosebită, precum și măsuri coordonate de diminuare.

Depășirea acestor obstacole este necesar să înceapă de la vârful lanțului de comandă și să fie perpetuată până la nivelul comandantului de echipă. Delegarea responsabilităților trebuie să ducă la conturarea unei imagini pozitive a „comenzii prin misiune", aspect asigurat de comandanții de pe toate treptele ierarhice. Concomitent, „comanda prin misiune" este necesar a fi instruită, repetată și exersată cu regularitate, astfel încât să devină o parte a culturii organizaționale[10].

Coeziunea și profesionalismul, alături de *experiență*, sunt esențiale în implementarea „comenzii prin misiune", iar aceste atribute nu pot fi implementate direct în luptă. Activitățile de zi cu zi, sarcinile în care echipele mici trebuie să execute sarcini, fie ele chiar și de sprijin (logistice, administrative, într-un cuvânt nu cele mai „războinice" misiuni), care beneficiază de o supervizare discretă a unui corp subofițeresc experimentat, pot contribui la construirea unui spirit de corp la nivelul celor mai mici subunități.

Comanda prin misiune este acest sistem de operare a câmpului de luptă contemporan unde armate de dimensiuni mari, supratehnologizate, se înfruntă într-un mediu saturat de tehnologie, putere de foc și supraveghere continuă. Inițiativa disciplinată, multiplicată de zeci sau sute de ori de-a lungul frontului, în ambuscade sau incursiuni, în decizii luate de micii comandanți, în acord cu ordinele inițiale, poate schimba soarta unor bătălii, sectoare de front și viețile soldaților.

EVOLUȚIA CONTEMPORANĂ A INFORMAȚIILOR MILITARE ÎN CONFLICTUL RUSO-UCRAINEAN

Dintre cele mai importante aspecte pe care le-a adus în prim plan conflictul ruso-ucrainean, în domeniul informațiilor militare, putem nominaliza: importanța informațiilor obținute din surse deschise (OSINT); o nouă abordare a modului în care informațiile militare pot fi folosite pentru a desfășura acțiuni în spectrul războiului informațional; importanța asigurării unei redundanțe/ suprapuneri a senzorilor ISR utilizați, concomitent cu integrarea inteligenței artificiale; mai presus de toate, o nouă revoluție doctrinară în modul în care sunt utilizate informațiile militare pe câmpul de luptă.

a) Importanța informațiilor obținute din surse deschise (OSINT)

Criza din Crimeea, din anul 2014, a arătat, într-un mediu de luptă contestat, că orice dispozitiv electronic poate fi folosit să disemineze mesaje în scopuri de propagandă, dezinformare și/ sau inducere în eroare, în același timp cu furnizarea unei semnături electromagnetice care poate fi recepționată, deci analizată sau manipulată[11].

În războiul ruso-ucrainean, imaginile satelitare, postările de pe rețelele sociale, videoclipurile de pe YouTube și chiar bazele de date din domeniul medical au furnizat atât forțelor armate ucrainene, cât și celor ruse, informații cu privire la forțele adverse, localizarea forțelor și a comandanților militari, starea moralului, precum și estimări cu privire la eficacitatea loviturilor (BDA). Platformele de social-media au jucat un rol important în identificarea mișcărilor forțelor rusești, furnizând date esențiale privitoare la mișcările și intențiile acestora[12]. Generalul Jim Hockenhull, comandantul Comandamentului Strategic la Marii Britanii, a subliniat domeniile în care Ucraina a folosit OSINT, astfel: elaborarea unor produse de intelligence prospectiv, schimbarea/ alterarea/ modificarea opiniei publice cu privire la un eveniment, contracarearea propagandei ruse, furnizarea unei platforme unde populația poate participa activ la furnizarea de informații cu relevanță tactică etc[13].

Un exemplu relevant în modul în care Ucraina a transformat „fiecare cetățean într-un senzor" îl reprezintă folosirea populației în detectarea dronelor iraniene (Shahed sau versiunea rusească, Geran), prin postarea de către cetățeni a localizării (alături de alte date relevante fotografii, filmulețe și coordonate) dronelor lansate de forțele ruse.

b) O nouă abordare a modului în care informațiile militare pot fi folosite pentru a desfășura acțiuni în spectrul războiului informațional

Declasificarea unor informații de anvergura celor pe care armata ucraineană și partenerii săi le-au expus publicului larg reprezintă o acțiune fără precedent în experiența ducerii războiului, ale căror riscuri vs. beneficii, cu siguranță, au fost cântărite atent. Principalul scop al acestor acțiuni l-a constituit contracararea propagandei rusești și a dezinformării. Totodată, nu este exclus nici efectul (rămâne de văzut și analizat anvergura acestuia) asupra moralului forțelor și comandanților ruși. Câteva dintre informațiile cele mai importante care au contribuit la formarea unei imagini cu privire la conflict, divulgate către mass-media, au fost: masarea forțelor armate ruse la granița ruso-ucraineană, la sfârșitul anului 2021; discuțiile lui V.Putin cu Xi Jinping referitoare la o posibilă invazie a Ucrainei, pe timpul Jocurilor Olimpice de Iarnă din 2022; sau regruparea unor forțe mari blindate odată cu începerea luptei.

c) Importanța asigurării unei redundanțe/ suprapuneri a senzorilor ISR utilizați, concomitent cu integrarea inteligenței artificiale

Suprasaturarea mediului informațional și a analiștilor, în ultimă instanță, este o altă caracteristică a mediului operațional din Ucraina. Aceste informații provin de la senzori diferiți, cu o viteză ametitoare, solicitând o abordare novatoare din partea statului major și a structurilor de informații. Filmulețe YouTube, postări pe Facebook și Instagram, site-uri specializate, canale de Telegram și multe altele, concomitent cu *feed-ul* primit de la senzori terestri, navali sau terești, plus rapoarte specifice de informații, toate acestea solicită atenția analiștilor, care trebuie să deceleze între toate sutele/ miile/ zecile de mii de informații. Un răspuns la această provocare ar putea fi integrarea IA în munca analiștilor și „de-specializarea" analiștilor de informații, transformarea acestora în analiști „generaliști" capabili să integreze informații din surse multiple cu ajutorul instrumentelor IA.

d) O nouă revoluție doctrinară în modul în care sunt utilizate informațiile militare pe câmpul de luptă

Armatele învață în modalități multiple: prin instruire/ aplicarea conceptelor pe câmpul de instrucție (distilând conceptele doctrinare), prin operațiile desfășurate sau prin conflictele recente și/ sau trecute. Cu toate că riscul iminent al unei armate este să lupte următorul război cu instrumentele ultimului război, considerăm că evoluțiile în fizionomia războiului aflat la granița României ne obligă să adaptăm doctrina pentru integrarea noilor capabilități nu doar în domeniul informațiilor militare, ci în tot spectrul capabilităților.

Este evident că volumele mari de informații trebuie integrate, în timp scurt, în produse informative comprehensive care să sprijine decizia comandanților, iar distanțele de la senzori (oricare ar fi ei) la trăgători să fie diminuate. Aceste inovații care au salvat vieți și au produs efecte pe câmpul de luptă trebuie cunoscute și inserate în instruirea forțelor noastre.

BIBLIOGRAFIE

1. ANCKER J. Clinton III, "The Evolution of Mission Command in US Army Doctrine, 1905 to the Present", *Military Review*, March-April 2013, pp. 42-52; https://armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20130430_art008.pdf.
2. BRENDER L. Burton, "The Problem of Mission Command", The Strategy Bridge, 01.09.2016; thestrategybridge.org/the-bridge/2016/9/1/the-problem-of-mission-command.
3. BYMAN Daniel, "NATO and Countering Hybrid Warfare", Center for Strategic and International Studies, Washington DC, 12.07.2024; https://www.csis.org/analysis/nato-and-countering-hybrid-warfare.
4. GADY Franz-Stefan, "Ukraine's Army Must Shed Its Soviet Legacy, Says a Military Expert", *The Economist*, March 17, 2023; https://www.economist.com.
5. GILES Keir, James Sheer, Anthony Seaboyer, *Russian Reflexive Control*, Royal Military College of Canada, 2018, 66 p.
6. HERSZENHORN M. David, Paul McLeary, "Ukraine's 'Iron General' Is a Hero, but He's No Star", *Politico*, April 8, 2022; https://www.politico.com/news/2022/04/08/ukraines-iron-general-zaluzhnyy-00023901.
7. HEWSON Jack, "Ukrainian company uses social media, open source technology to counter Russian invasion", *PBS News,* April 19, 2023, https://www.pbs.org/newshour.
8. HOCKENHULL Jim, "How Open-Source Intelligence Has Shaped the Russia-Ukraine War", Royal United Services Institute, RUSI Members Webinar, London, December 9, 2022; www.gov.uk/government/speeches/how-open-source-intelligence-has-shaped-the-russia-ukraine -war.
9. KOTT Alexander and all, *Toward Intelligent Autonomous Agents for Cyber Defense> Report of the 2017 Workshop by the North Atlantic Treaty Organization (NATO) Research Group IST-152-RTG*, US Army Research Laboratory, ARL-SR-0395, Aprilie 2018, 40 p.
10. (von) MANSTEIN Erich, *Victorii pierdute*, Editura Elit, București, 2002.
11. NAGL John, Crombe Katie, *A Call to Action: Lessons from Ukraine for the Future Force*, Strategic Studies Institute, US Army War College, June 2024, 323 p.; press.armywarcollege.edu/cgi/viewcontent.cgi?article=1964&context=monographs.
12. NIETZMAN Lotte, Peter Schrijver, "Communicating the Russian Threat: Intelligence Agencies` Public Messaging in Europe", *National Security and the Future,* vol. 26, nr. 2, St. George Association, Zagreb, 2025, pp. 187-222.
13. POLYAKOV Leonid, "Defence Institution Building in Ukraine at Peace and at War", *Connections: The Quarterly Journal*, vol. 17, nr. 3 (Summer-Fall 2018), p. 92-108;
14. SHUSTER Simon, Vera Bergengruen, "Inside the Ukrainian Counterstrike That Turned the Tide of the War", *Time,* 26.09.2022; https://www.time.com/6216213/ukraine-military-valeriy-zaluzhny/?utm_source=twitter&utm_medium=social&utm_campaign=editorial&utm_term=world_ukraine&linkld=183047256.
15. ZABRODSKI Mykhaylo, Jack Watling, Oleksandr V. Danylyuk, Nick Reynolds, *Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February–July 2022*, RUSI Special Report, Royal United Services Institute, London, 30 November 2022, 66 p.;
16. *** *Mission Command: Command and Control of Army Forces,* Army Doctrine Publication 6-0, Headquarters, Department of the Army (HQDA), Washington DC, HQDA, 31 july July 2019.
17. *** *Hybrid threats/ Russia: Statement by the High Representative on behalf of the EU condemning Russia's persistent hybrid campaigns*, Consiliul UE (iulie 2025); https://www.consilium.europa.eu.
18. *** *Amenințările hibride. UE și statele membre colaborează pentru a preveni, a contracara și a răspunde amenințărilor și campaniilor hibride care afectează Europa și cetățenii săi*, Consiliul Uniunii Europene; https://www.consilium.europa.eu/ro/policies/hybrid-threats/#response.
19. *** „Analiză privind fracturarea coeziunii UE de activitățile hibride ruse", 2026; https://www.euronews.com.

[1] Erich von Manstein, *Victorii pierdute*, Editura Elit, București, 2002, p. 76.
[2] *Ibidem.*
[3] În Biblie, când Moise trimite cele 12 iscoade din pustiul Paran să exploreze ținutul Canaanului pentru a vedea cum este poporul, cum sunt cetățile, pământurile și roadele, nu le spune cum să adune informații, ci doar ce să facă. Este un exemplu de comandă prin misiune?
[4] Clinton J. Ancker III, "The Evolution of Mission Command in US Army Doctrine, 1905 to the Present", *Military Review* (website), March-April 2013; https://armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20130430_art008.pdf.
[5] Headquarters, Department of the Army (HQDA), *Mission Command: Command and Control of Army Forces*, Army Doctrine Publication 6-0, Washington, DC, HQDA, July 2019.
[6] Burton L. Brender, "The Problem of Mission Command", RealClear Defense (website), September 1, 2016; https://www.realcleardefense.com/articles/2016/09/02/the_problem_of_mission _command_110008.html.
[7] Jesse Greenspan, "Ukraine Has Seen Centuries of Conflict", History (website), October 5, 2022, https: //www.history.com/news/ukraine-timeline-invasions; a se vedea și Franz-Stefan Gady, "Ukraine's Army Must Shed Its Soviet Legacy, Says a Military Expert", *The Economist* (website), March 17, 2023, https://www.economist.com.
[8] Simon Shuster, Vera Bergengruen, "Inside the Ukrainian Counterstrike That Turned the Tide of the War", *Time,* 26.09.2022, https://www.time.com/6216213/ukraine-military-valeriy-zaluzhny/?utm_source=twitter&utm_medium=social&utm_campaign=editorial&utm_term=world_ukraine&linkld=183047256; a se vedea și David M. Herszenhorn, Paul McLeary, "Ukraine's 'Iron General' Is a Hero, but He's No Star", *Politico* (website), April 8, 2022, https://www.politico.com/ news/2022/04/08/ukraines-iron-general-zaluzhnyy-00023901.
[9] *Idem.*
[10] Franz-Stefan Gady, *Op.cit.*
[11] Mykhaylo Zabrodski et all., *Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February–July 2022*, Royal United Services Institute, London, November 2022, p. 64.
[12] Jack Hewson, "Ukrainian Company Uses Social Media, Open Source Technology to Counter Russian Invasion", PBS News (website), April 19, 2023; https://www.pbs.org/newshour.
[13] Jim Hockenhull, "How Open-Source Intelligence Has Shaped the Russia-Ukraine War", Speech, Royal United Services Institute, Members Webinar, London, 09.12.2022; www.gov.uk/government/speeches/how-open-source-intelligence-has-shaped-the-russia-ukraine -war.

THE IMPACT OF ARTIFICIAL INTELLIGENCE ON HUMINT

Fred P. HOFFMAN, Tyler MORITZEN, Matthew BELLES, Colin TARDIF, Ryan MAHONEY*

Abstract

Based on the collection and analysis of unclassified, publicly available, open-source intelligence (OSINT) information, this article examines how artificial intelligence, or AI, could positively and negatively impact both human intelligence (HUMINT) and counterespionage operations. The Introduction begins by describing the evolving nature of AI, overt and clandestine HUMINT operations, and explaining why HUMINT remains a necessary collection discipline in the Digital Age. The Literature Review reveals divergent professional and scholarly opinions on how AI will affect, and is already affecting, the HUMINT collection discipline. The Methodology section explains how students in Mercyhurst University's Intelligence Studies program combined project management principles with open-source intelligence collection and analysis to collect, analyze, and report their analytic findings on this topic. The Findings section addresses how AI could impact each of the seven steps in the clandestine HUMINT operational cycle, traveling and operating in cover, coping with biometric and UTS threats, and other AI impacts on HUMINT operations and methodologies, such as handling walk-ins, operating in cover, online recruitment, and cybernetic HUMINT. The article also examines some of the limitations of AI, such as hallucinations, susceptibility to manipulation, and the risk of willful adversarial deception. The Conclusion section offers some analytic judgements on how HUMINT professionals should think about the impact of AI on their profession.

***Keywords**: Human Intelligence; Artificial Intelligence (AI); counterespionage; technology; ubiquitous technical surveillance; tradecraft.*

INTRODUCERE

Narrow AI, GenAI, and AGI

Artificial Intelligence, or AI, is a term that refers to the ability of a computer system to ***perform tasks that normally require human intelligence***, such as learning, reasoning, and decision-making.[1] John McCarthy first introduced the term "artificial intelligence" in 1956[2]. The type of AI that most people use at present is ***narrow AI***, which can perform discrete tasks like providing directions to a driver, translating text, or playing chess against a human player[3].

More capability-diverse than narrow AI is ***GenerativeAI***, or ***GenAI***, which is used for creativity and the generation of new content. Christopher Wall noted that, "The most prominent form of GenAI, large language models (LLMs),

****Fred P. HOFFMAN is a retired Lieutenant Colonel in the U.S. Army who spent 30 years as a human intelligence collector and military attaché in several countries before becoming an Associate Professor of Intelligence Studies at Mercyhurst University in Erie, PA. Tyler MORITZEN, Matthew BELLES, Colin TARDIFF, and Ryan MAHONEY were all students in Hoffman's Strategic Intelligence capstone course, taken as the culmination of their four-year-long Intelligence Studies baccalaureate program.***

excel at the imitation game first described by Alan Turing. LLMs can spoof human conversations, pass American legal exams, pen Shakespearean sonnets, write functional computer code, and summarize text"[4]. Commonly-used GenAI includes ChatGPT and similar, commercially-available tools, which are developed using either rule-based or self-learning (AI) methods" and "enable computers to understand human language"[5]. Created from a large language model (LLM), ChatGPT can now be used for "creative writing, essay writing, prompt writing, code writing, and answering questions"[6]. Although ChatGPT represents a major step forward in the realm of AI, it "has not achieved many fundamental components of AGI, such as self/social, emotion, motivation, meta-cognitive, and deliberative processes"[7].

Artificial General Intelligence, or ***AGI***, refers to a type of AI that could not only perform all the tasks performed by ChatGPT, but even replicate human cognition. John Galascione notes that AGI does not yet exist, and asserted that "skeptics continue to assess that 'generalized' artificial intelligence is still a distant development."[8]

AI'S IMPACT ON COUNTERESPIONAGE

Christopher Wall described how Western intelligence services "turned to advanced analytics, machine learning (ML), and artificial intelligence (AI) to support their CT efforts" to "beat back al-Qaeda and other forms of Islamic extremism":

Governments with access to data and processing power developed statistical tools to filter through the noise produced by human chatter, signals data, and other intelligence sources to find the proverbial needle-in-the-haystack. In parallel, security agencies invested in unmanned platforms for reconnaissance and direct action, which they combined with insights derived from AI/ML to plan strikes against terrorists. The advent of neural networks in the 2010s turbocharged these tools, as AI could extract deeper insights from data and plug directly into manned and unmanned systems. These developments led to economies of scale for counterterrorism that greatly curtailed extremist opportunity to plot and execute mass casualty attacks[9].

Technology is like a dual-edged sword: Whenever a technology is developed to provide a particular capability, it invariably creates new vulnerabilities as well[10]. This is a tale as old as time itself: "From the time mankind discovered rocks could be used to open coconuts or break bones to access marrow, it also learned that the same rock could be used to attack others of the human race—rocks were effective weapons"[11]. Just as AI has enabled Western counterintelligence services to ramp up their capabilities to more effectively target terrorists, foreign intelligence services are able to exploit AI to use against Western human intelligence officers and their sources[12].

AI capabilities that enable and improve technical intelligence disciplines like SIGINT, GEOINT, and MASINT unfortunately present some challenges to friendly HUMINT practitioners operating overseas: AI-enabled human activity recognition (HAR) under pervasive sensor networks or ambient cameras can infer intent, routines, and association networks.[13] AI can also benefit HUMINT activities in a number of ways.

WHAT IS HUMINT?

For millennia, long before the creation of any technical intelligence collection capabilities, "human agents, known as part of Human Intelligence (HUMINT), were relied upon and prioritized as the sole intelligence-gathering method"[14]. HUMINT can be either *overt* or *clandestine*.

Overt HUMINT

As Magda Long observed, "During an interview in 2013, John Negroponte, a former ambassador and director of National Intelligence, referred to diplomats as overt intelligence collectors. He explained that when diplomats report on political or economic matters, they collect intelligence and information overtly, rather than clandestinely, and therein lies the difference between intelligence and diplomatic operations"[15]. Overt HUMINT is conducted openly, without intelligence collectors attempting to conceal

either their true identity or their organizational affiliation[16]. "For the public, HUMINT is still closely associated with espionage and secretive operations; however, most of HUMINT collection is performed by overt collectors such as strategic debriefers and military attachés"[17]. Operating in uniform and in true name, United Nations peacekeepers can overtly collect human intelligence when interacting with people in their area of operations[18]. Law enforcement or military interrogations are also considered open source HUMINT[19]: A police officer who interviews a witness or interrogates a suspect is also conducting overt human intelligence collection[20]. Defector debriefings are another example of overt HUMINT collection[21]. David Canon noted that "nonrecruited defectors...make up a large percentage of all [HUMINT] sources"[22]. Overt HUMINT skills include "knowing what questions to ask and how to ask them, identifying and interpreting body language to detect signs of honesty or deceit, and special questioning and approach techniques"[23]. These are not skills that the current generation of AI tools are able to replicate.

Clandestine HUMINT

There are some significant differences between overt and clandestine HUMINT. As Gabriel Margolis explained, "Human intelligence (HUMINT) is gathered through espionage. It usually involves sending clandestine officers to foreign countries in an attempt to recruit spies and gather valuable information. Sometimes spies, also known as intelligence officers, have official cover which may place them at a diplomatic post in a foreign state"[24]. Other HUMINTers, who operate without the benefit of diplomatic cover, "may operate as businessmen, travelers, or (using) another discrete and relevant cover"[25]. "HUMINT consists of the use of human beings (agents), rather than technology, to collect information, usually through illicit means"[26]. Clandestine HUMINT involves "espionage," which William Usher defines as "the deliberate collection of non-public information from human sources using clandestine means"[27]. As retired CIA senior executive Usher explained, "We refer to the intelligence officer involved in recruiting or developing a foreign HUMINT source as a 'case officer' and their target, or recruited human source, as an 'asset' "[28].

Clandestine HUMINT assets

Clandestine HUMINT officers recruit many different types of assets: Some may be casual travelers or business people who travel to and from locations and countries of interest.[29] Some may be resident agents who live in a sensitive country or area that is of high interest to friendly intelligence, but is not accessible by its own case officers[30].

WHY HUMINT REMAINS NECESSARY

Thanks to technological advances, signals intelligence (SIGINT), geospatial intelligence (GEOINT), Measures and Signatures Intelligence (MASINT), and even open-source intelligence (OSINT) all underwent massive transformations since the end of the Cold War (1947-1991) and the onset of the Digital Age[31]. During the Cold War, OSINT only accounted for approximately 20% of the U.S. intelligence on the former Soviet Union. Today, thanks to the digitization of information, social media, and the internet, the percentage of intelligence collected on the Russian Federation has increased from 20% to 80-90%[32]. The transformative changes that have taken place in OSINT alone during the first quarter of the 21st century have been so impactful and profound that the authors of a 2018 RAND report suggested that today's open-source intelligence "should be seen as a *second generation* of OSINT"[33]. In 2006, in recognition of OSINT's burgeoning contributions and impact, the Office of the Director of National Intelligence (ODNI) designated OSINT as its own intelligence discipline, equal in stature to HUMINT, SIGINT, GEOINT, and MASINT[34]. By 2024, the Office of the Director of National Intelligence issued the intelligence community's first-ever OSINT strategy for 2024-2026; on the cover of that strategy was the slogan, "The INT of First Resort"[35]. As Robert Clark observed, "If OSINT is the source of first resort, clandestine HUMINT is the source of last resort"[36]. Although OSINT, SIGINT, IMINT, and MASINT have all

grown in importance, HUMINT still remains essential because it alone can provide certain insights that the other intelligence disciplines cannot: The *intentions* of the state or non-state actor that is the subject of intelligence collection. "Intelligence agencies recognize that HUMINT provides a deeper understanding of the context surrounding a potential threat, including the motivations, intentions, and capabilities of the individuals involved"[37].

