Anul XVIII nr. 2/2026

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

GEOPOLITICĂ ȘI GEOECONOMIE

Europa (UE) încotro?
Daniel DĂIANU *5*

PERSPECTIVE GEOPOLITICE ȘI GEOSTRATEGICE

Noua arhitectură de securitate. Puteri mijlocii, puteri minore și minilaterale în reașezarea globală contemporană
Iulian CHIFU *15*

„Capcana lui Tucidide" și relevanța ei în secolul al XXI-lea
Ionuț-Răzvan BUCUR *33*

Pivotul tăcut al Eurasiei: Kazahstanul și fereastra strategică 2026–2035
George MINEA *46*

RĂZBOAIELE SECOLULUI XXI

Criza de securitate din Europa de Est: dinamici geopolitice și tehnice în conflictul ruso-ucrainean
Andreea-Amalia POPESCU-STĂNICĂ, Mihai-Laurențiu ZARIA *55*

Operațiile UAS în armata ucraineană și transformarea războiului într-un joc video – „armata de drone"
Ciprian-Constantin VOINEA *67*

Criminalitatea informatică în UE: evoluția amenințărilor cibernetice în contextul conflictului F.Rusă-Ucraina
Cosmin CÎRLAN *75*

TRANSFORMAREA MILITARĂ

Dilema control–inițiativă în conducerea operațiilor: condiționări organizaționale ale comenzii prin misiune

Radu PRIOTEASA *87*

INTELLIGENCE

How Artificial Intelligence could benefit HUMINT

Fred P. HOFFMAN, Tyler MORITZEN, Matthew BELLES, Colin TARDIF, Ryan MAHONEY *96*

EUROPA (UE) ÎNCOTRO?[1]

Academician Daniel DĂIANU[*]

Abstract

We seem to be at the end of an era. The demise of the old global order is already being talked about in a way that creates a lot of discomfort[2]. Uncertainty, unpredictability and insecurity at extreme levels are felt in markets, economies and political life, as well as in the diminished relevance of economic and political forecasts and scenarios. The international environment has not been so disrupted for many years, perhaps since the global financial crisis. Currently, an increasingly pressing geopolitical dynamic intervenes, with ongoing military conflicts in several regions of the globe.

How long Europe can count on the "security umbrella"provided by the Unites States was an unthinkable question until recently. From this perspective, Europe (EU) faces a series of challenges generated or accelerated by the new mandate of Trump Administration: a geopolitical shock, the application of Realpolitik ideas in interstate relations, an economic shock, the weakening of multilateralism in the institutional organization of the international system, or the confrontation between democracy and illiberalism (autocracy).

Keywords: *world order; european security; realpolitik; multipolarity; economic shock; defence spending; liberalism; autocracy.*

CONTEXT GENERAL

În ultimul an și jumătate a fost consternare între liderii europeni după mutările Administraţiei Trump în politica de securitate la nivel euro-atlantic şi în cea economică. Relaţia SUA cu F.Rusă a părut a fi privilegiată la Washington, iar un război economic şi comercial este în curs, cu tarife mult crescute[3] aplicate de actuala administrație europenilor, Canadei, Mexicului și multor alte ţări. Totodată, nu solicitarea Washingtonului ca europenii să aloce mai mult pentru apărare nedumereşte, ci viteza cerută pentru adaptare şi modul în care, peste Ocean, s-a procedat la reevaluarea relaţiei cu Rusia[4]. Surprinzătoare sunt şi revendicările administraţiei americane privind Groenlanda, teritoriu ce este parte din Danemarca, la rândul ei stat membru al NATO.

Europenii trebuie să mărească considerabil cheltuielile de apărare pentru a-și asigura securitatea -- pornind de la noua abordare a SUA privind încetarea focului în Ucraina și relația cu Moscova. Cheltuielile anuale de apărare s-ar ridica la procente din PIB pentru numeroase ţări, ceea ce poate destabiliza bugetele publice, în lipsa unor măsuri adecvate. Europenii au nevoie, în continuare, de sprijin militar din partea SUA (un *backstop*), în timp ce lideri importanţi din

[*] ***Daniel Dăianu a fost economist-șef al Băncii Naționale a României (1992-1997), ministru al Finanțelor (1997-1998) și membru în Consiliul de Administrație al Băncii Naționale a României (2014-2019). În prezent este președinte al Consiliului Fiscal.***

UE reiau tema „autonomiei strategice” (ce are accente gaulliste[5]). De altfel, oficialii europeni declară că ne îndreptăm către „o nouă ordine mondială”[6].

Asigurarea securității militare în Europa este de judecat într-un context economic, social și politic tot mai complicat. Criza financiară (2008), favorizată de excese ale industriei financiare și neglijența guvernelor și autorităților de reglementare și supraveghere, a accentuat tensiuni și fracturi sociale, a generat nemulțumire față de „elite” (*establishment*), în timp ce costul pentru bugetele publice a fost covârșitor. A urmat pandemia, care a dus la extinderea operațiunilor neconvenționale ale băncilor centrale și a mărit cheltuielile guvernamentale, împovărând în plus bugetele publice. Tranziția energetică și schimbările climatice au afectat și acestea bilanțurile publice și private, iar invazia Rusiei în Ucraina (inițiată în 2022) a amplificat efectele negative, a accentuat criza costului vieții (crescând mult costul energiei pentru europeni) și a intensificat confruntările hibride. Noile tehnologii, în special prin intermediul social media, transportă informaţie abundentă, dar creează multă confuzie şi adâncesc clivaje în societate, fragmentând-o. Inteligența artificială (IA) este o dominantă a vremurilor noastre: ea deschide oportunități fără limite, dar vine cu incertitudini imense; IA favorizează concentrarea puterii, poate spori inegalităţile economice şi sociale, inclusiv între ţări, și alimentează cursa noilor arme[7].

Contextul geopolitic tot mai tensionat a făcut din accesul la resurse şi materii prime (materiale) rare un obiectiv central al politicii de securitate pentru ţările cele mai puternice. Administraţia Trump judecă din această perspectivă şi a proximității geografice statutul Groenlandei sau chestiunea Canalului Panama, în timp ce China are o prezență economică activă în numeroase regiuni ale globului din aceleaşi considerente. Se poate vorbi, şi pe fondul schimbărilor climatice ca ameninţare existenţială, de o formă de *darwinism economic*.

Economia globală continuă să se fragmenteze, cu tendinţe mai clare de formare de blocuri comerciale şi regionalizare a lanţurilor de aprovizionare – inclusiv din raţiuni de securitate. Multilateralismul în relaţiile internaţionale slăbeşte. SUA încearcă să folosească moneda proprie ca instrument de protecţie economică şi are în vedere un nou „acord valutar”, care să influenţeze mişcări de capital şi comerciale.

În viața politică are loc o ascensiune a radicalismului, a curentului (ultra)conservator (și ca o contrareacție la mișcarea *woke*)[8], alunecarea unor democraţii către *anocraţii*[9], în timp ce repere ale democrației sunt puse în discuție. Multe guverne ale unor ţări democratice nu asigură bunuri publice în conformitate cu aşteptările cetăţenilor, ceea ce accentuează tensiuni sociale şi politice. Din acest punct de vedere, Martin Wolf vorbeşte despre o criză a capitalismului democratic[10]. Că democraţia priveşte, în esenţă, mecanisme de control reciproc instituţionalizate, care să prevină concentrarea abuzivă a puterii, arbitrariul în viaţa publică, pare să fie o idee subestimată în mod deliberat. Este pus în discuţie, uneori, însuşi conţinutul democraţiei în politica contemporană. O primă viziune ar fi cea tradiţională, ce priveşte democraţia ca „metodă” de a rezolva dispute şi, utilizând controale reciproce instituționalizate, de a preveni concentrarea puterii; altă viziune priveşte democraţia ca mijloc de a da voce, putere, cetăţenilor, chiar dacă s-ar renunţa la valori liberale[11]. Astfel, în lume are loc o confruntare ideologică între democraţie şi autocraţie (iliberalism)[12], ce se manifestă atât în relaţiile dintre state, cât şi în interiorul acestora.

Ascensiunea economică și tehnologică a Chinei, din ultimele decenii, a transformat-o în marele rival geopolitic al SUA, într-o lume multipolară. Doctrina de securitate a SUA relevează acest fapt de ani buni, într-o lume ce a depăşit momentul de „unipolaritate” instaurat imediat după căderea Zidului Berlinului.

REALPOLITIK IESE ÎN FAȚĂ

Suita de șocuri adverse mari (crizele evocate mai sus) s-a desfăşurat în condițiile eșecului globalizării neînfrânate[13], care a resuscitat protecționismul; crizele sunt însoțite de o

slăbire a cadrului multilateral, de ieșirea în față a *Realpolitik* în raporturile dintre marile puteri și între acestea și alte state. Se vorbește voalat, sau chiar deschis, de „sfere de influență", de importanța *hard power* în relațiile dintre state, în timp ce *soft power* își diminuează relevanța (din păcate). Discursul președintelui Donald Trump la ceremonia de la Academia West Point, din 24 mai 2025, a fost elocventă din acest punct de vedere[14].

Viziunea *Realpolitik* de peste Ocean era detectabilă în mediul academic (John J. Mearsheimer, de exemplu[15]), în centre de reflecţie strategică (RAND Corporation[16], Heritage Foundation, Quincy Institute for Responsible Statecraft), în reviste de politică externă (de exemplu, texte semnate de Richard Haass, Andrew Bacevich, Stephen Wertheim sau Graham Allison în revista *Foreign Affairs*[17]), la politicieni (actualul vicepreședinte JD Vance[18] sau Elbridge Colby, numărul doi acum în Pentagon, însărcinat cu *defense policy*[19]). Unii oficiali ai Administraţiei Trump vorbesc chiar de o nouă „doctrină Monroe", ca expresie a neo-izolaționismului (protecţionismului comercial) şi concentrării pe rivalitatea geopolitică cu China. Această gândire poate fi pusă în relaţie cu conceptul de *overstretch* (supraextindere), pe care Paul Kennedy l-a folosit cu decenii în urmă pentru a scruta limite ale puterii strategice a SUA[20]. Intervenţiile controversate în Irak şi Afganistan, ascensiunea economică şi tehnologică a Chinei şi glisarea puterii economice, la nivel global, către Asia au contribuit probabil la această schimbare de optică privind securitatea militară.

Într-o lume multipolară, țări dintre cele mai puternice par să relativizeze, chiar să lase în uitare, normele de drept internațional ce au ghidat (mai mult sau mai puțin) relațiile internaționale după Al Doilea Război Mondial şi în cadrul cărora instituţii multilaterale au jucat un rol-cheie. Şi este de subliniat că *normele de drept, în relaţiile internaţionale, au ajutat cel mai mult statele mici, mai ales în momente foarte grele.*

Adepţii *Realpolitik* se pot înşirui în analize şi sfaturi alături de George Kennan şi Hans Morgenthau, nume cu rezonanţă ale acestui filon de gândire strategică. Ideile *Realpolitik* contrastează cu gândirea neo-conservatoare (neocons)[21], care a dominat politica de securitate a SUA în ultimele decenii. Dar logica „balanţei de putere" nu trebuie să semnifice că se poate face orice în relaţiile interstatale, ca într-o „junglă". Kennan şi Morgenthau vedeau în instituţiile internaţionale temelii ale unei ordini mondiale care să prevină războaiele între marile puteri. Este de notat distincția pe care Thierry de Montbrial, fondator al IFRI (Institutul Francez de Relații Internaționale), o face între „abordarea realistă" și Realpolitik: prima abordare nu subestimează regulile și instituțiile în relațiile internaționale, dar ține cont de realitatea rece a unor relații de putere și interese naționale[22].

Conferința pentru Securitate de la München, din februarie 2025, a fost cea care a venit cu anunțuri șocante pentru europeni, care vedeau relația transatlantică drept fundamentul NATO (în calitate de organizație de apărare colectivă). De ani buni, încă din 2011, când Secretarul Apărării al SUA era Robert Gates, s-a reproșat partenerilor europeni că nu cheltuiesc suficient pentru apărare, deşi americanii au avut de câştigat în multe privinţe în virtutea statutului de hegemon geopolitic şi economic. În primul său mandat, președintele Trump a subliniat această nemulțumire, ce a fost întărită în ultimul an. Se cere europenilor să aloce considerabil mai mult pentru apărare, ținta fiind 5% ca pondere în PIB.

Dezangajarea, fie şi parţială, a SUA din Europa (ce ar fi motivată de rivalitatea globală cu China), anunţată de Casă Albă, este o lovitură grea pentru NATO și pune presiune mare pe țările și economiile statelor din UE. Cum și în ce condiții se vor realiza încetarea focului și pacea în Ucraina este de văzut; există necunoscute și dileme mari, inclusiv problema garanţiilor de securitate. Dar este clar că UE are nevoie de o capacitate de apărare superioară. Și are nevoie, totuşi, de cooperare cu SUA, care domină din punct de vedere militar și tehnologic NATO; multe achiziţii de echipament militar se fac, de altfel, din SUA.

Există un aspect ce trebuie să fie subliniat: *prezența americană postbelică în Europa a stăvilit animozităţi şi resentimente istorice*

între unele state europene. Plecarea SUA din Europa, fie și graduală, ar putea renaşte fantome ale trecutului. UE este un proiect ce a avut în vedere, în primul rând, pacea în Europa, nu numai reconstrucţia economică. Prin urmare, dezangajarea americană combinată cu o Uniune caracterizată de divergențe, neînţelegeri mari și de o coeziune slabă ar fi combustie periculoasă pentru vechiul continent. Europa are nevoie de aranjamente de securitate, aşa cum au fost acordurile de la Helsinki (1975), cu atât mai mult cu cât s-a intrat deja într-un nou Război Rece, iar această situaţie este de văzut la scară globală, China fiind marele rival geopolitic al SUA. În acest context, SUA trebuie să facă parte din noua arhitectură europeană de securitate.

Cât de ameninţate se simt statele europene se vede din declaraţiile preşedintelui Poloniei, care a evocat posibilitatea de obţinere a armei nucleare, din atitudinea cancelarului Germaniei, Friedrich Merz, care vrea independență militară faţă de SUA (o declaraţie stupefiantă dacă avem în vedere statutul Germaniei după Al Doilea Război Mondial şi istoria europeană), și din disponibilitatea Franţei de a oferi „umbrela nucleară" pentru celelalte ţări din UE[23].

Dialogul inițiat anul trecut de președintele Trump cu liderul de la Moscova, dincolo de obiectivul declarat de a stopa războiul în Ucraina, poate fi interpretat și ca o încercare de a face o breșă în BRICS, de a decupla Rusia de China. Dar acest obiectiv este de pus în balanţă cu riscul îndepărtării posibile a ţărilor din Europa democratică. Şi este posibil ca, drept replică, europenii (UE) să-și dezvolte relaţiile cu China şi India, ca tentativă de ieşire din impas şi pentru a avea mai mult spaţiu de manevră.

Sunt mize geopolitice mari, ce pot lăsa țările europene (UE) în poziție periferică şi cu o capacitate de apărare precară. Președintele Trump a avut discuții și cu președintele Chinei. Din punct de vedere al controlului armamentului nuclear, al combaterii pandemiilor, din perspectiva utilizării IA, asemenea discuții au sens. Dar dacă „lăsarea din braţe" a europenilor şi un inerent „efect de demonstraţie" ar declanşa o nouă cursă a înarmării, pentru obţinerea vectorului nuclear, unde se va ajunge?

O problemă pentru europeni priveşte cine este persoana sau instituția cea mai autorizată să vorbească cu administraţia americană, să participe la eventuale negocieri; la fel cum Henry Kissinger (tot un adept al *Realpolitik*) întreba, cu multe decenii în urmă, cui să dea telefon în Europa. Pe de altă parte, noua politică de securitate a SUA poate induce mai multă coeziune în UE, o strângere a relaţiilor militare, şi nu numai, cu alte ţări (ex.: cu Regatul Unit, în special). Se spune, de altfel, că dezangajarea SUA din Europa ar putea conduce la un „moment hamiltonian"[24] pentru UE, cu efecte de adâncire a cooperării militare şi economice, inclusiv cu formarea unei *capacităţi fiscale* comune.

ȘOCUL ECONOMIC: UN „MOMENT HAMILTONIAN" PENTRU UE?

Tarifele comerciale aplicate pe scară largă, măsurile dezordonate ce amplifică incertitudinea și imprevizibilitatea pe pieţe pot conduce la inflaţie mai înaltă, la stagnare economică (stagflaţie) și la recesiune. Băncile centrale ar fi puse în situaţia ingrată de a crește ratele de politică monetară din nou, în condiţiile în care economiile îşi pierd din suflu. Și este de văzut dacă cheltuielile sporite de apărare (un „keynesism" militar) ar contrabalansa factorii ce încetinesc economiile – având în vedere gradul de incertitudine și aversiunea la riscuri din mediul privat. Totodată, cheltuielile sporite de apărare deturnează resurse de la acoperirea nevoilor civile, ceea ce poate accentua tensiuni sociale şi politice. Se poate recurge la împrumuturi, dar există limite din acest punct de vedere. Decizia Germaniei de a renunța la limita îndatorării pentru a-și permite cheltuieli sporite pentru apărare și infrastructură poate ajuta creșterea economică în UE, însă cât de semnificativ poate fi acest lucru rămâne de văzut.

Poate şocul reprezentat de măsurile SUA să inducă o creştere a coeziunii în UE în anumite domenii? Se poate prezuma că da, dacă se va avansa pe calea formării unei „capacităţi fiscale"

comune, dacă o „comunitate europeană pentru apărare" ar deveni realitate, dacă pieţele interne din UE se vor integra mai bine. Dar există numeroase imponderabile, inclusiv faptul că UE nu este, totuşi, un stat federal; coordonarea politicilor naţionale şi luarea unor decizii comune rămâne o mare problemă în Uniune[25]. Că în Canada se imaginează o alăturare la blocul comercial al UE[26] spune mai mult despre şocul administrat de tarifele americane şi sugestia Casei Albe ca vecinul de la nord să devină al 51-lea stat american, decât despre forţa şi perspectivele UE. O întrebare este şi în ce scenariu Canada ar putea intra în UE, deşi pare poate o fantezie.

Trebuie subliniat că simpla adunare a PIB-urilor naţionale din UE şi a capacităţilor militare (tancuri, avioane, personal militar în armatele naţionale etc) este un exerciţiu simplist în a proiecta o forţă de descurajare împotriva unor agresiuni; este nevoie de mai mult în acest scop şi, în principal, de capabilităţi combinate în mod organic şi de acţiuni comune, de integrare mai adâncă.

Euro ar putea câştiga greutate în tranzacţiile internaţionale (în care deţine acum în jur de 20%, conform datelor BCE) dacă zona euro va fi mai coezivă și dacă o capacitate fiscală comună se va forma. Creşterea economică în UE ar putea fi sprijinită dacă cheltuielile mai mari pentru apărare ar avea efect de multiplicare semnificativ[27]. În această ecuaţie apare decizia din Germania de a elimina restricţia la îndatorare.

Accentul pus de Casă Albă pe dereglementare în domeniul financiar (inclusiv privind activele cripto) este un pericol pentru stabilitatea financiară. O nouă dereglementare a sistemului financiar, în combinaţie cu lipsa de reglementare a IA, poate aduce necazuri mari pe pieţele financiare. Şi este discutabilă logica includerii unor active cripto în rezervele SUA atât timp cât dolarul este oricum moneda de rezervă principală a lumii. Presiunea către dereglementare a pieţelor financiare există şi în Europa, pe fondul dificultăţilor economice, dar prea uşor se uită lecţiile crizei financiare izbucnite în 2008[28].

Războiul comercial poate antrena unul valutar, cu implicaţii privind funcţionarea pieţelor financiare și dinamica investiţiilor. A mai fost un episod asemănător, ce a provocat un cutremur în sistemul financiar internaţional: în 1971, Administraţia Nixon a anunţat renunţarea la legarea dolarului de aur, ceea ce a dat o lovitură mortală sistemului de la Bretton Woods[29] (care avea ca ax central această legătură[30]) şi care se baza pe cursuri fixe, dar ajustabile. După ruperea acestei legături, s-a trecut la cursuri de schimb flotante, la creşterea masivă a mişcărilor de capital. Stephen Miran, consilier economic al Administraţiei Trump, vorbeşte despre un „Mar-a-Lago Accord" (un Plaza 2) care să taxeze (inclusiv prin tarife) alte țări pentru beneficiul de a folosi moneda americană ca rezervă valutară; scopul ar fi de a reduce deficitul comercial al SUA[31]. Totul se încadrează într-o „logică tranzacţională" de tipul *quid pro quo*: avantajele oferite de SUA (inclusiv protecţie militară) să fie compensate de beneficiari într-un fel sau altul. Trebuie spus că o schimbare tectonică pentru sistemul financiar internaţional a fost şi Big-Bang-ul londonez din 1986, de dereglementare a sistemului financiar, care a fost urmat de abolirea regimului Glass-Steagall în SUA (ce era parte din reformele New Deal ale preşedintelui Franklin Delano Roosevelt). Această dereglementare a favorizat financiarizarea sistemelor economice, operaţiuni speculative și a fragilizat sistemul financiar şi economiile, în ansamblu[32].

Sentimentul în rândurile Administraţiei Trump este că e necesară o politică care să readucă în SUA industrii strategice de bază (de exemplu, microprocesoare), fără de care puterea industrială şi tehnologică în confruntarea cu China este periclitată. Nevoia unei politici industriale mai ferme s-a observat şi în mandatul preşedintelui Biden (prin The Inflation Reduction Act), cum a fost articulată şi de consilerul său pe securitate naţională, Jake Sullivan[33]. Dar acum politica americană se profilează ca o îmbinare de naţionalism economic (protecţionism) agresiv şi neo-izolaţionism. De remarcat că protecţionismul strategic a fost propovăduit de Clyde Prestowitz cu decenii în urmă, acesta având în vedere ascensiunea economică a Japoniei[34], care invadase piaţa americană cu automobile şi produse electronice[35]. Acum este vorba însă despre o ţară, China, care are datele economice,

tehnologice şi demografice de a fi un competitor mult mai puternic pentru SUA decât Japonia cu ani în urmă.

Unii încearcă să descrie competiţia dintre SUA şi China în termeni de „geoeconomie" (*geoeconomics*) şi este adusă în discuţie o lucrare a lui Albert Hirschman, din 1945, *National Power and the Structure of Foreign Trade*[36]; Hirschman studiase protecţionismul, autarhia, fenomene ce defineau vremurile de război. Analizele trebuie, însă, să aibă în vedere că lumea de astăzi este mult mai interdependentă economic şi tehnologic, chiar dacă fragmentarea şi regionalizarea s-au accentuat în ultimul deceniu, inclusiv ca rezultat al crizelor şi din raţiuni de securitate.

Recomandările lui Stephen Miran, ce încearcă să ofere susţinere teoretică „doctrinei Trump" în relaţiile cu celelalte ţări, pot conduce la perturbaţii majore pe plan internaţional, la contracţie economică şi puseuri inflaţioniste, ce ar putea avea un efect de bumerang chiar pentru economia americană[37]. Un efect neintenţionat ar putea fi un euro cu influenţă mai mare în relaţiile internaţionale, mai ales dacă zona euro ar avea mecanisme mai bune de funcţionare.

În cursul anului 2025 SUA au anunţat retragerea din unele organizaţii internaţionale, ceea ce se înscrie în politica de renunţare la multilateralism în relaţiile internaţionale. Să ne imaginăm ce s-ar întâmpla dacă Washingtonul ar renunţa să sprijine FMI şi Banca Mondială, deşi tot *Realpolitik* ar dicta să nu o facă întrucât China ar fi probabil gata să suplinească, nu numai financiar, un asemenea pas. Iar europenii nu ar sta pe margine. Fapt este că la ultimele reuniuni ale FMI şi BM, secretarul trezoreriei americane, Scott Bessent, a reafirmat sprijinul SUA pentru cele două organizaţii internaţionale, dar a cerut o reformă a agendei acestora.

În noul context economic şi geopolitic, UE va fi obligată să mobilizeze resurse interne, între altele, de redeschidere de mine, de resuscitare a industriei de oţel. Și aceste măsuri ar fi parte dintr-o politică industrială pe care Uniunea o avea în vedere pentru a rezista în competiţia globală. Acum, însă, intervin considerente de securitate militară.

RESURSE SPORITE PENTRU APĂRARE[38] LA NIVELUL UE

O capacitate de apărare superioară, eficace, reclamă considerabil mai multe resurse alocate domeniului militar în statele membre din UE și o cooperare militară mai adâncă între acestea în producţie şi achiziţii de armament. Pandemia a fost un fel de război, dar acum este vorba despre arme militare propriu-zise, de capacitate de a răspunde și la atacuri cibernetice/hibride.

Comisia Europeană (CE) a pus în practică un plan de cca. 800 miliarde de euro pentru apărare, căutând modalităţi de finanţare publică şi privată. S-a decis recurgerea la clauza derogatorie (*escape clause*) privind regulile fiscale pentru o perioadă de patru ani, dar efectele pentru datoriile publice și deficite nu pot fi evitate. Bugetele naționale și cel al UE vor suferi probabil o restructurare, care să prevadă resurse noi destinate apărării; tendințele de trecere la „economii de război" vor fi evidente. Instituțiile financiare specializate europene au de jucat un rol important în acest sens – Banca Europeană de Investiții este menţionată în mod expres de documente ale CE. Garanţii de stat care să mobilizeze resurse din sectorul privat pot fi avute în vedere – așa cum o face o inițiativă a guvernului italian[39].

Alocarea unor resurse mai mari pentru apărare este de judecat în raport cu implementarea programului de creștere a competitivității UE (apropo de Raportul Draghi, Raportul Letta etc). Fiindcă o industrie de apărare mai dezvoltată în ţările UE nu înseamnă automat competitivitate de ansamblu sporită; pot creşte exporturi de armament, dar UE are oricum surplus de cont curent (România cu deficitul său foarte mare este un caz aparte). Media în UE a cheltuielilor pentru apărare, la nivelul statelor membre, a fost în jur de 2% din PIB. Să ajungi la 5% din PIB, dacă admitem exigența maximală a SUA, semnifică mai mult decât o dublare, ca medie, a acestor cheltuieli pentru țările din UE; ar fi un șoc pentru bugetele publice, chiar dacă se poate argumenta că pentru apărare, securitate, nu trebuie să eziți[40]. Realist este să credem că se va ajunge la o medie

în UE de cca. 3,5% din PIB, dar cu diferenţe între state.

Suspendarea din nou a regulilor fiscale, şocul necesităţii de reînarmare, nu pot escamota îngreunarea situaţiilor bugetare. Este de notat că această suspendare nu s-ar aplica la toate cheltuielile de apărare, ci numai la creşterea acestora şi doar pentru o perioadă de patru ani. Altfel spus, după patru ani, consolidarea fiscală ar trebui să intre în acţiune peste tot, dar de la un nivel mai înalt.

Mobilizarea unui volum atât de mare de resurse este un proces complicat. În plus, este necesară armonizarea poziţiilor statelor membre din UE privind dezvoltarea industriei de apărare în Europa, achiziţii comune (din Europa și din afară). Uniunea mizează şi pe cooperarea în domeniul militar cu Marea Britanie, Norvegia, Canada, Turcia și, eventual, alte ţări, însă fondul de apărare de 150 miliarde euro este destinat finanţării de armament cu precădere din state UE.

Dezvoltarea industriei de apărare în UE poate fi un mare proiect comun, cum a fost Airbus, o adaptare la noua realitate geopolitică a politicii industriale europene. Întrebarea este dacă un asemenea program (admiţând că s-ar realiza la parametrii imaginaţi) poate conduce la inovaţie intensă, la recuperarea decalajelor faţă de SUA şi alte ţări. Acest program are nevoie de o colaborare strânsă, sistematică, între ţările angrenate.

CĂTRE CE ORDINE MONDIALĂ MERGEM?

O lume multipolară este mai complicată întrucât îngreunează ajungerea la înţelegeri privind probleme capitale – cum sunt proliferarea armelor de distrugere în masă, combaterea pandemiilor, schimbarea climatică, etc., în timp ce balanţa de putere, privită în dinamica ei, implică competiţie pentru resurse şi cursa înarmărilor. Este drept că se pot imagina acorduri care să stăvilească această cursă (mai ales un control al armelor nucleare) sau privind utilizarea inteligenţei artificiale[41], care, în sine, poate reprezenta şi ea o ameninţare existenţială[42].

Lumea spre care mergem este una dominată de forţa economică, tehnologică și militară a SUA şi a Chinei, ca superputeri globale. Rusia, care are capacităţi militare de temut, încearcă să revină în ecuaţia de putere din Europa prin formarea unei sfere de influenţă proprii. De altfel, cu o logică de *Realpolitik* tot mai intensă în relaţiile interstatale, sferele de influenţă revin în actualitate.

Locul UE în viitoarea ordine globală depinde de modul în care îşi va dezvolta vectori de forţă – economică, tehnologică şi militară. Iar din acest punct de vedere, trebuie spus că Uniunea are de rezolvat probleme majore ce derivă, esenţialmente, din faptul că nu are o structură de guvernanţă de tip federal[43], iar mecanismele alternative se lasă aşteptate. Şi nu este clar dacă războiul din Ucraina şi provocările globale vor înclina balanţa în favoarea unor procese de dezvoltare a coeziunii interne. În materie de securitate, UE trebuie să coopereze cu state din afara Uniunii – Regatul Unit, Norvegia, Islanda etc.

Ordinea mondială depinde și de tensiunile interne din diverse țări, care sunt alimentate de cauze economice, „războaie culturale” (între, de exemplu, conservatori şi progresişti, între generaţii[44]), de progresul tehnologic (impactul IA), aglomerarea urbană, demografie, îmbătrânirea populaţiei etc. Şi, peste toate, se desfăşoară confruntarea dintre autocraţie şi democraţie (liberalism – ce nu trebuie confundat, însă, cu pieţe neînfrânate[45]). Crizele au favorizat accente autoritariste şi în societăţile democratice, ceea ce am numit „sindromul civilizaţiilor hidraulice”, făcând referire la perspectiva ca lupta pentru hrană şi apă să ducă la ceea ce istoricul german Karl Wittfogel numea „civilizaţii hidraulice”[46].

Dezordinea în lume se poate accentua dacă societăţile vor fi mai fragile, cu funcţii de reglare economică şi socială erodate, cu tentaţii autoritariste în proliferare. Robert D. Kaplan identifică asemenea tendinţe în *The Coming Anarchy*[47], pe care le vede mai pregnante în ultimii ani; acesta vorbeşte despre slăbirea democraţiei în lume, de un „Weimar global”[48]. Kaplan face adesea referire în argumentaţia sa la Oswald Spengler (cel care a vorbit despre declinul Occidentului acum mai bine de 100 de ani[49]) şi aminteşte de Aleksandr Soljeniţîn

(faimosul dizident anticomunist rus şi conservator ca viziune politică). Sunt şi alte lucrări care caută să desluşească cauze pentru slăbirea democraţiei în lume[50].

SECURITATEA ÎN EUROPA

Creșterea cheltuielilor pentru apărare este necesară pentru că lumea devine mult mai periculoasă și parcă lipsită de reguli, cu multă dezordine şi pericole la tot pasul[51]. Pierderea „dividendului păcii" era clară de ceva timp. Și există o expresie validată de istorie, cu relevanță pentru vremurile noastre: când „elefanții se luptă", vai de iarbă, de cei mici.

Este în interesul României și al celorlalte țări europene ca Uniunea să fie mai coezivă și să își dezvolte capacitatea proprie de apărare (industria de armament), iar NATO să nu slăbească. Industria de apărare în România trebuie să se dezvolte și aranjamentele de tip *offset* ar susţine acest scop. Dar industria de apărare a României nu trebuie să fie gândită în afara acţiunilor conjugate la nivel european (UE). De asemenea, este vital ca relația transatlantică să nu se erodeze fatalmente și trebuie să fie evitat un război comercial de anvergură şi prelungit între SUA și UE; un astfel de conflict ar provoca pagube mari, putând destabiliza chiar și economia globală (am putea asista la noi puseuri inflaţioniste, la recesiune pe ambele maluri ale Atlanticului, iar economia României ar fi puternic lovită).

Relația cu SUA trebuie să fie aprofundată, așa cum trebuie să avem relații fructuoase cu Franța, Marea Britanie, Germania, Italia și, nu în ultimul rând, cu Polonia. Turcia merită atenție din acest punct de vedere, ea fiind o putere regională cu influență tot mai mare. Țările cu care ne învecinăm intră, desigur, în ecuația de securitate. În noul context, diplomația va fi tot mai complexă și se va desfășura atât pe traseul intereselor colective, cât și prin relații bilaterale.

NATO trebuie să rămână o organizație relevantă, ce asigură garanții de securitate pentru statele membre, cu un Articol 5 funcțional, și este de dorit ca SUA să nu neglijeze NATO. Importanța UE pentru România este greu de subestimat, deoarece Uniunea s-a născut, în principal, ca un proiect de pace – deci nu numai pentru reconstrucție economică. O Uniune mai divizată, mai fragilă, ar fi de rău augur pentru securitatea europeană; ne-am putea întoarce către o istorie cenuşie a Europei, un exemplu fiind perioada interbelică. Remarca este valabilă și pentru NATO[52]. Pe acest fundal, anii care vin vor fi marcaţi de confruntarea dintre democraţie şi autocraţie și de tensiuni geopolitice.

[1] Acest text preia din Introducerea la volumul meu *Crizele și tentația autoritaristă* (Iași, Polirom 2025) și dintr-un alt text semnat de mine în *România – Zona Euro, Monitor*, nr. 18, 2025. Ideile principale au fost prezentate și în cadrul seminarului internațional "Penser l'Europe" (București, 2-3 octombrie 2025). O variantă în limba engleză, "The Security of Europe (EU) and *RealPolitik* – The Transatlantic Relationship Is in Great Danger", a apărut în *Romanian Journal of European Affairs*, vol. 25, nr. 1, June 2025.

[2] Martin Wolf, „The old global order is dead", *Financial Times*, 7 mai 2025.

[3] Care amintesc de legislația protecționistă Smoot-Hawley Tariff Act din 1930, din perioada depresiunii economice.

[4] Vezi și editorialul din *The Economist*, „America's new foreign policy", 15 martie 2025. În text se spune că noua politică externă a SUA a creat o „criză de încredere" profundă în rândurile zecilor de țări care și-au încredințat securitatea în mâinile Americii după Al Doilea Război Mondial. Trebuie menționat, totuși, că semne ale unei noi relații cu Rusia erau observabile din timpul primului mandat al președintelui D.Trump.

[5] Generalul Charles de Gaulle, președinte al Franței după Al Doilea Război Mondial, a fost un susținător ardent al intereselor naționale, în contextul hegemoniei americane în Europa occidentală, în cadrul NATO.

[6] Vezi și Ursula von der Leyen, citată de *Politico*: „EU slams the door on US in colosal defense plan", 19 martie 2025.

[7] Vezi și Henry Kissinger, Eric Schmidt și Daniel Huttenlocher, *The Age of AI*, John Murray Publishers, Londra, 2022.

[8] Are loc un „război cultural", în lumea occidentală, între conservatori și „progresiști". Mișcarea ultraconservatoare poate fi interpretată și ca reacție anti-elite, contra unui stat perceput ca deconectat de la grijile cetățenilor simpli (vezi și Nathan Levine, „The idea at the heart of populism", *New York Times*, 7-8 iunie, 2025). Conflictul poate fi văzut ca fiind între valori tradiționale și o modernitate impusă, uneori parcă forțat, de elite sub forma unei *corectitudini politice*.

[9] Anocrațiile nu sunt autocratii depline, dar nici democrații (Barbara F. Walter, *How Civil Wars Start: And How to Stop Them*, Viking, Londra, 2022). Pentru erodarea democrației în lumea occidentală vezi și Jonathan Sumption, *The Challenges of Democracy and the Rule of Law*, Profile Books, Londra, 2025.

[10] Martin Wolf, *The Crisis of Democratic Capitalism*, Penguin Books, Londra, 2024. Robert Reich spunea, după criza financiară, că sistemul capitalist trebuie să lucreze pentru cei mulți, nu pentru cei puțini (*Saving Capitalism: For the Many, Not the Few*, Vintage Books, New York, 2016), iar Paul Collier introduce repere etice în discuția despre capitalism (*The Future of Capitalism: Facing the New Realities*, Allen Lane, Londra, 2018).

[11] Profesorul indian Pratab Bhanu Mehta a făcut această distincție într-o prelegere la London School of Economics. El spune că democrația implică atât valori, cât și puterea cetățenilor (*empowerment*). Dar când cei care votează se simt marginalizați, ei pot renunța la valorile liberale în favoarea unui lider puternic (vezi Gideon Rachman, „Trump and the two visions of democracy", *Financial Times*, 21 ianuarie, 2025).

[12] Pornind de la puterea copleșitoare a giganților din domeniul tehnologiei informațiilor și comunicațiilor, Yanis Varoufakis vorbește despre „tehnofeudalism" (*Technofeudalism: What Killed Capitalism*, The Bodley Head, Londra, 2023). În contrast, Marc Andreessen și Peter Thiel, antreprenori care dețin companii în domeniul tehnologiei informațiilor, sunt promotori ai unui optimism tehnologic, ai libertarianismului tehnologic (vezi și „The Andreessen-Horrowitz Manifesto", 16 octombrie 2023. Disponibil online: https://a16z.com/the-techno-optimist-manifesto/).

[13] Un „liberalism nedemocratic" (cum spunea Yahsa Mounk în „Illiberal democracy or undemocratic liberalism", *Project Syndicate*, 6 iunie 2016) care a favorizat marea criză financiară.

[14] „Trump gives commencement address at West Point stressing a «New Era»", *New York Times*, 24 mai, 2025.

[15] John J. Mearsheimer, *The Great Delusion: International Dreams and International Realities*, Yale University Press, New Haven, 2018.

[16] Vezi și Samuel Charap, „An unwinnable war: Washington needs an endgame in Ukraine", *Foreign Affairs*, iulie/august 2023. În același număr din *Foreign Affairs*, Carter Malkasian pledează pentru un armistițiu în Ucraina pe modelul coreean („The Korea model: Why an armistice offers the best hope for peace in Ukraine").

[17] Graham Allison vorbește explicit despre „sfere de influență" în „The New Spheres of Influence", *Foreign Affairs*, martie-aprilie 2020.

[18] J.D. Vance, „The math on Ukraine does not add up", *New York Times*, 12 aprilie 2024.

[19] Elbridge Colby, *The Strategy of Denial: American Defense in an Age of Great Power Conflict*, Yale University Press, New Haven, 2021.

[20] Paul Kennedy, *The Rise and Fall of the Great Powers*, Vintage Books, New York, 1987.

[21] O analiză nuanțată a abordării neoconservatoare face Francis Fukuyama în *After the Neocons*, Yale University Press, New Haven, 2006. Fukuyama a fost și el adept al acestei abordări (să ne amintim de lucrarea sa, *The End of History*, 1990).

[22] Thierry de Montbrial, "L'Ere des Confrontations", Paris, Dunod, 2025.

[23] În anii recenți, nu putine voci, inclusiv ale unor politicieni, au făcut asemuire cu anii premergători celui de-Al Doilea Război Mondial. Vezi și Olivier Wieviorka, „Le context actuel presente des ressemblences avec la situation qui prevalait avant la Deuxieme Guerre Mondiale", *Le Monde*, 5 martie 2025.

[24] Analogia se face cu contribuția lui Alexander Hamilton la crearea unui buget federal și a unei trezorerii comune a SUA. Hamilton a fost secretar al Trezoreriei SUA între 1785 și 1791.

[25] La reuniunea de la Paris, din 26 martie 2025, au fost 230 experți militari din 30 de țări. Ne dăm seama cât de dificilă este coordonarea programelor de creștere a capacității de apărare când atât de multe țări sunt angrenate.

[26] Mark Carney, premierul Canadei (fost șef al Băncii Angliei și, anterior, al Băncii Centrale a Canadei), a afirmat că relația tradițională cu SUA nu mai există.

[27] Institutul de Economie Mondială din Kiel apreciază un coeficient de multiplicare de 0,6-1 pentru cheltuieli de apărare. Astfel, cheltuieli mai mari de 800 de miliarde de euro (150 de miliarde din fondul de apărare plus 650 de miliarde euro prin bugetele naționale și alte surse) ar putea da un impuls fiscal important economiilor UE. Dar cifrele sunt aproximative și constrângerile bugetare nu au cum să nu opereze. Iar cheltuielile se vor întinde pe mai mulți ani.

[28] În *Financial Times*, Martin Arnold nota că „EU watchdogs warn that weakening rules risks another financial crash", 23 martie 2025.

[29] Sistem multilateral creat pentru a regla relațiile financiare internaționale după Al Doilea Război Mondial.

[30] Este de amintit că John Maynard Keynes, unul dintre cei mai mari economiști ai secolului trecut, a avut în minte crearea „bancor", ca *unit of account* (unitate de cont), care să stea la baza sistemului monetar internațional. Dolarul a devenit, în timp, vulnerabil din cauza cheltuielilor militare foarte mari ale SUA în anii '60 și '70, fapt care a dus la ruperea legăturii cu aurul, ca activ financiar.

[31] Stephen Miran, „A user's guide to restructuring the global trading system", Hudson Bay Capital, noiembrie 2024.

[32] Am abordat această problematică în câteva volume, între care *Când finanța subminează economia și corodează democrația* (Polirom, 2012) și *Băncile centrale, criza și postcriza* (Polirom, 2018), *Which Way Goes Capitalism* (CEU Press, 2009).

[33] Jake Sullivan, „The sources of American economic power: A foreign policy for a changed world", *Foreign Affairs*, noiembrie-decembrie, 2023

[34] Clyde Prestowitz, *Trading Places: How We Are Giving Our Future to Japan and How to Reclaim It*, Basic Books, New York, 1993

[35] Ezra Vogel, profesor la Harvard, vorbea despre *Japan Inc.* pentru a descrie structurile neocorporatiste ale sistemului economic japonez.

[36] Vezi și Gillian Tett, „How to make sense of Donald Trump's tariffs", *Financial Times*, 4 aprilie 2025.

[37] Vezi Raghuram Rajan, „Un dollar attractif est-il vraiment un fardeau pour les Americaines?", *Le Monde*, 21 martie 2025. Rajan a fost șef al Băncii Centrale a Indiei și economist-șef la FMI, în prezent fiind profesor la Chicago Business School; Maurice Obstfeld „Let's stop the trade deficit game", *PIIE*, 19 martie 2025. *Wall Street Journal*, *Financial Times*, *The Economist* și alte publicații au numeroase analize critice la adresa politicii economice a Administrației Trump – mai cu seamă că ele privesc favorabil multilateralismul în relații economice internaționale (unii ar spune că sunt promotoare ale *globalismului*). Dar sunt și puncte de vedere ce susțin politica comercială a Administrației Trump (Lori Wallach, „What Trump's Critics Are Getting Wrong", *Project Syndicate*, 29 martie 2025; sau John Michelson, „The Case for Tariffs", *The Wall Street Jornal*, martie 31 2025).

[38] Cheltuielile de apărare sunt mai cuprinzătoare decât cele strict militare.

[39] Italian proposal for a European Security and Industrial Innovation Initiative, Brussels, 11 martie 2025 (Catalysing private investment through EU guarantees and efficiently targeted member state commitments).

[40] În Franța, de pildă, dezvoltarea industriei de apărare reclamă revederea priorităților în bugetul public („Pour financer le rearmement la France revoit ses priorites", *Le Monde*, 19 martie 2025).

[41] Unii văd IA ca un *panaceum* la toate relele din lume.

[42] Cum este și schimbarea climatică.

[43] Cum au, de exemplu, SUA.

[44] Vezi, de pildă, Neil Howe, *The Fourth Turning Point: What the Seasons of History Tell Us About How and When This Crisis Will End*, Simon & Schuster, New York, 2023.

[45] Liberalismul, ca regim politic (democrația), privește în esență separarea puterilor în stat (*check and balances*), nu o doctrină economică de *laissez-faire*.

[46] Am evocat acest scenariu în *Economia și pandemia*, Polirom, Iași, 2021.

[47] Robert D. Kaplan, *The Coming Anarchy*, Random House, New York, 2000.

[48] Republica de la Weimar epitomizează, după Kaplan, instabilitate intrinsecă și deșertăciune (criza morală), care duc la pierderea democrației ca spirit și practică/ Robert D. Kaplan, *Waste Land: A World in Permanent Crisis*, C. Hurst&Co., Londra, 2025.

[49] Oswald Spengler, *The Decline of the West* (*Der Untergang des Abendlandes*), 1918/ 2022.

[50] Printre care Barbara F. Walter (*op. cit.*), ce utilizează noțiunea de „anocrație'; sau Steven Levitsky și Daniel Ziblatt, *How Democracies Die*, Random House, Londra, 2018.

[51] Thierry de Montbrial vorbea despre o asemenea lume încă din primul mandat al președintelui Trump: *Vivre le temps des troubles*, Albin Michel, Paris, 2017.

[52] Primul secretar general al NATO, Lord Ismay, afirma că rostul organizației era următorul: „Keep the Soviet Union out, the Americans in, and the Germans down".

NOUA ARHITECTURĂ DE SECURITATE. PUTERI MIJLOCII, PUTERI MINORE ȘI MINILATERALE ÎN REAȘEZAREA GLOBALĂ CONTEMPORANĂ

Iulian CHIFU*

Abstract

The turbulences of the current world order – unpredictability in the changes of the US politicies, belicose revisionism of Russia and aspiration to hegemony of China - are making the middle and minor powers to prepare their backup plans on security and defense through their geographic proximity with the wars, the options to align with grand powers, to balance in between them or the inclination to team up with other middle powers to offset the pressure and have a saying in the reassessing of the new world order. The theories of middle powers, minor powers and minilaterals begin to play a more important role since the status quo and continuity through transformation and not demolishing the liberal world order are the choices of the liberal democracy countries and the European project. The need of extra – security guarantees is pushing to the new architecture of security involving new regional complementary settings and formats of cooperation for credible defense and deterrence in the Eastern Flank.

Keywords: *middle powers; minor powers; minilaterals; multilateralism; balancing; alignment.*

INTRODUCERE ȘI METODOLOGIE

Cel de-al doilea mandat Trump a marcat schimbarea reală și așezarea evoluțiilor anterioare pe tendințe mai lesne de identificat și de decriptat[1]. Astfel, principala confruntare, una epică și constantă, s-a decantat între *lumea bazată pe reguli* versus *politicile de putere*. Iar aici par să revină în prim-plan – de dispărut nu au dispărut niciodată – „politica de putere", utilizarea forței armate pentru soluționarea problemelor de politică externă sau a nivelurilor de ambiție nemăsurate ale unor lideri, respectiv „politica de Mare Putere", abordarea tranzacțională,

* ***Iulian Chifu este prof. univ. dr., președintele Centrului pentru Prevenirea Conflictelor și Early Warning București, specializat în analiză de conflict și decizie în criză. A fost consilier prezidențial (2011-2014) și consilier de stat al prim-ministrului României (2021-2023).***

negociere între marile puteri a avantajelor pe seama celorlalți actori din sistemul internațional[2].