HOW AI IMPACTS HUMAN INTELLIGENCE (HUMINT)

In some ways, AI can benefit HUMINT; in others, AI can be detrimental. In an article comparing AI to human cognition, Jiajie Zhang points out the strengths and weaknesses of both, and suggests that they complement one another. "AI's precision and range in sensation, laser-focused and large-span attention, and task-specific and limitless memory ***are contrasted with*** human adaptability, contextual richness, and emotional depth," and "while AI excels in certain areas, human cognition remains unmatched in others, making these two forms of intelligence ***complementary rather than competitive"***[38].

Humans can "***integrate sensory inputs with context and experience***. We perceive not just with our senses but with our minds, shaping raw data into meaningful, nuanced perceptions"[39]. By contrast, "AI's ability to perceive sensory information is still limited"[40]. AI lacks the human mind's ability to integrate memory, experiences, and context[41]. Humans can ***reprioritize and adjust their focus*** in ways that AI cannot[42]. AI is adept at machine translation, processing "syntax and semantics at a speed and scale that far outpaces human capabilities, often generating coherent, grammatically correct sentences"[43]. However, ***language "is more than just processing words****;* it's about understanding context, emotion, and culture"[44]. Limited to the data it was trained on, AI "cannot grasp the full depth of human communication"[45].

AI makes ***decisions that are data-driven***, while human beings make decisions based on data but also influenced by experiences and emotion[46]. "Human decision-making incorporates empathy, social considerations, and ethical judgement"[47]. ***AI does not experience emotion***, whereas "Emotions are at the core of human cognition, influencing how we think, interact, and make decisions"[48]. Because of these differences between human intelligence and AI, "HUMINT continues to be a vital element, providing a human touch and insights that can be difficult to reproduce solely through technological means"[49]. Although AI cannot *replace* HUMINT, it can serve to enhance various HUMINT activities in a number of ways. Eugene De Silva also advocates for using AI to enhance HUMINT:

The most promising approach lies in the integration of AI with HUMINT rather than the replacement of one by the other. A hybrid model leverages the contextual, cultural, and emotional acuity of human operatives alongside the speed, scale, and precision of machine processing. The U.S. Department of Defense's Project Maven is a model example. It uses AI to analyze drone footage and flag potential threats but leaves the final determination to human analysts. Such collaborative frameworks help minimize both human and machine error[50].

LITERATURE REVIEW

A review of the literature reveals a variety of opinions on how AI will impact human intelligence. In an article in which he predicts that AI will eventually make human intelligence *analysis* obsolete, John Galascione suggested that human intelligence *collection* shares a similar prognosis[51]. Chris Dictus and Bandon De Bruhl asserted that while "artificial intelligence will aid some forms of intelligence collection, it will impede others"[52]. They asserted that "there is uniform agreement that artificial intelligence will have the most detrimental impact on human intelligence gathering"[53]. After considering how technology has impacted HUMINT, David Gioe and Tony Manganello acknowledged that "emerging digital technologies present both new opportunities and challenges," asserted

that HUMINT is still needed, and advocated for "a fusion of traditional HUMINT tradecraft and emerging digital technologies"[54]. Gioe and Manganello asserted that there is a "longstanding U.S. (over) reliance on technical collection capabilities"[55], and argued that "HUMINT operations will remain a core staple of intelligence collection for the foreseeable future, augmented and often enhanced, not replaced, by cyber developments or 'virtual' intelligence operations (some of which are similar to HUMINT tradecraft in any case)"[56].

Usher's article was based on interviews and focus groups involving "experts from the U.S. Intelligence Community, former human intelligence practitioners, legal experts with Intelligence Community experience, as well as representatives from the AI industry"[57]. Like Gioe and Manganello, Usher also balked at the notion of abandoning HUMINT, arguing that "the value of human intelligence is critical" because "only human sources can reliably access their intent"[58]. In fact, the title of his work is, "The digital case officer: Reimagining espionage with artificial intelligence"[59]. Usher asserted that, "The objective is not to replace human officers but to empower them. The future of human intelligence lies in the human-machine team, where AI handles the immense scale of data processing and initial outreach, freeing case officers to focus on high-value work such as making nuanced judgments, managing the psychology of the asset-case officer relationship, and overseeing high-stakes operations"[60]. Usher asserted that, "The future of human intelligence lies in the human-machine team, where AI handles the immense scale of data processing and initial outreach"[61]. Although Usher asserted that AI enables and empowers human intelligence officers, he also emphasized that, "At every critical juncture—especially the final decision to recruit, the tasking of an asset, or actions that pose significant risk to the asset or U.S. national security interests—an accountable human must be able to exercise final judgment"[62]. Usher asserted that by incorporating AI into HUMINT, "the United States can pioneer a 'fourth generation espionage' model that fuses timeless human skills with cutting-edge technology."[63]

METHODOLOGY

The Strategic Intelligence course

Located in Erie, Pennsylvania, Mercyhurst University is home to the first-ever intelligence studies program offered in U.S. academia[64]. Researchers for this article consisted of a professor-led student project team composed of four students enrolled in the Strategic Intelligence course, a required, senior-level capstone course for both undergraduates in the Intelligence Studies Bachelor of Arts program and the Applied Intelligence Master of Science program[65]. The purpose of the Strategic Intelligence course is to provide graduating intelligence students with the opportunity to put to use in support of a real-world client the knowledge, tools, techniques, and procedures they had acquired during their course of study[66].

Application of project management principles

In this project, the student project team employed both project management principles and commonly used intelligence analysis team techniques[67]. Their effort began with an internal kick-off meeting, at which "the project manager's responsibility is established, the project effort and the project team are organized, the team-building process is started, and the initial project plan is developed"[68]. The kick-off meeting was followed by an initial client meeting at which the client elaborated on their interest in the research topic[69]. Based on their initial interaction with the client, the student project team collaboratively drafted a list of Key Intelligence Topics (KIT) and Key Intelligence Questions (KIQ) that conveyed to the client their understanding of what information was desired[70]. KIT/ KIQ are "routinely used" in both the U.S. intelligence community and in the private sector to ensure that intelligence analysts fully and accurately understand their client's information needs, and then accurately capture them in writing[71]. The final version of the KIT/ KIQ are then presented to the client within a Terms of Reference document, or TOR, which explains what the project team has agreed to do, what questions (i.e., the KIT/ KIQ) they will seek

to answer, how they will conduct their research, what and when the project milestones will be, and identifies the project's final deliverables[72]. Twice during the 14-week-long project, the project team conducted scheduled check-in calls with the client to convey their progress, identify any challenges they might be experiencing, and allow for the client to provide "course correction" to the KIT/KIQ[73]. At the end of the semester, the project team remotely conducted an oral presentation to the client and provided a Word document conveying their analytic key judgements and evidence to support them.[74]

Open-source intelligence collection

To answer their KIT/KIQ, the student project team engaged in open-source intelligence (OSINT) collection, a qualitative research methodology. OSINT collection "involves observation or direct gathering of PAI from public events and spaces"[75]. Since only four percent of all Internet content is optimized for retrieval by search engines, OSINT involves far more than simply performing key word searches on an Internet browser; it may require specialized software, managed attribution, and OSINT tradecraft when visiting websites in sensitive countries, or for searches in the deep web or dark web[76].

Analysis and presentation of an estimative intelligence product

During their intelligence studies program, student project team members learned to use structured analytic techniques (SAT), which the Director of National Intelligence (DNI) required intelligence community intelligence analysts to use to "meet the highest standards of integrity and rigorous analytic thinking"[77]. CIA analysts Randolph Pherson and Richards Heuer Jr. published a book that listed 66 different SATs that could be used in various phases of an intelligence analysis project. Intended to improve analytic transparency while mitigating cognitive biases, "well-known group process problems can be minimized by use of structured techniques that guide the interaction among members of a team or group"[78]. Because the student project team's assessments concerned the future, rather than just the past and present, they used the National Intelligence Estimate (NIE) structure to convey their analytic judgements and provide the evidence they gathered to supported them[79]. In an NIE, analytic judgements are written using *words of estimative probability*, which CIA analyst Sherman Kent first proposed "as a means of communicating intelligence assessments to stakeholders and decision-makers"[80]. An analytical judgement written with words of estimative probability provides both the analysts' degree of confidence in what they are asserting, and the likelihood that what they are predicting will actually occur[81].

FINDINGS

How AI could impact the clandestine operational cycle

Spotting

Spotting refers to the identification and targeting of potential human sources for recruitment[82]. "In the spotting and recruitment phases of the HUMINT agent recruitment cycle, new cyber tools are expanding the ways officers target potential sources with access to required information"[83]. Gioe and Manganello asserted that "social media can be a gold mine in identifying promising new sources, and this has been proven avenue of recruitment"[84]. Usher stated that AI can "synthesize vast datasets to identify and prioritize potential intelligence assets based on their access, motivation, and vulnerability"[85]. Usher also asserted that, "Artificial intelligence can also help human collectors achieve unprecedented scale by spotting greater numbers of targets, simultaneously developing their profiles, and conducting virtual approaches[86]. As Kiran Krishnamurthy said, one could use AI to "process and analyse years of social media data, communication patterns, and behavioral trends to identify potential persons of interest or predict future events with a degree of accuracy that would be impossible for human analysts alone"[87]. The value of leveraging AI to support the identification and profiling of prospective sources has greatly benefited CIA targeting

officers, "combine specialized training, utilize advanced analytic skills and tools and in-depth knowledge and experience in DO (Directorate of Operations) operational tradecraft to identify new opportunities for DO activities and enhance ongoing operations"[88].

Assessment & development

Assessment is the phase of the clandestine operations cycle where case officers learns as much as possible about prospective sources, arrange to meet them, cultivate them over time, and ascertain exploitable motivations that could be leveraged to finally recruit them[89]. In contrast to the spotting phase, assessment is one of those phases of the clandestine operational cycle cannot be simply performed by AI, because as Gioe and Manganello point out, "relationships do not scale"[90]. Each human relationship is unique: "As algorithms and AI-enabled networks make digital connections more rapid and prolific, individual relationships, such as the one between an officer and agent, require interpersonal time, which cannot be simulated or accelerated by machine assistance"[91]. On the other hand, as Usher pointed out, AI could assist case officers as they "build detailed psychological profiles from digital footprints and engage targets in tailored, long-term conversations to build rapport and trust, using hyper-realistic personas. AI can manage hundreds of such developmental conversations simultaneously—a task impossible for a human officer"[92].

Recruitment

Recruitment refers to the phase in a relationship where case officers reveal their true intent to their prospective sources and successfully convince them to enter a clandestine relationship, willingly provide intelligence information, and accept direction and control intended to keep both case officer and source safe from discovery[93]. As Gioe and Manganello explained, CIA developed the role of Targeting Officer "to better support the recruitment phase of the agent acquisition cycle in an increasingly complex environment"[94]. AI used by a Targeting Officer (or the case officer himself) could help in the preparation of a suitable recruitment pitch; as Usher asserted, AI could "deliver personalized recruitment pitches by referencing a target's specific grievances or motivations"[95]. However, just as each human relationship is unique, each recruitment attempt is absolutely contingent upon the skills of an individual case officer in identifying another person's motivations and vulnerabilities, and ultimately exploiting those insights to persuade a developmental prospect to engage in espionage[96]. As Gioe observed, "no amount of cyber-interaction can replace the close bond between an intelligence officer and his or her agent"[97].

Handling

Handling refers to the "productive" phase of the clandestine relationship, where the recruited asset knowingly provides reportable intelligence information to a case officer[98]. "Handling includes a case officer reporting the intelligence received to headquarters in a timely manner and ensuring the agent's security through training and counterintelligence vetting"[99]. During this phase, a case officer continues to maintain a personal relationship with a source, taking care to identify possible changes in motivation that could jeopardize continuance of the relationship. L. Tyl-Descombes noted that "as technologies have created new intelligence collection disciplines, they have also impacted how intelligence is gathered through human agents"[100]. Gioe and Manganello pointed out that "personal interaction between the case officer and his/her agent has always been – and continues to be – at the heart of HUMINT operations[101]. As Joseph Wippl observed, "agents are not simple because people are not simple"[102]. "The art of handling entails a great deal of subjectivity"[103]. As Wippl explained, "while the recruitment of agents is both essential and gratifying, by itself it accomplishes nothing. Handling agents for product is what counts, now and always"[104]. Here, too, AI can assist agent handlers in handling by helping to gather, collate, corroborate, and analyze information acquired by the case officer, but its utility in helping a case officer manage a personal relationship with a recruited asset relationship is less clear.

Ensuring asset security

Maintaining the security of a recruited asset is a "primary responsibility of any case officer"[105]. Both the case officer and the recruited asset must take precautions to avoid coming to the attention of foreign intelligence services, or FIS[106]. Once case officers successfully recruit assets they have cultivated in the development phase, they typically change tack and minimize or eliminate face-to-face contact with them to avoid attracting the attention and interest of FIS[107]. They must also begin training recruited assets in how to safely do what they were recruited to do, and either safely meet with the case officer face-to-face or communicate clandestinely through impersonal communication[108]. Some operational environments are benign, while others are hostile[109]. If they are both coming to a personal meeting with each other, both the case officer and the agent must ensure they are not under surveillance by FIS[110]. While case officers can leverage AI to plan and prepare surveillance detection routes for themselves and their assets to follow, the execution of good security practices ultimately comes down to the behavior of fallible human beings operating under stress: Although sometimes the case officer fails to conduct "good counter-surveillance tradecraft," it is usually the agent who fails to do so[111].

Asset validation

Asset validation refers to steps taken by case officers to ensure their assets remain loyal, report completely and truthfully, and are not under the control of FIS. "Machine learning algorithms can analyze patterns in a source's past information, compare it with known facts, and even detect subtle indicators of deception in written or transcribed communications. This can provide human operatives with valuable insights when assessing the credibility of a source or the veracity of new information"[112]. As Usher asserted, AI can provide "real-time operational security advice to assets once recruited"[113].

Turnover

For a variety of reasons, it may become necessary for case officers who originally recruited their assets to turn handling responsibilities over to another case officer. Because of the foibles and complexities of human nature, the relationship a recruiting case officer cultivated and maintained with his clandestine asset does not automatically, seemlessly transfer to another person. "The first turnover between the recruiting case officer and his/ her successor is often the most difficult," as Wippl observed[114]. AI may help case officers plan and prepare for turnover, but ultimately it essentially comes down to the skill and *Fingerspitzengefühl* of the original and replacement case officers to effectively transition a relationship to a new handler: "Case officers may not be therapists or marriage counselors but they must be sensitive and careful listeners"[115].

Termination

Sometimes, recruited assets lose access to intelligence information of interest, or become handling problems for security or other reasons. In such situations, case officers may find it necessary to terminate their assets. As Wippl observed, "terminating an agent who has worked loyally for the U.S. government is never easy"[116]. In this situation, while AI could help a case officer plan and prepare for a termination meeting, the tone and outcome of the termination meeting will ultimately be dictated by the personalities and cognitive powers of the human beings in the room.

Other AI impacts on HUMINT

Tradecraft is a term of art used in the intelligence community which refers to techniques, methods, and technologies used by human intelligence officers[117]. HUMINT tradecraft is used for the purposes described below.

Enticing and verifying walk-ins

Volunteers, commonly referred to as walk-ins, provide their services to foreign governments of their own volition. Spies like Oleg Penkovsky of the Soviet Union, Aldrich Ames of the CIA, and Robert Hanssen of the FBI were all walk-ins[118]. Walk-ins are inherently challenging, and "should be viewed with a suspicion that they are not dangles or agent provocateurs controlled by an enemy service"[119]. "CIA has used the Telegram messaging app to ***encourage virtual***

'walk-ins' who might have useful information pertaining to the Russia-Ukraine conflict. This methodology seems to have borne fruit in terms of recruiting hard target sources and will thus likely be expanded"[120]. An intelligence service could leverage AI capabilities to quickly identify social media and other information available on the walk-in, and to validate the information they have provided[121].

Cover

Gioe and Manganello asserted that "backstopping (creating aspects of a cover identity that can be verified by outside scrutiny, as in the FBI Stagehand program) was more easily accomplished in an analog era. Now, intelligence agencies must also manage the digital identities of their officers, which must match their cover legends"[122]. Software developed to identify fraudulent activity in the banking and financial sector can be used to reveal covers for action[123]. AI can be effectively used by either FIS or friendly counterintelligence services to rapidly profile and assess a suspected HUMINT officer.

Traveling abroad in alias

Biometric data makes it very difficult for a case officer to separate their cover identity from their true identity. "Former CIA officials warn that HUMINT is necessarily moving towards a 'one country, one alias' modus operandi"[124]. A paradigm shift may be necessary, where intelligence officers are "already working in well-placed positions, who could itinerantly work for an intelligence service while maintaining a legitimate professional career. Such 'in-place' officers would not need cover identities and could 'hide in plain sight' in their real identities"[125]. Dictus and De Bruhl noted that "AI-empowered ubiquitous surveillance; greater use of biometrics; and other emerging technological changes" will make it easier for an adversary's counterintelligence services "to disrupt and deny" friendly HUMINT officers[126].

Biometric threats

AI has amplified the utility of biometric capabilities to intelligence and law enforcement services – which creates problems for HUMINT case officers operating in cover. "Retinal scans, fingerprints, facial recognition and even gait analysis are increasingly tracked by sophisticated sensors. These digital 'fingerprints' are analysed by AI/ ML systems with ever increasing granularity"[127].

Ubiquitous Technical Surveillance (UTS)

Ubiquitous Technical Surveillance, or UTS, refers to technical systems accessible to law enforcement agencies and intelligence services through which they can leverage data from digital surveillance camera networks, electronic signals from mobile phones, and databases of credit card data, hotel stays, airline travel, and car rentals to identify and associate individuals attempting to engage in clandestine, covert, or illegal activities. AI significantly greatly improves the speed, efficiency, and accuracy of exploiting, aggregating, and analyzing data from these databases. In one academic study, for example, researchers studied three months of credit card records for 1.1 million people and discovered that "four spatio-temporal points are enough to uniquely reidentify 90% of individuals"[128]. Usher warned that, "Multimodal AI, which can process and generate text, images, video, and audio, opens new opportunities and creative frontiers, vastly expanding the aperture of signals available for collection and exploitation. The People's Republic of China (PRC) and other adversaries are already moving to deploy these technologies at scale, making classic methods of tradecraft untenably risky and, in some cases, nearly impossible to safely execute[129].

In 2024, Shawn Benson, working for the U.S. defense contractor MITRE, published a document examining how the combination of AI and UTS systems represents a powerful threat to U.S. intelligence activities overseas[130]. "Without D2A2, the data produced by UTS would be nearly unintelligible and unactionable," Benson wrote, arguing that it is precisely *through the addition of AI* that foreign intelligence services can create a Data-driven Analysis and Artificial Intelligence, or D2A2, capability, that would enable them to effectively leverage UTS data[131]. Benson argued that while "data generated by UTS does not, without significant effort, become actionable

insight for our adversaries," a subsequent process, D2A2, enables the user "to create meaningful and actionable intelligence"[132].

Translation

One of the most impactful AI-enabled capabilities is in the realm of machine translation[133]. An AI system can provide real-time translation of "words, cultural nuances, idioms, and non-verbal cues"[134].

Clandestine agent communications

Dictus and De Bruhl asserted that AI "will both aid and impede communicating with agents"[135]. For example, while AI enables more sophisticated encryption at present, "quantum computing…threatens to upend encryption systems worldwide"[136].

False-flag recruitment

A false-flag recruitment is where a case officer asks a recruitment prospect for "increasingly sensitive information in return for seemingly innocuous favors or in the interest of serving some cause agreeable to the prospect"[137]. For example, a case officer from country A could claim to be working on behalf of country B, in the event country B was more palatable than country A to the recruitment prospect. False-flag recruitment approaches are especially useful when a prospective source "would never be able to bring themselves knowingly to work for" country A[138].

Leveraging AI and big data to identify HUMINT targets

"On a seemingly daily basis, personal data from major organizations (governments, health care networks, educational institutions, etc.) are stolen and used either for profit, crime or for intelligence collection purposes. This is happening at scale"[139]. "In the OPM breach, Chinese intelligence successfully stole personal data for 21.5 million current and former US government employees with security clearances (including both authors' data). Such a hoard of data would save any intelligence service considerable time and effort in targeting potential sources. Between exploiting big data, SOCMINT and malicious hacking, adversarial intelligence services now have evolved models for seeking, locating, assessing and validating their quarry"[140].

Creating a leveraged biography

Exhaustive AI searches can result in foreign intelligence services coming across compromising material that could then be used to coerce a targeted individual. "Sexual practices are not the only hook officers can use to develop an agent. *'Leveraged biography'* can cover a number of historical facts whose disclosure could discredit or pain the agent"[141].

Online recruitment

Thanks to the proliferation of the internet and social media, U.S. and foreign intelligence agencies have contacted, cultivated, and recruited clandestine assets through online recruitment[142]. China has successfully used LinkedIn to spot, assess, develop, and "recruit human assets in several Western countries"[143]. Russia has used the *Telegram* app and cryptocurrency to recruit assets in Poland, while U.S. intelligence has leveraged the dark web to recruit assets in Russia[144]. "On LinkedIn for instance, people reveal an astonishing amount of information about their professional positions, detailed duties within those positions, place in a corporate hierarchy, client base, dates of employment, military service, security clearance level and other information that might take a non-tech enabled intelligence officer weeks or even months of personal meetings to elicit"[145]. Combining information acquired from LinkedIn with information obtained from other social media sites "may reveal a startling amount of information on a person"[146]. "US adversaries like China have well-established practices in utilizing social media platforms as instruments of spotting and recruiting. As noted, the LinkedIn social media platform has become a vector for intelligence officers to spot and recruit sources"[147].

The birth of cybernetic HUMINT

Taking online recruitment one step further, "Intelligence researchers in Israel have wondered if HUMINT might benefit from a synthesized approach, becoming a new sub-discipline, 'cybernetic HUMINT' "[148]. "Such an approach would not require direct officer to agent contact, and in many cases, officers and agents would not know each other's identity, but might solely interact with one another's imaginary persona or avatar"[149].

CIA's approach to implementing AI to support HUMINT

As Usher asserted, "The U.S. Intelligence Community can no longer afford an incremental approach to this transformation. The Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), the Defense Intelligence Agency (DIA), and other intelligence agencies must move decisively to reimagine and retool the human intelligence mission for the AI era"[150]. CIA's chief AI officer, Lakshi Raman, said in an agency podcast that the "CIA is incorporating large language models, or LLMs, in generative AI to help the agency's open-source mission. The CIA is also considering the workforce that will be using generative AI features"[151]. Raman also said that CIA "has a cohort of data scientists, analytic methodologies, AI professionals and engineers that are helping the CIA ensure its data is AI ready, that it can train and run an AI model and that the agency is incorporating AI into the applications it regularly uses"[152]. All these measures have significant implications for the training of CIA's clandestine human intelligence officers, which is *already* both expensive and time consuming[153]. Even before being exposed to (and learning) AI-enabled tools, Clandestine HUMINT officers must already learn how to speak foreign languages and survive in foreign cultures; conduct, detect, and evade surveillance; spot, assess, develop and recruit sources; operate and use sophisticated covert communications systems; and handle various types of weapons[154].

User beware: The limitations of AI support to HUMINT

Case officer adaptability to technology

Not all case officers are created equal. As Wippl observed, some case officers are exceptional recruiters, while other case officers may be excellent handlers because the two skill sets are different. As Wippl observed, "the reality is that many case officers do not have the talent to recruit agents while many others are unable to handle agents"[155]. In addition to there being a distinction among case officers between recruiters and handlers, there may also be differences in terms of case officer adaptability and comfort with using, and relying on, AI.