O altă falie suprapusă a acestui tip de confruntare, din nou una tradițională și constantă, chiar dacă cu intensitate diferită în istorie, este cea între *revizionism* și *statu-quo*. Actorii care își doresc o continuare a lumii liberale așa cum e ea cunoscută, cu aspirații spre democrație, economie de piață și stat de drept, cu acorduri de liber schimb și cooperare loială, respectând angajamentele luate, se confruntă cu actorii care-și doresc schimbarea tectonică și în tot a regulilor jocului existent, care nu-i mai satisface sau față de care au pretenția că raportul de forțe s-a schimbat, iar nevoia de a restabili echilibrele subzistă. Dar și aici apar noutăți.

Mai întâi, și actorii ce-și doresc *statu-quo*-ul regulilor nu sunt neapărat imobili și doresc, la rândul lor, adaptarea sistemului ordinii mondiale la evoluții și realități: o transformare graduală și consimțită de toți membrii comunității, nicidecum o distrugere completă, o *tabula rasa* a actualei ordini mondiale și înlocuirea cu un construct reclădit de la zero, cu amenințarea hiatusului și a pauzei de putere care ar permite oricui să intervină și să preia controlul asupra formulei reașezărilor globale.

Opțiunea distrugerii complete a sistemului existent se pliază mai degrabă pe abordările revizioniștilor, dornici să reclădească sistemul pe baza propriilor convingeri, viziuni, proiecte și aspirații. Din acest punct de vedere, atât America lui Trump[3] - prin documente electorale, discursul de inaugurare și pozițiile publice repetate, dar și documentele noi adoptate, adică Strategia de Securitate Națională[4] și Strategia Națională de Apărare[5], cât și Rusia lui Putin - prin „doctrina Putin”[6] și documente ultimative (ca propunerile către OSCE și NATO)[7] - au asemenea dorințe, în timp ce China lui Xi Jinping optează pentru a păstra parțial sistemul și a-l aduce la o formulă care promovează propriile aspirații, pretinzând că dorește menținerea sau doar transformarea sistemului, unul care i-a facilitat postura de *challenger global* în doar 35 de ani, și nu distrugerea absolută și reclădirea după propriile principii[8].

Nu întâmplător, înclinația spre reguli și multilateralism, care să îngrădească marile puteri, a mai rămas în pedigree-ul Uniunii Europene, a liberal-democrațiilor globale, cu tendințe de adaptare și de evoluție în continuare, sistemul supraviețuind și fiind funcțional în paralel cu puseele de tip revizionist venite, cu precădere, de la marile puteri – SUA, China – sau de la actorii care joacă și se pretind în continuare mari puteri – Rusia – chiar dacă dimensiunea *capacității geopolitice* și a criteriilor de putere[9] ar plasa-o mai degrabă la nivel de putere regională, putere mijlocie cu pretenții și deținătoare de arme nucleare (chiar neacceptabilitatea utilizării armei nucleare în contemporaneitate a redus nivelul și calitatea asocierii Rusiei la primele două Mari Puteri)[10].

Lumea liberală suferă pusee și impulsuri distructive din partea celor trei, dar cu proiecte sensibil diferite pentru lumea de mâine, formule în construcție care se suprapun și coexistă deja cu lumea democrat-liberală prin efectul greutății strategice și forței celor trei actori sau al aventurismului unora dintre ei. Dar ea nu a dispărut, din contra, pe alocuri chiar prosperă și se extinde, inclusiv geografic[11]. Doar că atractivitatea și capacitatea de a impune reguli scade pas cu pas, în unele puncte și pe anumite dimensiuni chiar dramatic[12].

METODOLOGIE

Ne-am propus aplicarea ***teoriei rolurilor puterilor mijlocii*** în arhitectura globală, dar și cea a rolului și locului puterilor minore în eșafodajul de securitate și al relațiilor internaționale, folosind cadrul de democratizare tehnologică[13] și al recuperării decalajelor în cazul asimetriilor de portanță geopolitică (*capacitate geopolitică*)[14] de secol 21, împingând către nevoia de asociere multilaterală pentru conservarea lumii bazate pe reguli. De asemenea, am utilizat ***teoria și practica minilateralelor*** pentru a vedea rolul și funcționalitatea acestora în promovarea intereselor puterilor mijlocii și a includerii intereselor comune ale puterilor minore prin complementaritate, asigurare suplimentară și

de rezervă în materie de securitate, apărare și descurajare.

Cazul particular dezbătut este ***flancul estic al NATO și UE***, de la Marele Nord la Marea Neagră, statele din linia întâi care se confruntă cu dorința de a-și verifica, accesa și valorifica garanțiile de securitate tradiționale, apartenența la NATO, cu Articolul 5[15], și apartenența la UE, inclusiv Articolul 42.7[16], în paralel cu un anumit nivel de neîncredere în reașezările globale care relativizează sau introduc amendamente la aceste angajamente[17], cel puțin la nivel declarativ. Nevoia formulelor de reasigurare reciprocă, regională/complementară, a determinat înclinația spre *minilaterale*, tot așa cum nevoia unor garanții certe de securitate în contextul războiului de agresiune al Rusiei în Ucraina a adus și reflecția pentru propriile acorduri și garanții dincolo de cele deja existente.

Teza noastră este că statele din linia întâi, din flancul estic al NATO și UE, au tendința de a completa arhitectura de securitate, antrenând, din dorința de a-și promova propriile interese, chiar *o reconfigurare a securității și apărării europene* prin sinteză, complementaritate și geometrie variabilă. În acest cadru, obiectivele secundare pe care le abordăm sunt faptul că ***Turcia și Ucraina dobândesc un rol primordial în securitatea europeană*****,** în timp ce înregistrăm o renaștere a interesului și rolului puterilor minore la nivelul securității europene, tradus inclusiv prin dorința de revenire la politica de extindere a UE ca principală politică de succes europeană post-Război Rece.

TEORII ALE PUTERILOR MIJLOCII

James Manicom și Jeffrey Reeves definesc ***puterile mijlocii*** drept *actori capabili* care contribuie la relațiile internaționale în spații care nu sunt în prim-planul intereselor marilor puteri[18]. Puterile mijlocii sunt state cu un nivel lesne de perceput privind influența la nivel internațional, care posedă capabilități materiale și de putere globale sub cele ale marilor puteri, dar în fața statelor mici[19]. Ele nu sunt în mod necesar puteri regionale. Înclinația acestor state este către *preferințe multipolare în politica externă* și predispoziția către un comportament de actor bun, deschis, constructiv, respectând regulile și cu o doză sănătoasă de altruism pentru ordinea mondială, dar și pentru apărarea propriului interes[20].

Definiția marchează lipsa unui consens în privința atributelor concrete materiale care definesc statutul de putere mijlocie – geografie, populație, cheltuieli militare, capacitate diplomatică – toate la un anumit nivel urmând să determine statutul de putere mijlocie[21]. Și chiar în cazul înclinațiilor spre multilateralism și reguli, devine problematic statutul atunci când nu există o legătură cauzală între rădăcina unui comportament la nivel internațional și dimensiunile unui anumit stat sau poziția în ierarhia internațională, sau dacă crede sau nu în internaționalism liberal. Pentru că Statele Unite au creat sistemul din postura de mare putere și hegemon, în timp ce puterile mijlocii sunt înclinate, indiferent de tipul de regim, să acționeze *colaborativ și multilateral*, cu precădere[22]. Cercetările recente arată că perceperea vulnerabilității proprii motivează mai degrabă acest comportament[23].

Puterile mijlocii nu sunt suficient de puternice ca să acționeze singure și nici atât de mici încât să li se pară inutilă urmărirea propriului interes național[24]. În momente de competiție a marilor puteri, ele pot fi *„honest brokers”* – mediatori corecți, deci pot construi încrederea care poate să soluționeze sau măcar să controleze bătăliile hegemonice ale marilor puteri. În plus, utilizând coaliții de tip *like-minded states*, puterile mijlocii *pot limita excesele puterilor hegemonice* încadrându-le în instituții și norme internaționale. Asta pentru că puterile mijlocii, spre deosebire de statele mici, sunt mai puțin înclinate să dezvolte relații de dependență de marile puteri[25]. Totuși, *în condiții de unipolaritate, rolul devine nerelevant* dacă nu există tendința de îndiguire a exceselor hegemonului împreună sau dacă nu se coalizează pe teme înguste, de tip „niche diplomacy” – diplomația de nișă sau orientată spre un tip de expertiză funcțională și birocratică pe o temă internațională, în care realizează coagularea în calitate de catalizator[26].

Există și efecte secundare și „deraieri“ atunci când luăm în considerare mai ales *auto-identificarea ca putere mijlocie* și constructul identității naționale pe o asemenea bază[27] (ca în cazul Rusiei în raport cu statutul de mare putere), o exagerare fără legătură cu caracteristicile generale și capacitatea statului. Aici primează mai degrabă dorința de a se afirma și *înclinația spre activism* în relațiile internaționale, o exagerare asumată, chiar dacă motivația poate fi profund altruistă, iar conținutul nu acoperă realitatea factuală a caracteristicilor de putere mijlocie.

Actorul în sine mimează comportamentul unei puteri mijlocii sau mari, în funcție de autoidentificare, dar și privilegiile acestei categorii – pe care le caută, de fapt, pentru uz intern. Și se poate vedea când resursele sale nu pot susține acest comportament și statut revendicat. Australia, de exemplu, a asumat angajamentul pentru internaționalism liberal și credința în rolul de lider al puterilor mijlocii și minore în relațiile internaționale, care este mai degrabă o declarație de intenție și instrument de atracție pentru coagulare de coaliții decât dovada reală a statutului de putere mijlocie, afirmat și asumat, dar susținut alternativ, cu suișuri și coborâșuri, în ultimii 35 de ani[28].

Puterile mijlocii au tendința să fie *stabilizatori* și *purtătorii de legitimitate* ai ordinii mondiale, chiar dacă sunt diferite ca nivel de ambiție și substanță a elementelor de putere[29]. Puterile mijlocii tradiționale devin agenți liberi de încredere care pot să se alăture, într-o competiție lansată, noii puteri emergente sau să rămână loiali puterii în declin, fără garanții de prezervare a angajamentelor anterioare sau de protecție la retalierea puterii în devenire[30].

Schimbarea de hegemon și „capcana lui Tucidide” nu duc automat la rupturi și turbulențe tectonice decât în sistemele bazate pe putere și poziții fixe predefinite[31]. Puterile mijlocii fac alegeri conștiente, atunci când sunt necesare, pe baze normative, de valori și principii comune și nu neapărat de predicție a reașezărilor, prin aliniere cu cel puternic[32]. De exemplu, într-un caz de bipolaritate antagonică în Indo-Pacific, SUA-Japonia și Taiwanul, de o parte, și China, de alta, Canada va trebui să facă o alegere evidentă pentru că revizionismul chinez îi micșorează forța de exprimare[33], în timp ce Coreea de Sud, Thailanda sau Indonezia ar putea alege o formulă de nealiniere sau balansare, din cauza dependenței economice și de securitate de China[34].

Ordinea mondială este creată și desenată mai degrabă de idei și norme decât de puterea în sine. Pe de altă parte, dacă puterea revizionistă în creștere atacă fundamentele normelor liberale, ale comerțului internațional, securității sau guvernanței globale, există la nivelul puterilor mijlocii toate elementele pentru varianta asocierii în scopul *balansării* acestui hegemon în devenire. Diplomația agilă a puterilor mijlocii ar putea include și Brazilia, Turcia, India, Africa de Sud sau Indonezia[35]. De exemplu, deși rivalitatea SUA-China alunecă spre confruntare, Australia a încercat balansarea cu atenție între cele două relații atât de mult cât a putut, însă, în final, echilibrul a devenit dificil de menținut[36].

În cazul de față, practic fiecare temă strategică sau economică ce privește Australia implică direct competiția geopolitică între SUA și China[37]. Și totuși, problema strategică fundamentală este revizionismul chinez față de lumea bazată pe reguli și slăbirea primatului strategic al SUA pentru a-și promova propria dominație. Iar asta arată că Beijingul a optat pentru schimbarea sistemului pentru a se potrivi propriei istorii și culturi strategice, în încercarea de a obține un avantaj comparativ[38]. De aceea, Carta Albă din 2017 a Australiei plasează alianța SUA-Australia în centrul abordării unui Indo-Pacific stabil[39].

Autodefinirea/autoidentificarea ca putere mijlocie este susținută de criterii – „gata să își asume, în cea mai mare măsură, *propria apărare,* fără a avea mijloacele de a constrânge sau amenința serios state cu capacități echivalente în materie de putere și influență, reușind să determine arhitectura și funcționarea unor părți specifice din sistemul internațional potrivit propriilor interese”[40]. Deci o cuplare a capacității de apărare și putere militară alături de influență diplomatică, prin angajarea în organizații și

structuri internaționale. Iar la capitolul statelor care continuă să creeze echilibre și să balanseze între diferitele mari puteri – SUA, China, Rusia chiar – pot fi identificate statele din Golf sau cele din Asia Centrală[41].

ROLUL ȘI RELEVANȚA PUTERILOR MINORE ÎN SECOLUL 21

Puterile minore sunt un principiu activ al comunității internaționale, care vizează state cu capacitate redusă, dar, nicidecum, fără amprentă internațională sau posibilitate de a alege sau chiar acționa la nivel redus pe arena internațională. E relevant să vedem atât modul de definire, cât și teoriile care vizează puterile minore și nivelurile lor de influență în raport cu marii actori, în timp de război sau în organizații internaționale, ca mod de întrebuințare a calităților și abilităților lor, inclusiv în structuri în care votul contează. Și aici diferența între stat mic și putere minoră poate fi relevantă la nivelul nuanțelor.

Puterea minoră este un stat cu capacități limitate pentru a-și satisface nevoile de securitate și apărare proprii, dar *mai degrabă independent în politica externă* și gândirea sa, capabil să proiecteze *influență moderată* în anumite regiuni[42]. Puterile minore fie au format alianțe, fie au adoptat poziția de neutralitate pentru a acoperi limitările. ***Statele mici*** sunt cele limitate ca teritoriu, populație, capabilități militare și economice; statul mic poate fi și geografic relevant, dar *fără capacități administrative și militare de luat în seamă*[43].

Între abordările de comportament definitorii la nivelul puterilor minore se numără următoarele: sunt susținătoare ale lumii bazate pe reguli și ale instituțiilor multilaterale, care le oferă mai multă securitate și influență decât dacă ar acționa singure; participarea scăzută la relațiile internaționale; accent pe economie; susținerea internaționalismului; *formarea de alianțe*; aversiunea față de risc și înclinația spre referințe morale, la nivelul arenei internaționale[44]. Puterile minore mai sunt definite drept state cu resurse materiale și diplomatice atât de restrânse încât liderii *se concentrează doar pe integritatea teritorială și protecția suveranității și independenței,* fără a avea ambiții vizând obiective cu relevanță globală[45].

Temele legate de puterile minore se regăsesc cu precădere în relația cu acțiunile marilor puteri și reacțiile celor considerați *proxy* – față de sovietici și americani în timpul Războiului Rece sau chinezi mai recent[46]. În altă abordare se subliniază varianta neo-imperialistă, în care cei doi mari vizau controlul și extinderea influenței, dar care costau, la rândul lor, un anumit nivel de împrumut al puterii *hard* către statul client[47]. Atractivitatea față de aceste state, puteri minore, venea de la o mare varietate de atribute – resurse minerale (petrolul din Orientul Mijlociu, mineralele din Congo), locație geografică (ex.: Cuba), poziționare strategică relevantă în raport cu oponentul sau rivalul (ex.: Islanda). Clienții obțineau, deci, bani, sprijin militar și politic contra unui anumit *nivel de influență în beneficiul propriu* față de puterile mari.

Cu precădere în *perioade de crize*, puterile minore exercitau o influență disproporționată față de marile puteri[48]. Exemplele relevante sunt drepturile de pescuit ale Islandei, atacate de Marea Britanie și reglate de SUA și NATO, în 1960, pentru a nu periclita securitatea Alianței în zona de nord a Oceanului Atlantic. Preluarea în 1968 a USS Pueblo de către nord-coreeni și criza rachetelor din Cuba (1962) sunt alte exemple[49]. Mai putem cita Egiptul și criza Canalului de Suez (1956).

Dacă este să vorbim despre *influența în organizații internaționale,* două propoziții sunt concomitent valabile: puterile minore exercită o influență semnificativă asupra deciziilor în cele mai importante organizații internaționale, în timp ce marile puteri desfășoară constrângeri substanțiale în aceste instituții, influențând puterile minore[50]. Nici în organizațiile în care sunt majoritare (prin număr) puterile minore nu pot schimba regimuri contra marilor puteri[51], deoarece acestea s-ar putea retrage și ar schimba relevanța instituțiilor respective[52]. De aici și importanța marilor puteri – abilitatea de a constrânge puterile minore să consimtă la cooperarea multilaterală în asemenea instituții, chiar dacă nu le avantajează direct[53].

Studii desfășurate la nivelul instituțiilor financiare și a UE arată că puterile minore exercită influență substanțială în comportamentul acestor instituții[54]. Coalițiile de puteri minore au capacitatea de a bloca acorduri comerciale multilaterale[55], iar la nivelul UE noile studii evidențiază influența substanțială a puterilor minore în organizație[56]. Dominația puterilor majore din UE – puteri mijlocii altfel – este contrabalansată sau chiar depășită de puterile minore membre, pe baza regulilor de veto și președinție rotativă, dar și ținând de caracteristicile personale ale liderilor[57]. Alte instrumente sunt veto-ul credibil și amenințările de ieșire din organizație[58].

Și în materie de *alianțe* și *securitate*, studiile arată elemente comportamentale relevante. Astfel, puterile minore caută alianțe pentru a-și crește securitatea, bazate, la origine, pe garanții din partea marilor puteri pentru protecția teritoriului și populației împotriva agresiunii militare, așa cum în Războiul Rece marile puteri sau superputerile căutau, de fapt, expansiunea influenței politicilor externe și militare și blocarea influenței rivalilor pe spațiile alese[59]. Puterile minore preferă *securitatea colectivă* în prevenirea conflictelor armate dacă se bazează pe acorduri multilaterale, crescând securitatea puterilor minore și permițându-le să-și păstreze *un anumit grad de flexibilitate în politica lor externă.*

Și mai interesant pentru analiza noastră, în cazul particular al statelor din Flancul Estic, în cazul unui război inter-statal angajamentele din cadrul alianțelor ce conțin doar puteri mijlocii și minore sunt cel mai probabil să fie respectate și onorate, în comparație cu cele care conțin mari puteri alături de puteri mijlocii și minore[60]. De asemenea, e mai probabil să te alături aliaților când este vorba despre de un acord defensiv sau când majoritatea aliaților se implică în război, iar beligeranții sunt puteri minore[61].

Consensul este că *puterile minore încearcă să evite războaiele.* Totuși, nu de fiecare dată acestea sunt doar victime ale agresiunii, ci au făcut alegeri care au escaladat în loc să diminueze disputele[62]. Războiul apare atunci când un stat are perspectiva de a obține concesii mai importante de la oponent prin război decât prin negocierea în timp de pace[63]. Însă, puterile minore care ajung să se confrunte într-un conflict interstatal convențional cu o mare putere vor pierde, în cele mai multe cazuri, acest conflict asimetric[64], războaiele de acest fel fiind foarte costisitoare, iar cel puternic câștigă, statistic, de fiecare dată[65].

Totuși, structura instituțională a actorului mai slab, *îmbunătățirea coordonării și moralul* pot surprinde actorul mai puternic[66]. În plus, personalitățile angajate pun mai mult preț pe morală și preocupări deontologice[67]. Intervin, deseori, și factori interni care generează decizii de politică externă riscante, atunci când există o distribuție disproporționată a beneficiilor și pierderilor[68]. Tot așa cum natura democratică, supervizarea publică și transparența costurilor fac societățile liberale mai sensibile la război și le crește aversiunea față de angajarea în confruntări militare cu pierderi de vieți[69].

MINILATERALELE ȘI CREȘTEREA RELEVANȚEI LOR CONTEMPORANE

Al treilea element teoretic util în analiza noastră este cel al ***minilateralelor.*** Apărute, inițial, ca structuri informale în cadrul instituțiilor multilaterale[70] cu o mai mare coeziune, minilateralele desemnează, de fapt, un mecanism stabilit de *grupuri mici de state* acoperind anumite teme și care au drept reflecție *formate informale* diferite de instituțiile internaționale multilaterale clasice[71]. De exemplu, în regiunea Indo-Pacifică, unde instituțiile multilaterale atotcuprinzătoare nu soluționează problemele regionale, s-au format foarte multe minilaterale[72].

Minilateralismul este consolidat ca un trend diplomatic facilitând dialogul între parteneri aleși, fără a fi instituționalizat și *evitând angajamente juridice constrângătoare* asupra propriilor strategii. Forumurile de tip minilateral sunt lesne de constituit, dar trecerea spre formalizare este mult mai puțin frecvent întâlnită[73]. Minilateralismul se referă la *o temă sau o amenințare specifică*, un element de securitate

care privește mai puține state, cu aceleași interese și pe o perioadă limitată de timp. Formele mari de acțiune colectivă migrează deseori în formate mai restrânse, mai informale și de acțiune colectivă în cadrul formatelor multilaterale care devin prea largi și extinse. Procesul este numit chiar o formă revizuită de multilateralism pentru a crește forța de cooperare între participanți[74].

Minilateralele din domeniul securității au ***trei trăsături predominante**:* număr mic de participanți față de formatele multilaterale obișnuite; caracteristici ad-hoc, care le fac să se creeze și să dispară rapid, fără urme instituționale; înclinație spre formulele clasice de securitate sau amenințări tradiționale[75]. E o abordare mai țintită, cu cel mai mic număr de state necesar unui impact cât mai mare pe o temă particulară, deci rezolvă o *problemă de optimizare*[76]. Este o formulă voluntară mai degrabă decât una contractuală, concentrată pe o temă concretă mai degrabă decât pe abordarea comprehensivă și se referă, cu precădere, la *preocupări regionale* decât globale, cu abordare de jos în sus, de cele mai multe ori, decât una de sus în jos[77].

Pentru eficiență și șanse reale de succes, e necesar ca participanții să fie cei potriviți și indispensabili. Pe de altă parte, minilaterale au un caracter profund de funcționare bazată pe relații interpersonale foarte bune între lideri[78]. Nu rareori, minilateralele sunt acuzate a fi o organizație în sânul unei alte organizații sau, în anumite cazuri, formule de ajustare de poziții, guvernare sectară și dirijare a deciziei, dincolo de prevederile statutare, la nivelul organizațiilor multilaterale. Totuși, grupurile mici se bazează pe un nivel mult mai mare de *interacțiune și încredere*, fără ca acest lucru să fie, în sine, o garanție a succesului.

La avantajele minilateralelor mai putem adăuga nivelul redus de birocratizare, discuții mai oneste și directe, flexibilitate pentru acorduri ad-hoc și nivel mai redus de costuri. Altfel, minilaterala poate deveni o „sabie cu două tăișuri" atunci când vorbim despre *lipsa de ierarhie* sau reguli și *un vacuum de leadership*. Câteodată informalitatea duce la pierderea concentrării pe obiective, în lipsa principiilor de organizare, a cadrelor și instituționalizării[79]. *Ambiguitatea,* care e altă caracteristică a minilateralelor și a rezultatelor convenite, poate avea un caracter strategic, atunci când obiectivele sunt largi și limbajul vag creează spațiu pentru membrii care nu sunt de acord cu acțiunile promovate, chiar dacă există consens în privința intereselor rezonabile[80].

O altă abordare subliniază, totuși, caracterul de instituție internațională al minilateralelor[81], cu toate caracteristicile aferente, deși pot fi definite drept „aranjamente explicite negociate între actori internaționali care prescriu sau autorizează comportamente"[82]. Grupurile minilaterale nu sunt, totuși, alianțe bazate pe tratate formale sau instituții formalizate[83]. Sunt caracterizate de invitații selective, cu formate mai degrabă *asociabile coaliților de voință* și excluderea statelor neinvitate[84].

Nu există o formă unanim agreată a definiției sau conținutului conceptului de minilateralism[85], în schimb există legătura creată prin reunirea celor afectați de tema în cauză discutată[86]. Atunci când suntem în cazul *minilateralei în cadrul unei organizații multilaterale*, existența acordurilor din organizația multilaterală are impact direct asupra minilateralei, ordonându-i și limitându-i mișcările și creând dificultăți și tensiuni între cei invitați și cei excluși, fapt ce reclamă întotdeauna o motivație solidă pentru a nu afecta multilaterala în sine.

FLANCUL ESTIC, STATELE DIN LINIA ÎNTÂI ȘI ARHITECTURA DE SECURITATE EUROPEANĂ

Am studiat cazul Mării Negre și al realizării minilateralelor și acordurilor regionale de securitate complementare, în formula convergenței cu NATO – în contextul transferului de responsabilitate de la SUA către componenta europeană, cu păstrarea umbrelei nucleare și a „componentelor critice" ale apărării convenționale[87], cu Uniunea Europeană - în formatul reconstituirii complementare a capabilităților și a industriei de apărare, inclusiv prin programele SAFE, de împrumuturi la dobânzile UE, și al Coaliției de Voință condusă de Franța și Germania – succesoarea grupului

Raimstein[88], cu o plus-valoare relevantă în materie de integrare a actorilor extra-euroatlantici, dar din spațiul statelor liberal democratice, după un format tip „Afganistan" în precedentele reuniuni NATO, împreună cu aspirația și dorința statelor mijlocii de a construi formate complementare pentru garanții directe și reasigurare la nivel regional.

Rezultatul subliniază, deopotrivă, *rolul puterilor minore în noul conglomerat coeziv de tip minilaterală,* cu relevanță la nivelul Flancului Estic, de la Marele Nord la Marea Neagră, dar și nevoia de implicare a Turciei – cea de-a doua armată a NATO și prima din Europa, dar și a Ucrainei – cu 700-800 mii de militari antrenați în cea mai importantă confruntare pe scară largă de secol 21, utilizând toate categoriile de arme occidentale. De altfel, un studiu special despre rolul Ucrainei și Turciei în formatul de asigurare a securității, apărării și descurajării Europei[89] relevă și explică preocuparea specifică a statelor din Flancul Estic, din prima linie – concepte acceptate astăzi și la nivel UE – pentru formate noi, complementare, asiguratoare ale arhitecturii de securitate europene. Acestea trebuie să aducă rapid soluții, până la consumarea creșterii capacității și preluării complete și depline a atribuțiilor și componentelor capabilităților americane retrase de către statele europene.

Au rezultat câteva **concluzii:**

- ***aranjamentele regionale*** de securitate și apărare devin elemente cheie într-o arhitectură întărită și recalibrată, care adaugă un sistem de parteneriate strategice și minilaterale, toate în condițiile *convergenței și solidarității puterilor mijlocii* și un rol critic tot mai relevant al puterilor minore;
- ***Formatul B9 plus Nordefco plus Ucraina*****,** care a avut loc la București, ar trebui să adauge Turcia și să determine elementele de coeziune necesară, fără slăbirea miezului, care să permită întărirea Flancului Estic pe dimensiunea de apărare și descurajare;
- într-un context de deficit al unei componente de putere clasică sau capacitate geopolitică (în sensul definit de studiul publicat de Henry Jackson Society), structurile coagulative de puteri mijlocii au două soluții: ***extinderea arealului geografic*** – vezi Turcia și Ucraina, cu grijă mare pentru coeziune, ceea ce înseamnă menținerea matricii de principii și valori comune care definesc identitatea grupului și care nu trebuie să slăbească, și *implicarea puterilor minore*[90];
- ***rolul puterilor minore este în creștere*** prin aportul direct pe care îl au, în elemente unice, relevante, strategice, plus valoare adăugată, creștere de legitimitate, dar și prin aportul capacității proprii militare și strategice, ca și al producției și piețelor, dar mai ales al componentelor solidarității și a acordului cu *constructele puterilor mijlocii de reechilibrare a marilor puteri;*
- ***nivelul de ambiție*** reprezentat de aceste constructe, inclusiv instituționalizate, ale puterilor mijlocii este mult mai important pentru puterile minore regionale decât perspectiva fagocitării, alinierii și *lipsei de capacități de influență și realizare a propriilor interese* în raport cu marile puteri;
- dezbaterea pe baza ***criteriilor de eficiență*** a raportului dintre *diluarea unor principii coezive* și *extinderea până la greutatea strategică* a unui construct care să echilibreze marile puteri rămâne un punct cheie al construcției conglomeratelor de puteri mijlocii și minore;
- ***Marea Neagră, Flancul Estic și Ucraina*** constituie surse de legitimitate și capabilități ale constructelor inclusive de securitate regională în acest spațiu, complementare NATO și UE;
- ***discuția despre integrarea Turciei și Ucrainei în UE*** poate fi nuanțată prin abordarea testului regional, comportamentul și funcționarea în cadrul structurilor bilaterale și angajamentelor de securitate cu statele regiunii și probarea utilității ca premisă pentru angajarea alături de UE și, ulterior, *integrarea în componenta de securitate și apărare,* dacă

cea instituțională europeană e greu de abordat în prima fază[91];

- ***complementaritatea securității regionale*** poate fi salvatoare, cu mai multe valori de întrebuințare: mai întâi, cea a asigurării unui *timp suficient de tranziție* pentru renașterea capabilităților europene, dar și ***reasigurarea statelor din prima linie***, din Flancul Estic transatlantic, de la Marele Nord la Marea Neagră, prin capabilități suficiente și asocierea cu state cu experiență în acțiuni militare și cu argumente puternice în materie de *apărare și descurajare, de reziliență societală*, de creativitate și inventivitate tehnologică[92].

Am identificat cinci argumente intrinseci, legate de propriile atribute, pentru care **Turcia** trebuie să fie inclusă în securitatea europeană:

1. ***Motive de securitate.*** Turcia deține capabilități, industrie militară, pregătire, cea de-a doua armată din NATO, controlul strâmtorilor (indispensabile Rusiei și proiecției puterii sale în mările calde) și aparține de Flancul Estic. De aici, necesitatea de a complini Flancul Estic, alăturând Formatului B9 al statelor Europei Centrale și de Est membre NATO cele cinci state nordice din NORDEFCO – Norvegia, Finlanda, Suedia, Danemarca și Islanda – și Turcia, pentru a avea un Flanc Estic complet de la Marele Nord la Marea Neagră.
2. ***Securitate economică, energie și competiție globală****:* numai prin integrarea Turciei și Ucrainei se poate complini Europa cu peste 500 de milioane de locuitori, capabilă să intre în competiția globală cu actori precum China și SUA și să aibă o piață comună reunită și o șansă la nivelul concurenței cu marile blocuri economice. Doar așa pot UE și statele ei membre să aspire la statutul de putere globală.
3. ***Interesul crescut pentru Marea Neagră și Regiunea Extinsă a Mării Negre.*** Dacă despre strategia americană pe Marea Neagră este greu să mai adăugăm ceva, Marea Britanie a revenit în regiune, UE a adoptat o Strategie pentru Marea Neagră – cu componentă strategică și de securitate, așa cum Franța sau Germania au redescoperit Marea Neagră (pentru că aici este „marele joc") – ambele au strategii la Marea Neagră și interese.
4. ***Existența unor exerciții/inițiative legate de securitatea la Marea Neagră din care Turcia face parte deja.*** E vorba despre MCM, misiunea statelor NATO riverane Mării Negre care marchează cooperarea pentru deminare și anunță cooperarea extinsă pentru securitatea infrastructurii critice submarine și maritime, securitatea maritimă în sens mai larg. Fără a fi un NATO în cadrul NATO și fără a rezerva responsabilitatea doar la nivelul statelor riverane, fiind necesară reluarea misiunilor aliate de reasigurare imediat ce se va putea, misiunea rămâne cea mai tangibilă și prezentă formulă aliată de funcționare pe Marea Neagră.
5. ***Sistemul sofisticat de parteneriate strategice din regiune,*** inclusiv parteneriatele bilaterale România-Polonia, România-Turcia, Polonia-Suedia, România-Ucraina, România-Republica Moldova, trilateralele România-Polonia-Turcia și România-Ucraina-Republica Moldova, formatul București 9 și Inițiativa celor Trei Mări. Nu uităm, desigur, toate formatele parteneriale de reasigurare cu Ucraina semnate de numeroase state din regiune sau noua propunere și structură de producție comună de drone inițiată de Ucraina[93].

Argumentele **Ucrainei** sunt mult mai simplu de valorificat. Am văzut deja propunerea cancelarului Merz, poate inabil formulată sub eticheta de „membru asociat"[94], dar cu un conținut ce merită abordat și considerat de către Ucraina până la consumarea negocierilor clusterelor și capitolelor integrării în UE, care vor lua timp. Preocuparea la nivelul UE există deja, cu integrarea Ucrainei la nivel militar, pe componentele de apărare și descurajare.

Argumentele sunt următoarele: ***mutarea evidentă a centrului de greutate al NATO către Europa*** și a centrului de gravitație la nivel european către Europa Centrală și de Est, după lansarea războiului de agresiune al Rusiei în Ucraina, și creșterea capabilităților și preocupărilor pentru apărare în această regiune. Adăugăm ***reziliența, dorința de a lupta*** – *intangibilele de război*[95] – ca și ***producția industrială, inovația și dezvoltarea teatrului de operații de secol 21***, adică tot elemente care recomandă înclinația spre Ucraina, Turcia, Polonia, cu cele mai relevante investiții și către celelalte state din Flancul Estic, cel mai expus agresiunii ruse[96].

În consecință, perspectiva **utilizării instrumentarului minilateralelor,** ca precursoare și test pentru angajamente pe termen lung, și instituționalizarea relațiilor de securitate în Flancul Estic al UE și NATO, caracteristicile opțiunilor puterilor mijlocii de a se coagula pentru a constitui o formulă de ***balansare a marilor puteri,*** rolul și locul de legitimare și valoare adăugată a puterilor minore, dar mai ales nevoia contiguității geografice, a coeziunii și solidarității regionale, creează premisele complementarității structurilor noii arhitecturi de securitate europene. Iar punctul de plecare este ***Flancul Estic, statele din linia întâi,*** care pot asigura cadrul de integrare pentru Ucraina și Turcia și pot testa deschiderea spre menținerea respectării și nediluării excesive a valorilor fundamentale care asigură coeziunea instituțională a unei arhitecturi de securitate a Europei, incluzând NATO, UE, Coaliția de Voință și proiectele regionale, deopotrivă.

BIBLIOGRAFIE

1. AKSOY Deniz, Jonathan Rodden, “Getting into the game: legislative bargaining, distributive politics, and EU enlargement”, *Public Finance and Management*, vol. 9, nr. 4, 2009, pp. 613–643.
2. ALLEN A. Michael, Benjamin O. Fordham, ”From Melos to Baghdad: Explaining resistance to militarized challenges from more powerful states”, *International Studies Quarterly*, vol. 55, nr. 4, 2011, pp.1025–1045.
3. ANUAR Amalina, Nazia Hussain, *Minilateralism for Multilateralism in the Post-COVID Age. Challenges to Minilateralism*, Policy Report, S. Rajaratnam School of International Studies, January 2021, 11 p.; https://www.jstor.org/stable/resrep28278.5.
4. ARREGUÍN-TOFT Ivan, ”How the Weak Win Wars. A Theory of Asymmetric Conflict”, *International Security*, vol. 26, nr. 1, Harvard Kennedy School, 2001, pp. 93–128.
5. BOBIC Marinko, *Why minor powers risk wars with major powers. A comparative study of the post-Cold War era*, Bristol University Press, 2019.
6. BRADY Anne-Marie (ed.), *Small States and the Changing Global Order: New Zealand Faces the Future*, coll. The World of Small States, Springer, 2019.
7. BUENO de Mesquita Bruce, Alastair Smith, Randolph M. Siverson, James D. Morrow, *The Logic of Political Survival*, Cambridge, MA, The MIT Press, 2005.
8. CARR Andrew, “Is Australia a middle power? A systemic impact approach”, *Australian Journal of International Affairs*, vol. 68, nr. 1, 2014, pp. 70-84; DOI:10.1080/10357718.2013.840264.
9. CHAN Lai-Ha, Maria Rost Rublee, ”The promise of AUKUS: implications of its minilateral institutional form”, *Australian Journal of International Affairs*, vol. 78, nr. 6, 2024, pp. 848-868; DOI: 10.1080/10357718.2024.2421369.

10. CHIFU Iulian, Teodor Frunzeti, ”Trump Doctrine. The Principled Realism”, *Strategic Impact*, nr. 68-69, 2018, pp.7-17.
11. CHIFU Iulian, *Actori, relații și politică de putere în secolul 21*, Editura RAO, București, 2022, ISBN 978-606-006-817-4, volumul 1 din tetralogia *Reconfigurarea Securității și a Relațiilor Internaționale în Secolul 21.*
12. CHIFU Iulian, ”Securitatea tehnologică. Un nou domeniu de strictă actualitate a securității viitorului”, *Infosfera*, nr. 2/2021, pp.13-22.
13. CHIFU Iulian, „Reziliența în război și caracteristicile intangibile. Cazul războiului de agresiune al Rusiei în Ucraina”, *Infosfera*, nr. 3/2023.
14. CHIFU Iulian, *Strategia de Securitate Europeană în era Trump. Chinurile facerii și limitele documentului în era turbulențelor globale,* Calea europeană, 12 iunie 2026; https://www.caleaeuropeana.ro/iulian-chifu-strategia-de-securitate-europeana-in-era-trump-chinurile-facerii-si-limitele-documentului-in-era-turbulentelor-globale/
15. CHIFU Iulian, *Marea Neagră într-o arhitectură de securitate întărită: minilaterale, convergența puterilor mijlocii, rolul critic al puterilor minore*, Calea Europeană, 9 iunie 2026; https://www.caleaeuropeana.ro/iulian-chifu-marea-neagra-intr-o-arhitectura-de-securitate-intarita-minilaterale-convergenta-puterilor-mijlocii-rolul-critic-al-puterilor-minore/
16. CHIFU Iulian, *Noua arhitectură de securitate a Europei: rolul Ucrainei și al Turciei*, Calea Europeană, 25 mai 2026; https://www.caleaeuropeana.ro/iulian-chifu-noua-arhitectura-de-securitate-a-europei-rolul-ucrainei-si-al-turciei/
17. CÎRSTOIU Florin-Cătălin & co, *Medical Response Strategy in Case of Radiation Emergency Caused by the War in Ukraine*, Springer 2023.
18. COOPER F. Andrew (ed.), *Niche Diplomacy: Middle Powers after the Cold War*, Macmillan Press, Houndmills, UK, 1997.
19. COOPER F. Andrew, Richard A. Higgott, Kim Richard Nossal, *Relocating Middle Powers: Australia and Canada in a Changing World Order*, UBC Press, Vancouver,1993.
20. COOPER F. Andrew, Timothy M. Shaw, *The Diplomacies of Small States: Between Vulnerability and Resilience*, Palgrave Macmillan, New York, 2009.
21. COOPER A. David, ‘‘Challenging Contemporary Notions of Middle Power Influence: Implications of the Proliferation Security Initiative for `Middle Power Theory`”, *Foreign Policy Analysis,* vol. 7, nr. 3, 2011.
22. COPELOVITCH Mark, Daniel Nielson, Ryan Powers and Michael J. Tierney, *The Unipolar Fallacy: Common Agency, American Interests, and International Financial Institutions*, Prepared for presentation at the 2014 PEIO Conference, 2014, 48 p.
23. DAVIS Malcolm, *Australia as a rising Middle Power*, RSIS Working Paper, nr. 328, S. Rajaratnam School of International Studies, 2020, 36 p.; http://www.jstor.com/stable/resrep24285.
24. DIEHL F. Paul, Joseph Levgold (eds.), *Regional conflict management*, Bloomsbury Academic, 2003.
25. DOMAŃSKA Maria, *Putin's article: historical revisionism at the service of great-power politics*, 19 June 2020; https://www.osw.waw.pl/en/publikacje/analyses/2020-06-19/putins-article-historical-revisionism-service-great-power-politics.
26. (von) ELSUWEGE Peter, Roman Petrov, *Towards an “Associate Membership” Status for Ukraine?,* 28 May 2026, https://verfassungsblog.de/towards-an-associate-membership-status-for-ukraine/
27. FINDLEY G. Michael, Scott Edwards, ”Accounting for the Unaccounted: Weak-Actor Social Structure in Asymmetric Wars’, *International Studies Quarterly*, vol. 51, nr. 3, 2007, pp. 583–606.
28. GABRIEL João Paulo Nicolini, Henoch Gabriel Mandelbaum, Carlos Eduardo Carvalho, *The Quad: One More ‘Minilateral’ Initiative, Not an Embryonic Military Alliance in the Indo-Pacific Region*, 13 august 2020; https://www.researchgate.net/publication/343626022_The_Quad_One_More_'Minilateral'_Initiative_not_an_Embryonic_Military_Alliance_in_the_Indo-Pacific_Region, DOI: 10.21530/ci.v15n2.2020.1014.

29. GEE Austin, Robert G. Patman, ”Small state or minor power? New Zealand’s Five Eyes membership, intelligence reforms, and Wellington’s response to China’s growing Pacific role”, *Intelligence and National Security*, vol. 36, nr. 1, pp. 34-50; DOI: 10.1080/02684527.2020.1812876.
30. GILLEY Bruce, Andrew O’Neil (eds,), *Middle Powers and the Rise of China*, Georgetown University Press, 2014.
31. GILLEY Bruce, ”Middle powers during great power transitions: China's rise and the future of Canada-US relations”, *International Journal*, vol. 66, nr. 2 (*Canada, the US, and China: A new Pacific triangle?*), Spring 2011, Sage Publications, pp. 245-264.
32. GINGES Jeremy, Scott Atran, ”War as a moral imperative (not just practical politics by other means)”, în *Proceedings of the Royal Society B: Biological Sciences*, vol. 278, nr. 1720, 2011, pp. 2930–2938.
33. GLASER L. Charles, *Rationalist Theory of International Politics. The Logic of Competition and Cooperation*, Princeton, NJ, Princeton University Press, 2010.
34. GLOSSERMAN Brad, Scott A. Snyder, *The Japan–South Korea Identity Clash: East Asian Security and the United States*, Columbia University Press, New York, 2015.
35. GRUBER Lloyd, *Ruling the World: Power Politics and the Rise of Supranational Institutions*, Princeton, NJ, Princeton University Press, 2000.
36. HASTIE Andrew, “We must see China – the opportunities and the threats – with clear eyes”, *The Sydney Morning Herald*, August 8, 2019; www.smh.com.au/politics/federal/we-must-see-china-the-opportunities and-the-threats-with-clear-eyes-20190807-p52eon.html.
37. HAWKINS G. Darren, David A. Lake, Daniel L. Nielson, Michael J. Tierney (eds.), *Delegation and Agency in International Organizations*, vol. 32, Cambridge University Press, 2006.
38. HOLSTI J. Kalevi, “National Role Conceptions and the Study of Foreign Policy”, *International Studies Quarterly*, vol. 14, nr. 3, 1970, pp. 233–309.
39. JIANG Wenran, ”Seeking a strategic vision for Canada-China relations”, *International Journal*, vol. 64, nr. 4, 2009, p. 908.
40. JAISHANKAR Dhruva, “The Real Significance of the Quad”, Australian Strategic Policy Institute, October 24, 2018.
41. JORDAAN Eduard, ”The concept of a middle power in international relations: Distinguishing between emerging and traditional middle powers”, *Politikon: South African Journal of Political Studies*, vol. 30, nr. 2, 2003, p. 167.
42. KAHLER Miles, ”Multilateralism with small and large numbers”, *International Organization*, vol. 46, nr. 3, The MIT Press, 1992, pp. 681-708.
43. KATZENSTEIN J. Peter, *Small States in World Markets: Industrial Policy in Europe*, Ithaca, NY, Cornell University Press, 1985.
44. KATZENSTEIN J. Peter (ed.), *The Culture of National Security: Norms and Identity in World Politics*, Columbia University Press, New York, 1996.
45. KAWASAKI Tsuyoshi, ”Strangers no longer: The identity shift in the Canada-Japan relationship”, *International Journal*, vol. 64, nr. 4, 2009, pp. 879-890.
46. KEOHANE O. Robert, ‘‘Lilliputians’ Dilemmas: Small States in International Politics”, *International Organization*, vol. 23, nr. 2, 1969, pp. 291–310.
47. KIM Hyung Min, ”Comparing measures of national power”, *International Political Science Review*, vol. 31, nr. 4, 2010, pp. 405-427.
48. KIM Sung-Mi, Sebastian Haug, Susan Harris Rimmer, “Minilateralism Revisited: MIKTA as Slender Diplomacy in a Multiplex World”, *Global Governance*, vol. 24, nr. 4, Brill, 2018, pp. 475-489.
49. KOREMENOS Barbara, Charles Lipson, Duncan Snidal, “The Rational Design of International Institutions”, *International Organization*, vol. 55, nr. 4, The MIT Press, 2001, pp. 761–799.
50. KRASNER D. Stephen, *Structural Conflict: The Third World Against Global Liberalism*, Berkeley, CA, University of California Press, 1985.
51. LEONARD Mark, *Europe’s soft-power problem*, European Council on Foreign

Relations, 5 may 2022; https://ecfr.eu/article/europes-soft-power-problem/.

52. LEWIS G. David, Aniseh Bassiri Tabrizi (eds.), *Regional Powers and Post-NATO Afghanistan*, NATO Defense College, 2021; https://www.jstor.org/stable/resrep33620.12.
53. MALIK Salma, "US war in Iraq in the light of the major and minor powers conflict", *The Turkish Yearbook*, vol XXV, pp. 83-106, 2004.
54. MATCHETT Leah, "Minilateralism and Backlash in the Nuclear Security Summit: The Consequences of Nuclear Governance Outside the IAEA", *Security Studies*, vol. 30, nr. 5, 2021, pp. 823–859.
55. MIKKO Mattila, "Fiscal transfers and redistribution in the European Union: do smaller member states get more than their share?", *Journal of European Public Policy*, vol. 13, nr. 1, 2006, pp. 34–51.
56. MIKULASCHEK Christoph, *Minor powers' influence in international organizations: Empirical evidence exploiting the natural experiment of African representation on the UN Security Council*, Paper prepared for presentation at the 8th Annual Conference on the Political Economy of International Organizations, February 12-14, 2015.
57. MOON E. Bruce, "The Foreign Policy of the Dependent State", *International Studies Quarterly*, vol. 27, nr. 3, 1983.
58. MORAVCSIK Andrew, *The Choice for Europe: Social Purpose and State Power from Messina to Maastricht*, Ithaca, NY, Cornell University Press, 1998.
59. MUELLER John, "The Iraq Syndrome", *Foreign Affairs*, vol. 84, nr. 6, Council on Foreign Relations, 2005, pp. 44–54.
60. NAIM Moises, "Minilateralism: The magic number to get real international action", *Foreign Policy*, 2009, June 21, 2009; http://foreignpolicy.com/2009/06/21/minilateralism/.
61. NARLIKAR Amrita, *Bargaining over the Doha development agenda: coalitions in the World Trade Organization*, Latin American Trade Network Working Paper, nr. 36, 2005.
62. OYE A. Kenneth , "Explaining Cooperation under Anarchy: Hypotheses and Strategies", *World Politics*, vol. 38, nr. 1, Cambridge University Press, 1985, pp. 1-24.
63. PANDA Jaganath, Daewon Ohn, "Minilateralism and the new Indo-Pacific order: theoretical ambitions and empirical realities", *Australian Journal of International Affairs*, vol. 78, nr. 6, 2024, pp. 767-781; https://doi.org/10.1080/10357718.2024.2410411.
64. PATRICK Stewart, "The New `New Multilateralism`: Minilateral Cooperation, But at What Cost?", *Global Summitry: Politics, Economics, and Law in International Governance*, Global Summitry Project, vol. 1, nr. 2, 2015, pp. 115–134.
65. PEKKANEN M. Saadia, John Ravenhill, Rosemary Foot (eds.), *The Oxford Handbook of the International Relations of Asia*, New York, Oxford University Press, 2014.
66. REITER Erich, Heinz Gärtner (eds.), *Small States and Alliances*, Physica-Verlag, Heidelberg, 2001, pp 15–23; https://doi.org/10.1007/978-3-662-13000-1_3.
67. REWIZORSKI Marek (ed.), *The European Union and the BRICS. Complex Relations in the Era of Global Governance*, Springer, 2015.
68. RICHEY Mason, Daewon Ohn, "It's fine in practice, but how about in theory? State-of-the-art minilateralism between expectations and reality", *Australian Journal of International Affairs*, vol. 78, nr. 6, 2024, pp. 782-807; https://doi.org/10.1080/10357718.2024.2409361.
69. ROGERS James (ed.), *Audit of geopolitical capability*, Henry Jackson Society, 2019; https://henryjacksonsociety.org/wp-content/uploads/2019/01/HJS-2019-Audit-of-Geopolitical-Capability-Report-web.pdf.
70. ROSEN J. Eitan, *The influence of minor powers during the Cold War*, BA Thesis, State University of New York, May 2021.
71. ROSS S. Robert, Feng Zhu (eds.), *China's Ascent: Power, Security, and the Future of International Politics*, Cornell University Press, 2008.
72. SCHNEIDER J. Christina, "Weak States and Institutionalized Bargaining Power in International Organizations", *International Studies Quarterly*, vol. 55, nr. 2, 2011, pp. 331-355.