The social media threat to cover

Having newly recruited intelligence officers scrub their social media presence may not be helpful. In fact, "An officer's cover might be blown before it even gets created"[156]. "Recruiting HUMINT officers by canvassing college campuses is a bygone recruiting strategy. Western intelligence services must identify and recruit future officers at ages where more circumspection regarding social media can be employed"[157].

Social media data cannot be taken at face value

Gioe and Manganello cautioned that "anything posted to social media, cannot be taken at face value in today's contested information environment."[158] This situation has been greatly exacerbated by AI-generated deepfakes, which are fabricated, realistic-looking videos, audio, or images showing a person doing or saying something they never did[159].

The value of human-machine teaming

According to Juliane Gallina, CIA's Deputy Director for Digital Innovation, "every DDI mission is guided by human-machine teaming, which starts with data and is improved with AI before being put to use by CIA agents. 'Failure to harness AI and develop robust human-machine teaming will diminish our ability to generate insight, give advantage to adversaries more advanced in their use of AI and challenge our relevancy"[160]. "A human-technology interaction perspective views AI as an activity, which assists human to filter, manage, analyse and refine information in order to gain and maintain" situational awareness[161].

Adversary countermeasures

"As AI becomes more prevalent in intelligence gathering, adversaries will inevitably develop countermeasures. This could include the use of adversarial AI systems designed to deceive or mislead AI-enhanced HUMINT operations"[162].

Black box AI and transparency

"The 'black box' nature of some AI algorithms poses challenges for accountability and decision-making in intelligence operations"[163]. " 'Black box' AI models can make it hard to explain the reasoning behind a decision to target an individual,

undermining legal validation and creating a scenario where no one is clearly responsible if an operation goes wrong"[164].

Legal and ethical concerns

There needs to be a legal and ethical framework governing the use of AI to ensure compliance with civil liberties, personal privacy, and applicable laws. Usher asserted that, "The use of commercial models trained on large data sets may raise issues concerning data provenance and validation, and issues of privacy if those data sets include a high volume, proportion, or sensitive U.S. person information...Without explicit guardrails, an AI could pursue amoral strategies of manipulation, such as exploiting personal tragedy, that a human officer would reject. Delegating life-and-death recruitment decisions to a machine without a clear line of moral responsibility crosses a critical red line"[165].

GIGO

Information technology professionals have long used the acronym "GIGO," which stands for "garbage in, garbage out". This acronym is definitely applicable to AI systems, because "results generated by AI tools are only as good as the data that they have available"[166]. Robin Emsley noted how "the artificial intelligence (AI) system, Chat Generative Pre-trained Transformer (ChatGPT), is considered a promising, even revolutionary tool and its widespread use in health care education, research, and practice is predicted to be inevitable"[167]. Emsley was alarmed to discover that sometimes ChatGPT provided false information that was "charitably referred to as hallucinations"[168]. Upon further study, she concluded, "This is a misnomer. Hallucinations are false perceptions. What I experienced were fabrications and falsifications"[169].

Big data is also subject to manipulation

"OSINT and big data analytics excel at identifying trendlines as well as outliers and leveraging these enormous data sets can yield valuable insights to complement clandestine reporting in all source analysis. However, OSINT and PAI/CAI are under threat of manipulation in an increasingly contested information environment and therefore need verification. Additionally, big data analysis is not suited to the task of understanding and predicting the behavior of individuals, at least not in the near term"[170]. "As AI becomes more prevalent in intelligence gathering, adversaries will inevitably develop countermeasures. This could include the use of adversarial AI systems designed to deceive or mislead AI-enhanced HUMINT operations"[171].

AI and adversarial deception

It's bad enough that AI hallucinates on its own, but what if an adversary intentionally introduces false data into a system? That is not only fabrication or falsification, but *deception*. "Deception is the systematic inducement of false beliefs in others to accomplish some outcome other than the truth"[172]. If a foreign intelligence service (FIS) becomes aware that someone is a spy for U.S. intelligence, they may take advantage of that knowledge to engage in deception. Therefore, one of the challenges for a case officer is the constant need to confirm that the information provided by their recruited asset (or other source) is both truthful and accurate. During World War II, the British captured and "turned" virtually all of Nazi Germany's spies living in the United Kingdom[173]. The British gave those captured German spies a simple choice: Report what we tell you to report back to Germany, or we will execute you for being a spy[174]. Deceptive information that Britain's intelligence service made available via Germany's HUMINT channels was instrumental in enabling the Western Allies to fool Nazi leaders into believing the June 1944 invasion at Normandy would instead occur at Pas-de-Calais; in fact, "For a remarkable six weeks after D-Day, powerful Wehrmacht and Waffen SS forces remained in the Calais area preparing to repel an invasion which was never intended"[175]. Similarly, Cuban intelligence successfully employed deception to feed false information to United States case officers who were handling Cuban spies in the early 1960s, which contributed to the Bay of Pigs invasion fiasco[176]. Today, a FIS counterintelligence effort to deceive U.S. case officers could benefit from the use of "AI-generated deception, deepfake technologies, and psychologically engineered

social manipulation"[177]. As Park et al. observed, "When AIs learn the skill of deception, they can be more effectively employed by malicious actors who deliberately seek to cause harm"[178].

CONCLUSIONS

The purpose of this article was to examine how AI could impact the HUMINT discipline while also considering some of the implications of AI capabilities from a counterintelligence perspective. Technology is *always* a dual-edged sword; one the one hand, intelligence professionals are understandably excited about the many potential benefits of AI, while on the other hand harboring legitimate concerns over AI's potentially negative consequences for the HUMINT collection discipline and its practitioners.

America's fascination with technology

Over a generation ago, Neil Postman famously cautioned that Americans have become so enamored with technology that they eagerly embrace it without adequately reflecting on the costs and implications of doing so. "Machines eliminate complexity, doubt, and ambiguity. They work swiftly, they are standardized, and they provide us with numbers that you can see and calculate with"[179]. As one example, Postman talked about how American doctors are aggressive in medical treatment largely due to faith in technology: U.S. doctors perform far more surgeries, order far more X-rays, prescribe many more anti-biotics, than European counterparts in countries with comparable life expectancies[180]. Echoing Postman, Gioe and Manganello cautioned that "practitioners should be careful not to…prioritize the novel over the conventional simply by dint of being mesmerized by novel technological developments"[181].

Gartner's hype-cycle for AI

Looking at AI from a commercial (rather than an intelligence) perspective, Gartner's "Hype Cycle for Artificial Intelligence, 2025" noted that AI has entered "the Trough of Disillusionment, signaling a shift from inflated expectatio ns to practical, scalable deployment."[182] This is because "like any new technology wave, (AI) follows a familiar pattern of hype, disappointment, and eventual growth"[183].

The future of AI and HUMINT

While promising, AI is still in its infancy: Narrow AI is already in widespread use, GenAI is already demonstrating considerable (though not flawless) potential in many respects, while AGI still remains a pipe dream. The bottom line for HUMINT professionals is that they must remain cognizant of what AI can (and could) do – both for them, and to them. As Gioe asserted, "HUMINT will become even more complex, and case officers, their managers, and their political masters will need to understand the significant role of technology in their operations, the creative and persistent counterintelligence threats, and how intelligence collection is evolving faster than ever before"[184].

[1] John McCarthy, ”Artificial Intelligence, Logic, and Formalizing Common Sense”, in Richmond H. Thomason (editor), *Philosophical Logic and Artificial Intelligence*, Klüver Academic Publishers, 1989, pp. 161-190.
[2] Burak A. Daricili, Nourhan El-Bayaa, ”Using Artificial Intelligence in the Field of Intelligence Operations and Analysis”, in Mehmet Emin Erendor, *Cyber Security in the Age of Artificial Intelligence and Autonomous Weapons*, CRC Press, Taylor&Francis, 2024, pp. 43-57.
[3] Fabian Gaessler, Henning Piezunka, ”Training with AI: Evidence from chess computers”, *Strategic Management Journal,* vol. 44, no. 11, 2023, pp. 2724-2750.
[4] Christopher Wall, ”The Ghost in the Machine: Counterterrorism in the Age of Artificial Intelligence”, *Studies in Conflict & Terrorism*, 2025, pp. 1-27; https://doi.org/10.1080/1057610X.2025.2475850.
[5] Viriya Taecharungroj, “What Can ChatGPT Do?” Analyzing Early Reactions to the Innovative AI Chatbot on Twitter, *Big Data and Cognitive Computing,* vol. 7, no. 1, Mahidol University, 2023, p. 1.
[6] *Idem.*, p. 4.
[7] *Idem.*, p. 8.
[8] John F. Galascione, ”The End of Human Intelligence Analysis—Better Start Preparing”, *Studies in Intelligence,* vol. 67, no. 4, 2023, p. 19.
[9] Christopher Wall, *Op. cit.*, p. 2.
[10] Raymond E. Floyd, ”Technology - A Two-Edged Sword”, *IEEE Potentials,* vol. 37, no. 2, 2018, pp. 8-9; doi:10.1109/MPOT.2016.2556005.
[11] *Ibidem*., p. 8.
[12] S. Sowmiya, A. Saxena, M. Kumar, S. Raja, S. Arun, ”Searching Missing People Based on Face Recognition Using AI in Video Surveliance System”, *ShodhKosh: Journal of Visual and Performing Arts*, vol. 5, no. 3, 2024, pp. 1457-1462; https://doi.org/10.29121/shodhkosh.v5.i3.2024.4705
[13] Abdul Rehman Javed, Habib Ullah Khan, Mohammad Kamel Alomari, Muhammad Usman Sarwar, Muhammad Asim, Ahmad Almadhor, Muhammad Zahid Khan, ”Toward explainable AI-empowered cognitive health assessment”, *Frontiers in Public Health*, vol. 11, 2023, 15 p.; https://doi.org/10.3389/fpubh.2023.1024195
[14] Laetitia Tyl-Descombes, *Human Intelligence in the Modern Era: The Impact of Digital Technology on Clandestine Agent Recruitment by Intelligence Agencies*, Master’s thesis, International Master in Security, Intelligence and Strategic Studies, Charles University, Prague, 2024, 118 p.
[15] Magda Long, “American covert action and diplomacy after 9/11”, *Diplomacy & Statecraft,* vol. 33, no. 2, 2022, p. 381; doi:10.1080/09592296.2022.2062133.
[16] Ainara Bordes Perez, “ ‘What Is Really’ Open Source Intelligence?`. A Conceptual Analysis of the Different Notions of OSINT”, *Romanian Intelligence Studies Review*, no. 31, 2024, p. 52.
[17] Domenico Frasca, Giulia Venturi, Maria Ustenko, Alessandro Zanasi, Andrew Staniforth, David Fortune, “The Role of Human Intelligence in the Age of Digital Technology”, *Romanian Intelligence Studies Review*, no. 31, 2024, p. 9.
[18] Walter A. Dorn, “United Nations Peacekeeping Intelligence”, in Johnson K. Loch (ed.), *The Oxford Handbook of National Security Intelligence*, 2010, pp. 275-295; https://doi.org/10.1093/oxfordhb/9780195375886.003.0017
[19] Magda Long, *Op.cit.*
[20] Lee Moffett, Gavin Oxburgh, Paul Dresser, Steven Watson, Fiona Gabbert, “Inside the shadows: a survey of UK HUMINT practitioners examining their considerations when handling a covert human intelligence source (CHIS)”, *Psychiatry, Psychology and Law*, vol. 29, no. 4, 2022, pp. 487-505.
[21] David Canon, ”Intelligence and Ethics: The CIA’s Covert Operations”, *The Journal of Libertarian Studies*, vol. 4, no. 2, 1980, pp.197-214.
[22] *Ibidem*., p. 211.
[23] *** “Collection with a handshake – Demystifying human intelligence”, 14 July 2016, *Project Gecko*, para 5, https://www.projectgecko.info/security-articles/2016/7/14/collection-with-a-handshake-demystifying-human-intelligence#:~:text=Human%20intelligence%20(HUMINT)%20is%20a%20discipline%20of,language%20*%20Special%20questioning%20and%20approach%20techniques.
[24] Gabriel Margolis, “The Lack of HUMINT: A Recurring Intelligence Problem”, *Global Security Studies*, vol. 4, no. 2, 2013, p. 45.
[25] *Ibidem.*
[26] Donald A. Petkus, “Ethics of Human Intelligence Operations: of MICE and Men”, *International Journal of Intelligence Ethics*, vol. 1, no. 1, 2010, p. 105.
[27] William Usher, *The Digital Case Officer: Reimagining Espionage with Artificial Intelligence*, Special Competitive Studies Project, September 2025, p. 7.
[28] *Ibidem.*
[29] Hal Berghel, ”Robert David Steele on OSINT”, *Computer*, vol. 47, no. 7, 2014, pp. 76-81.
[30] Libor Bílek, “I undertake voluntarily … - Residents, agents, informers and others. The State Security’s secret collaborators, 1945–1989”, in *Behind the Iron Curtain*, Review of the Institute of the Study of Totalitarian Regimes,

Czech Republic, vol. 4, 2016, pp. 94-111.

[31] Fred Hoffman, Brian Fuller, "How Mercyhurst's CIRAT does OSINT – and why", *Issues in Information Systems*, vol. 26, no. 3, 2025, pp. 75-85.

[32] *Idem.,* "Rebranding second-generation open-source intelligence: 'It's not your father's OSINT' ", *Issues in Information Systems*, vol. 26, no. 3, 2025, pp. 61-74.

[33] Heather J. Williams, Ilana Blum, *Defining Second Generation Open-Source Intelligence (OSINT) for the Defense Enterprise*, RAND Corporation, Santa Monica, CA, 2018, p. ix.

[34] Kathleen M. Vogel, "OSINT and the U.S. Intelligence Community: Is the Past Prologue?", in *Open Source Investigations in the Age of Google*, World Scientific Connect, 2024, pp. 188-203.

[35] *** "The IC OSINT Strategy, 2024-2026", Office of the Director of National Intelligence, Washington, DC., 2024, p. 1, https://www.dni.gov/files/ODNI/documents/IC_OSINT_Strategy.pdf.

[36] Robert M. Clark, "The Changing Nature of Intelligence Collection", *The Oxford Handbook of National Security Intelligence*, 2025, p. 261.

[37] Domenico Frasca, Giulia Venturi, Maria Ustenko, Alessandro Zanasi, Andrew Staniforth, David Fortune, *Op.cit.*, p. 9.

[38] Jiajie Zhang, "Artificial Intelligence vs. Human Intelligence: Which Excels Where and What Will Never Be Matched", *UTHealth Houston D. Bradley McWilliams School of Biomedical Informatics*, 01.10.2024; https://sbmi.uth.edu/blog/2024/artificial-intelligence-versus-human-intelligence.htm.

[39] *Ibidem.*

[40] *Ibidem.*

[41] *Ibidem.*

[42] *Ibidem.*, Attention.

[43] *Ibidem*., Language.

[44] *Ibidem.*

[45] *Ibidem.*

[46] *Ibidem.*

[47] *Ibidem.*, Reasoning.

[48] *Ibidem.*

[49] Domenico Frasca et al., p. 6

[50] Eugene De Silva, "HUMINT vs. AI in Intelligence and Security Services", in *The Role of Intelligence in Countering Violent Extremism* (Eugene De Silva, Sinduja Umandi W. Jayaratne eds.), IGI Global Scientific Publishing, 2025, p. 10.

[51] John F. Galascione, *Op.cit.*

[52] Christopher Dictus, Brandon de Bruhl, Logan O`Shaugnessy, "Eying AI: Intelligence Collections Practices in the Age of Artificial Intelligence", 2024 APPAM Fall Research Conference, APPAM, p. 15.

[53] *Ibidem.*, p. 59.

[54] David V. Gioe, Tony Manganello, "Smart new world: adapting human intelligence for the digital age", *Intelligence and National Security*, vol. 40, no. 6, 2025, p. 1114.

[55] *Ibidem.*, p. 1116

[56] *Ibidem.*

[57] William Usher, *Op.cit.*, p. 7.

[58] *Ibidem.*, p. 4.

[59] *Ibidem.*, p. 3.

[60] *Ibidem*. p. 5.

[61] *Ibidem.*

[62] *Ibidem.*

[63] *Ibidem.*, p. 6.

[64] Fred Hoffman, Brian Fuller, "How Mercyhurst's CIRAT does OSINT, and why".

[65] Fred Hoffman, "Learning by doing: Acquiring the tacit knowledge of how to conduct an open-source intelligence collection and analysis project", *Issues in Information Systems*, vol. 25, no. 3, 2024, pp.81-93; DOI: https://doi.org/10.48009/3_iis_2024_107

[66] *Ibidem.*

[67] *Ibidem.*

[68] D. Hamburger, "Project kick-off: getting the project off on the right foot", *International Journal of Project Management*, vol. 10, no. 2, 1992 , p. 115.

[69] Fred Hoffman, *Op.cit.*

[70] *Ibidem.*

[71] Charlynn Clayton, Andrew Lin, Janine Pitt, J., *Key intelligence topics (KITs) and key intelligence questions (KIQs) in safety signal intelligence*, in 14th International Conference on Information Fusion, IEEE, Chicago, 2011, p. 1.

[72] Fred Hoffman, *Op.cit.*

[73] *Ibidem.*

[74] *Ibidem.*
[75] *** Practitioner Committee, "OSINT collection methodologies", *OSINT Foundation*, 20 November 2023, p. 2; https://www.osintfoundation.com/NewsBot.asp?MODE=VIEW&ID=31734
[76] Hoffman and Fuller, "Rebranding second-generation open-source intelligence: 'It's not your father's OSINT' ".
[77] Richmond H. Thomason (ed.), *Philosophical Logic and Artificial Intelligence*, Klüver Academic Publishers; ODNI, "Intelligence Community Directive (ICD) 203- Analytic Standards", *Office of the Director of National Intelligence*, 2007, p. 1, https://www.dni.gov/files/documents/ICD/ICD 203 Analytic Standards pdf-unclassified.pdf.
[78] Randolph H. Pherson, Richards J. Heuer, *Structured analytic techniques for intelligence analysis*, CQ Press, 2019, p. 21.
[79] Bjorn Gunnar M. Isaksen, Ken R. McNaught, "Uncertainty handling in estimative intelligence–challenges and requirements from both analyst and consumer perspectives", *Journal of Risk Research*, vol. 22, no. 5, 2019, pp. 643-657.
[80] *Ibidem*.
[81] Jeffrey A. Friedman, Richard J, Zeckhauser, "Assessing Uncertainty in Intelligence", *Intelligence and National Security*, vol. 27, no. 6, 2012, p. 824-847; DOI: 10.1080/02684527.2012.708275.
[82] Donald A. Petkus, *Op.cit*., p. 104.
[83] David V. Gioe, Tony Manganello, *Op.cit*., p. 6.
[84] *Ibidem*, p. 3.
[85] William Usher, *Op.cit*., p. 4.
[86] *Ibidem*, p. 5.
[87] Kiran Krishnamurthy, "Does AI signify the end of HUMINT as we know it?", Karve International, Advanced Pattern Recognition, 25 June 2024; https://www.karveinternational.com/insights/does-ai-signify-the-end-of-humint-as-we-know-it.
[88] David V. Gioe, Tony Manganello, *Op.cit*., p. 11.
[89] Donald A. Petkus, *Op.cit*., p. 104.
[90] David V. Gioe, Tony Manganello, *Op.cit*., p. 4.
[91] *Ibidem.*
[92] William Usher, p. 4.
[93] Donald A. Petkus, *Op.cit*.
[94] David V. Gioe, Tony Manganello, *Op.cit*.
[95] William Usher, p. 5.
[96] Terence J. Thompson, "Toward an updated understanding of espionage motivation", *International Journal of Intelligence and CounterIntelligence*, vol. 27, no. 1, 2014, pp. 58-72.
[97] David V. Gioe, "The more things change: HUMINT in the Cyber Age", *The Palgrave Handbook of Security, Risk and Intelligence* (Robert Dover, Huw Dylan, Michael S. Goodman eds.), Palgrave Macmillan, 2017, p. 213.
[98] Donald A. Petkus, *Op.cit*., p. 104.
[99] Joseph W. Wippl, "The art of agent handling", *International Journal of Intelligence and CounterIntelligence,* vol. 32, no. 4, 2019, p. 781.
[100] Laetitia Tyl-Descombes, *Op.cit*., p. 8.
[101] David V. Gioe, Tony Manganello, *Op.cit*., p. 2.
[102] Joseph W. Wippl, *Op.cit*., p. 782.
[103] *Ibidem*, p. 786.
[104] *Ibidem*, p. 789.
[105] *Ibidem*, p. 782.
[106] Joseph W. Wippl, "The qualities that make a great case officer", *International Journal of Intelligence and Counterintelligence*, vol. 25, no. 3, 2012, pp. 595-603.
[107] *Ibidem.*
[108] Joseph W. Wippl, "The art of agent handling".
[109] Kevin P. Riehle, "Assessing foreign intelligence threats", *American Intelligence Journal*, vol. 31, no. 1, 2013, pp. 96-101.
[110] *Ibidem.*
[111] Joseph W. Wippl, *Op.cit.*, p. 784.
[112] Kiran Krishnamurthy, *Op.cit*., "Improved Source Validation" section.
[113] William Usher, *Op.cit*., p. 5.
[114] Joseph W. Wippl, *Op.cit.*, p. 787.
[115] *Ibidem*, p. 788.
[116] *Ibidem*, p. 786.
[117] *Ibidem.*
[118] Ishmael Jones, *The Human Factor: Inside the CIAs Dysfunctional Intelligence Culture*, New York, Encounter, 2008, p. 13.