73. SIVERSON M. Randolph, Joel King, "Attributes of National Alliance Membership and War Participation, 1815-1965", *American Journal of Political Science*, vol. 24, nr. 1, 1980, pp. 1-15.
74. SLAPIN B. Jonathan, "Exit, Voice, and Cooperation: Bargaining Power in International Organizations and Federal Systems", *Journal of Theoretical Politics*, vol. 21, nr. 2, 2009, pp.187-211.
75. STONE W. Randall, *Controlling Institutions: International Organizations and the Global Economy*, Cambridge, UK, Cambridge University Press, 2011.
76. TALLBERG Jonas, "Bargaining Power in the European Council", *Journal of Common Market Studies*, vol. 46, nr. 3, 2008, pp. 685–708.
77. TOW T. William, "Minilateral security's relevance to US strategy in the Indo-Pacific: challenges and prospects", *The Pacific Review*, vol. 32, nr. 2, 2019, pp. 232-244; DOI: 10.1080/09512748.2018.1465457.
78. UNGERER Carl, "The 'Middle Power' Concept in Australian Foreign Policy", *Australian Journal of Politics and History*, vol. 53, nr. 4, 2007.
79. VARRALL Merriden, "Does China's rise threaten the rules-based order?", *The Interpreter*, June 7, 2017; www.lowyinstitute.org/the-interpreter/does-china-rise-threaten-rules-based-order.
80. VIOLA Lora Anne, "US Strategies of Institutional Adaptation in the Face of Hegemonic Decline", *Global Policy*, vol. 11, nr. 3 (special issue: *Global Power Shifts: How do International Institutions Adjust?*), Wiley, 2020, pp. 28–39.
81. XI Jinping, *Global Security Initiative*, 21 April 2022; https://en.chinadiplomacy.org.cn/gsi/index.shtml.
82. WESTAD Odd Arne, *The Global Cold War: Third World Interventions and the Making of Our Times*, Cambridge University Press, 2005.
83. WUTHNOW Joel, "US 'Minilateralism' in Asia and China's Responses: A New Security Dilemma?", *Journal of Contemporary China*, vol. 28, nr. 115, 2019, pp. 133-150.
84. *** European Commission, *EU-Mercosur agreement*, 3 September 2025, https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/mercosur/eu-mercosur-agreement_en;
85. *** European Commission, *EU-India Free Trade Agreement, Investment Protection Agreement and Geographical Indications Agreement*, 27 January 2026, https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/india/eu-india-agreements_en.
86. *** Official Journal of the European Union, *Consolidated version of the Treaty of functioning of the European Union*, 26.10.2012; https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:en:PDF.
87. *** *The North Atlantic Treaty*, Washington DC, 4 April 1949; https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/1949/04/04/the-north-atlantic-treaty.
88. *** Department of Foreign Affairs and Trade, Australian Government, "Opportunity, Security, Strength: The 2017 Foreign Policy White Paper", November 23, 2017; www.dfat.gov.au/news/news/Pages/opportunity security-strength-the-2017-foreign-policy-white-paper.
89. *** The White House, *Restoring Truth and Sanity to American History*, Executive Order, 27 march 2025; https://www.whitehouse.gov/presidential-actions/2025/03/restoring-truth-and-sanity-to-american-history/
90. *** The White House*, National Security Strategy of the United States of America*, November 2025; https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf.
91. *** US Department of War, *2026 NDS. National Defense Strategy*, 23 January, 2026; https://media.defense.gov/2026/Jan/23/2003864773/-1/-1/0/2026-NATIONAL-DEFENSE-STRATEGY.PDF.
92. *** OSCE Secretariat, *Statement of Mr Sergey Lavrov, Minister of Foreign Affairs of the Russian Federation*, Stockholm, 2 December 2021; https://cdn.osce.org/sites/default/files/f/documents/a/c/506840.pdf.
93. *** Bundesrepublik Deutschland, Der Bundeskanzler*, Letter to the EU institutions*, 28 May 2026, https://newunionpost.eu/wp-content/uploads/2026/05/260518-BK-letter-to-PEC-et-al.pdf.

[1] Iulian Chifu, Teodor Frunzeti, ”Trump Doctrine. The Principled Realism”, *Strategic Impact,* nr. 68-69, 2018, pp.7-17.
[2] Iulian Chifu, *Actori, relații și politică de putere în secolul 21,* Editura RAO, București, 2022, ISBN 978-606-006-817-4, Volumul 1 din tetralogia *Reconfigurarea Securității și a Relațiilor Internaționale în Secolul 21.*
[3] The White House, Restoring Truth and Sanity to American History, Executive Order, 27 march 2025; https://www.whitehouse.gov/presidential-actions/2025/03/restoring-truth-and-sanity-to-american-history/
[4] The White House, *National Security Strategy of the United States of America,* November 2025; https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf
[5] US Department of War, *2026 NDS. National Defense Strategy,* 23 January, 2026; https://media.defense.gov/2026/Jan/23/2003864773/-1/-1/0/2026-NATIONAL-DEFENSE-STRATEGY.PDF.
[6] Maria Domańska, *Putin's article: historical revisionism at the service of great-power politics,* 19 June 2020; https://www.osw.waw.pl/en/publikacje/analyses/2020-06-19/putins-article-historical-revisionism-service-great-power-politics.
[7] OSCE Secretariat, *Statement of Mr Sergey Lavrov, Minister of Foreign Affairs of the Russian Federation,* Stockholm, 2 December 2021; https://cdn.osce.org/sites/default/files/f/documents/a/c/506840.pdf.
[8] Xi Jinping, *Global Security Initiative,* 21 April 2022; https://en.chinadiplomacy.org.cn/gsi/index.shtml.
[9] James Rogers (ed.), *Audit of geopolitical capability,* Henry Jackson Society, 2019; https://henryjacksonsociety.org/wp-content/uploads/2019/01/HJS-2019-Audit-of-Geopolitical-Capability-Report-web.pdf.
[10] Iulian Chifu, ”Russian Provoked Nuclear Disaster, Attack or Accident: Scenarios, Probability and Consequences”, în Florin-Cătălin Cîrstoiu & co, *Medical Response Strategy in Case of Radiation Emergency Caused by the War in Ukraine,* Springer 2023, pp.71-24.
[11] European Commission, *EU-Mercosur agreement,* 3 September 2025, https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/mercosur/eu-mercosur-agreement_en; European Commission, *EU-India Free Trade Agreement,* Investment Protection Agreement and Geographical Indications Agreement, 27 January 2026, https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/india/eu-india-agreements_en.
[12] Mark Leonard, *Europe's soft-power problem,* European Council on Foreign Relations, 5 may 2022; https://ecfr.eu/article/europes-soft-power-problem/.
[13] Iulian Chifu, ”Securitatea tehnologică. Un nou domeniu de strictă actualitate a securității viitorului”, *Infosfera,* nr. 2/2021, pp.13-22.
[14] James Rogers, Op.cit.
[15] *The North Atlantic Treaty,* Washington D.C. - 4 April 1949; https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/1949/04/04/the-north-atlantic-treaty.
[16] Official Journal of the European Union, Consolidated version of the Treaty of functioning of the European Union, 26.10.2012; https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:en:PDF.
[17] Iulian Chifu, *Strategia de Securitate Europeană în era Trump. Chinurile facerii și limitele documentului în era turbulențelor globale,* Calea europeană, 12 iunie 2026; https://www.caleaeuropeana.ro/iulian-chifu-strategia-de-securitate-europeana-in-era-trump-chinurile-facerii-si-limitele-documentului-in-era-turbulentelor-globale/
[18] James Manicom, Jeffrey Reeves, ”Locating Middle Powers in International Relations Theory and Power Transitions, în Bruce Gilley and Andrew O'Neil (eds,), *Middle Powers and the Rise of China,* Georgetown University Press, 2014.
[19] Idem, p. 27.
[20] Andrew F. Cooper, Richard A. Higgott, Kim Richard Nossal, *Relocating Middle Powers: Australia and Canada in a Changing World Order,* UBC Press, Vancouver,1993, pp. 20–25.
[21] David A. Cooper, ‘‘Challenging Contemporary Notions of Middle Power Influence: Implications of the Proliferation Security Initiative for `Middle Power Theory` ”, *Foreign Policy Analysis,* vol. 7, nr. 3, 2011, pp. 317-319.
[22] Robert O. Keohane, ‘‘Lilliputians' Dilemmas: Small States in International Politics”, *International Organization,* vol. 23, nr. 2, 1969, pp. 291–310.
[23] Andrew Fenton Cooper, Timothy M. Shaw, *The Diplomacies of Small States: Between Vulnerability and Resilience,* Palgrave Macmillan, New York, 2009.
[24] James Manicom, Jeffrey Reeves, *Op. cit.,* p. 41.
[25] Bruce E. Moon, ‘‘The Foreign Policy of the Dependent State”, *International Studies Quarterly,* vol. 27, nr. 3, 1983, p. 315.
[26] Andrew F. Cooper, ‘‘Niche Diplomacy: A Conceptual Overview”, în Andrew F. Cooper (ed.), *Niche Diplomacy: Middle Powers after the Cold War,* Macmillan Press, Houndmills, UK, 1997, pp. 9–13.
[27] Kalevi J. Holsti, ‘‘National Role Conceptions and the Study of Foreign Policy”, *International Studies Quarterly,* vol. 14, nr. 3, 1970, pp. 233–309; Ronald L. Jepperson, Alexander Wendt, Peter J. Katzenstein, ‘‘Norms, Identity, and Culture in National Security”, în Peter J. Katzenstein (ed.), *The Culture of National Security: Norms and Identity in World Politics,* Columbia University Press, New York, 1996, pp. 33–75.
[28] Carl Ungerer, ‘‘The 'Middle Power' Concept in Australian Foreign Policy”, *Australian Journal of Politics and History,* vol. 53, nr. 4, 2007, p. 519.

[29] Eduard Jordaan, "The concept of a middle power in international relations: Distinguishing between emerging and traditional middle powers", *Politikon: South African Journal of Political Studies,* vol. 30, nr. 2, 2003, p. 167.
[30] Bruce Gilley, "Middle powers during great power transitions: China's rise and the future of Canada-US relations", *International Journal,* vol. 66, nr. 2 (Canada, the US, and China: A new Pacific triangle?), Spring 2011, Sage Publications, pp. 245-264.
[31] Hyung Min Kim, "Comparing measures of national power", *International Political Science Review,* vol. 31, nr. 4, 2010, pp. 405-427.
[32] Jeffrey Legro, "Purpose transitions: China's rise and the American response", în Robert S. Ross, Feng Zhu (eds.), *China's Ascent: Power, Security, and the Future of International Politics,* Cornell University Press, 2008, pp. 163-190.
[33] Andrew F. Cooper, Richard A. Higgott, Kim Richard Nossal, Op.cit.; a se vedea și Andrew Cooper, *Op.cit.,* pp. 1-24.
[34] Wenran Jiang, "Seeking a strategic vision for Canada-China relations", *International Journal,* vol. 64, nr. 4, 2009, p. 908.
[35] Tsuyoshi Kawasaki, "Strangers no longer: The identity shift in the Canada-Japan relationship", *International Journal,* vol. 64, nr. 4, 2009, pp. 879-890.
[36] Malcolm Davis, *Australia as a rising Middle Power,* RSIS Working Paper, nr. 328, S. Rajaratnam School of International Studies, 2020, 36 p.; http://www.jstor.com/stable/resrep24285.
[37] Andrew Hastie, "We must see China – the opportunities and the threats – with clear eyes", *The Sydney Morning Herald,* August 8, 2019; www.smh.com.au/politics/federal/we-must-see-china-the-opportunities and-the-threats-with-clear-eyes-20190807-p52eon.html.
[38] Varrall Merriden, "Does China's rise threaten the rules-based order?", *The Interpreter,* June 7, 2017; www.lowyinstitute.org/the-interpreter/does-china-rise-threaten-rules-based-order.
[39] Department of Foreign Affairs and Trade, Australian Government, "Opportunity, Security, Strength: The 2017 Foreign Policy White Paper", November 23, 2017, p. 4.; www.dfat.gov.au/news/news/Pages/opportunity security-strength-the-2017-foreign-policy-white-paper.
[40] Andrew Carr, "Is Australia a middle power? A systemic impact approach", *Australian Journal of International Affairs,* vol. 68, nr. 1, 2014, pp. 70-84; DOI:10.1080/10357718.2013.840264.
[41] Thomas Hegghammer, "Small and Middle Powers", în David G. Lewis, Aniseh Bassiri Tabrizi (eds.), *Regional Powers and Post-NATO Afghanistan,* NATO Defense College, 2021; https://www.jstor.org/stable/resrep33620.12.
[42] Austin Gee, Robert G. Patman, "Small state or minor power? New Zealand's Five Eyes membership, intelligence reforms, and Wellington's response to China's growing Pacific role", *Intelligence and National Security,* vol. 36, nr. 1, pp. 34-50; DOI: 10.1080/02684527.2020.1812876.
[43] Baldur Thorhallsson, "Small States and the Changing Global Order: What Small State Theory Can Offer New Zealand Foreign Policymaking", pp. 379–393, în Anne-Marie Brady (ed.), *Small States and the Changing Global Order: New Zealand Faces the Future,* The World of Small States, Springer, 2019.
[44] Salma Malik, "US war in Iraq in the light of the major and minor powers conflict", *The Turkish Yearbook,* vol XXV, pp. 83-106, 2004.
[45] Volker Krause, David J. Singer, "Minor Powers, Alliances, and Armed Conflict: Some Preliminary Patterns", în Erich Reiter, Heinz Gärtner (eds.), *Small States and Alliances,* Physica-Verlag, Heidelberg, 2001, pp 15–23; https://doi.org/10.1007/978-3-662-13000-1_3.
[46] Odd Arne Westad, *The Global Cold War: Third World Interventions and the Making of Our Times,* Cambridge University Press, 2005.
[47] Eitan J. Rosen, *The influence of minor powers during the Cold War,* BA Thesis, May 2021, State University of New York, 38 p.
[48] B. Thorhallsson, *Op. cit.,* p. 34.
[49] *Ibidem.*
[50] Christoph Mikulaschek, *Minor powers' influence in international organizations: Empirical evidence exploiting the natural experiment of African representation on the UN Security Council,* Paper prepared for presentation at the 8th Annual Conference on the Political Economy of International Organizations, February 12-14, 2015.
[51] Peter Katzenstein, *Small States in World Markets: Industrial Policy in Europe,* Ithaca, NY, Cornell University Press, 1985; Andrew Moravcsik, *The Choice for Europe: Social Purpose and State Power from Messina to Maastricht,* Ithaca, NY, Cornell University Press, 1998; Randall W. Stone, *Controlling Institutions: International Organizations and the Global Economy,* Cambridge, UK, Cambridge University Press, 2011.
[52] Stephen D. Krasner, *Structural Conflict: The Third World Against Global Liberalism,* Berkeley, CA, University of California Press, 1985.
[53] Lloyd Gruber, *Ruling the World: Power Politics and the Rise of Supranational Institutions,* Princeton, NJ, Princeton University Press, 2000.
[54] Mona M. Lyne, Daniel L. Nielson, Michael J. Tierney, "Who delegates? Alternative models of principals in development aid", în Darren G. Hawkins, David A. Lake, Daniel L. Nielson and Michael J. Tierney (eds.), *Delegation and Agency in International Organizations,* vol. 32, Cambridge University Press, 2006, pp. 41–76; a se vedea și Mark Copelovitch,

Daniel Nielson, Ryan Powers and Michael J. Tierney, *The Unipolar Fallacy: Common Agency, American Interests, and International Financial Institutions,* Prepared for presentation at the 2014 PEIO Conference, 2014, 48 p.

[55] Amrita Narlikar, *Bargaining over the Doha development agenda: Coalitions in the World Trade Organization,* Latin American Trade Network Working Paper, nr. 36, 2005; Donna Lee, "Bringing an Elephant into the Room: Small African State Diplomacy in the WTO", în Andrew F. Cooper, Timothy M. Shaw (eds.), *The Diplomacy of Small States: Between Vulnerability and Resilience,* Palgrave Macmillan, London, 2009, pp. 195–206.

[56] Mattila Mikko, "Fiscal transfers and redistribution in the European Union: do smaller member states get more than their share?", *Journal of European Public Policy,* vol. 13, nr. 1, 2006, pp. 34–51; Deniz Aksoy, Jonathan Rodden, "Getting into the game: legislative bargaining, distributive politics, and EU enlargement", *Public Finance and Management,* vol. 9, nr. 4, 2009, pp. 613–643.

[57] Jonas Tallberg, "Bargaining Power in the European Council", *Journal of Common Market Studies,* vol. 46, nr. 3, 2008, pp. 685–708.

[58] Jonathan B. Slapin, "Exit, Voice, and Cooperation: Bargaining Power in International Organizations and Federal Systems", *Journal of Theoretical Politics,* vol. 21, nr. 2, 2009, pp.187-211; Christina J. Schneider, "Weak States and Institutionalized Bargaining Power in International Organizations", *International Studies Quarterly,* vol. 55, nr. 2, 2011, pp. 331-355.

[59] Volker Krause, David J. Singer, *Op. cit.,* https://doi.org/10.1007/978-3-662-13000-1_3.

[60] Randolph M. Siverson, Joel King, "Attributes of National Alliance Membership and War Participation, 1815-1965", *American Journal of Political Science,* vol. 24, nr. 1, 1980, pp. 1-15.

[61] *Ibidem.*

[62] Marinko Bobic, *Why minor powers risk wars with major powers. A comparative study of the post-Cold War era,* Bristol University Press, 2019.

[63] Charles L. Glaser, *Rationalist Theory of International Politics. The Logic of Competition and Cooperation*, Princeton, NJ, Princeton University Press, 2010.

[64] Ivan Arreguín-Toft, "How the Weak Win Wars. A Theory of Asymmetric Conflict", *International Security*, vol. 26, nr. 1, Harvard Kennedy School, 2001, pp. 93–128.

[65] Michael A. Allen, Benjamin O. Fordham, "From Melos to Baghdad: Explaining resistance to militarized challenges from more powerful states", *International Studies Quarterly*, vol. 55, nr. 4, 2011, pp.1025–1045.

[66] Michael G. Findley, Scott Edwards, "Accounting for the Unaccounted: Weak-Actor Social Structure in Asymmetric Wars', *International Studies Quarterly*, vol. 51, nr. 3, 2007, pp. 583–606.

[67] Jeremy Ginges, Scott Atran, "War as a moral imperative (not just practical politics by other means)", în *Proceedings of the Royal Society B: Biological Sciences*, vol. 278, nr. 1720, 2011, pp. 2930–2938.

[68] Bruce Bueno de Mesquita, Alastair Smith, Randolph M. Siverson, James D. Morrow, *The Logic of Political Survival*, Cambridge, MA, The MIT Press, 2005.

[69] John Mueller, "The Iraq Syndrome", *Foreign Affairs*, vol. 84, nr. 6, Council on Foreign Relations, 2005, pp. 44–54.

[70] João Paulo Nicolini Gabriel, Henoch Gabriel Mandelbaum, Carlos Eduardo Carvalho, *The Quad: One More 'Minilateral' Initiative, Not an Embryonic Military Alliance in the Indo-Pacific Region*, 13 august 2020; https://www.researchgate.net/publication/343626022_The_Quad_One_More_'Minilateral'_Initiative_not_an_Embryonic_Military_Alliance_in_the_Indo-Pacific_Region, DOI: 10.21530/ci.v15n2.2020.1014.

[71] Dhruva Jaishankar, *The Real Significance of the Quad*, Australian Strategic Policy Institute, October 24, 2018; Joel Wuthnow, "US 'Minilateralism' in Asia and China's Responses: A New Security Dilemma?", *Journal of Contemporary China*, vol. 28, nr. 115, 2019, pp. 133-150.

[72] Michael J. Green, "Strategic Asian triangles", în Saadia M. Pekkanen, John Ravenhill, Rosemary Foot (eds.), *The Oxford Handbook of the International Relations of Asia*, New York, Oxford University Press, 2014, pp. 758-774.

[73] William T. Tow, "Minilateral security's relevance to US strategy in the Indo-Pacific: challenges and prospects", *The Pacific Review*, vol. 32, nr. 2, 2019, pp. 232-244; DOI: 10.1080/09512748.2018.1465457.

[74] Miles Kahler, "Multilateralism with small and large numbers", *International Organization*, vol. 46, nr. 3, The MIT Press, 1992, pp. 681-708; Brad Glosserman, Scott A. Snyder, *The Japan–South Korea Identity Clash: East Asian Security and the United States*, Columbia University Press, New York, 2015; Kenneth A. Oye, "Explaining Cooperation under Anarchy: Hypotheses and Strategies", *World Politics*, vol. 38, nr. 1, Cambridge University Press, 1985, pp. 1-24.

[75] Victor D. Cha, "The dilemma of regional security in East Asia: Multilateralism versus bilateralism", în Paul F. Diehl, Joseph Levgold (eds.), *Regional conflict management*, Bloomsbury Academic, 2003, pp. 104–122.

[76] Moises Naim, "Minilateralism: The magic number to get real international action", *Foreign Policy*, 2009, June 21, 2009; http://foreignpolicy.com/2009/06/21/minilateralism/.

[77] Stewart Patrick, "The New `New Multilateralism`: Minilateral Cooperation, But at What Cost?", *Global Summitry: Politics, Economics, and Law in International Governance*, Global Summitry Project, vol. 1, nr. 2, 2015, pp. 115–134.

[78] Amalina Anuar, Nazia Hussain, *Minilateralism for Multilateralism in the Post-COVID Age. Challenges to Minilateralism*, Policy Report, S. Rajaratnam School of International Studies, January 2021, 11 p.; https://www.jstor.org/stable/resrep28278.5.

[79] Sung-Mi Kim, Sebastian Haug, Susan Harris Rimmer, "Minilateralism Revisited: MIKTA as Slender Diplomacy in a Multiplex World", *Global Governance*, vol. 24, nr. 4, Brill, 2018, pp. 475-489.