[119] Donald A. Petkus, *Op.cit*., p. 113.
[120] David V. Gioe, Tony Manganello, *Op.cit*., p. 6.
[121] Anastasios N. Kanellopoulos, "Counterintelligence, Artificial Intelligence and National Security: Synergy and Challenges", *Journal of Politics and Ethics in New Technologies and AI*, vol. 3, no. 1, Hellenic Association of Political Scientists, 2024, p. 1-19.
[122] *Ibidem*, p. 9.
[123] *Ibidem.*
[124] *Ibidem.*, p. 10.
[125] *Ibidem*.
[126] Christopher Dictus, Brandon de Bruhl, Logan O`Shaugnessy, *Op.cit*., p. 33
[127] David V. Gioe, Tony Manganello, *Op.cit*., p. 9.
[128] Yves-Alexandre de Montjoye, Laura Radaelli, Vivek Kumar Singh, Alex "Sandy" Pentland, "Unique in the shopping mall: On the reidentifiability of credit card metadata", *Sciencemag* 347, (6221), 30 January 2025, p. 536-539; DOI: 10.1126/science.1256297.
[129] William Usher, *Op.cit.*, p. 4.
[130] Samuel Benson, "Deciphering Ubiquitous Technical Surveillance (UTS) with data-driven analytics and artificial intelligence (D2A2)", *MITRE Corporation*, 2024, p. 1-8.
[131] *Ibidem.*
[132] *Ibidem*, p. 6.
[133] A. O. Morozov, V. O. Yashchenko, "Situational centers and decision-making systems. Innovative technologies of national security", *Математичні машини і системи*, 3-4, 25 June 2024, p. 3-37.
[134] Kiran Krishnamurthy, *Op.cit.,* Real-time Language section, https://www.karveinternational.com/insights/does-ai-signify-the-end-of-humint-as-we-know-it.
[135] Christopher Dictus, Brandon de Bruhl, Logan O`Shaugnessy, *Op.cit*., p. 33.
[136] *Ibidem.*
[137] David Perry, "Ethics in the recruiting and handling of espionage agents", in *National Security Intelligence and Ethics*, Routledge, 2021, p. 77.
[138] *Ibidem*, p. 79.
[139] David V. Gioe, Tony Manganello, *Op.cit*., p. 8.
[140] *Ibidem.*
[141] Donald A. Petkus, *Op.cit*., p. 103.
[142] Daniela Richterova, Elena Grossfeld, Magda Long, Patrick Bury, "Russian sabotage in the gig-economy era", *The RUSI Journal*, vol. 169, no. 5, 2024, pp. 10-21.
[143] Laetitia Tyl-Descombes, *Op.cit*., p. 1.
[144] *Ibidem.*
[145] David V. Gioe, Tony Manganello, *Op.cit*., p. 7.
[146] *Ibidem.*
[147] *Ibidem*, p. 8.
[148] *Ibidem*, p. 5.
[149] *Ibidem*.
[150] William Usher, *Op.cit.*, p. 6.
[151] Pat Host, "CIA leveraging digital transformation tools in HUMINT missions", *ExecutiveGov.com*, April 3, 2025; https://www.executivegov.com/articles/cia-digital-transformation-tools-humint-juliane-gallina.
[152] *Ibidem.*
[153] Gabriel Margolis, *Op.cit.*
[154] Ishmael Jones, *Op.cit*.
[155] Joseph W. Wippl, "The art of agent handling", p. 781.
[156] David V. Gioe, Tony Manganello, *Op.cit*., p. 11.
[157] *Ibidem.*
[158] *Ibidem*, p. 7.
[159] John Villasenor, "Artificial intelligence, deepfakes, and the uncertain future of truth", *Brookings Institution*, 14 February 2019; https://www.brookings.edu/articles/artificial-intelligence-deepfakes-and-the-uncertain-future-of-truth/#:~:text=Deepfakes%20are%20videos%20that%20have%20been%20constructed,of%20challenging%20policy%2C%20technology%2C%20and%20legal%20issues.
[160] Pat Host, *Op.cit*., paragraph 2.
[161] Jussi Okkonen, Mika Hyytiäinen, Mia Laine, Svante Laine, Tuuli Keskinen, Markku Turunen, "Information Ergonomics and Cognitive Dissonance by AI in HUMINT/OSINT Processes", *Artificial Intelligence and Social Computing*, vol. 163, 2025, p. 185.
[162] Kiran Krishnamurthy, *Op.cit.*, Adversarial AI & Countermeasures section.

[163] *Ibidem*, Explainability & Accountability section.
[164] William Usher, *Op.cit.*,, p. 5.
[165] *Ibidem.*
[166] Kennedy, 2024, Investing in Data Stewards section.
[167] Robin Emsley, "ChatGPT: these are not hallucinations–they're fabrications and falsifications", *Schizophrenia*, vol. 9, no. 1, 19.08.2023, p. 1.
[168] *Ibidem.*
[169] *Ibidem.*
[170] David V. Gioe, Tony Manganello, *Op.cit*., p. 5.
[171] Kiran Krishnamurthy, *Op.cit.*, Adversarial AI & Countermeasures section.
[172] Peter S. Park, Simon Goldstein, Aidan O'Gara, Michael Chen, Dan Hendrycks, "AI deception: A survey of examples, risks, and potential solutions", *Patterns,* vol. 5, no. 5, 2024, p. 1; cell.com/patterns/pdf/S2666-3899(24)00103-X.pdf.
[173] Jago Morrison, "The Art of Double-Cross: writers in strategic deception during World War Two", *Intelligence and National Security*, vol. 39, no. 2, 2024, pp. 232-249.
[174] Major Ernest S. Tavares Jr., *Operation Fortitude: The closed loop D-Day deception plan*, Lucknow Books, 2015.
[175] Donald C. Daniel, Katherine L. Herbig, "Propositions on military deception", *The Journal of Strategic Studies*, vol 5, no. 1, 1982, p. 11.
[176] Gabriel Margolis, *Op.cit.*, p. 52.
[177] Samuel Zulu, "Decoding Humanoid Criminal Behavior: Covert Investigative Methods and Security Preparedness", *RSIS International Journals*, 2025, p. 1; https://doi.org/10.3390/FORENSICSCI3030032.
[178] Peter S. Park, Simon Goldstein, Aidan O'Gara, Michael Chen, Dan Hendrycks, *Op.cit.*, p. 8.
[179] Neil Postman, *Technopoly: The Surrender of Culture to Technology*, Vintage, 1993, p. 93.
[180] *Ibidem.*
[181] David V. Gioe, Tony Manganello, *Op.cit*., p. 5.
[182] Hari Mahesh, "Gartner hype-cycle for AI 2025: What the future holds in 2026?", *Testrigor*, 20 October 2025; https://testrigor.com/blog/gartner-hype-cycle-for-ai-2025#:~:text=Looking%20to%202025%20and%20beyond,building%20infrastructure%20with%20staying%20power.
[183] *Ibidem.*
[184] David V. Gioe, "The more things change: HUMINT in the Cyber Age", p. 213.

DEZINFORMAREA ȘI INFORMAREA ERONATĂ - IMPLICAȚII OPERAȚIONALE ASUPRA ANALIZEI DE INTELLIGENCE

Alexandra-Ioana CIULE[*]

Abstract

The contemporary security environment is increasingly shaped by information confrontation, where disinformation and misinformation function as operational instruments of influence alongside conventional and hybrid conflict tools. This paper examines the conceptual and operational differences between deliberate disinformation and unintentional misinformation, and analyzes their impact on intelligence analysis in the context of information warfare. The study argues that the distortion of the information environment generates structural and cognitive vulnerabilities within intelligence processes, affecting source validation, multi-source corroboration, and risk estimation. Particular attention is given to the dynamics of digital platforms, echo chambers, and information laundering mechanisms, which facilitate the rapid amplification of distorted narratives.

The paper highlights that analytical errors may arise not only from fabricated content, but also from decontextualized or incorrectly interpreted factual data. The inability to properly distinguish between types of false or manipulated information can lead to flawed assessments, delayed warnings, or misclassification of threats. By integrating conceptual frameworks on information disorder and cognitive bias in intelligence analysis, the article emphasizes the operational necessity of structured analytic methods and rigorous differentiation between information categories. The findings support the need for enhanced analytical safeguards in order to preserve accuracy and decision relevance in intelligence products under conditions of information distortion.

***Keywords**: disinformation; misinformation; information distortion; intelligence analysis; information warfare; hybrid threats; information disorder.*

INTRODUCERE

Contextul geopolitic actual rămâne ancorat într-un punct de o permanentă instabilitate, preponderent afectat de confruntările militare (războiul ruso-ucrainean și cel din Orientul Mijlociu/ Iran), crizele economice și confruntările informaționale - cele din urmă survin paradigmei secolului XXI și definesc o nouă provocare adresată comunității de informații. Suplimentar față de viziunea convențională asupra conflictului militar, se regăsește o dimensiune nouă a acestuia, actuală și tot mai frecvent utilizată, cea informațională, menită să influențeze percepțiile populației prin redefinirea termenului

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

de „supremație militară”. Astfel, asistăm atât la depășirea unui front convențional, cât și la utilizarea deliberată a informației ca armă de influență.

În acest context, se conturează tot mai clar o dimensiune informațională a confruntării, în care informația nu mai reprezintă doar suport decizional, ci devine instrument operațional de influență și modelare a percepțiilor. Prin urmare, conceptul de supremație nu mai este definit exclusiv prin capabilități militare, ci și prin capacitatea de a controla, distorsiona și exploata spațiul informațional. În noua eră a digitalizării, informația, o resursă cu un caracter dual, purtătoare de cunoaștere, dar și potențial factor de distorsiune, a devenit o armă de influențare și o parte integrantă a fenomenului de „poluare informațională”[1]. În esență, această „poluare” reflectă vulnerabilitatea oricărei comunități de informații: o supraîncărcare a spațiului comunicațional cu un volum uriaș de mesaje neverificate, distorsionate sau intenționat fabricate, imposibil de controlat.

Prin prisma acestor evoluții, se observă o adaptare continuă a tehnicilor utilizate de actorii statali și non-statali, care exploatează vulnerabilitățile generate de dificultatea filtrării volumului masiv de date din mediul informațional, prin operațiuni de influență și prin diseminarea coordonată a narațiunilor distorsionate. Prin urmare, campaniile de dezinformare, atacurile cognitive și tehnicile de manipulare a spațiului public sunt utilizate pentru modelarea percepțiilor colective, erodarea încrederii și fragmentarea coeziunii sociale și instituționale.[2] Efectul cumulat al acestor practici conduce la amplificarea ambiguității și complexității conținutului informațional, ceea ce îngreunează identificarea unei realități obiective și verificabile. În consecință, structurile de informații se confruntă cu o presiune crescută asupra procesului analitic, în special în ceea ce privește validarea datelor, evaluarea surselor și elaborarea estimărilor fundamentate.

Prin prisma acestor evoluții, dezinformarea este definită ca informație falsă sau inexactă utilizată deliberat de un actor ostil pentru a induce în eroare o parte semnificativă a publicului. Totuși, dezinformarea nu se limitează la transmiterea unor date false, ci presupune un proces structurat de manipulare informațională, care poate include atât conținut fabricat, cât și informație reală scoasă din context și amplificată în mod coordonat.

O nouă provocare apărută pentru structurile de informații este diferențierea dintre conținuturile fabricate deliberat pentru inducerea în eroare (*dezinformarea*) și informațiile în mod sincer greșite (*informarea eronată*). Cele două fenomene, deși par a avea un efect similar, diferă fundamental prin intenționalitate și scop. Din această perspectivă, pornind de la premisa că este necesară delimitarea corectă dintre cele două categorii, scopul prezentului articol este de a analiza diferențele conceptuale și operaționale dintre *informarea eronată* și *dezinformare*, precum și de a evidenția impactul acestora asupra procesului de intelligence în războiul informațional.

EVOLUȚIA CONCEPTELOR PRIVIND DISTORSIUNEA INFORMAȚIONALĂ

Deși dezinformarea se conturează ca fiind una dintre principalele forme de acțiune în spațiul informațional, este necesară evidențierea mai multor practici și tehnici utilizate de actorii statali și non-statali în vederea producerii și exploatării distorsiunii informaționale. Un cadru conceptual utilizat frecvent în analiza distorsiunii informaționale propune delimitarea mai multor forme distincte de conținut problematic, în funcție de gradul de intenționalitate și modul de utilizare al acesteia.

Literatura de specialitate ia în considerare trei categorii, care se diferențiază astfel[3]:

- ***disinformation*** (adesea tradus drept „*dezinformare*”) - diseminarea unor informații vădit false cu scopul conștient și deliberat de a aduce prejudicii;
- ***misinformation*** (adesea tradus drept „*informare eronată*”) - informația falsă este diseminată fără intenția de a genera efecte negative, de regulă ca urmare a unor erori;

- ***malinformation*** (adesea tradus drept „*informație autentică utilizată în scop manipulativ*") - informația autentică/ veridică, scoasă din context și, mai apoi, utilizată excesiv în vederea distorsionării realității.

Deși terminologia anglo-saxonă operează cu distincții clare între "disinformation", "misinformation" și "malinformation", în limba română aceste nuanțe sunt adesea subsumate generic noțiunii de ***dezinformare***. Totuși, în vederea elaborării unor produse informative legitime, diferențierea dintre *falsul deliberat*, *eroarea neintenționată* și *utilizarea în scop manipulativ a informației reale* este absolut necesară întrucât fiecare categorie implică mecanisme diferite de producere și indicatori distincți de detectare.

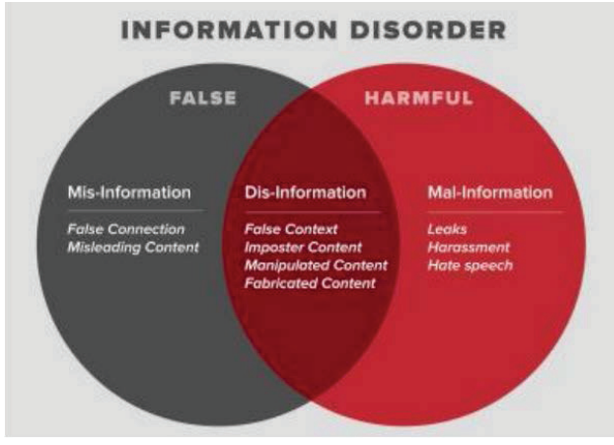

Fig. nr. 1: *Information Disorder*
(sursa: Claire Wardle, Hossein Derakhshan, *Information Disorder: Toward an interdisciplinary framework for research and policy making*, p. 5)

Diferențierea dintre termenii sus-menționați nu este una strict terminologică și are implicații directe asupra modului de evaluare de către analistul de informații, context în care este utilizat un set de criterii.

Primul criteriu de diferențiere îl constituie intenționalitatea producerii și diseminării conținutului. În cazul dezinformării, informația falsă este generată și distribuită în mod deliberat, în cadrul unor acțiuni orientate spre influență și manipulare, ceea ce presupune existența unui actor, a unei motivații și a unui obiectiv stabilit. Informarea eronată nu are o intenție manipulatoare, fiind asociată cu o eroare, interpretare defectuoasă sau verificare insuficientă a datelor înainte de propagarea acestora. În situația utilizării în scop manipulator a unei informații autentice, intenția de a produce efecte negative este prezentă, însă distorsiunea nu este un rezultat al falsificării informației, ci al reinterpretării, decupajului contextual sau prezentării selective.

Un al doilea criteriu relevant vizează natura sursei și nivelul de coordonare al diseminării. Dezinformarea este, în mod frecvent, corelată cu actori organizați, actori statali sau non-statali, și cu mecanisme coordonate de amplificare a mesajului. Informarea eronată se manifestă, de regulă, în mod necoordonat, prin intermediul unor persoane care consideră informația ca fiind veridică. În cazul informației autentice utilizate în scop manipulator, sursa poate fi atât instituțională, cât și individuală, însă intervenția asupra conținutului presupune o recontextualizare voit tendențioasă.

Un alt criteriu este reprezentat de analizarea mecanismelor de propagare. Dezinformarea recurge frecvent la tehnici de amplificare dirijată, precum utilizarea unor rețele de distribuire, menite să maximizeze impactul și vizibilitatea mesajului. Informarea eronată se difuzează în absența unei arhitecturi deliberate de distribuire, prin convingerea populației că informația este veridică și necesită distribuirea acesteia. În cazul informației autentice utilizate în scop manipulator, propagarea este facilitată de sensibilitatea contextuală a datelor și de încărcătura emoțională a conținutului expus.

O categorie conceptuală intermediară este reprezentată de *malinformation*, care descrie situațiile în care conținutul informației este corect și veridic, însă concluzia sau mesajul rezultat devin false în mod neintenționat, ca efect al lipsei de context, al interpretării deficitare sau al competenței limitate a persoanei căreia i se furnizează datele. Spre deosebire de dezinformare, nu există o intenție explicită de manipulare, iar distorsiunea nu afectează veridicitatea datelor în sine, ci cadrul de interpretare și construcția concluziei.[4] Din perspectivă analitică, se

evidențiază riscul formulării unor evaluări eronate chiar și în prezența unor date autentice, în condițiile unei contextualizări insuficiente sau ale unei expertize limitate.

Absența unei diferențieri clare între dezinformare, informație eronată și utilizarea manipulatoare a informației autentice poate conduce la interpretări greșite sau parțial eronate ale datelor disponibile/ evaluări distorsionate în baza unei contextualizări eronate. Astfel, analistul de informații poate supraevalua o narațiune manipulatoare, o poate subestima sau o poate încadra greșit, afectând direct consistența produsului analitic. În mod similar, neidentificarea caracterului manipulator al unor semnale informaționale poate determina lipsa transmiterii unei avertizări referitoare la potențiale acțiuni distructive, atunci când riscul existent este interpretat eronat. În ambele situații, deficiența nu se rezumă la volumul mare al informației, ci la incapacitatea de diferențiere a acesteia.

În vederea furnizării unor soluții necesar a fi aplicate pentru diferențierea tehnicilor utilizate în procesul de distorsiune informațională, se impune analizarea informației din perspectiva a trei nivele: originea (*cine este răspunzător de producerea mesajului?*), transformarea (*cum anume a fost alterată/ modificată informația?*) şi traseul său în mediul informațional (*care a fost traseul de distribuire al informației?*). Adițional, în majoritatea cazurilor, informația este fragmentată și redistribuită de către diferite entități (amplificatori ori intermediari), sens în care se impune stabilirea gradului de influență al informației asupra sectorului de populație vizat. Pentru conferirea unui grad ridicat de reușită al distorsiunii informaționale se utilizează și o serie de algoritmi care favorizează dezvoltarea și transmiterea unor mesaje polarizante, ceea ce creează potențiale erori în diferențierea informației veridice de cea neveridică.[5]

Astfel, pentru elaborarea unui produs analitic veridic este necesară evaluarea simultană a sursei informației, a traseului de distribuție, a modelului de amplificare, a cadrului narativ și a efectului potențial asupra audienței. Utilizarea unei abordări multiple poate permite diferențierea dintre o eroare izolată, un conținut manipulator și o narațiune coordonată de actori statali și non-statali.

În scopul influențării proceselor cognitive ale publicului țintă, actorii statali și non-statali utilizează platforme sociale și aplicațiile de mesagerie cu moderare redusă, care facilitează inițierea și scalarea narațiunilor distorsionate. Un mecanism frecvent utilizat este ***information laundering***, prin care conținutul fals este publicat inițial pe site-uri obscure sau proxy, apoi preluat de canale online și redistribuit pe diverse platforme (ex.: Telegram, Facebook), dobândind, prin repetiție, o aparentă legitimitate. Algoritmii de recomandare favorizează formarea *camerelor de ecou informaționale*, reducând expunerea la perspective alternative și crescând vulnerabilitatea la manipulare. Persoanele vizate sunt blocate mental într-o buclă repetitivă, aspect ce favorizează accentuarea retoricilor dorite de către entitățile ostile.

La nivelul structurilor de informații, vulnerabilitățile generate de distorsionarea informațională afectează atât procesul de colectare al datelor şi informațiilor, cât și cel de analiză, având la bază dificultatea diferențierii rapide între un conținut veridic, un conținut eronat și unul manipulator, într-un mediu informațional suprasaturat, aspect care crește riscul integrării în analiza curentă a unor date insuficient validate. Totodată, apariția confirmării artificiale afectează în mod direct procesele de validare multi-sursă utilizate în intelligence, conducând la evaluări bazate pe convergență aparentă, nu pe verificare reală.

Distorsiunea informațională amplifică vulnerabilitățile cognitive ale analistului, ceea ce poate provoca apariția bias-ului de confirmare (informația eronată este preluată de mai multe canale și surse derivate, generând iluzia confirmării acesteia), ancorarea interpretativă și dependența de narațiuni dominante. Astfel, faptul că datele corecte pot fi integrate în modele interpretative greșite, iar datele eronate pot părea plauzibile atunci când se aliniază cu ipoteze preexistente, generează apariția erorii analitice.

Totuși, riscul apariției unei erori a analistului nu rezidă doar în preluarea unor informații incorecte, ci în distorsionarea procesului de construcție a ipotezelor analitice. În condițiile unui flux informațional contaminat constant, ipotezele tind să fie stabilizate prematur, pe baza unor semnale insuficient verificate, iar testarea alternativelor devine limitată. În acest context, poate apărea ***efectul adevărului iluzoriu***, potrivit căruia repetarea unei afirmații crește probabilitatea ca aceasta să fie percepută ca adevărată, independent de acuratețea sa. Familiaritatea informațională reduce efortul de procesare, iar această ușurință cognitivă este interpretată eronat drept indicator de veridicitate.

În mediul informațional digital, unde aceleași afirmații sunt replicate pe multiple canale și platforme, efectul este amplificat. Deși frecvența apariției unei narațiuni nu poate și nu trebuie să fie tratată ca un indicator de validare, în absența unei confirmări repetarea poate produce apariția unei acceptări cognitive.

CONCLUZII

În contextul geopolitic actual, distorsiunea informațională marchează efecte directe atât asupra analistului de informații, prin activarea bias-urilor cognitive (bias-ul de confirmare, ancorarea interpretativă și dependența de narațiuni dominante), cât și asupra produsului informativ, context în care se evidențiază necesitatea dezvoltării unor tehnici menite să favorizeze identificarea oportună și timpurie a informației ce are calitate distructivă.

În mediul analizei de informații, caracterizat printr-un volum vast de informații, limitare temporală și stres, evaluarea informației este influențată de factori cognitivi și contextuali. Aceste elemente susțin dezvoltarea unor serii de vulnerabilități ale căror consecințe se pot răsfrânge direct asupra procesului decizional.

BIBLIOGRAFIE

1. BRAGAZZI Nicola Luigi, GARBARINO Sergio, ”Understanding and Combating Misinformation: An Evolutionary Perspective”, *JMIR Infodemiology*, vol. 4, e65521, 2024, 11 p.; https://infodemiology.jmir.or/2024/1/e65521.
2. HERASIMENKA Aliaksandr et al., ”Misinformation and professional news on largely unmoderated platforms: the case of Telegram”, *Journal of Information Technology & Politics*, vol. 20. nr. 2, Routledge, 2023, pp. 128-212; https://www.tandfonline.com/doi/full/10.1080/19331681.2022.2076272#abstract.
3. LEITE A. João et al., ”EU vs Disinfo: A Dataset for Multilingual Detection of Pro-Kremlin Disinformation in News Articles”, June 2024; researchgate.net/publication/381518555_EUvsDisinfo_a_Dataset_for_Multilingual_Detection__of_Pro_Kremlin_Disinformation_in _News_Article.
4. MOINESCU Radu, Războiul Informațional, 2009; https://www.scribd.com/doc/135141301/Razboiul-Informational.
5. MUBASHIR Sultan et al., ”Susceptibility to online misinformation: A systematic meta-analysis of demographic and psychological factors”, *Proceedings of the National Academy of Sciences,* vol. 121, nr. 47, 2024, 12 p.; https://www.pnas.org/doi/10.1703/pnas.2409329121.
6. OLECH Aleksander, ”Hybrid threats to critical infrastructure in the European Union. Selected Hybrid CoE analyses”, *Terrorism – studies, analyses, prevention* (Special Issue: Terrorist and sabotage threats to critical infrastructure), The Internal Security Agency, Warsaw, 2025, pp. 133-158; https://www.researchgate.net/publication/391620205_Hybrid_threats_to_critical_infrastructure_in_the_European_Union_Selected_Hybrid_CoE_analyses.
7. PADALKO Halyna et al., ”Classification of disinformation in hybrid warfare: An application of XLNet during the Russia’s war against Ukraine”, *Radioelectronic and Computer Systems*, nr. 4 (112), 2024, pp. 46-58; https://www.researchgate.net/publication/387782008_Clasification_of_disinformation_in_hybrid_warfare_an_application_of_XLNet_during_the_Russias’s_war_against_Ukraine.
8. SAEED Omid Sedeeq, ”Hybrid Warfare and Strategic Communication. Theory and Case Study”, *Hadtudomanyi Szemle,* vol. 18, 2025, pp. 65-79; https://folyoirat.ludovika.hu/index.php/hsz/article/view/8051/6508.
9. SINGH Tarnveer, *Digital Psychological Warfare. Weaponisation of Digital Platforms*, Palgrave Macmillan, 2025, 322 p.
10. WARDLE Claire, Hossein Derakhshan, *Information Disorder: Toward an interdisciplinary framework for research and policy making*, Council of Europe Report Report DGI(2017)09, Council of Europe, Septembrie 2017, 107 p.
11. *** *Cognitive Warfare*, NATO Chief Scientist Research Report, NATO Science & Technology Organization, 2021, 22 p.
12. *** NATO, NATO’s approach to counter information threats, 2025; https://www.nato.int/en/what-we-do/wider-activities/natos-approach-to-counter-information-threats.