[80] Marina Larionova, Andrey Shelepov, "Is BRICS Institutionalization Enhancing its Effectiveness?", în Marek Rewizorski (ed.), *The European Union and the BRICS. Complex Relations in the Era of Global Governance*, Springer, 2015, pp. 39-55; Prashanth Parameswaran, "The limits of minilateralism in ASEAN", *The Straits Times*, February 2018.

[81] Lai-Ha Chan, Maria Rost Rublee, "The promise of AUKUS: implications of its minilateral institutional form", *Australian Journal of International Affairs*, vol. 78, nr. 6, 2024, pp. 848-868; DOI: 10.1080/10357718.2024.2421369.

[82] Barbara Koremenos, Charles Lipson, Duncan Snidal,"The Rational Design of International Institutions", *International Organization*, vol. 55, nr. 4, The MIT Press, 2001, pp. 761–799.

[83] Mason Richey, Daewon Ohn, "It's fine in practice, but how about in theory? State-of-the-art minilateralism between expectations and reality", *Australian Journal of International Affairs*, vol. 78, nr. 6, 2024, pp. 782-807; https://doi.org/10.1080/10357718.2024.2409361.

[84] Leah Matchett, "Minilateralism and Backlash in the Nuclear Security Summit: The Consequences of Nuclear Governance Outside the IAEA", *Security Studies*, vol. 30, nr. 5, 2021, pp. 823–859.

[85] Jaganath Panda, Daewon Ohn, "Minilateralism and the new Indo-Pacific order: theoretical ambitions and empirical realities", *Australian Journal of International Affairs*, vol. 78, nr. 6, 2024, pp. 767-781; https://doi.org/10.1080/10357718.2024.2410411.

[86] Lora Anne Viola, "US Strategies of Institutional Adaptation in the Face of Hegemonic Decline", *Global Policy*, vol. 11, nr. 3 (special issue: *Global Power Shifts: How do International Institutions Adjust?*), Wiley, 2020, pp. 28–39.

[87] The White House*, National Security Strategy of the United States of America*, November 2025; https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf.

[88] Iulian Chifu, *Marea Neagră într-o arhitectură de securitate întărită: minilaterale, convergența puterilor mijlocii, rolul critic al puterilor minore*, Calea Europeană, 9 iunie 2026; https://www.caleaeuropeana.ro/iulian-chifu-marea-neagra-intr-o-arhitectura-de-securitate-intarita-minilaterale-convergenta-puterilor-mijlocii-rolul-critic-al-puterilor-minore/

[89] Iulian Chifu, *Noua arhitectură de securitate a Europei: rolul Ucrainei și al Turciei*, Calea Europeană, 25 mai 2026; https://www.caleaeuropeana.ro/iulian-chifu-noua-arhitectura-de-securitate-a-europei-rolul-ucrainei-si-al-turciei/

[90] Iulian Chifu, *Marea Neagră .....*

[91] Iulian Chifu, *Noua arhitectură de securitate a Europei .....*

[92] Iulian Chifu, *Marea Neagră .....*

[93] Iulian Chifu, *Noua arhitectură de securitate a Europei.*

[94] Bundesrepublik Deutschland, Der Bundeskanzler*, Letter to the EU institutions*, 28 May 2026, https://newunionpost.eu/wp-content/uploads/2026/05/260518-BK-letter-to-PEC-et-al.pdf; Peter von Elsuwege, Roman Petrov, *Towards an "Associate Membership" Status for Ukraine?,* 28 May 2026, https://verfassungsblog.de/towards-an-associate-membership-status-for-ukraine/

[95] Iulian Chifu, "Reziliența în război și caracteristicile intangibile. Cazul războiului de agresiune al Rusiei în Ucraina", *Infosfera*, nr. 3/2023, pp. 13-20.

[96] Iulian Chifu, *Noua arhitectură de securitate a Europei.*

„CAPCANA LUI TUCIDIDE” ȘI RELEVANȚA EI ÎN SECOLUL AL XXI-LEA

Ionuț-Răzvan BUCUR*

Abstract

This essay examines the relevance of the "Thucydides Trap" concept, formulated by Graham Allison, for analyzing the major geopolitical rivalries of the 21st century. Proceeding from the premise that the Allisonian model, while useful as a diagnostic tool, offers an incomplete explanation of contemporary dynamics, the paper tests the theoretical framework by applying it to three current case studies: the United States – People's Republic of China rivalry, the United States – Russian Federation confrontation, and the United States – Islamic Republic of Iran conflict. The essay takes as its starting point the reconstruction of the concept's genesis, framing it within a theoretical foundation. Subsequently, the research develops three distinct conflict architectures: the canonical pattern of the rising power, the declining power trap, and preventive hegemonic war. The essay argues that contemporary nuclear rivalries compel a transition toward proxy warfare and demonstrates that the internal vulnerability of the dominant power, theorized by analogy with the stasis described by Thucydides, constitutes a neglected dimension of strategic competition.

Keywords: *Thucydides Trap; strategic competition; power; conflict; Sino-American rivalry; preventive war; proxy war.*

INTRODUCERE

Conceptul *„Capcana lui Tucidide”* a devenit, în ultimul deceniu, un reper al dezbaterii despre rivalitățile dintre marile puteri. Originile sale se află în analiza pe care istoricul grec Tucidide a dedicat-o Războiului Peloponesiac, iar premisa lui este că atunci când o putere ascendentă amenință să detroneze puterea dominantă, tensiunea rezultată împinge sistemul spre război. Ordinea internațională de după Războiul Rece a fost construită pe așteptarea că redistribuirile de putere vor putea fi gestionate prin instituții și norme comune, însă ascensiunea Republicii Populare Chineze, războiul din Ucraina și conflictul declanșat în februarie 2026 de Statele Unite și Israel împotriva Iranului au pus această așteptare sub semnul întrebării

De aici pornește o întrebare fundamentală: sistemul internațional contemporan reproduce logica care a generat marile conflicte ale trecutului sau asistăm la forme inedite de rivalitate pe care instrumentarul clasic le explică doar parțial? Ipoteza noastră este că modelul lui Graham Allison, deși valoros ca instrument de diagnosticare, rămâne incomplet. Trei trăsături esențiale ale prezentului (armele nucleare,

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

interdependența economică și capacitatea actorilor revizioniști de a submina democrațiile din interior) impun completarea cadrului clasic cu trei categorii suplimentare. Acestea sunt „capcana puterii în declin", războiul preventiv hegemonic și vulnerabilizarea internă, fenomen denumit, după modelul antic, un *„cal troian"* instituțional. Altfel spus, marile puteri ale momentului gravitează mai degrabă în jurul „capcanei lui Tucidide", adoptând arhitecturi de conflict menite să evite confruntarea directă, în timp ce îi redistribuie constant costurile.

Relevanța temei abordate derivă din faptul că descrie tipare istorice și, în egală măsură, avertizează decidenții asupra riscului de conflict sistemic în punctele nevralgice ale ordinii actuale. Eseul este structurat în trei capitole. Primul reconstituie geneza și fundamentele teoretice ale conceptului, pornind de la rivalitatea antică dintre Sparta și Atena, ajungând la reformulările moderne ale lui Organski și Gilpin, incluzând și criticile aduse modelului. Al doilea aplică acest cadru analitic asupra celor trei rivalități majore ale momentului, tratate drept arhitecturi distincte. Ultimul capitol examinează două mecanisme principale prin care marile puteri își gestionează astăzi rivalitatea, analizând specific războiul prin proxy și tacticile de subminare internă a puterii dominante.

GENEZA ȘI FUNDAMENTELE TEORETICE ALE „CAPCANEI LUI TUCIDIDE"

Sparta și Atena: originile istorice ale conceptului

Pentru a înțelege *„Capcana lui Tucidide"* în profunzimea ei, trebuie reconstituit contextul din care provine. La mijlocul secolului al V-lea î.Hr., lumea greacă era dominată de două puteri cu structuri politice, economice și militare radical diferite. Sparta era o oligarhie militară terestră, cu o economie bazată pe exploatarea unei populații de servi (*hiloții*[1]), a cărei supraveghere constantă impunea un conservatorism strategic și o prudență extremă în angajarea forțelor departe de Pelopones. Modelul său de organizare socială era stabil, dar static, orientat spre menținerea echilibrului intern și a hegemoniei în Pelopones, prin sprijinirea regimurilor oligarhice aliate[2].

Atena era, prin contrast, o democrație comercială și maritimă în plină expansiune, a cărei putere se baza pe controlul fluxurilor financiare. În urma victoriei asupra perșilor, la Salamina (480 î.Hr.), și a formării Ligii de la Delos[3] (478 î.Hr.), Atena a transformat treptat această alianță defensivă într-un imperiu naval centralizat. Momentul decisiv al acestei transformări a fost mutarea tezaurului Ligii de la Delos la Atena (454 î.Hr.), act care a permis utilizarea tributului nu doar pentru apărarea comună, ci și pentru finanțarea programului politic și de dezvoltare promovat de Pericle și consolidarea democrației prin plata funcțiilor publice[4].

Această ascensiune spectaculoasă a Atenei a generat în Sparta o anxietate profundă, pe care Tucidide o identifică drept cauza fundamentală a conflictului. Sparta nu se temea doar de capacitatea militară a Atenei, ci și de dinamismul său incontrolabil și de posibilitatea ca un imperiu naval bogat să poată susține un război de uzură pe termen lung, neutralizând superioritatea terestră a Spartei[5]. Tucidide sintetizează această dinamică în celebra sa teză: *„Adevărata cauză a războiului, deși cel mai puțin mărturisită în public, a fost, în opinia mea, creșterea puterii Atenei și alarma pe care aceasta a trezit-o în Sparta, făcând războiul inevitabil"*[6].

Declanșatorul imediat al războiului (disputele privind Corcyra și Potideea între 435 și 432 î.Hr.) a reprezentat doar scânteia care a activat tensiunea structurală acumulată în deceniile de *Pentecontaetia*[7]. Dincolo de motivațiile tradiționale legate de prestigiu și onoare, decizia Spartei de a declanșa războiul a fost dictată fundamental de identificarea unei ferestre de oportunitate strategică. Sub presiunea constantă a aliaților corintieni, elita spartană a conștientizat că orice amânare a confruntării i-ar fi permis Atenei să își consolideze decisiv avantajul naval prin absorbția flotei din Corcyra. O asemenea evoluție ar fi înclinat balanța de putere într-un mod iremediabil în defavoarea sa. În esență, această convingere că timpul lucrează împotriva

puterii hegemonice a acționat ca un motor psihologic, transformând o competiție structurală într-un conflict militar deschis.

Un alt element tucididian relevant este Dialogul Melian (416 î.Hr.), care marchează punctul în care Atena abandonează orice pretenție de hegemonie în favoarea unei tiranii imperiale. În fața refuzului melienilor de a se supune, generalii atenieni au formulat explicit legea naturală a puterii: *„Cei puternici fac ceea ce le permite puterea, iar cei slabi suferă ceea ce trebuie să sufere”*[8]. Această transformare ilustrează ciclul puterii în care fosta putere ascendentă, care invoca dreptatea împotriva perșilor, devine puterea instalată care își apără poziția prin forță, confirmând viziunea lui Tucidide asupra naturii umane neschimbătoare în condiții de presiune extremă.

De la Tucidide la Allison: reconstrucția modernă a conceptului

Graham Allison a extras intuiția tucididiană din contextul antichității și a transpus-o într-un model analitic aplicabil relațiilor internaționale. El a întocmit un *„dosar de caz”* cuprinzând 16 tranziții de putere din ultimele cinci secole, în care o putere ascendentă a amenințat să detroneze o putere hegemonică. Rezultatele acestui test empiric au evidențiat că, în 12 dintre cele 16 situații studiate, rivalitatea structurală s-a soluționat prin război[9]. Allison definește *„capcana lui Tucidide”* drept stresul structural natural și periculos care apare atunci când o putere emergentă perturbă echilibrul stabilit, generând o reacție defensivă dublată de teamă în rândul puterii instalate[10]. Existența celor patru cazuri în care tranziția s-a realizat fără conflict demonstrează că ieșirea din logica *„capcanei lui Tucidide”* depinde de adaptările profunde ale atitudinilor guvernamentale și sociale. Cel mai des invocat exemplu în acest sens este *„marea reapropiere”* dintre Marea Britanie și Statele Unite, de la începutul secolului al XX-lea, un transfer de hegemonie facilitat nu doar de identitatea culturală și lingvistică comună, ci și de recunoașterea de către Londra a supremației americane în emisfera vestică în schimbul unei alianțe tactice împotriva Germaniei.

№	Period	Ruling Power	Rising Power	Domain	Result
1	Late 15th century	Portugal	Spain	Global empire and trade	No war
2	First half of 16th century	France	Hapsburgs	Land power in western Europe	War
3	16th and 17th centuries	Hapsburgs	Ottoman Empire	Land power in central and eastern Europe, sea power in the Mediterranean	War
4	First half of 17th century	Hapsburgs	Sweden	Land and sea power in northern Europe	War
5	Mid-to-late 17th century	Dutch Republic	England	Global empire, sea power, and trade	War
6	Late 17th to mid-18th centuries	France	Great Britain	Global empire and European land power	War
7	Late 18th and early 19th centuries	United Kingdom	France	Land and sea power in Europe	War
8	Mid-19th century	France and United Kingdom	Russia	Global empire, influence in Central Asia and eastern Mediterranean	War
9	Mid-19th century	France	Germany	Land power in Europe	War
10	Late 19th and early 20th centuries	China and Russia	Japan	Land and sea power in East Asia	War
11	Early-20th century	United Kingdom	United States	Global economic dominance and naval supremacy in the Western Hemisphere	No war
12	Early-20th century	United Kingdom supported by France, Russia	Germany	Land power in Europe and global sea power	War
13	Mid-20th century	Soviet Union, France, UK	Germany	Land and sea power in Europe	War
14	Mid-20th century	United States	Japan	Sea power and influence in the Asia-Pacific region	War
15	1940s–1980s	United States	Soviet Union	Global power	No war
16	1990s–present	United Kingdom and France	Germany	Political influence in Europe	No war

Fig. 1 *– 16 rivalități analizate de Graham Allison*
(sursa: https://www.theatlantic.com/international/archive/2015/09/united-states-china-war-thucydides-trap/406756/, accesată la data de 12 mai 2026)

Totuși, aplicabilitatea acestui model la relația contemporană dintre SUA și R.P.Chineză este contestată de numeroși cercetători, care subliniază că absența afinităților ideologice și interdependența economică dată de globalizare, inexistente la momentul conflictului dintre Atena și Sparta, creează o dinamică diferită, unde riscul provine din posibilitatea ca o putere emergentă care consideră că este în declin să acționeze impulsiv[11].

Teoria tranziției de putere: Organski, Gilpin și tradiția realistă

Argumentul lui Allison se înscrie într-o tradiție teoretică care a contestat profund dogma clasică a echilibrului puterii. În lucrarea sa de referință (*World Politics,* 1958), A.F.K. Organski a propus o paradigmă diferită de viziunea tradițională, demonstrând că paritatea de putere generează, de fapt, momentul de risc maxim pentru declanșarea unui conflict. Conform modelului tranziției de putere, probabilitatea unui război sistemic atinge cota maximă atunci când un actor emergent, susținut de o expansiune rapidă a resurselor sale interne (demografice

și industriale), ajunge să egaleze capacitățile puterii dominante. Această tensiune structurală erupe inevitabil în momentul în care statul aflat în ascensiune își manifestă deschis nemulțumirea față de regulile și distribuția beneficiilor din *statu-quo*-ul internațional impus de hegemon[12].

Valoarea de durată a acestui cadru de analiză a fost recunoscută inclusiv de Robert Gilpin, care a evidențiat permanența trăsăturilor fundamentale ale relațiilor internaționale de-a lungul mileniilor, acestea fiind definite invariabil de o luptă continuă pentru resurse și putere într-un mediu anarhic. Teoreticianul a susținut explicit superioritatea relatării lui Tucidide privind războaiele hegemonice în fața oricărei alte generalizări din domeniu, considerând-o un fundament indispensabil pentru dezvoltarea modelelor contemporane[13].

Prin sinteza acestor contribuții teoretice majore, Allison reușește să dezvolte un instrument analitic cu o dublă valență. Pe de o parte, acesta îndeplinește o funcție descriptivă esențială pentru ordonarea logică a datelor istorice din ultimele cinci secole. Pe de altă parte, instrumentul capătă o puternică dimensiune prescriptivă, avertizând factorii de decizie asupra urgenței de a recalibra eforturile diplomatice în scopul evitării unui deznodământ violent în cadrul actualei rivalități sino-americane.

În final, reconstituirea atentă a genezei conceptului evidențiază caracterul selectiv al lecturii pe care Allison o aplică textelor scrise de Tucidide. Istoricul atenian a evitat să formuleze o teorie a tranziției de putere în sensul propus de Organski[14], preferând să construiască o analiză axată pe rolul fricii structurale, ca motor principal al deliberării politice viciate. Celebra referință din prima sa carte, vizând expansiunea Atenei și alarma pe care aceasta a declanșat-o în Sparta, ilustrează înainte de toate un mecanism psihologic și instituțional, distanțându-se clar de rigorile unei legi a puterii materiale. Organski și Gilpin au rafinat ulterior această intuiție timpurie pentru a o integra într-un model probabilistic, abordare căreia Allison i-a conferit o formă empirică sistematică. Totuși, valoarea incontestabilă a acestor contribuții rămâne condiționată de aplicarea lucidă a aparatului conceptual, impunând o distincție permanentă între limitele analogiei istorice și predicțiile analitice structurale.

TREI RIVALITĂȚI ANALIZATE PRIN PRISMA „CAPCANEI LUI TUCIDIDE”

SUA – R.P. Chineză: cazul tucididian al puterii ascendente

Republica Populară Chineză a parcurs o tranziție rapidă spre statutul de putere regională dominantă în Asia de Est. De la un PIB de aproximativ 1,2 trilioane de dolari, în anul 2000, economia chineză a ajuns la aproximativ 19,8 trilioane USD în 2024, reprezentând în jur de 17% din PIB-ul mondial, față de 29,8 trilioane USD ai SUA. Această creștere a fost însoțită de modernizarea radicală a Armatei Populare de Eliberare a R.P.Chineze și de proiecția influenței prin Inițiativa „Belt and Road”, cu investiții cumulate de peste 2,5 trilioane USD, din 2005 până în prezent[15]. Strategia de Securitate Națională a SUA din 2025 reflectă această realitate, identificând R.P.Chineză drept singurul competitor care deține atât intenția, cât și capacitatea de a reconfigura ordinea internațională[16]. Această dinamică a ascensiunii este nuanțată de teza *„Chinei la apogeu”*, care sugerează că Beijingul s-ar putea confrunta cu un declin structural cauzat de criza demografică, datorii financiare și scăderea productivității. Conform acestei perspective, riscul major nu provine dintr-o creștere continuă a puterii statutului chinez, ci din *„*zona de pericol*”* în care o putere aflată la zenit, temându-se că viitorul va fi mai puțin favorabil decât prezentul, devine mult mai impulsivă și predispusă la agresiune pentru a-și securiza obiectivele înainte ca fereastra sa de oportunitate strategică să se închidă definitiv. În această ecuație, „capcana lui Tucidide” este dublată de o vulnerabilitate distinctă, numită *„capcana puterii în declin”*[17]. În acest context, teama pierderii ireversibile a momentului istoric acționează ca un catalizator puternic, declanșând conflicte pe care o putere aflată pe o traiectorie ascendentă stabilă le-ar fi evitat în mod firesc.

Rivalitatea sino-americană este multidimensională și a evoluat de la un model bazat pe „decoupling" (decuplare totală) spre unul de „de-risking"[18] și fragmentare structurală tehnologică și economică. Dimensiunea economică a generat un război al tarifelor început sub prima Administrație Trump și menținut de cea a președintelui Biden, devenind apoi o dispută pentru supremație în domenii precum semiconductorii și energia verde. În plan militar, Strâmtoarea Taiwan rămâne punctul critic, nu doar din rațiuni de prestigiu pentru Beijing, ci și pentru rolul ei în controlul lanțurilor de aprovizionare. Dimensiunea tehnologică adaugă o nouă arenă de confruntare, cuprinzând inteligența artificială, rețelele 5G și tehnologiile cuantice, considerate decisive pentru echilibrul de putere pe termen lung[19]. Pentru Washington, miza nu mai este doar descurajarea militară, ci, foarte probabil, împiedicarea R.P.Chineze de a atinge autosuficiența tehnologică în sectoarele decisive.

Dinamica recentă demonstrează, însă, că rivalitatea oscilează constant între o escaladare și dezescaladare negociată, realitate care validează pe deplin ipoteza unui model teoretic incomplet. În noiembrie 2025, cele două state au perfectat un acord comercial limitat, prin care Statele Unite au redus la jumătate (de la 20% la 10%) tarifele asociate fentanilului și au prelungit exceptările aferente Secțiunii 301[20] până în noiembrie 2026. În contrapartidă, Beijingul a suspendat, pentru un an, controlul exporturilor de pământuri rare, măsură instituită inițial în luna octombrie a aceluiași an[21]. O reorientare și mai surprinzătoare s-a produs în intervalul decembrie 2025 – ianuarie 2026, urmare a deciziei Administrației Trump de a autoriza vânzarea cipurilor avansate de inteligență artificială către China, anulând astfel restricțiile anterioare. Condiționarea acestei măsuri de colectarea, de către guvernul american, a 25% din valoarea vânzărilor companiei Nvidia a atras critici vehemente din partea foștilor oficiali[22]. Decizia a fost percepută drept o tranzacționare periculoasă a securității naționale în schimbul unor concesii strict comerciale. Tabloul geopolitic a suferit noi complicații în februarie 2026, odată cu hotărârea Curții Supreme de Justiție a SUA privind limitarea puterii președintelui de a utiliza legea IEEPA[23] pentru impunerea tarifelor. Drept urmare, executivul american a ridicat restricțiile inițiale, introducând în schimb un tarif global de 10% pe o perioadă de 150 de zile, invocând Secțiunea 122 din Legea comerțului[24]. Această succesiune de oscilații ilustrează limpede o rivalitate gestionată prin tranzacții pragmatice succesive, contrazicând direct teza unui determinism inerent al conflictului.

Pe de altă parte, o trăsătură distinctivă a strategiei chineze actuale este construcția unei „economii cetate", menită să asigure autosuficiența în sectoare critice și să reducă expunerea la sancțiuni. Totodată, recunoașterea oficială a statului chinez ca un competitor de tip *„near-peer"* în Strategia de Securitate Națională a SUA din 2025 marchează o schimbare de paradigmă în care Washingtonul nu mai privește rivalitatea ca pe o confruntare ideologică, ci ca pe un concurs al producției industriale și tehnologice. Un fapt notabil este că însuși președintele Xi Jinping a invocat explicit *„capcana lui Tucidide"* la finalul ultimei întrevederi oficiale cu șeful statului american de la Beijing, chestionând dacă *„pot China și Statele Unite să depășească așa-numita Capcană a lui Tucidide și să creeze o nouă paradigmă pentru relațiile dintre marile puteri?"*[25]. Această referință directă demonstrează că modelul funcționează nu doar ca instrument analitic academic, ci și ca potențial cadru de negociere și relaționare diplomatică la cel mai înalt nivel. Cazul rivalității sino-americane rămâne cel mai bun exemplu al *„capcanei lui Tucidide"*, în sensul existenței unei puteri ascendente reale, care provoacă hegemonia unei puteri instalate în toate dimensiunile puterii.

SUA - Federația Rusă: „capcana puterii în declin"

Relația dintre Statele Unite și Federația Rusă ilustrează o variantă diferită a logicii tucididiene, fiind guvernată de anxietatea declinului în locul ambițiilor specifice unei puteri aflate în ascensiune. Având în vedere decalajul economic imens înregistrat în anul 2025 (PIB-ul Federației Ruse a fost doar de 2,08 trilioane

USD, comparativ cu cele 30,51 trilioane USD al SUA), capacitatea Moscovei de a susține un efort hegemonic pe termen lung este limitată. În acest context, modelul clasic propus de Graham Allison beneficiază de completarea oferită de cercetătorii Hal Brands și Michael Beckley, prin teza *„capcanei puterii în declin”*. Conform acestei perspective, un actor revizionist confruntat cu o stagnare severă, survenită după o perioadă de prosperitate, dezvoltă un comportament pronunțat impulsiv. Statul va acționa agresiv pentru a preîntâmpina pierderile viitoare, încercând să profite de o fereastră de oportunitate strategică aflată pe punctul de a se închide definitiv[26].

Agresiunea declanșată împotriva Ucrainei, un conflict care a erodat substanțial prestigiul militar al Moscovei și a epuizat resurse financiare considerabile, se înscrie perfect în acest tipar de acțiune. Abordarea confirmă aplicarea unui veritabil *„keynesianism militar”*[27], un mecanism prin care statul își mobilizează ultimele rezerve interne exclusiv pentru a forța o reconfigurare a ordinii internaționale în favoarea sa[28]. Sustenabilitatea acestui model de subzistență strategică se află sub o amenințare directă, generată de ritmul accelerat de consumare a rezervelor acumulate de-a lungul deceniilor anterioare. Fondul Bunăstării Naționale, pilonul tradițional al rezilienței macroeconomice ruse, a înregistrat o prăbușire dramatică a activelor lichide. Resursele sale s-au redus de la 113,5 miliarde USD, în momentul declanșării invaziei, la aproximativ 36,4 miliarde USD la începutul anului 2025, proiecțiile economice indicând o epuizare completă în cursul anului 2026[29]. Această vulnerabilitate financiară, combinată cu o rată ridicată a inflației și un exod masiv al capitalului uman înalt calificat, limitează sever opțiunile decizionale. Kremlinul este constrâns să prioritizeze obiectivele militare imediate în detrimentul oricăror planuri de diversificare economică, o direcție care adâncește inevitabil dependența față de R.P.Chineză pentru asigurarea tehnologiilor critice și a materiilor prime industriale.

O abordare analitică alternativă propune o inversare a polilor de percepție. Privind dinamica de securitate europeană din această perspectivă, Occidentul a acționat *de facto* ca o putere ascendentă în vecinătatea imediată a Rusiei, prin extinderea succesivă a Alianței Nord-Atlantice și atragerea politică a Ucrainei în sfera de influență a Uniunii Europene. În consecință, Moscova reacționează asemenea unei puteri instalate la nivel regional, încercând să blocheze o tendință de marginalizare percepută drept o amenințare existențială la adresa propriei identități de mare putere. William Burns, în perioada mandatului său de ambasador la Moscova, avertiza încă din februarie 2008 asupra acestui risc major. El sublinia că o eventuală aderare a Ucrainei la NATO ar reprezenta *„cea mai luminoasă dintre toate liniile roșii”* pentru întreaga elită rusă în ansamblul ei, depășind cu mult nivelul strict al cercului decizional condus de Vladimir Putin[30]. Avertismentul arăta clar că oricare dintre facțiunile politice de la Kremlin ar interpreta o asemenea perspectivă drept o provocare directă la adresa intereselor naționale fundamentale. Alimentată de acest complex al încercuirii occidentale, viziunea strategică a liderilor ruși a transformat teritoriul ucrainean dintr-un simplu stat vecin într-un teren de luptă decisiv pentru supraviețuirea Rusiei ca pol de putere în sistemul internațional.

Discursul susținut de Vladimir Putin la Conferința de Securitate de la München, în februarie 2007, rămâne documentul programatic al acestei temeri structurale, reprezentând o articulare timpurie a nemulțumirii profunde față de ordinea unipolară condusă de Statele Unite. Diferența esențială față de prototipul Spartei antice constă în natura statutului apărat. În loc să protejeze o hegemonie consolidată și stabilă, Federația Rusă urmărește să se mențină pe poziția unei *„puteri suficient de bune”*, apelând intens la tactici hibride și la instrumente de *sharp power*[31] pentru a-și compensa vulnerabilitatea economică în raport cu Alianța Nord-Atlantică.

Această poziție o transformă, în mod paradoxal, într-un actor mult mai imprevizibil și periculos pe termen scurt. O mare putere dominată de percepția că timpul lucrează împotriva sa și că restul lumii îi exploatează slăbiciunea temporară

devine puternic predispusă la asumarea unor riscuri militare majore, din dorința de a forța un echilibru capabil să îi garanteze prestigiul. Prin urmare, depășind tiparul clasic al unei forțe aflate în plină expansiune, agresiunea rusă reprezintă, în esență, reacția violentă a unui stat care conștientizează că închiderea ferestrei sale de oportunitate ar echivala cu o condamnare la irelevanță istorică[32].

Pe fondul acestei degradări continue a capacităților sale convenționale, arsenalul nuclear reprezintă instrumentul prin care Moscova reușește să mai mențină o formă de paritate simbolică și strategică în raport cu Statele Unite. Expirarea tratatului *New START*, în luna februarie a acestui an, cumulată cu revizuirea doctrinei nucleare rusești din 2024, marchează o tranziție evidentă către o postură de descurajare de tip coercitiv. Printr-o asemenea manevră strategică, riscul nuclear este transformat într-o pârghie de șantaj, concepută pentru a restrânge drastic spațiul de acțiune al puterii hegemonice.

SUA-Iran: războiul hegemonic preventiv

La data de 28 februarie 2026, Statele Unite și Israel au lansat Operațiunea *„Epic Fury”,* o campanie fulgerătoare constând în aproximativ 900 de lovituri aeriene executate pe parcursul a 12 ore. Țintele principale au vizat infrastructura militară iraniană și eșaloanele superioare ale regimului de la Teheran. Fundamentul strategic al acestei ofensive a pornit de la premisa că Iranul, pe fondul sancțiunilor și al protestelor interne din luna ianuarie a.c., ar fi incapabil să mai susțină o rezistență organizată în eventualitatea eliminării Liderului Suprem[33]. O dimensiune critică a acestui conflict este reprezentată de conturarea unei divergențe strategice profunde între Washington și Tel Aviv, o fractură care a complicat semnificativ desfășurarea operațiunilor și perspectivele de soluționare. În viziunea Israelului, capacitățile balistice iraniene și rețeaua regională de interpuși constituie amenințări de natură existențială, impunând o neutralizare totală. Prin contrast, Statele Unite au prioritizat securizarea imediată a Strâmtorii Hormuz și evitarea angrenării într-un nou conflict prelungit, capabil să deturneze resurse vitale de la competiția strategică principală din regiunea Indo-Pacifică. Această asimetrie de interese i-a plasat pe factorii de decizie americani într-o *„capcană a credibilității”.* Astfel, Washingtonul s-a văzut obligat să calibreze fin necesitatea unei descurajări militare ferme în raport cu riscul unei escaladări masive, perspectivă puternic respinsă de un public intern deja alarmat de volatilitatea prețurilor la combustibil[34].

Evoluțiile ulterioare au generat un blocaj cvasitotal al tranzitului maritim, moment în care Iranul a mutat centrul de greutate al conflictului asupra controlului Strâmtorii Hormuz. Începând cu data de 4 martie 2026, Garda Revoluționară Islamică a apelat la un arsenal hibrid compus din mine maritime, drone și ambarcațiuni de mici dimensiuni pentru a controla libertatea de navigație în regiune. Prin această mișcare tactică, un punct strategic vital, prin care tranzitează anual peste o cincime din volumul global de petrol și de gaze naturale lichefiate, a fost transformat într-un instrument major de presiune geopolitică.

Sub autoritatea noului lider, Mojtaba Khamenei, Teheranul a instituit un regim discriminatoriu de control și de taxare a navelor comerciale, măsură extremă care a redus traficul la doar 5% din volumul său obișnuit. Repercusiunile economice imediate ale acestor acțiuni au forțat statele asiatice, în calitatea lor de beneficiare principale ale rutei, să inițieze negocieri diplomatice bilaterale cu Iranul în vederea obținerii unui acces selectiv pentru navele considerate *„non-ostile”*[35]. Această paradigmă validează în mod direct teza *„capcanei puterii în declin”*, argumentată anterior în cadrul celorlalte două rivalități.

Un alt element de noutate tactică îl constituie implementarea de către Teheran a unui sistem sofisticat de taxare, instrumentat de Corpul Gardienilor Revoluției Iraniene. Prin intermediul acestui mecanism, tranzitul maritim prin strâmtoare a devenit strict condiționat de obținerea prealabilă a unui aviz de securitate. Pentru a eluda arhitectura restrictivă a sancțiunilor americane, Iranul a solicitat ca plata acestor taxe

să fie efectuată inclusiv în yuani chinezești. O asemenea decizie a facilitat comerțul direct cu Beijingul, transformând controlul maritim într-o veritabilă pârghie de presiune politică. Drept consecință, această strategie a subminat profund eforturile Statelor Unite de a coagula o coaliție internațională de securitate. Mai mult, manevra a constrâns marile puteri asiatice să negocieze aranjamente diplomatice individuale cu Teheranul, o situație care evidențiază clar limitele puterii militare convenționale a hegemonului atunci când este confruntat cu strategii asimetrice[36].

Efectul strategic major al acestui conflict asupra competiției globale constă în redistribuirea costurilor în favoarea R.P.Chineze. Statul chinez beneficiază din plin de distragerea atenției și a alocării resurselor americane către un teatru de operațiuni periferic. După cinci săptămâni de ostilități, Pakistanul a reușit să intermedieze un armistițiu fragil în perioada 7-8 aprilie 2026, un demers susținut printr-un impuls diplomatic decisiv din partea Beijingului. Ulterior, confruntarea a migrat către o paradigmă a *„războiului economic fragmentat”*, în cadrul căruia Statele Unite au impus un contra-embargou porturilor iraniene, în vreme ce Teheranul a menținut o serie de restricții selective, autorizând exclusiv tranzitul navelor aparținând unor state „prietene”, precum R.P.Chineză sau Pakistan. Această conjunctură ilustrează perfect modul în care R.P.Chineză capitalizează strategic pe seama *„vulnerabilității prin angajare”* a SUA în teatrele secundare de conflict[37]. Beijingul reușește, astfel, să își consolideze influența în rândul Sudului Global fără a se fi implicat direct în ostilități. În același timp, Washingtonul se vede constrâns să își epuizeze resursele militare pentru restabilirea libertății de navigație, fiind nevoit să lanseze eforturi operaționale majore, similare misiunii Project Freedom.

Evoluțiile din cursul lunii mai 2026 au acutizat această stare de incertitudine geoeconomică, transferând costurile conflictului asimetric direct asupra pieților globale. Pe fondul prelungirii restricțiilor de navigație impuse de Teheran, sectorul energetic a reacționat printr-o volatilitate extremă. Cotațiile internaționale ale barilului de petrol au înregistrat o ascensiune fulminantă, generând presiuni inflaționiste majore și vulnerabilizând implicit stabilitatea economică americană pe plan intern. În acest climat profund volatil, discursul președintelui Donald Trump a adoptat o linie a presiunii maxime, dublată de un apel ferm la partajarea efortului strategic. Liderul de la Casa Albă a reiterat imperativul restabilirii imediate a libertății de tranzit, solicitând totodată o implicare financiară și operațională mult mai asumată din partea aliaților asiatici și europeni, dependenți de această rută maritimă. Declarațiile prezidențiale au pendulat constant între proiecția unei forțe militare copleșitoare, menite să descurajeze definitiv regimul iranian, și dorința pragmatică de a proteja consumatorul american de șocul prețurilor la carburanți. Această dinamică ilustrează perfect dilema strategică a Washingtonului, constrâns să navigheze între imperativul menținerii credibilității sale de garant al securității globale și evitarea unor costuri economice capabile să erodeze capitalul politic al administrației.

Analiza structurală demonstrează o distanțare clară a acestui conflict de criteriile *„capcanei lui Tucidide”*, formulate de Graham Allison, principala divergență constând în absența elementului esențial al parității dintre o putere ascendentă și una instalată. Din punct de vedere cantitativ, în anul 2025, economia iraniană (evaluată la aproximativ 356,5 miliarde USD) reprezenta o simplă fracțiune în comparație cu forța economică a Statelor Unite. În absența acestui echilibru al forțelor, modul de acțiune se înscrie în logica *„războiului preventiv hegemonic”*[38]. În cadrul acestei arhitecturi strategice, puterea dominantă alege să intervină decisiv pentru a neutraliza o capacitate adversă în plină dezvoltare, anticipând și prevenind transformarea acesteia într-o amenințare existențială iremediabilă. Această abordare decizională este alimentată exact de teama față de o potențială *„Atena de mâine”*, un mecanism psihologic și strategic pe care Tucidide l-a identificat drept motorul fundamental al războiului hegemonic.

RĂZBOAIELE PRIN PROXY ȘI CALUL TROIAN

O trăsătură distinctivă a rivalităților contemporane, comparativ cu modelul clasic allisonian, constă în externalizarea deliberată a conflictului către teatre terțiare. În contextul descurajării nucleare, o confruntare frontală între marile puteri ar reprezenta o decizie strategică irațională. Astfel, actorii statali de prim rang optează constant pentru transferul costurilor majore ale competiției globale asupra unor state de dimensiuni reduse, transformându-le în zone tampon.

Războiul din Ucraina ilustrează perfect acest mecanism asimetric. Sprijinul masiv acordat de Washington forțelor ucrainene, materializat prin armament de precizie și produse de intelligence, facilitează degradarea progresivă a capacităților militare rusești în absența oricărui contact direct între cele două puteri nucleare. Analiza lui Amos Fox demonstrează complementaritatea strategiilor de *proxy* adoptate de ambele tabere, acestea alimentând un război de uzură caracterizat prin epuizarea rapidă a stocurilor și pierderi umane disproporționate[39]. Prin susținerea acordată Moscovei sub forma transferurilor tehnologice cu aplicabilitate militară și a sprijinului diplomatic, R.P.Chineză reușește să își consolideze influența în rândul Sudului Global, menținându-și totodată statutul de non-beligerant[40]. Astfel, acest teatru de operațiuni funcționează ca un veritabil meta-proxy al rivalității globale, reconfigurând arhitectura alianțelor la o scară care depășește cu mult granițele ucrainene.

Conflictul din Iran reproduce aceeași paradigmă. Deturnarea forțelor americane către securizarea Golfului Persic îi oferă Beijingului un spațiu de manevră extins în regiunea Indo-Pacifică, în timp ce navele sale comerciale tranzitează nestingherit Strâmtoarea Hormuz datorită unor aranjamente bilaterale cu Teheranul.

Departe de a oferi o soluție de stabilizare sistemică, arhitectura războaielor prin interpuși amplifică vulnerabilitățile *„capcanei lui Tucidide”*. Resursele militare, financiare și politice angrenate în aceste teatre periferice sunt deturnate de la competiția esențială pentru supremație tehnologică, adevăratul teren de decizie pentru miza hegemoniei globale pe termen lung. În definitiv, purtarea conflictelor prin proxy prelungește deznodământul rivalității, generând costuri progresive suportate aproape exclusiv de actorii statali care găzduiesc fizic războiul pe propriul teritoriu.

O a doua dimensiune strategică esențială, adesea neglijată în analizele contemporane, vizează subminarea puterii dominante din interior. Fundamentul teoretic al acestei perspective se regăsește în analiza dedicată de Tucidide revoltei din Corcyra, în cartea a III-a a *Istoriei* sale. Prin descrierea războiului civil al facțiunilor (cunoscut sub conceptul de *stasis*), istoricul formulează observația conform căreia luptele interne distrug cetățile cu o eficiență superioară oricărei invazii armate, deoarece răstoarnă sistemul de valori, transferă loialitățile de la comunitate către facțiune și deschid adversarilor externi căi de penetrare inaccesibile pe câmpul de luptă[41]. Declinul istoric al Atenei a fost declanșat, în esență, de coruperea procesului decizional, inferioritatea strategică manifestată ulterior reprezentând un rezultat derivat. Un exemplu relevant este votarea dezastruoasei expediții siciliene, sub influența retoricii lui Alcibiade, în pofida avertismentelor raționale formulate de Nicias.

Transpus în contextul american contemporan, acest mecanism de eroziune se manifestă pe trei paliere interconectate. Primul palier constă în capturarea elitelor, prin crearea unor dependențe financiare și instituționale de către puterile rivale (în mediile academic, economic și politic). Cercetătorul Rush Doshi documentează eforturile strategice asidue ale R.P.Chineze de a construi un ecosistem de influență în cadrul universităților, al centrelor de analiză și al firmelor de consultanță străine[42]. Al doilea palier implică operațiunile de influențare menite să amplifice fracturile politice interne prin dezinformare și susținerea mișcărilor care contestă angajamentele politice. Interferențele ruse în alegerile americane din 2016 demonstrează natura profund sistematică a acestui tipar subversiv. Cel de-al treilea palier,

caracterizat printr-o subtilitate aparte, îmbracă forma autofagiei strategice, un proces intern autogenerat și independent de manipulările externe. O clasă politică orientată exclusiv către ciclul electoral tinde să sacrifice investițiile vitale în apărare, în autonomia tehnologică și în coeziunea alianțelor pentru a obține câștiguri populiste imediate. Această dinamică transformă aparatul de stat într-un adevărat *„cal troian”*.

Prin urmare, eșecul puterii dominante în fața „capcanei lui Tucidide” survine predominant pe fondul erodării capacității sale interne de a funcționa ca un actor strategic coerent. Acest deznodământ atestă pierderea prudenței instituționalizate ca virtute politică, acel concept de *sophrosyne*[43] a cărui absență a fost identificată de Tucidide drept cauza fundamentală a prăbușirii hegemoniei ateniene.

CONCLUZII

Analiza întreprinsă în acest eseu demonstrează că, deși *„capcana lui Tucidide”* rămâne la baza marilor rivalități contemporane, manifestarea sa este profund nuanțată de realitățile secolului al XXI-lea. Testarea empirică a modelului teoretic, prin aplicarea sa la cele trei rivalități principale ale momentului, a generat concluzii diferențiate, arătând că doar rivalitatea americano-chineză se încadrează fidel tiparului *allisonian.* Celelalte două rivalități sunt încadrate în alte teorii ale relațiilor internaționale, de actualitate în mediul internațional de securitate curent.

În final, *„capcana lui Tucidide”* rămâne un model teoretic valabil, deși intrinsec incomplet în fața multiplicării metodelor de subminare specifice actualului sistem internațional. Lecția pe care Tucidide o formula pentru Atena secolului al V-lea î.Hr. se menține neschimbată pentru marile puteri ale secolului al XXI-lea, demonstrând că un conflictul major devine inevitabil exclusiv atunci când frica, orgoliul național și coruperea deliberării politice interne substituie judecata strategică lucidă, instrumentele contemporane ale acestei degradări dovedindu-se incomparabil mai subtile și mai dificil de contracarat.

BIBLIOGRAFIE

1. ALLISON Graham, *Destined for War: Can America and China Escape Thucydides's Trap?*, Houghton Mifflin Harcourt, Boston, 2017.
2. ALLISON Graham, ”The Thucydides's Trap: Are the U.S. and China Headed for War?”, în *The Atlantic*, 24 septembrie 2015.
3. BRANDS Hal, Beckley Michael, *Danger Zone: The Coming Conflict with China*, W.W. Norton and Company, 2022.
4. BRANNEN Samuel, *Four Scenarios for Geopolitical Order in 2025-2030: What Will Great Power Competition Look Like?*, Center for Strategic and International Studies (CSIS), 16 septembrie 2020.
5. BURNS J. William, *The Back Channel: A Memoir of American Diplomacy and the Case for Its Renewal*, Editura Random House, 2019.
6. BYMAN Daniel, *Iran's Strait of Hormuz Gambit and the Limits of U.S. Military Power*, Center for Strategic and International Studies (CSIS), 20 aprilie 2026.
7. DESCH C. Michael, ”Balancing Away from War: How the USA and China Can Side-step the Thucydides' Trap”, în *The Chinese Journal of International Politics*, vol. 18, nr. 2, Oxford University Press, 2025.
8. FREDERICK Bryan et al., *The Consequences of the Russia-Ukraine War*, RAND Corporation, 2025.
9. FOERSTER Morrison, *United States and China Reach Trade Agreement: Takeaways for Export and Supply Chain Controls*, 13 noiembrie 2025.

10. FOX C. Amos, *The U.S. and Russia: Competing Proxy Strategies in the Russo-Ukrainian War*, The Strategy Bridge, 1 iunie 2023.
11. GILPIN Robert, *War and Change in World Politics*, Cambridge University Press, 1981.
12. GREEN J. Michael, *The Iran War and Strategic Competition in Asia*, CSIS Podcasts (The Asia Chessboard), 7 aprilie 2026.
13. GU Yuebing, *China as a "near-peer": what the US 2025 National Security Strategy really signals*, Blavatnik School of Government, University of Oxford, 19 ianuarie 2026.
14. HANANIA Richard, "Graham Allison and the Thucydides Trap Myth", în *Strategic Studies Quarterly*, vol. 15, nr. 4, Air University Press, iarna 2021.
15. KAGAN Donald, *The Outbreak of the Peloponnesian War*, Cornell University Press, 1969.
16. KANG C. David, Xinru Ma, "Power Transitions: Thucydides Didn't Live in East Asia", în *The Washington Quarterly*, vol. 41, nr. 1, primăvara 2018.
17. LAMB Kate, "What is the Thucydides Trap and why did Xi Jinping mention it in his meeting with Donald Trump?", *The Guardian*, 15 mai 2026.
18. LEBOW Richard Ned, "Thucydides and Deterrence", în *Security Studies*, vol. 16, nr. 2, Routledge, aprilie-iunie 2007.
19. LOFT Philip, *Israel/US-Iran conflict 2026: Reopening the Strait of Hormuz*, House of Commons Library, Londra, 24 aprilie 2026.
20. LYNCH III F. Thomas, Jeffrey Mankoff, Phillip C. Saunders, "Mid-Decade Great Power Geostrategic Dynamics", în *Strategic Assessment 2025: Evolving Great Power Competition at Mid-Decade*, NDU Press, 2025.
21. MISENHEIMER Alan Greeley, *Thucydides' Other "Traps": The United States, China, and the Prospect of "Inevitable" War*, National War College, National Defense University Press, iunie 2019.
22. NAKASHIMA Ellen, Long Zhao, Klimkin Pavlo, Ciaramella Eric, *Is China Willing to Influence Russia on the Ukraine War?*, Carnegie Endowment for International Peace, 2026.
23. ORGANSKI A.F.K., *World Politics*, Alfred A. Knopf, 1958.
24. RATNER Michael (coord.), *Iran Conflict and the Strait of Hormuz: Impacts on Oil, Gas, and Other Commodities*, Congressional Research Service (CRS), 11 martie 2026.
25. STRASSLER B. Robert (ed.), *The Landmark Thucydides: A Comprehensive Guide to the Peloponnesian War*, Free Press, 1996.
26. SU Ali Ercan, *Robert Gilpin in Realist Paradigm of International Relations Discipline: Research Program, State and International System*, în LAÜ Sosyal Bilimler Dergisi (EUL Journal of Social Sciences), vol. 15, nr. 1, iunie 2024.
27. THUCYDIDES, *The History of the Peloponnesian War*, tradus de Richard Crawley, The Internet Classics Archive.
28. *** Brookings Institution, *How China reads the 2025 US National Security Strategy*, 8 decembrie 2025.
29. *** Congressional Research Service, *U.S.-China Trade Relations*, IF11284, 4 martie 2026.
30. *** Harvard Kennedy School's Belfer Center for Science and International Affairs, *Thucydides's Trap Case File*.
31. *** The National, *How does Iran view the Strait of Hormuz stalemate?*, 16 aprilie 2026.
32. *** The White House, *National Security Strategy of the United States of America*, noiembrie 2025.