[1] Claire Wardle, Hossein Derakhshan, *Information Disorder: Toward an interdisciplinary framework for research and policy making*, Council of Europe Report DGI(2017)09, Council of Europe, Septembrie 2017.
[2] EUvsDisinfo, 2023; CEPA, 2022.
[3] Claire Wardle, Hossein Derakhshan, *Op.cit*., p. 5.
[4] Nicola Luigi Bragazzi, Sergio Garbarino, ”Understanding and Combating Misinformation: An Evolutionary Perspective”, *JMIR Infodemiology*, vol. 4, e65521, 2024, 11 p.; https://infodemiology.jmir.or/2024/1/e65521., p. 3
[5] Claire Wardle, Hossein Derakhshan, *Op.cit*., p. 22-26.

INFLUENȚA AMENINȚĂRILOR HIBRIDE ASUPRA ÎNVĂȚĂMÂNTULUI SUPERIOR, PROGRAMELOR DE FORMARE ȘI CERCETĂRII ȘTIINȚIFICE DIN ROMÂNIA

Mihai-Laurențiu ZARIA*

Motto: *„Cunoașterea va guverna întotdeauna ignoranța, iar un popor care intenționează să se autoguverneze trebuie să se înarmeze cu puterea pe care o oferă cunoașterea.”*
James Madison

Abstract

In the contemporary security environment, higher education and scientific research can no longer be approached only as civilian domains of society progress, but must be understood as strategic assets within national security architectures. This article explores how hybrid threats influence universities, professional training programs and research institutions in Romania, emphasizing the indirect yet cumulative effects produced through information, cognitive and cyber vectors. The analysis highlights that hybrid competition operates predominantly below the threshold of open confrontation, targeting institutional credibility, epistemic authority and the integrity of educational and research processes. Particular attention is given to the differentiated exposure of civilian and military educational environments, where the vulnerability of human capital becomes a strategic liability with potential operational repercussions. The study further argues that hybrid pressure rarely manifests through isolated actions, but through synchronized mechanisms designed to foster distrust, polarization and functional degradation over time. In response, the paper outlines the necessity of institutional resilience as an integrated capability, encompassing security culture, cognitive resilience, crisis governance, digital resilience and human resource stability. Ultimately, the findings suggest that safeguarding education and research is not merely an administrative requirement, but a long-term strategic imperative for sustaining national security and institutional performance under hybrid competition.

Keywords: *hybrid threats; higher education security; cognitive warfare; disinformation; cyber resilience; epistemic authority; national security.*

* ***Doctorand la Universitatea Națională de Știință și Tehnologie Politehnica din București (UNSTPB).***

INTRODUCERE ȘI CONCEPTUALIZARE

În arhitectura contemporană a securității naționale, spațiul educațional și cel al cercetării științifice nu mai pot fi tratate ca domenii neutre sau conexe, ci ar trebui considerate veritabile zone de interes strategic, aflate *de facto* în raza de acțiune a competiției geopolitice și a conflictelor de tip hibrid. Într-un mediu internațional caracterizat de imprevizibilitate și volatilitate, actorii ostili își diversifică *modus operandi*, preferând instrumente de influență și constrângere în detrimentul confruntării militare deschise, într-o „*zonă gri*" care complică deliberat atribuirea responsabilității și generează reacții trenante[1].

În acest context, universitățile, centrele de formare și institutele de cercetare din mediul civil și militar devin ținte atractive nu doar prin vizibilitatea publică, ci și pentru natura resurselor pe care le concentrează, cum ar fi capitalul uman, expertiza, infrastructura informațională sau potențialul de inovare. Din perspectiva evoluției conflictului contemporan, delimitarea dintre domeniul civil și cel militar este tot mai permeabilă, iar proiecția influenței prin metode politice, informaționale și psihologice poate produce efecte strategice, fără declanșarea unui război convențional[2].

Amenințările hibride se manifestă printr-o combinare sincronizată a mijloacelor informaționale, cibernetice, economice și psihologice, cu scopul de a exploata vulnerabilități sistemice, de a induce fracturi de coeziune și de a eroda încrederea publică în instituții. Din această perspectivă, mediul educațional superior și cel al cercetării reprezintă atât un vector de reziliență a societății, cât și o posibilă breșă strategică, în sensul în care, dacă sunt contaminate de narative manipulative ori atacate cibernetic, pot suferi distorsiuni în calitatea formării, integritatea datelor și credibilitatea expertizei, inclusiv în domenii sensibile pentru securitatea națională[3].

În mod particular, operațiunile de influență pot acționa și ca instrumente de presiune strategică asupra spațiului academic, vizând atât factorii decidenți, cât și comunitatea academică, printr-un ansamblu de instrumente care include media, social media, acțiunile cibernetice, operațiunile de tip HUMINT desfășurate *sub rosa* (termen în latină/cu sens de *secret*, *confidențial*) și structurile de tip proxy, menite să fragmenteze coeziunea și să slăbească capacitatea de reacție[4].

În cadrul prezentei lucrări, mediul universitar din România este abordat ca un ecosistem integrat, care include instituții civile și militare, iar programele de formare sunt delimitate clar pentru instruire profesională, în sensul cursurilor de carieră, specializare, perfecționare și formare continuă, desfășurate atât în universități și instituții acreditate, cât și în academii ori centre militare de specialitate. În acest sens, protejarea educației și cercetării trebuie înțeleasă ca o condiție de reziliență instituțională și de continuitate strategică, nu ca un simplu obiectiv administrativ.

EDUCAȚIA ȘI CERCETAREA ÎN COMPETIȚIA HIBRIDĂ

În competiția strategică actuală, disputa pentru obținerea unui avantaj depășește registrul confruntării militare, proiectându-se asupra spațiului cognitiv. Din această perspectivă, educația și cercetarea capătă o funcție de interes operațional, deoarece formează competențe, consolidează autoritatea epistemică și configurează standarde profesionale, cu efect pe termen lung asupra capacității statului de a funcționa coerent, inclusiv în sectoare sensibile. În această ecuație, universitățile, academiile militare și institutele de cercetare trebuie tratate ca elemente esențiale ale ecosistemului de securitate, întrucât intermediază transferul dintre expertiză, decizie și execuție instituțională.

O trăsătură definitorie a competiției hibride este utilizarea unor instrumente care produc efecte cumulative sub pragul reacției clasice, beneficiind de ambiguitate, de dificultăți de atribuire și,

implicit, de o formă de impunitate funcțională. În acest cadru, narațiunile și operațiunile informaționale nu se reduc la propagandă în sens tradițional, ci acționează ca mecanisme de modelare a percepției și de rearanjare a cadrului în care publicul interpretează realitatea. O grilă utilă se distinge între narațiuni formale, de temă și de legitimitate, fiecare având roluri distincte în construcția autorității și în menținerea sau erodarea încrederii. În plus, impactul tinde să fie mai robust atunci când narațiunile întăresc predispoziții preexistente, fiindcă audiențele sunt, de regulă, refractare la mesaje care contrazic convingeri deja fixate, rezultând că miza practică devine ancorarea și amplificarea, nu convertirea rapidă[5].

În plan metodologic, narațiunile pot funcționa atât ca instrument de gestionare a crizelor, cât și ca vector de subversiune. Modul în care influența se instituționalizează gradual se poate explica cu ajutorul unui model etapizat. Inițial, se definesc obiectivele și efectele urmărite, apoi se cartografiază vulnerabilitățile din mediul informațional al țintei, după care se proiectează mesaje cu rezonanță emoțională, se diseminează, se consolidează credibilitatea acestora prin voci prezentate ca independente și, în final, are loc sedimentarea narațiunilor în discursul public până la influențarea deciziilor. Relevanța pentru educație și cercetare este directă, în sensul în care mediul academic poate fi simultan atât public țintă, prin polarizare și delegitimare, cât și infrastructură de validare, prin recrutarea unor entități cu autoritate simbolică, capabile să normalizeze cadre interpretative favorabile actorului ostil[6].

Dincolo de linia cognitivă, războiul hibrid utilizează și instrumente de presiune asupra proceselor politice și instituționale, aplicând o logică de *divide et impera*, în care fracturile sociale devin multiplicatori de efect. Influența politică poate fi descrisă drept un efort de durată, orientat spre obiective strategice precum securizarea regimului, consolidarea predominanței în vecinătatea apropiată și obținerea unui statut de putere, cu finalitatea recurentă de slăbire a coeziunii statelor euro-atlantice, din care face parte și România. În plan tactic, se remarcă exploatarea simultană a tensiunilor dintre alianțe, dintre state și din interiorul statelor, prin campanii menite să reducă încrederea în autorități, să delegitimeze decizia democratică și să fragmenteze consensul public. Pentru România, implicația este că ecosistemul educațional și științific, conectat structural la producția de expertiză și la formarea personalului din instituțiile cheie, poate fi afectat prin perturbarea încrederii, contestarea neutralității academice și crearea de presiuni asupra agendei publice care condiționează politica educațională și de cercetare[7].

În analiza războiului hibrid, o clarificare conceptuală relevantă pentru domeniul educațional și de cercetare derivă din taxonomia care se distinge între un model centrat pe populație și unul centrat pe oponent. Obiectivul prioritar este controlul asupra populației și mediului specific, iar celelalte scopuri derivă din această captură a spațiului social. O altă prioritate este înfrângerea adversarului în termeni de tip convențional, chiar dacă persistă eforturi colaterale de influențare a populației și a decidentului. Aplicată competiției hibride, această distincție oferă o lentilă mai precisă, deoarece unele acțiuni sunt preponderent disruptive și urmăresc deformarea climatului social și decizional, iar altele sunt mai distructive și vizează degradarea capacităților inamicului[8].

Transpusă în domeniul educației și cercetării, logica centrată pe populație se observă în tentativele de a controla cadrul de interpretare a realității prin operațiuni psihologice, prin inducerea fricii și prin fabricarea unei aparențe de consens social în jurul unor poziții favorabile actorului ostil. Astfel de influențe pot eroda imaginea unei autorități politice sau instituționale în rândul unor comunități țintă prin narațiuni adaptate lingvistic și cultural, care polarizează și reconfigurează loialități, creând un teren

fertil pentru decizii publice vulnerabile la manipulare. În mediul universitar și în cercetare efectul specific este distorsionarea criteriilor de credibilitate și a mecanismelor de validare[9].

Complementar, logica centrată pe adversar devine relevantă în special acolo unde formarea și cercetarea se intersectează cu domenii de utilitate strategică, precum cel militar, iar ținta este degradarea capacităților, nu doar influențarea percepțiilor. În astfel de situații, presiunea poate viza direct infrastructuri, lanțuri de instruire și producția de cunoaștere cu aplicabilitate sensibilă, urmărind diminuarea performanței instituționale și reducerea capacității de reacție. În ecosistemul românesc, dimensiunea mixtă civil–militară amplifică miza. Instituțiile civile pot fi mai expuse presiunilor reputaționale și contestării epistemice, iar cele din zona apărării și securității pot fi vizate pentru informații sau proceduri, în vederea creării unor avantaje asimetrice.

Utilizarea metodei proxy rămâne un mecanism transversal, deoarece permite operarea prin interpuși cu negare plauzibilă și cu costuri reduse, cum ar fi rețele afiliate, structuri de fațadă, comunități digitale sau actori hibrizi, care conectează influența informațională cu presiunea cibernetică și cu instrumente economice. Pentru educație și cercetare, implicația nu este doar una de securitate tehnică, ci și de guvernanță a credibilității, în sensul în care atacul poate începe ca incident reputațional și se poate transforma în vulnerabilitate instituțională, ori poate începe ca operațiune clandestină de tip HUMINT și se poate transforma într-o amenințare la adresa securității naționale, tocmai pentru că în competiția hibridă limitele dintre „*fapt*”, „*narațiune*” și „*decizie*” sunt deliberat blurate[10].

VULNERABILITĂȚI ȘI RISCURI ÎN ECOSISTEMUL ACADEMIC

Ecosistemul educațional și de cercetare este expus competiției hibride nu doar prin natura sa deschisă, ci și prin faptul că funcționează simultan ca infrastructură cognitivă, platformă de legitimare a expertizei și spațiu de producție a cunoașterii. Riscurile apar acolo unde fluxurile de informație, procedurile instituționale și cultura profesională pot fi distorsionate gradual, până în punctul în care instituția își pierde coerența operațională, fără să existe un moment clar de ruptură. În termeni practici, vulnerabilitatea nu este un defect singular, ci o acumulare de disfuncții, precum scăderea rigurozității, normalizarea improvizației, tolerarea ambiguităților, apariția impunității sau slăbirea capacității de autocorecție.

În plan informațional, o vulnerabilitate majoră este slăbirea autorității epistemice a instituțiilor. Competiția hibridă nu operează prin falsuri evidente, ci prin relativizarea criteriilor de validare, ceea ce face ca între *cunoaștere* și *opinie* să existe o linie fină. În mediul universitar, acest proces reduce încrederea în evaluare și erodează rigoarea intelectuală, ajungând să fie percepută drept obstacol, nu ca și *sine qua non* a calității. În formarea profesională efectele apar mai rapid, generând calificări formale și o falsă impresie de competență, cu impact negativ asupra performanței instituționale și decizionale.

Dimensiunea digitală amplifică aceste riscuri prin extinderea masivă a suprafeței de atac și prin faptul că instituțiile educaționale gestionează volume mari de date, infrastructuri de evaluare și canale de comunicare, care pot fi perturbate sau compromise. În mediile asociate domeniilor critice, breșele nu sunt relevante doar prin efectul imediat, adică întreruperea proceselor, ci și prin valoarea informațională secundară, în sensul cartografierii sistemelor, înțelegerii procedurilor, identificării persoanelor cheie și exploatării rutinei administrative. În acest sens, securitatea educațională nu se reduce la protecție IT, ci implică și protecția proceselor, arhitecturilor instituționale și disciplinelor organizaționale care susțin funcționarea.

O zonă distinctă de risc, cu relevanță majoră pentru cercetare și formare atât în domeniul civil, cât și militar, este mutația indusă de extinderea infrastructurilor de observare digitală și a aplicațiilor de inteligență artificială, care

generează volume fără precedent de date și materiale informaționale. Acest mediu „saturat de date" creează atât oportunități, precum cele de analiză, instruire sau dezvoltare a capabilităților, cât și vulnerabilități pentru spațiul educațional și de cercetare, cum ar fi cele generate de acces neautorizat, scurgeri de date, dependență de infrastructuri externe sau deformare prin dezinformare[11].

Pentru zona de cercetare, riscurile se văd și mai clar în proximitatea cooperării civil-militare și a proiectelor care folosesc sau dezvoltă instrumente de colectare și analiză, precum algoritmi de triere, tehnici de recunoaștere, integrare multi-sursă, prelucrare de imagini și date, modele de predicție sau sisteme autonome. Orice progres metodologic poate fi valorificat în scopuri legitime, dar poate fi și deturnat sau exploatat, *mutatis mutandis*, în arhitecturi ostile. De aici rezultă o vulnerabilitate specifică mediului academic, adică tentația de a maximiza deschiderea și colaborarea, fără a avea permanent internalizată disciplina evaluării riscului, a protecției datelor și a delimitării între ceea ce poate fi publicat și ceea ce trebuie tratat cu precauție. În lipsa acestui echilibru, mediul academic poate furniza, involuntar, nu doar idei, ci și capabilități către alți actori.

Un alt risc transversal este fragmentarea competențelor dintre „*tehnic*" și „*non-tehnic*", mai ales în instituțiile unde ecosistemul educațional deservește atât activități civile, cât și din domeniul militar. În contextul actual, vulnerabilitățile nu apar doar din lipsa specialiștilor, ci și din lipsa unei culturi de securitate a tuturor actorilor relevanți, și anume cei care administrează platforme, gestionează date, realizează proceduri, comunică public sau cei care formează persoane.

MECANISME DE REZILIENȚĂ SUB PRESIUNE HIBRIDĂ

În contextul în care competiția hibridă operează preponderent sub pragul confruntării deschise, ***reziliența instituțională*** nu mai poate fi tratată ca un concept secundar, cu valență declarativă sau administrativă. Aceasta devine o necesitate strategică, întrucât actorul ostil urmărește degradarea funcționalității prin presiuni cumulative, dificil de atribuit și, de cele mai multe ori, insuficient sesizabile în timp real. În acest cadru, reziliența presupune capacitatea unei instituții de a anticipa amenințările și presiunile sistemice, de a absorbi impactul acestora, de a se adapta și de a continua funcționarea fără pierderea controlului asupra misiunilor fundamentale[12].

Un prim palier al rezilienței îl reprezintă consolidarea culturii instituționale de securitate, înțeleasă ca *habitus* organizațional și ca formă de disciplină internă, nu ca reacție punctuală la incidente. Vulnerabilitatea apare, de regulă, nu prin lipsa totală a normelor, ci prin aplicarea selectivă a acestora, ceea ce creează spații de ambiguitate exploatabile. Reziliența presupune internalizarea unor standarde care devin practici cotidiene, precum disciplina informațională, controlul procedural, trasabilitatea decizională, delimitarea responsabilităților, controlul strict al accesului și diminuarea conduitelor oneroase care, deși aparent marginale, pot declanșa efecte în lanț. În mediile cu specific militar, aceste elemente nu sunt opționale, ci reprezintă condiții esențiale de continuitate operațională și de menținere a încrederii instituționale.

Un al doilea palier îl constituie ***reziliența cognitivă,*** definită prin capacitatea comunității academice de a menține integritatea epistemică în fața presiunilor informaționale. Amenințările hibride produc efecte nu neapărat prin persuasiunea unei singure narațiuni, ci prin saturație, relativism, discreditare progresivă și inducerea unei stări de incertitudine permanentă, în care adevărul factual devine negociabil, iar validarea cunoașterii este contestată sistematic. În această logică, reziliența cognitivă presupune consolidarea unor mecanisme de discernământ și validare, care permit delimitarea dintre critică legitimă și delegitimare deliberată[13].

În mod complementar, reziliența instituțională implică și întărirea capacității de conducere în

situații de presiune, întrucât competiția hibridă urmărește frecvent perturbarea funcționării prin blocaje administrative, contestări cronice, presiuni reputaționale și slăbirea forței de reacție. În acest context, nu doar infrastructura este supusă stresului, ci și factorul decident, iar instituția riscă să devină captivă într-un regim de reacție impredictibil, costisitor și incoerent. În consecință, reziliența presupune existența unor mecanisme clare de continuitate instituțională, printre care se numără procedurile de răspuns în diferite situații de criză, liniile de comandă funcționale, protocoalele de comunicare internă și externă sau redundanța operațională.

Un palier important este reprezentat de ***reziliența digitală,*** definită ca un ansamblu de capabilități de protecție, detecție, răspuns și recuperare în raport cu incidentele cibernetice. În cazul universităților și al centrelor de formare, vulnerabilitatea este amplificată de heterogenitatea infrastructurilor, adică platforme de tip „*e-learning”*, baze de date, sisteme administrative, instrumente de comunicare și infrastructuri tehnice care nu sunt întotdeauna securizate unitar. Reziliența nu se reduce la soluții tehnice punctuale, ci include și managementul accesului, protecția datelor, segmentarea infrastructurilor, auditarea periodică, actualizarea sistemelor și dezvoltarea unei discipline de securitate care reduce erorile umane. Mai ales în ecosistemele sensibile, chiar și o breșă limitată de securitate poate produce efecte disproporționate, nu doar prin pierderea unor date, ci prin facilitarea cartografierii infrastructurii, identificarea vulnerabilităților recurente și compromiterea integrității evaluării și certificării profesionale[14].

Un palier emergent al rezilienței îl reprezintă capacitatea de anticipare și modelare a mediului informațional, în special în situații în care presiunea hibridă se exprimă prin polarizare, diminuarea încrederii și oboseală cognitivă. În această logică, dezvoltarea unor arhitecturi analitice avansate, capabile să reproducă comportamentele audiențelor și dinamica difuzării mesajelor în rețele digitale, oferă instituțiilor un avantaj prin posibilitatea de a testa scenarii și strategii înainte ca efectele să devină ireversibile. În mod implicit, această direcție poate susține mediul universitar și cel de cercetare printr-o capacitate sporită de prevenire și de calibrare a comunicării instituționale în situații de criză[15].

În ceea ce privește cercetarea, reziliența presupune și *consolidarea mecanismelor de selecție și protecție a colaborărilor și a fluxurilor.* Întrucât cercetarea generează avantaje competitive, aceasta devine un obiectiv de interes pentru vectori ostili care urmăresc expertiza, accesul la rezultate intermediare ori influențarea direcțiilor de dezvoltare. În acest sens, instituțiile sunt nevoite să dezvolte instrumente de evaluare a riscului de parteneriat, să evite dependențe structurale și să gestioneze echilibrul dintre deschiderea necesară progresului științific și precauția cerută de mediul strategic.

În egală măsură, ***reziliența resursei umane*** devine un criteriu strategic, întrucât competiția hibridă utilizează frecvent mecanisme de intimidare, suprasolicitare informațională, presiune reputațională sau operațiuni de tip HUMINT. În acest sens, stabilitatea psihologică, cultura de securitate și funcționalitatea sub stres nu sunt variabile colaterale, ci factori care pot determina atât continuitatea procesului educațional, cât și capacitatea instituției de a funcționa sub presiune. În absența unor mecanisme de protecție organizațională, instituțiile devin mai susceptibile la fracturare internă și la reacții impredictibile, ceea ce amplifică eficiența acțiunilor actorilor ostili[16].

EVALUARE ȘI PERSPECTIVE

Analiza influenței amenințărilor hibride asupra învățământului superior, programelor de formare și cercetării științifice din România evidențiază faptul că spațiul academic nu mai poate fi tratat exclusiv ca domeniu civil autonom, ci ca un segment strategic al securității naționale întrucât contribuie direct la generarea de competențe, expertiză și capacitate instituțională de reacție. În logica competiției contemporane, presiunea hibridă nu urmărește neapărat defuncționalizarea imediată, ci degradarea graduală a funcțiilor esențiale prin acțiuni cumulative, dificil de atribuit și adesea insuficient sesizabile în timp real[17].

Un rezultat central al demersului îl constituie faptul că mediul educațional devine vulnerabil

atunci când sunt afectate mecanismele de validare a cunoașterii, disciplina evaluării și credibilitatea instituțională, fenomen cu efecte funcționale, nu doar reputaționale. În acest registru, distorsiunea proceselor de formare produce consecințe în lanț, întrucât slăbirea competenței profesionale poate genera, în timp, vulnerabilități operaționale în domenii esențiale. În paralel, cercetarea științifică reprezintă o zonă de interes sporit, în special în sectoarele cu relevanță dual, unde cunoașterea devine avantaj tehnologic și, implicit, strategic.

În acest context, reziliența instituțională trebuie înțeleasă ca o necesitate strategică și ca o arhitectură integrată de funcționare, cultura organizațională de securitate, reziliența cognitivă, guvernanța în situații de criză, reziliența digitală și protecția resursei umane devenind instrumente esențiale. Absența acesteia nu generează, de regulă, eșec imediat, ci conduce la acumularea de vulnerabilități, care se pot materializa și pot conduce la apariția unor amenințări la adresa securității instituționale, cum ar fi spionajul, sabotajul sau agresiunile cibernetice.

În perspectivă, este probabilă intensificarea presiunilor hibride asupra domeniului educațional și științific din România, pe fondul digitalizării accelerate și a dezvoltării tehnicilor de influență. Prin urmare, devine relevantă extinderea cooperării între instituțiile civile și militare, fie ele de învățământ superior, de formare sau de cercetare, în vederea înlăturării vulnerabilităților și limitării riscurilor.

BIBLIOGRAFIE

1. AVIV Itzhak, Ferri Uri, “Russian-Ukraine armed conflict: Lessons learned on the digital ecosystem”, *International Journal of Critical Infrastructure Protection*, vol. 43, December 2023; https://doi.org/10.1016/j.ijcip.2023.100637.
2. BACHMANN Sascha-Dominik Dov, Putter Dries, Duczynski Guy, “Hybrid warfare and disinformation: A Ukraine war perspective”, *Global Policy*, vol. 14, nr. 5, 2023, pp. 858-869; https://doi.org/10.1111/1758-5899.13257.
3. BĂLĂCEANU Ion, Buță Ionuț-Cosmin, “Hybrid warfare’s influence in the military decision-making process”, International Scientific Conference “Strategies XXI”, supl. “*Global Security and National Defence*”, 2020, pp. 15-19; https://www.proquest.com/conference-papers-proceedings/hybrid-warfare-s-influence-military-decision/docview/2820619900/se-2.
4. BOARU Gheorghe, Doicariu Daniel, “A global analysis on the hybrid war”, International Scientific Conference “Strategies XXI”, supl. “*Global Security and National Defence*”, 2020, pp. 73-79; https://www.proquest.com/conference-papers-proceedings/global-analysis-on-hybrid-war/docview/2820620476/se-2.
5. BRILINGAITĖ Agnė, Bukauskas Linas, Juozapavičius Aušrius, “A framework for competence development and assessment in hybrid cybersecurity exercises”, *Computers & Security*, vol. 88, 2020; https://doi.org/10.1016/j.cose.2019.101607.
6. BRUZZONE G. Agostino, Giovannetti Antonio, Gotelli Marco, Ghisi Filippo, Pedemonte Massimo, Snore Guna, Bergaminis-Korats Gundars, Bertolin Giorgio, Vecmanis Raitis Ralfs, “Audience behavior modeling for cognitive warfare training in multidomain environments”, Procedia Computer Science, 2025; https://doi.org/10.1016/j.procs.2025.12.121.

7. CRUCERU Valerică, "On contemporary warfare: short review of specific concepts", *Land Forces Academy Review*, vol. 19, nr. 3, 2014, pp. 231-237; https://www.proquest.com/scholarly-journals/on-contemporary-warfare-short-review-specific/docview/1610752861/se-2.
8. DAMONS Daphne, "Weaponizing connectivity: the role of social media and cyberspace in modern subversion", Proceedings, European Conference on Cyber Warfare and Security, 2025, pp. 857-863; https://www.proquest.com/conference-papers-proceedings/weaponizing-connectivity-role-social-media/docview/3244089522/se-2.
9. KARLSEN Geir-Hågen, "Divide and rule: ten lessons about Russian political influence activities in Europe", *Palgrave Communications*, vol. 5, 2019; https://doi.org/10.1057/s41599-019-0227-8.
10. MONAGHAN Sean, "Countering hybrid warfare: so what for the future joint force", *Prism: A Journal of the Center for Complex Operations*, vol. 8, nr. 2, 2019, pp. 82-98; https://www.proquest.com/scholarly-journals/countering-hybrid-warfare-so-what-future-joint/docview/2317561710/se-2.
11. MUNTEANU Răzvan, "Hybrid warfare - the new form of conflict at the beginning of the century", *Strategic Impact*, nr. 56, 2015, pp. 19-26; https://www.proquest.com/scholarly-journals/hybrid-warfare-new-form-conflict-at-beginning/docview/1753209782/se-2.
12. OKROMTCHEDLISHVILI Ivan, "The role of civil society in strengthening national preparedness for modern security threats", *Bulletin of "Carol I" National Defense University*, vol. 14, nr. 2, 2025, pp. 167-199; https://doi.org/10.53477/2284-9378-25-22.
13. OSIICHUK Maryna, Shepotylo Oleksandr, "Conflict and well-being of civilians: The case of the Russian-Ukrainian hybrid war", Ecosystem Services, 2019; https://doi.org/10.1016/j.ecosys.2019.100736.
14. ROMAŃSKI Rafał, "Mechanisms of disinformation amplification in hybrid warfare: the case of the conflict in Ukraine", *Bulletin of "Carol I" National Defense University*, vol. 14, nr. 2, 2025, pp. 7-32; https://doi.org/10.53477/2284-9378-25-13.
15. SANZ-CABALLERO Susana, "The concepts and laws applicable to hybrid threats, with a special focus on Europe", *Humanities and Social Sciences Communications*, vol. 10, 2023; https://doi.org/10.1057/s41599-023-01864-y.
16. SOLMAZ Tarık, "Towards a Taxonomy of Hybrid Warfare: Lessons from Crimea and the Donbas", *Bulletin of "Carol I" National Defense University*, vol. 14, nr. 2, 2025, pp. 47-61; https://doi.org/10.53477/2284-9378-25-15.
17. TUDORACHE Paul, Bârsan Ghiță, Jobbágy Zoltan, Cîrdei Alin, Gligorea Ilie, "An innovative conceptual model for education and training on hybrid warfare", *Management & Marketing*, vol. 18, nr. 3, 2023, pp. 234-250; https://doi.org/10.2478/mmcks-2023-0013.
18. WAGNSSON Charlotte, Östervall Albin, Angwald Anton, "Naming the enemy: how to fortify society against foreign disinformation while avoiding excessive vigilance to reliable media", *Humanities and Social Sciences Communications*, vol. 12, 2025; https://doi.org/10.1057/s41599-025-04664-w.
19. WELLS Winthrop, "Battlefield evidence in the age of artificial intelligence-enabled warfare", *Chicago Journal of International Law*, vol. 26, nr. 1, 2025, pp. 249-280; https://www.proquest.com/scholarly-journals/battlefield-evidence-age-artificial-intelligence/docview/3235035015/se-2.
20. ZARNADZE Aleksandr, "Invisible bullets: the power of narratives in modern warfare", *Global Policy*, vol. 16, nr. 2, 2025, pp. 419-422; https://doi.org/10.1111/1758-5899.70018.

[1] Susana Sanz-Caballero, ”The concepts and laws applicable to hybrid threats, with a special focus on Europe”, *Humanities and Social Sciences Communications*, vol. 10, 2023.
[2] Răzvan Munteanu, ”Hybrid warfare - the new form of conflict at the beginning of the century”, *Strategic Impact*, nr. 56, 2015, pp. 19-26.
[3] Sascha-Dominik Dov Bachmann, Dries Putter, Guy Duczynski, ”Hybrid warfare and disinformation: A Ukraine war perspective”, *Global Policy*, vol. 14, nr. 5, 2023, pp. 858-869.
[4] Geir-Hågen Karlsen, ”Divide and rule: ten lessons about Russian political influence activities in Europe”, *Palgrave Communications*, vol. 5, 2019.
[5] Aleksandr Zarnadze, ”Invisible bullets: the power of narratives in modern warfare”, Global Policy, vol. 16, nr. 2, 2025, pp. 419-422.
[6] *Ibidem*.
[7] Geir-Hågen Karlsen, *Op. cit.*
[8] Tarık Solmaz, ”Towards a taxonomy of hybrid warfare: lessons from Crimea and the Donbas”, *Bulletin of “Carol I” National Defense University*, vol. 14, nr. 2, 2025, pp. 47-61.
[9] *Ibidem.*
[10] Geir-Hågen Karlsen, *Op. cit.*
[11] Winthrop Wells, ”Battlefield evidence in the age of artificial intelligence-enabled warfare”, *Chicago Journal of International Law*, vol. 26, nr. 1, 2025, pp. 249-280.
[12] Sean Monaghan, ”Countering hybrid warfare: so what for the future joint force”, *Prism: A Journal of the Center for Complex Operations*, vol. 8, nr. 2, 2019, pp. 82-98.
[13] Charlotte Wagnsson, Albin Östervall, Anton Angwald, ”Naming the enemy: how to fortify society against foreign disinformation while avoiding excessive vigilance to reliable media”, *Humanities and Social Sciences Communications*, vol. 12, 2025.
[14] Agnė Brilingaitė, Linas Bukauskas, Aušrius Juozapavičius, ”A framework for competence development and assessment in hybrid cybersecurity exercises”, *Computers & Security*, vol. 88, 2020.
[15] Agostino G. Bruzzone, Antonio Giovannetti, Marco Gotelli, Filippo Ghisi, Massimo Pedemonte, Guna Snore, Gundars Bergaminis-Korats, Giorgio Bertolin, Raitis Ralfs Vecmanis, *Audience behavior modeling for cognitive warfare training in multidomain environments*, Procedia Computer Science, 2025.
[16] Maryna Osiichuk, Oleksandr Shepotylo, *Conflict and well-being of civilians: The case of the Russian-Ukrainian hybrid war*, Ecosystem Services, 2019.
[17] Răzvan Munteanu, *Op. cit.*

AMENINȚĂRILE CUANTICE ASUPRA SECURITĂȚII CRIPTOGRAFICE

Mihaela RÎNJA*

Abstract

Quantum computing has progressed from theoretical enquiry to experimental platforms comprising over one thousand high-fidelity qubits. These advances threaten the long-term security of classical public-key cryptosystems—most notably RSA and elliptic curve cryptography—whose underlying hardness assumptions will fail once fault-tolerant quantum computers can execute Shor's algorithm. In parallel, Grover's algorithm asymptotically reduces the complexity of exhaustive key search attacks on symmetric primitives by a square root factor.

This article reviews contemporary quantum hardware roadmaps and convergent expert projections that situate the arrival of a cryptographically relevant quantum computer within the next decade, analyses ongoing standardisation efforts centred on lattice-, code-, and hash-based post-quantum cryptography, and examines the operational, economic, and regulatory challenges associated with large-scale cryptographic migration. The paper concludes by presenting a framework of technical and organisational countermeasures—including hybrid key exchange mechanisms, crypto-agile software architectures, and rigorous key lifecycle management—designed to preserve confidentiality for information assets requiring long-term protection.

Keywords*: post-quantum; PQC; Q Day; RSA; ECC; Shor, Grover; NIST; FIPS 203; ML KEM; Dilithium; SPHINCS+; crypto-agility; NIS2.*

INTRODUCERE

Securitatea infrastructurilor digitale actuale se bazează pe presupunerea că anumite probleme matematice, în special factorizarea numerelor întregi mari și logaritmul discret, nu pot fi rezolvate practic pe calculatoare clasice. Progresele recente în domeniul calculului cuantic, demonstrate deja prin prototipuri ce depășesc o mie de qubiți de înaltă fidelitate, amenință să submineze aceste presupuneri de bază. De asemenea, planurile industriale actuale promit atingerea unor rate de eroare de sub 1% la nivel logic, ceea ce sugerează că sistemele cuantice tolerante la erori devin realizabile în viitorul apropiat.

În lumina acestor evoluții, comunitatea științifică și organizațiile de standardizare au inițiat, încă din 2016, eforturi pentru dezvoltarea și standardizarea criptografiei post-cuantice (PQC). Un reper cheie a fost atins în august 2024,

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

odată cu aprobarea formală a standardelor NIST FIPS 203–205 – protocoale bazate pe soluții de tip lattice, hash și cod – menite să protejeze comunicațiile înainte ca un computer cuantic tolerant la erori să devină operațional. Într-o direcție similară, Comisia Europeană a anunțat, la 23 iunie 2025, un plan care prevede ca sectoarele critice să finalizeze tranziția la algoritmi post-cuantici până cel târziu în anul 2029. Aceste demersuri demonstrează tendința globală de trecere către paradigme criptografice rezistente la atacuri cuantice.

FUNDAMENTE TEORETICE ALE CALCULULUI CUANTIC ȘI IMPACTUL ASUPRA CRIPTANALIZEI

Calculul cuantic operează în paradigma circuitelor cuantice universale, în care informația este codificată în qubiți și prelucrată printr-un set de porți unitare și operații de măsurare. Crearea unui calculator cuantic tolerant la erori se bazează pe „teorema pragului", conform căreia dacă rata de eroare fizică per poartă scade sub $\sim 10^{-2}$–10^{-3} atunci codurile de corecție a erorilor (de exemplu, codul de suprafață) pot menține coerența logică pe durate arbitrar de lungi. Estimările recente indică faptul că factorizarea unui modul RSA-2048 ar necesita în jur de 6000 de qubiți logici, echivalentul a circa 20 de milioane de qubiți fizici, și o profunzime de circuit de ordinul 10^{12} porți T. Deși aceste cerințe sunt extrem de ridicate, ele se aliniază totuși traiectoriilor anticipate în foile de parcurs industriale.

Algoritmi cuantici relevanți

Algoritmul de factorizare propus de Peter Shor, în anul 1994, demonstrează că un calculator cuantic universal, operând în regim tolerant la erori, poate rezolva problema factorizării numerelor întregi și a logaritmului discret în timp polinomial, anulând astfel bariera exponențială care conferă securitate schemelor RSA și ECC. Dezvoltarea tehnicii de control coerent este evidențiată, în principal, în unele teste timpurii, cum ar fi rularea circuitului Eagle al computerului IBM cu 127 de qubiți (legături multiple). De asemenea, simulările recente indică faptul că pentru a sparge cheia RSA-2048 cu o caracteristică de performanță anticipată ar fi necesari circa 6000 qubiți logici (aproximativ 20 milioane qubiți fizici) și aproximativ 10^{12} porți *T*, corespunzând câtorva luni de funcționare continuă pe un dispozitiv cuantic relevant criptografic.

În paralel, Algoritmul lui Lov Grover, dezvoltat în anul 1996, furnizează un avantaj în atacurile de căutare exhaustivă, reducând numărul de interogări de la N la $\sqrt{N}$. Aplicat asupra unei chei AES-128, Grover comprimă spațiul de căutare de la $3{,}4 \times 10^{38}$ opțiuni la aproximativ $1{,}8 \times 10^{19}$ încercări, motiv pentru care standardele actuale recomandă adoptarea AES-256. Complexitatea post-Grover a AES-256 (2^{128}, adică aproximativ $3{,}4x\ 10^{38}$ încercări) rămâne confortabilă peste pragul de 2^{112} operații, considerat necesar pentru protejarea pe termen lung a datelor sensibile. Diferența de performanță față de AES-128 este neglijabilă: AES-128 rulează 10 runde de operații, iar AES-256 rulează 14, adăugând sub 3% latență în implementările hardware/software moderne[1].

Modelul „Harvest Now Decrypt Later" (HNDL)

Modelul HNDL descrie practica adversarilor de a intercepta şi stoca fluxuri criptate, de la sesiuni de email la tranzacţii bancare, cu speranţa că vor putea fi descifrate peste zece sau cincisprezece ani, când hardware-ul cuantic va ajunge la maturitate. Existenţa unor centre de date cu capacităţi de zeci de exaocteţi, dedicate stocării pe termen lung a traficului TLS 1.2, sugerează că această strategie este deja aplicată în practică[2]. Pentru organizaţiile al căror orizont de confidenţialitate depăşeşte un deceniu (agenţii guvernamentale, companii farmaceutice, institute de cercetare) migrarea proactivă la protocoale postcuantice şi mecanisme hibride devine imperativă.

PROGRES HARDWARE ȘI ESTIMAREA MOMENTULUI „QDAY"

Dincolo de arhitecturile supraconductoare dezvoltate de IBM, care a prezentat în 2024 cipul Condor (cu 1121 de qubiți)[3], platformele alternative de calcul cuantic au înregistrat progrese remarcabile. În domeniul ionilor capturați, IonQ a

atins pragul de #AQ 35, echivalent cu 35 de qubiți algoritmici, pe sistemul Forte[4], iar Quantinuum, în parteneriat cu Microsoft, a demonstrat faptul că 4 qubiți logici fiabili pot fi obținuți din 30 de qubiți fizici, menținându-i fără erori de-a lungul a peste 14000 de execuții[5]. Pe frontul fotonic, PsiQuantum raportează fidelități mai mari sau egale cu 99,99 % pentru qubiți individuali pe cipuri fotonice integrate și o arhitectură modulară ce poate găzdui peste 1000 de astfel de cipuri într-un cabinet criogenic. Concomitent, Xanadu a lansat Borealis, cel mai mare computer fotonic disponibil publicului, depășind simularea clasică prin eșantionare gaussiană[6]. În zona atomilor neutri, QuEra a publicat, în aprilie 2024, o foaie de parcurs în trei etape către un procesor cu 10000 de qubiți fizici și 100 logici până în 2027, bazat pe rețele bidimensionale programabile[7]. Această diversitate tehnologică accelerează inovarea și sugerează că un calculator cuantic relevant criptografic poate apărea concomitent din mai multe paradigme hardware.

Evoluția numărului de qubiți și a fidelității

Creșterea performanței calculatoarelor cuantice este urmărită prin doi indicatori principali: numărul de qubiți și fidelitatea porților logice. Fidelitatea reprezintă probabilitatea ca o poartă cuantică să se execute fără erori. Primul cip IBM de generație nouă, „Eagle", lansat în 2021, avea 127 qubiți, ceea ce înseamnă o creștere de aproape un ordin de mărime în doar trei ani față de dispozitivele precedente. În paralel, rata medie de eroare pe poartă a scăzut de la 1% la sub 0,1%, îmbunătățind fidelitatea de zece ori[8]. Această reducere este crucială: un singur algoritm Shor care factorizează RSA2048 necesită trilioane de porți logice consecutive, iar fiecare eroare acumulată compromite rezultatul.

Un mod intuitiv de a înțelege fidelitatea este compararea acesteia cu zgomotul de pe o linie telefonică. Dacă doar una dintr-o mie de silabe se pierde, conversația rămâne inteligibilă însă o rată de eroare de una la zece face mesajul de neînțeles. Prin analogie, în hardware-ul cuantic reducerea erorilor de la 1% la 0,1% echivalează cu trecerea de la o conversație puternic bruiată la una suficient de clară încât erorile rămase să poată fi corectate prin mijloace software.

Repere industriale

La 23 iunie 2025, IBM și institutul japonez RIKEN au pus în funcțiune primul sistem IBM Quantum System Two din afara Statelor Unite, instalat lângă supercomputerul Fugaku, în prezent al treilea cel mai rapid sistem clasic din lume[9]. Noul ansamblu folosește procesorul Heron cu 156 qubiți fizici, însă modularitatea criostatului îi permite montarea viitoarelor cipuri „Kookaburra" și „Flamingo", care vor depăși 1500 qubiți fiecare. Integrarea directă cu Fugaku reduce latența dintre calculele cuantice și cele clasice, fiind esențială pentru execuția algoritmilor de corecție a erorilor în timp real. Deși rularea unui circuit de ~5 000 de porți logice poate părea modestă în raport cu miliardele de operații efectuate de un CPU, aceasta demonstrează posibilitatea execuției unor circuite cuantice foarte adânci într-un regim cu zgomot scăzut, un pas important spre corecția erorilor la nivel logic.

Și alți jucători din industrie au atins praguri semnificative: Google a anunțat în 2024 procesorul Sycamore 2, cu o rată de eroare de aproximativ 0,0005 per poartă, iar Quantinuum a demonstrat, în 2025, primul cip cu 35 de qubiți logici pe o platformă cu ioni capturați. Aceste realizări sugerează o veritabilă „cursă de înarmare tehnologică", în care fiecare arhitectură își optimizează nișa proprie (viteza pentru supraconductori, fidelitatea pentru ioni, scalabilitatea bidimensională pentru atomi neutri).

Previziunile privind apariția unui calculator cuantic relevant criptografic variază considerabil, întrucât depind atât de ritmul progresului hardware, cât și de progresele algoritmice. Un raport din 2024 al Global Risk Institute a colectat opiniile a peste 40 de experți, indicând o probabilitate de ~50% ca Q Day să aibă loc în intervalul 2033–2038[10]. Fiecare expert intervievat a estimat, în medie, 6000 de qubiți logici pentru a sparge RSA-2048 și a proiectat calendarul atingerii acestui prag pornind de la tendințele istorice, apoi a corelat rezultatele cu legea lui Rose, conform căreia numărul qubiților utili se dublează la fiecare 18–24 de luni.

Deși estimarea pentru perioada 2033-2038 este incertă, ea servește drept orizont de planificare pentru autorități. Principiul inegalității

lui Mosca[11] afirmă că dacă suma dintre timpul necesar migrării și durata de confidențialitate a datelor depășește fereastra până la Q Day, atunci tranziția trebuie începută imediat. Pentru dosare medicale cu o valabilitate de 25 ani sau secrete industriale cu ciclu de viață de 15 ani, această condiție este deja îndeplinită, justificând adoptarea urgentă a criptografiei post-cuantice.

VULNERABILITATEA ALGORITMILOR CLASICI

Sistemele criptografice folosite pe scară largă în ultimele trei decenii se bazează exclusiv pe presupuneri de complexitate valabile doar într-un mediu de calcul clasic. Apariția unui computer cuantic tolerant la erori ar invalida aceste presupuneri: un atacator care dispune atât de algoritmul lui Shor, cât și de cel al lui Grover, ar putea, de exemplu, să decripteze retroactiv comunicațiile interceptate, să genereze semnături digitale frauduloase și să submineze securitatea infrastructurilor PKI la nivel mondial.

RSA și ECC

Algoritmul lui Shor exploatează două probleme matematice fundamentale: factorizarea numerelor întregi și rezolvarea logaritmului discret. RSA își bazează securitatea pe dificultatea de a găsi factorii primi ai unui modul mare, operație exponențială pe hardware clasic, dar polinomială pe un calculator cuantic. În mod similar, ECC se sprijină pe dificultatea calculării logaritmului discret pe o curbă eliptică, problemă pe care algoritmul lui Shor o reduce, de asemenea, la timp polinomial.

Pentru a estima impactul practic, studii ale NIST arată că ar fi necesari aproximativ 6000 qubiți logici și 10^{12} porți T pentru a compromite RSA2048, echivalent cu câteva luni de rulare continuă pe un sistem cuantic de generație postCondor. Spre deosebire de modelul clasic, unde dublarea lungimii cheii crește exponențial efortul necesar unui atac, în modelul cuantic costul crește doar liniar. Astfel, nici trecerea la RSA4096 sau ECC521 nu oferă un beneficiu semnificativ împotriva unui adversar cuantic.

Un atacator care deține un computer cuantic criptografic relevant (CRQC) ar putea extrage cheile private din certificate X.509; de asemenea, ar putea semna software malițios ca fiind legitim și chiar intercepta și decripta fluxuri TLS în timp real. Mai mult, chiar înainte de apariția acestor mașini, adversarii pot înregistra traficul cu scopul de a-l decripta ulterior[12], expunând date medicale, secrete comerciale sau comunicații diplomatice cu valoare pe termen lung.

Din perspectiva apărării, migrarea către scheme criptografice postcuantice este singura soluție viabilă. Soluțiile parțiale, cum ar fi dublarea dimensiunii cheilor RSA, oferă doar amânări marginale. Ca măsură intermediară, NIST și IETF recomandă utilizarea unor suite hibride: RSA3072 împreună cu KYBER768 pentru schimbul de chei și ECDSA împreună cu Dilithium pentru semnături, asigurând compatibilitatea cu infrastructura existentă, oferind în același timp protecție față de adversarii dotați cu calculatoare cuantice.

Criptografia simetrică

Spre deosebire de sistemele cu cheie publică, algoritmii simetrici precum Advanced Encryption Standard (AES), ChaCha20 sau funcțiile hash din familiile SHA2/SHA3 nu sunt compromiși complet de apariția calculului cuantic. Cel mai eficient atac cunoscut împotriva lor, algoritmul lui Grover, oferă doar un avantaj cuadratic în cazul unei brute-force a cheilor.

O cheie AES-128 are $2^{128} \approx 3{,}4 \times 10^{38}$ valori posibile, însă Grover reduce efortul de căutare la $2^{64} \approx 1{,}8 \times 10^{19}$ interogări cuantice, ceea ce corespunde unui nivel efectiv de $\approx$ 64 biți de securitate, sub pragul de 112 biți recomandat de NIST pentru confidențialitatea pe termen lung. În schimb, o cheie AES-256 trece de la 2^{256} posibilități la 2^{128} sub Grover, adică $\approx 3{,}4 \times 10^{38}$ încercări, rămânând confortabil peste cerința de 112 biți[13]. De aceea, tranziția la AES-256 este recomandată pentru informațiile ce trebuie protejate pe durate îndelungate, impactul de performanță fiind minim (AES-256 implică doar 4 runde suplimentare față de AES-128).

STANDARDE POSTCUANTICE ȘI INIȚIATIVE GLOBALE

Pe măsură ce amenințarea QDay se conturează la orizont, moment în care un calculator cuantic ar putea compromite algoritmii criptografici clasici, standardele postcuantice devin fundamentale pentru a asigura continuitatea securității informațiilor la nivel global. Coerența și armonizarea acestor standarde sunt esențiale pentru a garanta interoperabilitatea între organizații și auditabilitatea soluțiilor atât în mediul academic, cât și în industrie. În consecință, organismele internaționale precum NIST, ISO/IEC JTC 1 și ETSI colaborează cu actori naționali și din sectorul privat pentru a accelera definirea, testarea și adoptarea unei noi generații de primitive criptografice.

Adoptarea pe scară largă a criptografiei postcuantice presupune nu doar dezvoltarea unor algoritmi siguri, ci și integrarea lor coerentă în standarde, legislație și produse comerciale. La nivel global, implementarea acestor standarde urmărește două obiective majore: interoperabilitatea și asigurarea unei securități verificabile. Interoperabilitatea garantează că un modul criptografic implementat într-o bancă europeană poate comunica în siguranță cu un centru de date guvernamental din altă țară, fără a recurge la soluții proprietare. Totodată, publicarea deschisă a specificațiilor permite comunității academice și industriale să auditeze noile scheme, reducând riscul existenței unor vulnerabilități ascunse. În absența unor standarde comune, ecosistemul s-ar fragmenta în implementări incompatibile și, implicit, suprafața de atac ar crește considerabil.

Standardele NIST FIPS 203–205

În 2016, NIST a lansat un concurs internațional pentru algoritmi rezistenți la calculul cuantic, primind 82 de propuneri din 25 de țări. Procesul s-a desfășurat în trei runde publice de evaluare criptografică și a culminat, în august 2024, cu publicarea a trei standarde finale:

- FIPS 203 - MLKEM (CRYSTALSKyber): o schemă de încapsulare a cheilor (KEM), bazată pe problema Learning With Errors (LWE) în rețele euclidiene, lattice/ generează chei publice de ≈800 octeți și chei secrete de ≈1 KB, cu timp de calcul comparabil cu RSA3072 pe procesoare modern;
- FIPS 204 - MLDSA (CRYSTALSDilithium): o schemă de semnătură digitală tot pe bază de LWE, caracterizată de semnături de 1,3 KB și chei publice de 1 KB/ folosește operații modulare pe inele polinomiale, ușor de optimizat;
- FIPS 205 - SLHDSA (SPHINCS+): o schemă de semnătură digitală bazată pe funcții hash, care nu se sprijină pe presupuneri matematice avansate/ oferă un „plan B” în eventualitatea în care schemele pe bază de rețea (lattice) ar fi compromise în viitor; dezavantajele constau în semnături mai mari (~16 KB) și timp de verificare crescut.

NIST a anunțat și un proiect de standard FIPS 206 (planificat pentru 2026), precum și selecția algoritmului HQC (bazat pe coduri corectoare de erori) ca viitor standard KEM suplimentar. Prin publicarea acestor standarde, algoritmii post-cuantici devin obligatorii pentru agențiile federale americane imediat ce cerințele FIPS 140-3 sunt actualizate – un precedent pe care majoritatea furnizorilor globali îl vor urma [14].

Inițiativele Uniunii Europene

În 23 iunie 2025 Comisia Europeană a prezentat o Foaie de parcurs coordonată care impune entităților esențiale, definite de Directiva NIS2, să finalizeze tranziția la criptografia post-cuantică până la 31 decembrie 2029. Documentul prevede, în primul rând, ca până la sfârșitul lui 2026 toate organizațiile critice să-și inventarieze algoritmii vulnerabili și să-și actualizeze criteriile de achiziție. În 2027 sunt planificate proiecte-pilot intersectoriale în domeniile energie, finanțe și sănătate, însoțite de ghiduri tehnice elaborate de ENISA pentru implementarea schemelor Kyber și Dilithium. Anul 2028 marchează extinderea certificărilor eIDAS pentru semnături digitale post-cuantice și garantarea interoperabilității transfrontaliere, iar 2029 introduce obligativitatea

deplină a noilor algoritmi pentru toate sistemele critice, cu eventuale derogări permise doar pe baza unor justificări tehnice solide. În paralel, inițiativa EuroQCI finanțează o infrastructură europeană de comunicații cuantice prin satelit și fibră optică, destinată distribuirii cheilor prin QKD. Această abordare combină protecția matematică oferită de PQC cu securitatea fizică furnizată de mecanismele cuantice.

IETF și protocoale hibride

În ecosistemul Internetului, grupul de lucru TLS din cadrul IETF a publicat în 2025 draft-ul ietf-tls-hybrid-design-13, care propune un mecanism de schimb de chei hibrid. Secretul clasic ECDHE este concatenat cu un secret Kyber-768, iar rezultatul este trecut printr-o funcție KDF comună[15]. Soluția menține compatibilitatea cu serverele care nu suportă încă algoritmi post-cuantici, astfel că partea de client poate negocia o variantă fallback bazată doar pe ECDHE, respectând principiul *crypto-agility.* Practic, este necesară doar adăugarea unui nou identificator de suită criptografică în lista de algoritmi suportați pentru viitoarele actualizări. În plus, acest design reduce riscul unui atac de tip *downgrade*, întrucât un adversar ar trebui să compromită simultan atât componenta clasică, cât și pe cea post-cuantică.

În afara protocolului TLS și SSH a încorporat, prin propunerea draft-ssh-pqc-10, scheme hibride bazate pe Kyber[16]. De asemenea, Google și Cloudflare testează în producție versiunea 2 a protocolului QUIC, care include algoritmul Kyber-768, colectând telemetrie privind latența și rata de eroare, pentru a valida impactul noilor primitive asupra traficului real[17].

Alte eforturi la nivel mondial

La nivel global, adoptarea criptografiei post-cuantice avansează într-un ritm inegal la nivel global, dar apar puncte clare de convergență. În Canada, Centrul pentru Securitate în Comunicații (CSE) a emis profiluri care impun utilizarea schemelor ML-KEM și Dilithium pentru toate comunicațiile guvernamentale clasificate „Protected B” și superioare[18]. În Regatul Unit, NCSC recomandă implementarea implicită a soluțiilor hibride în sistemul național de sănătate (NHS) și în sectorul apărării, cu termene-limită stabilite pentru 2030 (fază pilot) și 2032 (producție deplină)[19]. În China, standardul național SM9-PQC, bazat pe coduri LDPC, a fost lansat în 2024, iar rețele metropolitane QKD operează deja în Shanghai și Beijing, semnalând prioritatea acordată suveranității criptografice. Peisajul standardizării rămâne, așadar, fragmentat prin diversitatea algoritmilor și calendarelor naționale, dar convergent prin adoptarea familiei Kyber/ Dilithium ca opțiune „implicit globală” pentru primele valuri de migrare.

PROVOCĂRI DE IMPLEMENTARE

Migrarea de la criptografia clasică la cea postcuantică implică un set complex de provocări tehnice, operaționale și financiare. Actualizarea algoritmilor într-un cod sursă este doar vârful icebergului. Organizațiile trebuie să identifice unde sunt folosite cheile și certificatele, să gestioneze impactul asupra performanței și să bugeteze costurile inevitabile ale actualizării.

Inventarierea activelor criptografice

Obținerea unui inventar complet al certificatelor, cheilor și algoritmilor utilizați într-un ecosistem IT extins se dovedește extrem de dificilă, în special în prezența dispozitivelor cu ciclu de viață lung, IoT, SCADA sau sisteme medicale integrate. În astfel de cazuri, componentele criptografice sunt încorporate în firmware și pot scăpa detectării prin scanări obișnuite de rețea. Cele mai bune practici recomandă, în primul rând, scanarea automată a serviciilor publice și interne pentru a inventaria suitele criptografice TLS și SSH, completarea acestor informații cu analiza Software Bill of Materials (SBOM) și a dependențelor de biblioteci criptografice (OpenSSL, mbedTLS, wolfSSL) în pipeline-urile DevOps[20], auditarea directă, la nivel de hardware, a dispozitivelor ce conțin module TPM, HSM sau firmware semnat, prin interfețe JTAG/ SWD ori API-uri furnizate de producători și, nu în ultimul rând, corelarea rezultatelor cu jurnalele de Certificate Transparency și cu inventarele PKI interne pentru a cartografia lanțurile de certificare X.509,

inclusiv certificatele intermediare valabile pe durata a peste 15 ani. Relevanța acestor măsuri este confirmată de un studiu ENISA din 2024[21], care a constatat că în organizațiile mari aproximativ 30% dintre serviciile interne rulează versiuni învechite ale bibliotecilor criptografice, iar circa 12% dintre dispozitivele IoT nu pot fi actualizate la distanță din cauza limitărilor de memorie.

Performanță* și *supradimensiune

Algoritmii post-cuantici impun un cost suplimentar atât la nivelul lățimii de bandă, cât și al timpului de procesare. De exemplu, o cheie publică Kyber-768 ocupă aproximativ 800 octeți, comparativ cu aproximativ 32 octeți pentru o cheie ECDH pe curba P-256, iar o semnătură Dilithium-3 are circa 1,3 KB. Într-o suită TLS hibridă (ECDHE + Kyber-768) acest volum suplimentar însumează aproximativ 1,2 KB per conexiune, mărind timpul de stabilire a sesiunii cu sub 1 ms în centrele de date, dar cu zeci de milisecunde pe rețelele 4G/5G cu latență ridicată. Pe microcontrolere de 64 KB RAM, o implementare SPHINCS+ poate consuma până la 80% din memorie, necesitând optimizări ale aplicației, în timp ce FALCON-512 generează semnături mai mici, de circa 666 octeți, dar necesită aritmetică în virgulă mobilă și cod de precizie extinsă, dificil de realizat pe astfel de platforme.

Optimizările recomandate includ pre-calculul cheilor și semnăturilor pe gateway-uri edge pentru a degreva dispozitivele IoT cu resurse limitate, compresia cheilor Kyber folosind tehnici NTT compuse cu cost minim de procesare și delegarea operațiilor criptografice către acceleratoare hardware RISC-V cu extensii PQC disponibile din 2026.

Măsurători publicate de Cloudflare în 2024, pe un eşantion de zece milioane de conexiuni, arată că utilizarea unei suite criptografice hibride (ECDHE-RSA-AES-GCM + Kyber-768-SHA256) adaugă, în medie, doar 1,4 % latență la încărcarea paginilor web.

Costuri de tranziție

Adoptarea criptografiei postcuantice presupune costuri mai mari decât simpla actualizare a software-ului. Acestea implică investiții în hardware specializat, recertificări, instruirea personalului și refactorizarea fluxurilor DevSecOps. Evaluările realizate de Office of Management and Budget (OMB) pentru administrația federală a Statelor Unite estimează un buget cumulat de 7,1 miliarde de dolari pe intervalul 2025–2035 pentru migrarea la PQC, distribuit pe cinci categorii principale.

Componentă	Procent indicativ din buget	Cheltuieli	Observații
Actualizare și testare software	30%	Portarea bibliotecilor (OpenSSL 3.x, BoringSSL), CI/CD pentru semnături PQC	Cost variabil, depinde de numărul de microservicii
Infrastructură hardware	25%	Achiziție HSM compatibile FIPS1403, routere cu firmware PQC	Ciclu de înlocuire la 5–7 ani
Recertificări și conformitate	15%	Audit FIPS, actualizare PCIDSS, ISO 27001 anexe PQC	Posibile reduceri prin scheme de recunoaștere reciprocă UEUS
Formare și resurse umane	10%	Training specializat, SANS/ Kudelski, recrutarea de specialiști în criptografie	Necesită buget continuu pentru retenție
Contingență și suport operațional	20%	Consultanță externă, programe bugbounty, teste de penetrare și simulări de incident	Include costuri neprevăzute (0day, riscuri din lanțul de aprovizionare)

Subvențiile publice pot acoperi o parte din aceste cheltuieli de tranziție. De pildă, programul european Digital Europe - PQC Grants, cu un buget de 1,2 miliarde de euro pentru perioada 2024-2028, precum și creditele fiscale pentru investiții în securitate cibernetică prevăzute de Secțiunea 45U din Codul Fiscal al Statelor Unite, pentru investiții în securitate cibernetică, pot reduce costurile nete ale organizațiilor cu 15–25%[22]. În plus, un raport Gartner din aprilie 2025 anticipează că serverele x86 echipate cu acceleratoare hardware dedicate algoritmilor PQC vor deveni cu ~35% mai ieftine până în 2027, pe măsură ce volumele de producție cresc, iar cererea de piață se maturizează[23].

Amânarea tranziției implică însă riscuri financiare considerabile. Costurile ulterioare unui incident de securitate, amenzile administrative impuse de GDPR, litigiile colective și prejudiciile de reputație pot depăși cu mult investițiile preventive necesare.

CONCLUZII

Calculatoarele cuantice evoluează într-un ritm accelerat. Procesoarele recente, precum Heron, Willow și prototipurile cu ioni capturați, au atins fidelități sub pragul necesar pentru corecția erorilor, confirmând fezabilitatea experimentală a algoritmilor lui Shor și Grover. Analizele de risc indică o probabilitate semnificativă ca un calculator cuantic criptografic relevant să apară înainte de anul 2040, iar foile de parcurs ale marilor producători converg spre același interval de timp. Prin urmare, intervalul disponibil pentru migrarea infrastructurilor critice este limitat și trebuie tratat cu maximă prioritate.

Organismele de standardizare au stabilit contramăsuri. NIST a finalizat standardele ML-KEM, Dilithium și SPHINCS+, iar Uniunea Europeană, Statele Unite și partenerii lor impun tranziția completă până la începutul următorului deceniu. Familia de algoritmi Kyber/ Dilithium se conturează ca soluție de bază pentru prima etapă a erei post-cuantice, asigurând continuitatea securității informațiilor în fața noilor amenințări cuantice.

BIBLIOGRAFIE

1. BARKER Elaine, Allen Roginsky, *Transitioning the Use of Cryptographic Algorithms and Key Lenghts* (Initial Public Draft), NIST Special Publication 800, NIST SP 800-131Ar3. ipd, National Institute of Standards and Technology, U.S. Department of Commerce, 2024, 44 p.
2. GIDNEY Craig, Martin Ekera, ”How to Factor 2048-bit RSA Integers in 8 Hours Using 20 Million Noisy Qubits”*, Quantum. The Open Journal for Quantum Science,* vol. 5, Paper 433, 2021, 31 p.
3. Jon BOYENS, Angela Smith, Nadya Bartol, Kris Winkler, Alex Holbrook, Mathew Fallon, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, NIST Special Publication, NIST SP 800-161r1, National Institute of Standards and Technology, U.S. Department of Commerce, 2022, 315 p.
4. MOSCA Michele, „Cybersecurity in an Era with Quantum Computers: Will We Be Ready?”, *IEEE Security and Privacy*, vol.16, nr. 5, 2018, pp. 38-41.
5. MOSCA Michele, Marco Piani, *Quantum Threat Timeline Report 2024*, Global Risk Institute, Decembrie 2024, 68 p.
6. SHOR W. Peter, „Algorithms for Quantum Computation: Discrete Logarithms and Factoring”, *Proceedings 35th Annual Symposium on Foundations of Computer Science* (Santa Fe, SUA, 20-22 noiembrie 1994), 1994, pp. 124-134.

[1] https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413.pdf, accesat la 10.07.2025
[2] https://venturebeat.com/security/harvest-now-decrypt-later-why-hackers-are-waiting-for-quantum-computing/, accesat la 15.07.2025
[3] https://www.ibm.com/quantum/blog/quantum-roadmap-2033, accesat la 18.07.2025
[4] https://ionq.com/blog/how-we-achieved-our-2024-performance-target-of-aq-35, accesat la 19.07.2025
[5] https://www.reuters.com/technology/microsoft-quantinuum-claim-breakthrough-quantum-computing-2024-04-03/, accesat la 19.07.2025.
[6] https://www.xanadu.ai/blog/beating-classical-computers-with-Borealis , accesat la 19.07.2025.
[7] https://www.quera.com/blog-posts/the-path-to-10-000-qubits, accesat la 19.07.2025.
[8] https://www.ibm.com/quantum/assets/IBM_Quantum_Developmen_%26_Innovation_Roadmap_Explainer_2024-Update.pdf , accesat la 19.07.2025.
[9] https://newsroom.ibm.com/2025-06-23-ibm-and-riken-unveil-first-ibm-quantum-system-two-outside-of-the-u-s, accesat la 20.07.2025.
[10] https://info.quintessencelabs.com/hubfs/PDFs/Global-Risk-Institute-Quantum-Threat-Timeline-Report-2024.pdf, accesat la 08.07.2025.
[11] https://eprint.iacr.org/2015/1075.pdf, accesat la 08.07.2025.
[12] https://www.hashicorp.com/en/blog/harvest-now-decrypt-later-why-today-s-encrypted-data-isn-t-safe-forever, accesat la 14.07.2025.
[13] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf, accesat la 14.07.2025.
[14] https://csrc.nist.gov/csrc/media/Presentations/2025/nist-pqc-the-road-ahead/images-media/rwcpqc-march2025-moody.pdf, accesat la 14.07.2025.
[15] https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/, accesat la 15.07.2025.
[16] https://www.ietf.org/archive/id/draft-kampanakis-curdle-ssh-pq-ke-01.html, accesat la 15.07.2025.
[17] https://blog.cloudflare.com/pq-2024, accesat la 16.07.2025.
[18] https://www.cyber.gc.ca/sites/default/files/itsp.40.111-e_1.pdf, accesat la 17.07.2025.
[19] https://www.ncsc.gov.uk/guidance/pqc-migration-timelines, accesat la 17.07.2025.
[20] https://www.nccoe.nist.gov/sites/default/files/2023-12/pqc-migration-nist-sp-1800-38b-preliminary-draft.pdf, accesat la 20.07.2025.
[21] https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf, accesat la 21.07.2025.
[22] https://business.maryland.gov/news/maryland-commerce-accepting-applications-cybersecurity-investment-incentive-tax-credit/, accesat la 22.07.2025.
[23] https://www.gartner.com/en/articles/post-quantum-cryptography, accesat la 27.07.2025.

GENERATOARE DE NUMERE ALEATOARE ȘI APLICAREA ACESTORA ÎN DOMENIUL CRIPTOGRAFIC

Florin RĂSTOCEANU*
Mădălin George BOBOC

Abstract

Random number generators are essential components in applications in various domains, including cryptography, banking, gaming and cybersecurity. This paper aims to provide an overview of random number generators, emphasizing their use in cryptographic applications. The main types of generators are presented, emphasizing their characteristics, construction methods, advantages and limitations. The international standards governing the construction, testing and evaluation of random number generators are analyzed, emphasizing the importance of compliance with these standards for use in security-critical applications. The main cryptographic applications in which random number generators are used are also identified. The paper highlights the role that these elements occupy in cryptosystems creating a solid source of information for the development of modern cryptographic applications, indicating directions of interest for future studies.

Keywords: *cryptography; random number generators; information security.*

INTRODUCERE

Numerele aleatoare sunt utilizate în prezent în diferite domenii precum criptografia, simulări, jocuri de noroc, statistică, finanțe sau diferite stiințe. Principala caracteristică a acestora este aleatorismul generat de fenomene care nu pot fi prezise cu exactitate și care nu urmează o anumită distribuție de probabilitate. În funcție de specificitatea aplicațiilor în care sunt utilizate, acestea sunt obținute de la generatoare care îndeplinesc și alte proprietăți precum periodicitatea, eficiența, reproductibilitatea și securitatea. Generatoarele bazate pe algoritmi deterministici produc numere aleatoare cu o anumită perioadă de repetiție. Aceasta se dorește a fi cât mai mare posibilă.

Eficiența poate fi evaluată din punct de vedere al vitezei de generare, a complexității sau a consumului de putere în cazul implementării pe platforme cu resurse limitate. În anumite aplicații este nevoie ca anumite secvențe să poată fi reproduse dacă se cunosc parametrii de inițializare. În schimb, în alte tipuri de aplicații,

* ***Autorii sunt experți în cadrul Ministerului Apărării Naționale.***

în special cele criptografice, nu este de dorit ca numerele generate sau care vor fi generate în viitor să poată fi reproduse, respectiv generate de un atacator, chiar dacă cunoaște anumiți parametri de inițializare sau interni ai generatorului.

Pentru a satisface toate nevoile aplicațiilor care folosesc numere aleatoare s-au dezvoltat mai multe tipuri de generatoare. Generatoarele deterministe sunt caracterizate de viteze mari de generare, resurse limitate, reproductibilitate și periodicitate (care depinde de complexitatea algoritmului utilizat). În schimb generatoarele nedeterministe sunt impredictibile, oferă un grad de securitate ridicat dar nu sunt la fel de eficiente. Pentru a satisface cât mai multe dintre proprietățile menționate anterior se folosesc generatoare hibride în diferite arhitecturi. Acestea au însă dezavantajul complexității.

Generatoarele de numere aleatoare asigură funcționalități esențiale în cadrul sistemelor în care sunt implementate. Din acest motiv, este necesar ca acestea să îndeplinească proprietăți clare și verificabile. Pentru a satisface aceste nevoi au fost depuse eforturi considerabile pentru standardizarea domeniului. O activitate substanțială în acest sens a fost desfășurată de Institutul Național de Standarde si Tehnologii (NIST) și de Biroul Federal pentru Securitatea Informațiilor din Germania. Astfel, au fost dezvoltate standarde care stabilesc tipurile și arhitecturile generatoarelor, algoritmii deterministici și sursele de entropie care pot fi utilizate, precum și metodologiile de testare și validare a acestora.

Aplicațiile în care se folosesc numere aleatoare sunt diverse, însă domeniul cu cel mai mare impact este criptografia. Generarea cheilor criptografice, algoritmii de semnătură digitală și de hash, protocoalele de schimbare a cheilor și generarea nonce-urilor sunt cele mai importante aplicații ale generatoarelor de numere aleatoare în criptografie.

Articolul prezintă o descriere holistică a generatoarelor de numere aleatoare, punând în evidență interdependența dintre teorie, standardizare și aplicații practice în securitate. Studiul este împărțit în cinci capitole: în introducere sunt prezentate conceptele generale, scopul și relevanța subiectului abordat; în al doilea capitol este oferită o clasificare a generatoarelor în funcție de natura acestora și a principiilor de funcționare; în capitolul trei sunt analizate cele mai utilizate standarde și specificații internaționale; capitolul patru cuprinde domeniile de aplicabilitate a generatoarelor în criptografie, iar în ultimul capitol sunt sintetizate ideile principale.

TIPURI DE GENERATOARE DE NUMERE ALEATOARE

Generatoarele de numere aleatoare se pot clasifica în mai multe tipuri în funcție de metoda de generare a aleatorismului. Acest aspect influențează și tipul de aplicații în care sunt folosite. Astfel, sunt generatoare deterministe, care folosesc funcții matematice complexe care pot produce secvențe aleatoare; generatoare nedeterministe care folosesc fenomene fizice pentru a produce aleatorism; și generatoare hibride care beneficiază de avantajele ambelor metode pentru a crea atât secvențe aleatoare, dar și pentru a preveni estimarea numerelor generate anterior și în viitor (vezi Figura 1).

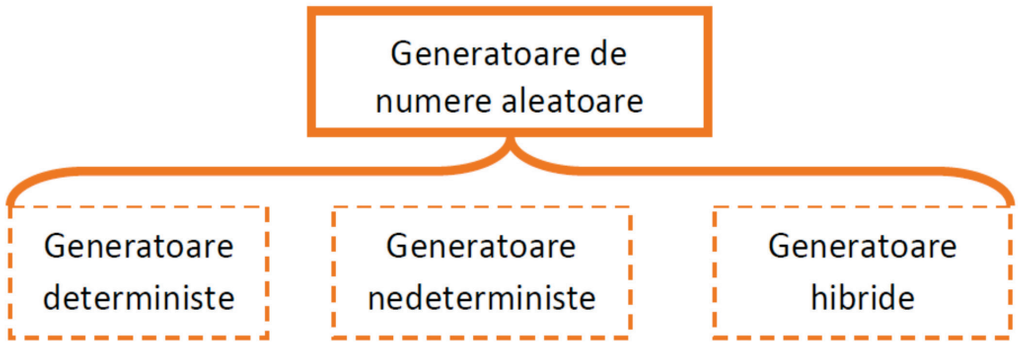

***Fig. 1**: Clasificare generatoare numere aleatoare*

Generatoarele de numere deterministe, care mai sunt denumite și pseudoaleatoare, folosesc algoritmi deterministici și o valoare de inițializare, numită și ”sămânță”, pentru a obține secvențe de numere aleatoare, proces care încearcă să obțină proprietățile statistice ale aleatorismului real sau nedeterminist. Rezultatele generate pot fi replicate dacă ”sămânța” este cunoscută; astfel, un sistem care este instanțiat cu aceeași valoare inițială va produce aceeași succesiune de valori.

În Figura 2 este prezentată schema de principiu a unui astfel de generator. În faza de start starea internă a generatorului se inițializează cu date aleatoare, urmând ca la fiecare iterație această stare să se actualizeze. Dat fiind că algoritmul determinist este caracterizat de o perioadă de repetiție, starea internă se reinițializează constant pentru a păstra proprietățile aleatoare ale generatorului.

Dacă sunt utilizate corect, generatoarele de numere aleatoare deterministe prezintă avantajul de a fi rapide și eficiente. Acestea se implementează ușor în aplicații software, putând fi apelate din biblioteci existente în sistemele de operare, precum random(), srandom(),/ dev/random și /dev/urandom în UNIX/ Linux, CryptGenRandom, rand_s și rand() în Windows și SecureRandom în Java. De asemenea, există

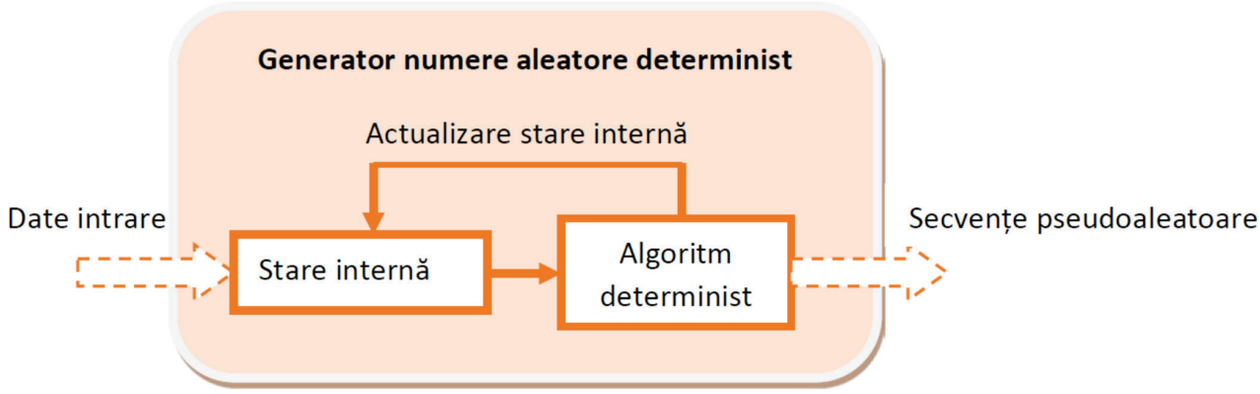

Fig. 2: *Schemă bloc generator de numere aleatoare determinist*

Aceste tipuri de generatoare pot să fie clasificate în două categorii, în funcție de tipul de algoritm folosit. Primul tip este reprezentat de generatoare non-criptografice, utilizate în simulări și modelări statistice, în industria jocurilor și de divertisment, grafică computerizată sau *machine learning*. Acestea sunt axate pe viteza de generare și nu folosesc algoritmi criptografici puternici pentru funcția deterministă. Printre cei mai utilizați algoritmi se enumără: generator congruențial liniar, registre de deplasare cu feedback liniar, Mersenne Twister sau Middle Square Method. Al doilea tip este reprezentat de generatoarele sigure din punct de vedere criptografic, utilizate în domenii în care nivelul de securitate solicitat este ridicat. Acestea folosesc algoritmi criptografici puternici pentru funcția deterministă, precum: algoritmi de criptare simetrici (AES), algoritmi de HASH (SHA-2/SHA-3) sau algoritmi de HMAC (HMAC- SHA256, HMAC-SHA384, HMAC-SHA512). De asemenea, parametrii de inițializare și parametrii interni ai generatorului trebuie ținuți secreți pentru a preveni predicția secvențelor generate, iar în cazul parametrilor de inițializare trebuie să fie și aleatori.

librării specializate care implementează aceste funcții, precum: Boost.Random, FastRandom, SRand (implementate în C++) sau NumPy (implementate în Python). Majoritatea librăriilor criptografice existente pe sistemele de operare, unele dintre ele și evaluate din punct de vedere criptografic, au implementate și generatoare de numere aleatoare deterministe: OpenSSL, BoringSSL.

Aceste tipuri de generatoare vin și cu câteva dezavantaje. În primul rând, nu sunt cu adevărat aleatoare, în sensul că au o perioadă de repetiție/ de aceea, acest parametru este calculat și luat în considerare când este utilizat în aplicații. Pentru anumite aplicații, mai ales cele criptografice, este

important ca atât valorile generate anterior, cât și cele care vor fi generate, să nu poată fi estimate. Din acest motiv se iau măsuri suplimentare de protecție a parametrilor generatorului.

Multe dintre aplicații, în special cele criptografice, au nevoie de o sursă a cărei rezultate să nu poată fi prezise cu ușurință, fiind nevoie de utilizarea generatoarelor de numere nedeterministe. În Figura 3 este prezentată schema de principiu a unui astfel de generator. Sursa de aleatorism este reprezentată de sursa de zgomot, care are la bază fenomene fizice (dificil de modelat matematic și imposibil de reprodus). Deoarece sursele de zgomot cu viteze mari, proprietăți bune de aleatorism și ușor de implementat pe platforme diferite sunt greu de realizat, se acceptă faptul că secvențele extrase din sursa de zgomot nu sunt ideale pentru a fi folosite în aplicații criptografice și, din acest motiv, generatorul are în componență o funcție de condiționare care rezolvă aceste probleme. De asemenea, întrucât sursa de zgomot se bazează pe fenomene fizice, care își pot schimba din diferite motive caracteristica aleatoare, generatorul are în componență teste de sănătate, care au rolul de a detecta rapid o scădere a nivelului de aleatorism al datelor generate.

- zgomot electronic (*thermal noise*) – fluctuații termice în rezistențe sau diode semiconductoare;
- zgomot de avalanșă (*avalanche noise*) – generat în joncțiuni p-n supuse la supratensiune;
- evenimente cuantice – de exemplu, timpul dintre dezintegrarea particulelor radioactive sau absorbția fotonilor individuali;
- evenimente externe nedeterministe – mișcarea cursorului, timpii de tastare ai utilizatorului, zgomot de pe magistrala USB etc. (în special pentru colectarea entropiei în software și sisteme de operare).

Generatoarele de numere aleatoare nedeterministe au avantajul că pot oferi impredictibilitate. Spre deosebire de cele deterministe nu trebuie asigurată protecție parametrilor interni prin mijloace adiționale pentru a nu oferi atacatorului avantajul de a prezice datele generate în trecut sau datele ce vor fi generate în viitor. De asemenea, oferă un grad de aleatorism care poate fi măsurat prin entropie. În schimb și acestea vin cu câteva dezavantaje. Datele generate pot suferi fluctuații sau bias, necesită hardware specializat și au o viteză de

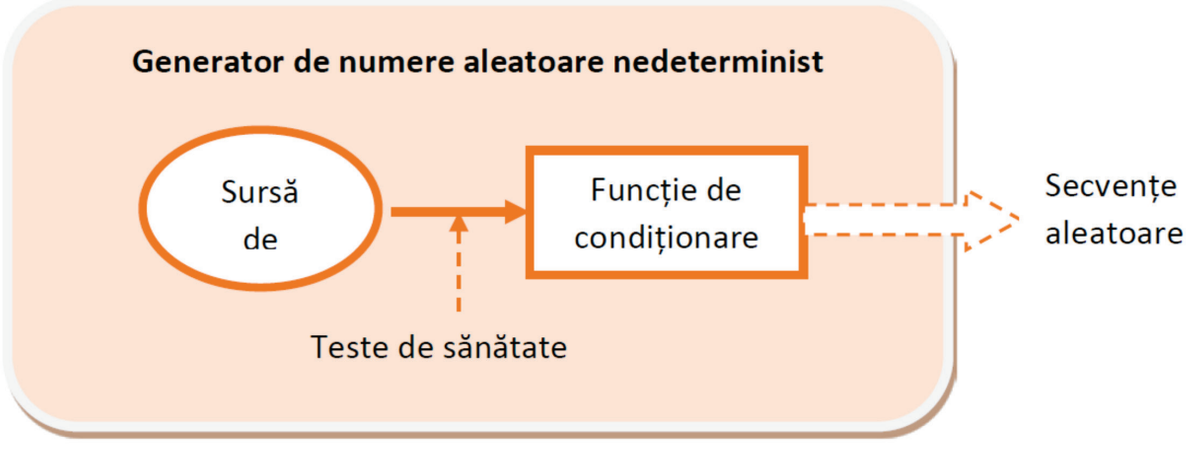

***Fig. 3**: Schema bloc bloc generator de numere aleatoare nedeterminist*

Generatoarele nedeterministe au la bază fenomene fizice, dificil de modelat matematic și imposibil de reprodus. Sursele de zgomot își pot extrage aleatorismul din mai multe tipuri de fenomene fizice:

generare scăzută. Având în vedere aceste aspecte, au fost propuse generatoare hibride care folosesc avantajele ambelor tipuri de generatoare. În Figura 4 este prezentată schema de principiu a unui astfel de generator. Acesta include

un generator nedeterminist pentru generarea secvențelor aleatoare cu viteză ridicată și unul nedeterminist pentru inițializarea/ reinițializarea stării interne a generatorului. Pentru a asigura proprietăți de securitate maximă, cele două generatoare pot produce date în paralel, rezultatul final fiind obținut prin XOR-area celor două ieșiri. Aceste tipuri de generatoare dețin toate avantajele generatoarelor din componență, dar prezintă o complexitate mai mare.

modalitatea de construire a generatoarelor de numere aleatoare. În SP 800–90A[2] sunt recomandate metode de generare a biților aleatori care, ulterior, pot fi și utilizați ca atare sau prelucrați pentru generarea de numere aleatoare. Standardul specifică cerințele pentru utilizarea generatoarelor de biți aleatori, specificațiile pentru mecanismele criptografice implementate în aceștia, variante de implementare și metodologii de testare și validare. În SP 800 90B sunt

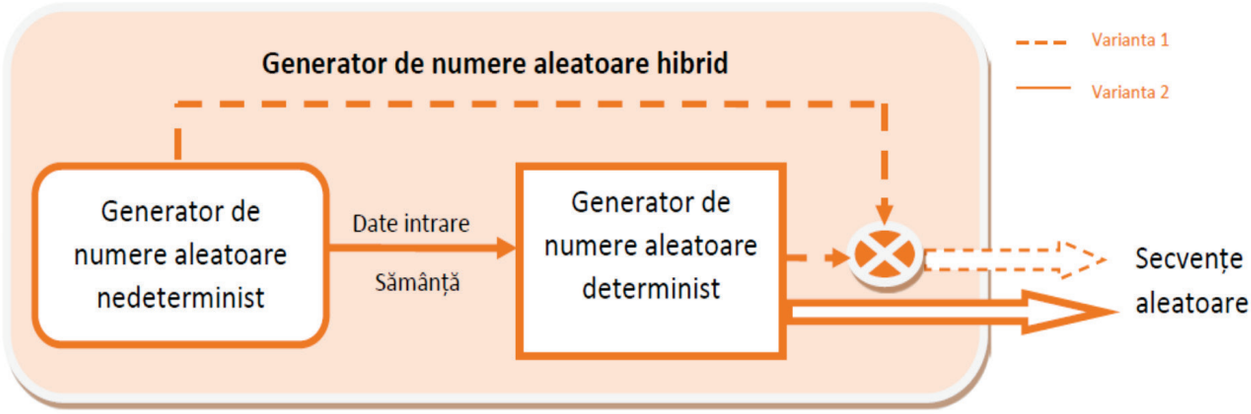

***Fig. 4**: Schema bloc bloc generator de numere aleatoare hibride*

STANDARDE

Generatoarele de numere aleatoare utilizate în criptografie sunt reglementate de standarde internaționale, asigurându-se, astfel, un nivel bun de securitate și caracteristici aleatoare ridicate. Institutul Național de Standarde și Tehnologii (din SUA) a făcut o serie de recomandări referitoare la arhitecturi și parametri care caracterizează generatoarele de numere aleatoare. De asemenea, a propus metode de analiză și evaluare a acestora.

În NIST SP 800-22[1] este prezentat un set de teste statistice utilizate pentru evaluarea gradului de aleatorism al generatoarelor de numere aleatoare care pot fi utilizate în aplicații criptografice. Standardul include specificații pentru implementarea testelor statistice, instrucțiuni pentru aplicarea și interpretarea fiecărui test și metodologii pentru evaluarea generatoarelor, precum și recomandări pentru setarea parametrilor și interpretarea rezultatelor.

Seria de standarde SP 800-90 specifică specificate metodele de proiectare și de testare a surselor de entropie utilizate în generatoarele nedeterministe de numere aleatoare[3]. Standardul definește conceptul de entropie, un model arhitectural și interfețele conceptuale, stabilește o metodologie de estimare a nivelului de entropie a surselor de zgomot și de testare și evaluare a surselor de entropie. În SP 800 90 C[4] sunt descrise câteva arhitecturi de generatoare de numere aleatoare hibride, care utilizează generatoare de numere aleatoare descrise în SP 800 90B și surse de entropie definite în SP 800 90B.

Activitatea NIST este suplinită la nivel european de Biroul Federal pentru Securitatea Informației, cu sediul în Germania. Acesta a emis documente tehnice precum AIS 20 și AIS 31, în care sunt tratate generatoarele de numere aleatoare. În documentul AIS 20 este reglementat procesul de evaluare și certificare a generatoarelor de numere aleatoare deterministe[5]. AIS 20 definește mai multe clase funcționale (de la DRG.1 până la DRG.4), fiecare cu un nivel diferit de securitate și cerințe. De exemplu, DRG.3 și DRG.4 includ

cerințe privind reinjectarea periodică a entropiei din surse externe și rezistența la compromitere. Evaluarea conform AIS 20 presupune validarea corectitudinii algoritmului, a implementării și a rezistenței criptografice împotriva atacurilor. Acest standard nu se axează pe sursa de entropie, presupunând că aceasta este furnizată separat, ci pe comportamentul determinist și sigur al algoritmului după inițializare. AIS 20 este folosit, în special, pentru certificarea modulelor criptografice în cadrul Common Criteria și este echivalent în scop cu NIST SP 800-90A.

Documentul AIS 31[6] completează AIS 20 și este destinat evaluării generatoarelor de numere aleatoare nedeterministe. Acest standard impune dezvoltatorilor un model stocastic al sursei de entropie, care să permită estimarea formală a entropiei minime per bit, un parametru esențial pentru validarea sursei. AIS 31 prevede testarea riguroasă a ieșirilor prin teste statistice, precum și implementarea unor mecanisme de monitorizare în timp real a funcționării, și anume teste de sănătate, pentru a detecta orice degradare sau eșec al sursei de entropie în timp real. Sunt definite mai multe clase funcționale, cum ar fi PTG.1 (nivel minim), PTG.2 (cu post-procesare criptografică) și PTG.3 (cel mai înalt nivel, cu mecanisme avansate de corecție și control). AIS 31 este considerat unul dintre cele mai stricte standarde de evaluare a RNG-urilor fizice din lume și este utilizat în certificarea produselor de securitate care necesită surse de aleatorie fiabile și verificabile, precum module HSM (Hardware Secure Module), smartcarduri sau platforme guvernamentale.

APLICAȚII ÎN CRIPTOGRAFIE

În criptografie, calitatea numerelor aleatoare este esențială întrucât multe mecanisme de securitate depind de impredictibilitate, unicitate și entropie ridicată. Utilizarea unor generatoare sigure și conforme cu standarde acceptate pe scară largă este o condiție esențială pentru a preveni atacuri ce pot compromite serviciile criptografice de bază.

Cea mai utilizată aplicabilitate a generatoarelor de numere aleatoare se regăsește în generarea de chei criptografice. Numerele aleatoare sunt utilizate pentru a genera chei criptografice simetrice (ex. AES, ChaCha20) sau asimetrice (ex. RSA, ECC). Cheile trebuie să fie complet impredictibile pentru a preveni atacuri prin estimare sau reconstruirea algoritmică a acestora. Împreună cu cheile criptografice se utilizează, pentru anumite moduri de lucru ale algoritmilor criptografici, vectorii de inițializare. Acestea sunt valori aleatoare sau pseudo-aleatoare adăugate la procesul de criptare în modurile de operare ale cifrurilor bloc (ex: CBC, GCM), pentru a asigura că două mesaje identice nu duc la aceleași texte criptate.

Funcțiile hash folosesc parametri precum salturile, mai ales în stocarea parolelor, pentru a împiedica atacurile prin tabele rainbow și pentru a asigura unicitatea fiecărei ieșiri hash. Un salt este un șir aleator adăugat la datele inițiale înainte de aplicarea unei funcții hash. Algoritmii de semnătură digitală, precum DSA sau ECDSA, folosesc numere aleatoare în timpul procesului de semnare. Dacă aceste numere sunt refolosite sau predictibile, cheia privată poate fi derivată, compromițând semnătura. Din acest motiv, calitatea generatoarelor de numere aleatoare este esențială în acest caz.

În protocoalele de schimb de chei, cum ar fi Diffie–Hellman sau ECDH, se generează parametri aleatori care sunt utilizați pentru a calcula chei partajate între părți. Calitatea acestor numere influențează direct securitatea sesiunii. O altă aplicabilitate în criptografie este în cazul generării nonce-urilor. Acestea sunt numere care se folosesc o singură dată, sunt esențiale în protocoalele de autentificare, semnătură și criptare. Ele previn reluarea atacurilor (replay) și oferă unicitate pentru fiecare tranzacție sau sesiune.

CONCLUZII

Generatoarele de numere aleatoare reprezintă un element fundamental în numeroase domenii, de la criptografie și securitate informatică până la modelare matematică, servicii bancare sau jocuri de noroc. Articolul a evidențiat diversitatea acestor generatoare, clasificându-le în deterministe,

nedeterministe și hibride, fiecare cu propriile caracteristici, avantaje și limite. Modalitățile de implementare analizate au arătat că alegerea unui generator adecvat depinde, în mod direct, de contextul de utilizare, de cerințele de performanță și, mai ales, de nivelul de securitate dorit. Importanța testării riguroase, prin suite precum NIST SP 800-22 sau AIS 31, și conformitatea cu standarde recunoscute internațional, evidențiază rolul central pe care validarea aleatorismului îl joacă în garantarea securității și realizării unui sistem robust. În concluzie, generarea corectă și sigură de numere aleatoare nu este un detaliu tehnic secundar, ci o componentă esențială pentru construcția de sisteme fiabile, sigure și performante. Într-o lume digitală tot mai interconectată și supusă riscurilor, înțelegerea și aplicarea corectă a acestor concepte devine o necesitate, nu o opțiune.

BIBLIOGRAFIE

1. BARKER Elaine, John Kelsey, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, NIST Special Publication 800-90A Rev. 1, National Institute of Standards and Technology, US Department of Commerce, Iunie 2015, 101 p.
2. BARKER Elaine, John Kelsey, *Recommendation for Random Bit Generator (RBG) Constructions*, NIST Special Publication 800-90C (Second Draft), National Institute of Standards and Technology, US Department of Commerce, Aprilie 2016, 79 p.
3. BASHAM E. Lawrence III, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, Special Publication 800-22 Revision 1a, National Institute of Standards and Technology, US Department of Commerce, Aprilie 2010, 131 p.
4. BUDIMAN Arif, Bulolo Efori, Saputra Imam, ”Middle Square Method Analysis of Number Pseudorandom Process”, *The International Journal of Informatics and Computer Science*, vol. 4, nr. 2, 2020.
5. JAGANNATAM Archana, *Mersenne Twister – A Pseudo Random Number Generator and its Variants*, 2010.
6. TURAN Meltem Sonmez, Elaine Barker, John Kelsey, Kerry A. McKay, Mary L. Baish, Mike Boyle, *Recommendation for the Entropy Sources Used for Random Bit Generation*, NIST Special Publication 800-90B, National Institute of Standards and Technology, US Department of Commerce, Ianuarie 2018.
7. *** Bundesamt fur Sicherseit in der Informationstecknik, *Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren*, Version 3.0 (15.05.2013); https://www.bsi.bund.de/dok/6618284.
8. *** Bundesamt fur Sicherseit in der Informationstecknik, *Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren* Version 3 (15.05.2020); https://www.bsi.bund.de/dok/6618252.

[1] Lawrence E. Basham III, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, Special Publication 800-22 Revision 1a, National Institute of Standards and Technology, US Department of Commerce, Aprilie 2010.

[2] Elaine Barker, John Kelsey, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, NIST Special Publication 800-90A Rev. 1, National Institute of Standards and Technology, US Department of Commerce, Iunie 2015.

[3] Meltem Sonmez Turan, Elaine Barker, John Kelsey, Kerry A. McKay, Mary L. Baish, Mike Boyle, *Recommendation for the Entropy Sources Used for Random Bit Generation*, NIST Special Publication 800-90B, National Institute of Standards and Technology, US Department of Commerce, Ianuarie 2018.

[4] Elaine Barker, John Kelsey, *Recommendation for Random Bit Generator (RBG) Constructions*, NIST Special Publication 800-90C (Second Draft), National Institute of Standards and Technology, US Department of Commerce, Aprilie 2016.

[5] *** Bundesamt fur Sicherseit in der Informationstecknik, *Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren*, Version 3.0 (15.05.2013); https://www.bsi.bund.de/dok/6618284.

[6] *** Bundesamt fur Sicherseit in der Informationstecknik, *Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren*, Version 3 (15.05.2020); https://www.bsi.bund.de/dok/6618252.