[1] Hiloți: populație de servi aparținând statului spartan, care nu aveau niciun fel de drepturi cetățenești, cu o situație socială intermediară între omul liber și sclav, putând fi împrumutați proprietarilor de pământ.

[2] Donald Kagan, *The Outbreak of the Peloponnesian War,* Cornell University Press, Ithaca, 1969, pp. 9-11.

[3] Liga de la Delos a fost o alianță militară și navală condusă de Atena, formată inițial pentru a continua lupta împotriva Imperiului Persan, după Războaiele Medice. Aceasta a devenit, treptat, un instrument de hegemonie ateniană, transformându-se într-un imperiu care a generat tensiuni majore cu Sparta și a dus, în cele din urmă, la Războiul Peloponesiac.

[4] Robert Gilpin, *War and Change in World Politics,* Cambridge University Press, Cambridge, 1981, pp. 22-24.

[5] Robert Strassler (ed.), *The Landmark Thucydides: A Comprehensive Guide to the Peloponnesian War,* Free Press, New York, 1996, p. 16, disponibil la https://archive.org/details/landmarkthucydid00thuc/page/n7/mode/2up, accesat la data de 8 mai 2026.

[6] Thucydides, *History of the Peloponnesian War,* trad. Richard Crawley, Penguin Books, Londra, 1972, I.23.6, disponibil la https://classics.mit.edu/Thucydides/pelopwar.mb.txt, accesat la data de 8 mai 2026.

[7] Pentecontaetia se referă la perioada dintre înfrângerea celei de-a doua invazii persane a Greciei (la Plataea, în 479 î.Hr.) și începutul Războiului Peloponesiac (431 î.Hr.).

[8] Michael C. Desch, ”Balancing Away from War: How the USA and China Can Side-step the Thucydides’ Trap”, în *The Chinese Journal of International Politics,* vol. 18, nr. 2, Oxford University Press, Oxford, 2025, pp. 162-163.

[9] Belfer Center for Science and International Affairs, Thucydides’s Trap Case File, disponibil la https://www.belfercenter.org/thucydides-trap/case-file, accesat la data de 8 mai 2026.

[10] Graham Allison, *Destined for War: Can America and China Escape Thucydides’s Trap?,* Houghton Mifflin Harcourt, Boston, 2017, p. xiv.

[11] Alan Greeley Misenheimer, *Thucydides’ Other “Traps”: The United States, China, and the Prospect of “Inevitable” War,* National Defense University Press, Washington, D.C., 2019, pp. 28-30.

[12] A.F.K. Organski, *World Politics,* Alfred A. Knopf, New York, 1958, p. 315.

[13] Robert Gilpin, *Op.cit.,* pp. 117-119.

[14] Dezvoltată de politologul A.F.K. Organski în 1958, teoria tranziției de putere afirmă că stabilitatea globală este asigurată atunci când există o asimetrie clară de putere, cu o singură putere dominantă (hegemon).

[15] Thomas F. Lynch III, Jeffrey Mankoff, Phillip C. Saunders, “Mid-Decade Great Power Geostrategic Dynamics”, în *Strategic Assessment 2025: Evolving Great Power Competition at Mid-Decade,* Editura NDU Press, Washington D.C., 2025, pp. 109-110.

[16] *National Security Strategy of the United States of America,* noiembrie 2025.

[17] Thomas F. Lynch III ș.a., *Op.cit.,* pp. 143-144.

[18] *De-risking* reprezintă o strategie mai nuanțată, susținută de SUA și UE, care vizează reducerea dependențelor strategice de China în sectoare critice (semiconductoare, minerale critice, tehnologii avansate), menținând în același timp relații comerciale în sectoare non-esențiale.

[19] Yuebing Gu, *China as a “near-peer”: what the US 2025 National Security Strategy really signals,* 19 ian. 2026, disponibil la https://www.bsg.ox.ac.uk/blog/china-near-peer-what-us-2025-national-security-strategy-really-signals, accesat la data de 9 mai 2026.

[20] Din Legea comerțului SUA din 1974.

[21] Morrison Foerster, *United States and China Reach Trade Agreement: Takeaways for Export and Supply Chain Controls,* 13 noiembrie 2025, disponibil la https://www.mofo.com/resources/insights/251113-united-states-and-china-reach-trade-agreement, accesat la data de 25 mai 2026.

[22] Chris McGuire, *The New AI Chip Export Policy to China: Strategically Incoherent and Unenforceable,* Council on Foreign Relations, 14 ianuarie 2026, disponibil la https://www.cfr.org/articles/new-ai-chip-export-policy-china-strategically-incoherent-and-unenforceable, accesat la data de 25 mai 2026.

[23] Legea IEEPA (International Emergency Economic Powers Act) din 1977 este o lege federală a Statelor Unite care autorizează președintele să declare o urgență națională și să reglementeze comerțul internațional sau să blocheze active străine ca răspuns la amenințări neobișnuite și extraordinare aduse securității naționale, politicii externe sau economiei SUA.

[24] Congressional Research Service, *U.S.-China Trade Relations,* IF11284, actualizat 4 martie 2026, disponibil la https://www.congress.gov/crs-product/IF11284, accesat la data de 25 mai 2026.

[25] Kate Lamb, ”What is the Thucydides Trap and why did Xi Jinping mention it in his meeting with Donald Trump?”, *The Guardian,* 15 mai 2026, disponibil la https://www.theguardian.com/us-news/2026/may/15/thucydides-trap-explained-xi-jinping-donald-trump-us-china-taiwan, accesat la data de 27 iun. 2026.

[26] Thomas F. Lynch III ș.a., *Op.cit,* pp. 132-133.

[27] Keynesianism-ul militar este o politică economică prin care guvernele stimulează cererea agregată și creșterea economică prin creșterea cheltuielilor militare. Derivat din economia keynesiană, acesta folosește cheltuielile de apărare ca instrument de management economic, fiind adesea favorizat deoarece cheltuielile militare pot fi mai puțin

controversate din punct de vedere politic decât cheltuielile sociale, oferind în același timp o stimulare economică la scară largă.

[28] Volodymyr Ishchenko, Ilya Matveev, Oleg Zhuravlev, *Russian Military Keynesianism: Who Benefits from the War in Ukraine?,* Ponars Eurasia, publicat la 27 noi. 2023, disponibil la https://www.ponarseurasia.org/russian-military-keynesianism-who-benefits-from-the-war-in-ukraine/, accesat la data de 9 mai 2026.

[29] Thomas F. Lynch III ș.a., *Op. cit.,* pp. 132-133.

[30] William J. Burns, *The Back Channel: A Memoir of American Diplomacy and the Case for Its Renewal,* Random House, New York, 2019, pp. 703-704.

[31] *Sharp power* reprezintă un concept utilizat pentru a descrie modul în care regimurile autoritare (precum China și Rusia) utilizează instrumente subtile, de multe ori ascunse, pentru a manipula, a exercita presiuni și a submina instituțiile democratice din alte țări. Spre deosebire de soft power sau hard power, sharp power se bazează pe manipulare, distorsionare și corodarea integrității instituționale.

[32] Thomas F. Lynch III ș.a., *Op. cit.,* pp. 107-109.

[33] Michael Ratner (coord.), *Iran Conflict and the Strait of Hormuz: Impacts on Oil, Gas, and Other Commodities,* Congressional Research Service (CRS), Washington, D.C., 11 martie 2026, p. 13.

[34] Daniel Byman, *Iran's Strait of Hormuz Gambit and the Limits of U.S. Military Power,* Center for Strategic and International Studies, Washington D.C., publicat la 20 apr. 2026, disponibil la https://www.csis.org/analysis/irans-strait-hormuz-gambit-and-limits-us-military-power, accesat la data de 10 mai 2026.

[35] Philip Loft, *Israel/US–Iran Conflict 2026: Reopening the Strait of Hormuz,* House of Commons Library, publicat la 24 apr. 2026, disponibil la https://researchbriefings.files.parliament.uk/documents/CBP-10636/CBP-10636.pdf, accesat la data de 10 mai 2026.

[36] Philip Loft, *Op.cit.*

[37] Michael J. Green, *The Iran War and Strategic Competition in Asia,* 7 aprilie 2026, disponibil la https://www.csis.org/podcasts/asia-chessboard/iran-war-and-strategic-competition-asia, accesat la data de 9 mai 2026.

[38] *National Security Strategy of the United States of America,* noiembrie 2025, p. 28.

[39] Amos C. Fox, *The U.S. and Russia: Competing Proxy Strategies in the Russo-Ukrainian War,* The Strategy Bridge, publicat la 1 iunie 2023, disponibil la https://thestrategybridge.org/the-bridge/2023/6/1/the-us-and-russia-competing-proxy-strategies-in-the-russo-ukrainian-war, accesat la data de 27 mai 2026.

[40] Ellen Nakashima, Zhao Long, Pavlo Klimkin, Eric Ciaramella, *Is China Willing to Influence Russia on the Ukraine War?,* Carnegie Endowment for International Peace, publicat la 4 martie 2026, disponibil la https://carnegieendowment.org/posts/2025/03/is-china-willing-to-influence-russia-on-the-ukraine-war, accesat la data de 27 mai 2026.

[41] Thucydides, *History of the Peloponnesian War,* pp. III.82-83.

[42] Rush Doshi, *The Long Game: China's Grand Strategy to Displace American Order,* Oxford University Press, Oxford, 2021, recenzia cărții disponibilă la https://www.researchgate.net/publication/355824156_The_long_game_China's_grand_strategy_to_displace_American_order, accesat la data de 27 mai 2026.

[43] Concept din Grecia Antică ce descrie o stare ideală de echilibru, moderație, autocontrol și stăpânire de sine.

PIVOTUL TĂCUT AL EURASIEI: KAZAHSTANUL ȘI FEREASTRA STRATEGICĂ 2026–2035

George MINEA*

Abstract

Kazakhstan rarely receives sustained attention in Western strategic thought, even though its position is much harder to substitute than its demographic and economic weight suggests. The paper asks how far Kazakh influence can extend, and over what horizon. Drawing on classical heartland geopolitics, the pivot-state tradition and recent literature on multi-vectorism, it identifies four reinforcing sources of leverage. The country holds a geographic position no other state shares, with long land borders on both Russia and China. Its material base combines a near-monopoly on uranium with large hydrocarbon reserves and a wide share of the critical raw materials the EU depends on. It controls the only viable Asia–Europe overland route that bypasses Russia. And its multi-vector diplomatic doctrine extracts simultaneous concessions from Washington, Beijing, Moscow and Brussels. Pipeline dependence on Russia, presidential succession, the falling Caspian Sea, the Russian-ethnic northern frontier and the risk of Chinese economic capture keep this window temporal rather than permanent. Four scenarios for the coming decade are weighed by probability. Kazakhstan is best read as a node power, a state whose weight comes from where it sits rather than what it produces, with consequences for European and Romanian strategic autonomy.

Keywords: *Kazakhstan; geopolitics; multi-vectorism; pivot state; critical raw materials; uranium; Middle Corridor; strategic autonomy; node power.*

INTRODUCERE

După invazia Rusiei în Ucraina (2022), atenția strategică occidentală s-a reorientat către spații tratate anterior ca periferii, iar Kazahstanul este un astfel de caz. Al nouălea stat al lumii ca suprafață (2,72 milioane km²), Kazahstanul are frontieră terestră lungă atât cu F.Rusă (7.591 km), cât și cu R.P.Chineză (1.782 km)[1], este cel mai mare producător mondial de uraniu, ocupă locul 12 la producția globală de țiței, deține rezerve din 21 dintre cele 34 de materii prime critice definite de UE și controlează singurul coridor terestru major Asia–Europa care ocolește F.Rusă. Cu toate acestea, apare rar ca subiect autonom în discursul strategic occidental, un decalaj între ponderea reală și vizibilitatea analitică ce motivează lucrarea de față.

Întrebarea de cercetare: în ce măsură și pe

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

ce orizont temporal poate Kazahstanul exercita o influență sistemică globală, dincolo de rolul atribuit clasic statelor medii post-sovietice? Ipoteza de lucru: patru factori (geografic, material, infrastructural și doctrinar) îi pot oferi Astanei o capacitate disproporționată față de greutatea sa demografică (aproximativ 20 de milioane de locuitori) sau economică (PIB nominal circa 285 de miliarde USD), dar într-o fereastră 2026–2035 limitată de vulnerabilități structurale.

CADRUL TEORETIC

Punctul de plecare este teza Heartland-ului, formulată de Halford Mackinder, în 1904, care susține că spațiul central eurasiatic este pivotul istoric al puterii globale[2]. Pe harta lui Mackinder, Kazahstanul ocupă partea de sud a Heartland-ului, astăzi fiind cea mai mare țară fără acces la oceanul planetar din lume. În 1997, Zbigniew Brzezinski actualiza cadrul elaborat de Mackinder și propunea conceptul de „Balcani Eurasiatici" pentru spațiul Asia Centrală–Caucaz–Orientul Mijlociu, pe care îl descria ca o zonă de instabilitate prelungită și miză strategică pentru hegemonul global[3]. Brzezinski recomanda cultivarea „statelor-pivot", dar lista sa originală, formulată la șase ani după dizolvarea URSS, nu includea Kazahstanul, încă perceput drept satelit al Moscovei.

În anul 1996, un articol publicat în revista *Foreign Affairs* de Robert Chase, Emily Hill și Paul Kennedy readucea în atenție conceptul de „stat-pivot". Potrivit autorilor, statul-pivot poate fi definit drept acel stat a cărui evoluție generează efecte sistemice asupra unei regiuni întregi[4]. Criteriile clasice (dimensiune relevantă, poziție geografică critică, efecte transfrontaliere în caz de instabilitate, interese ale marilor puteri în asigurarea stabilității sale) sunt astăzi îndeplinite cumulativ de Kazahstan. Literatura recentă completează cadrul prin conceptul de „multi-vectorialism", formalizat de Rachel Vanderhill, Sandra Joireman și Roza Tulepbayeva (2020), care descrie strategia puterilor secundare (mijlocii) care sunt prinse între centre concurente și care întreține, simultan, multiple relații semnificative pentru a-și maximiza autonomia[5]. Combinând cele trei tradiții (geopolitica mackinderiană pentru poziție, conceptul de stat-pivot pentru efect sistemic și multi-vectorialismul pentru palierul politic), se obține următoarea ipoteză de lucru: potențialul kazah depinde simultan de pârghiile materiale și de gradul de autonomie strategică asigurat de doctrina diplomatică.

GEOGRAFIA CA ACTIV STRUCTURAL

Patru caracteristici geografice definesc capitalul strategic kazah. Prima este reprezentată de lipsa accesului la oceanul planetar, singura frontieră maritimă fiind cea pe Marea Caspică, bazin endoreic[6]. Aceasta plasează Kazahstanul în interiorul Heartland-ului și ridică un cost semnificativ pentru orice angajament naval occidental, ceea ce explică parțial de ce doctrina americană a tratat regiunea ca fiind de importanță secundară până în 2022.

A doua, și cea mai importantă, vizează arealul de influență. Kazahstanul are simultan frontieră terestră lungă cu F.Rusă (7.591 km, cea mai lungă frontieră bilaterală terestră continuă din lume și a doua ca lungime totală, după cea dintre Canada și SUA) și cu R.P.Chineză (1.782 km). Această dublă vecinătate face din Kazahstan releul fizic între cele două puteri eurasiatice.

A treia este reprezentată de poziția centrală în Asia Centrală, cu frontieră terestră spre Uzbekistan, Kârgâzstan și Turkmenistan. Pentru orice proiect de integrare regională (BRI[7] chinezesc, Global Gateway european[8], C5+1 american[9]) Kazahstanul trece în zona necesității logistice.

A patra este distribuția inegală a populației (7,6 loc./km², cea mai mică densitate dintre statele G20-adiacente). Nordul gravitează economic spre F.Rusă, estul spre R.P.Chineză, sud-vestul (porturile Aktau și Kuryk) spre exporturile globale. Această asimetrie internă este, în același timp, vulnerabilitate (dificultatea controlului teritorial) și resursă (capacitatea de a oferi infrastructură în mai multe direcții).

Aceste patru caracteristici, luate împreună, produc o poziție pe care niciun alt stat nu o

reproduce, ceea ce corespunde definiției de „stat-pivot al Balcanilor Eurasiatici", chiar dacă Brzezinski însuși nu îl identifica explicit ca atare.

DIMENSIUNEA MATERIALĂ

Monopolul funcțional pe resursele de uraniu

Kazahstanul este, începând cu 2009, cel mai mare producător mondial de uraniu; în 2024 a furnizat 39% din producția mondială de minereu de uraniu, urmat de Canada (24%) și Namibia (12%)[10]/ Kazatomprom controlează circa 40% din piața globală și deține a doua rezervă mondială (14% din total, după Australia). Trei elemente susțin acest monopol funcțional. Primul este structura proprietății: sunt realizate *joint-ventures* cu Cameco (Canada), Orano (Franța), CNNC (R.P.Chineză), Rosatom (F.Rusă), Mitsubishi și Mitsui (Japonia), ceea ce face din Astana un nod în lanțul de aprovizionare al fiecărei puteri nucleare. Al doilea, tehnologia *in-situ recovery* (ISR)[11], cea mai eficientă din punct de vedere al costurilor. Al treilea element este reprezentat de contextul internațional: Prohibiting Russian Uranium Imports Act (SUA, 2024) și ieșirea Nigerului din lanțul de aprovizionare francez (2023), combinate cu 63 de reactoare în construcție la nivel global și cu relansarea nucleară pentru AI, fac din Kazahstan o resursă greu substituibilă[12]. Pentru România, contractele Nuclearelectrica–Kazatomprom, semnate începând cu 2023, sunt deja relevante pentru viitoarele unități Cernavodă 3 și 4 și pentru SMR-urile NuScale[13].

Hidrocarburi și paradoxul Conductei Caspice

Kazahstanul este al doisprezecelea producător mondial de țiței (circa 1,8 milioane barili/zi în 2024) și deține rezerve dovedite de aprox. 30 de miliarde de barili. Trei zăcăminte gigantice (Tengiz, controlat de compania Chevron; Kashagan, consorțiu Shell/ TotalEnergies/ CNPC; Karachaganak, condus de Shell/ Eni) concentrează 60–70% din producție. În 2025, Kazahstanul a furnizat 12,8% din importurile UE de țiței și a devenit al treilea furnizor la nivel european, după SUA și Norvegia (la egalitate)[14], în contextul reducerii cotei rusești de la 25,8% (2021) la 2,2% (2025).

Apare aici un paradox: 80% din exporturile petroliere kazahe trec prin Caspian Pipeline Consortium (CPC), o conductă de 1.511 km care traversează teritoriul rus și se termină la Novorossiisk[15]. În 2025, CPC a transportat 70,52 milioane de tone, însă vulnerabilitatea s-a manifestat în mod repetat, fie prin suspendarea de 30 de zile dispusă de o instanță rusă (iulie 2022), fie urmare a atacurilor ucrainene asupra stației Kropotkinskaya (februarie 2025, reducere de 30–40% a fluxului) sau asupra terminalului portuar (noiembrie 2025). În primul trimestru al lui 2026, producția kazahă a scăzut cu 20%, iar exporturile cu 22%, cu pierderi de peste 4 miliarde USD. Diversificarea (prin conducta Baku–Tbilisi–Ceyhan, conducta Kazahstan–China, ruta caspică nouă) avansează lent. În cel mai favorabil scenariu, cota CPC scade la 60% până în 2030.

Materii prime critice

Kazahstanul produce 19 din cele 34 de materii prime critice (CRM) definite de UE prin Critical Raw Materials Act și deține rezerve pentru 21 dintre ele[16]. Inventarul include cea mai mare rezervă mondială de crom (zăcământul Donskoye), plus titan, beriliu, mangan, cupru, zinc, tungsten și 160 de zăcăminte de pământuri rare (REE). Memorandum-ul de Înțelegere UE–Kazahstan, semnat în noiembrie 2022 (operațional din mai 2023), prevede integrarea lanțurilor de valoare pentru CRM, baterii și hidrogen verde[17]. La summitul UE–Asia Centrală, din aprilie 2025, a fost anunțat pachetul Global Gateway de 12 miliarde EUR, din care 2,5 miliarde EUR alocate CRM. În noiembrie 2025, contractul de 1,1 miliarde USD între Cove Capital Group (SUA) și operatori kazahi pentru tungsten a inclus obligația procesării locale, ceea ce contracarează pentru prima dată modelul tradițional de extracție–reexport, prin care valoarea adăugată migrează către R.P.Chineză. Statul chinez rămâne, totuși, actorul dominant prin faptul că importă 70% din metalele critice produse în Asia Centrală.

CONECTIVITATEA: CORIDORUL TRANS-CASPIC

Coridorul Trans-Caspic Internațional (TITR, „Coridorul Median") este o rețea multimodală de aproximativ 4.250 km de cale ferată, plus 500 km maritimi, care leagă vestul R.P.Chineze de Europa prin Kazahstan, Marea Caspică, Azerbaidjan, Georgia, Marea Neagră și Turcia. Este singura rută terestră viabilă Asia–Europa care ocolește Rusia. Volumele tranzitate au crescut semnificativ între 2022 și 2025, de la circa 500.000 tone la peste 4 milioane tone[18]. La Forumul de la Tashkent (27 noiembrie 2025), comisarul european pentru extindere, Marta Kos, a anunțat că volumele s-ar putea tripla din nou până în 2030.

Kazahstanul a devenit un partener indispensabil al UE, traseele trecând prin punctele feroviare Dostyk, Altynkol, Khorgos și prin porturile caspice Aktau și Kuryk. Linia Dostyk–Mointy, dublată cu finanțare BEI, va cvintupla capacitatea internă de transport. Pentru UE, sprijinirea coridorului are rațiuni geopolitice (alternativă fizică la tranzitul rus), economice (timp de tranzit redus la 14–18 zile) și strategice (transportul CRM și uraniul kazah). Pe de altă parte, R.P.Chineză a investit, prin intermediul BRI, 23 miliarde USD în Kazahstan doar în prima jumătate a anului 2025, ceea ce reprezintă aproximativ 20% din totalul investițiilor BRI la nivel global.

Există însă și unele limite structurale; astfel, o evaluare realizată de Carnegie Endowment (2026)[19] identifică patru blocaje critice:

a) capacitatea limitată a flotei caspice (maximum 6–8 milioane tone anual, chiar și după introducerea super-ferries-urilor);
b) scăderea nivelului Mării Caspice (proiecții de până la 6,5 m până în 2045) ar lăsa actualele dane Aktau/ Kuryk pe uscat și ar forța tranziția costisitoare la terminale offshore;
c) instabilitatea Caucazului de Sud;
d) decalajul de costuri: un container FEU[20] costă 3.500–4.500 USD pe Coridorul Median, față de 2.800–3.200 USD pe Coridorul Nordic.

Middle Corridor are așadar o fereastră de oportunitate, nu o poziție permanentă, fapt care, paradoxal, amplifică valoarea actuală a pârghiei kazahe. Pentru România, varianta nordică a Coridorului Median (prin Marea Neagră) vizează direct portul Constanța și deschide oportunitatea ca acesta să devină terminalul european principal al rutei, o pârghie subutilizată în diplomația de transport românească.

DOCTRINA MULTI-VECTOR 2.0

Multi-vectorialismul, formulat de fostul președinte Nazarbayev, în 1992, ca răspuns la dilema unui stat tânăr, prins între F.Rusă și R.P.Chineză, a avut un caracter predominant declarativ sub conducerea acestuia. Începând cu președintele Tokayev (din 2019), doctrina a intrat în faza „2.0" prin transformarea acesteia într-un instrument activ de extragere de concesii simultane de la patru centre de putere[21]. Trei diferențe se evidențiază față de etapa Nazarbayev: profesionalizarea diplomatică (Tokayev este diplomat de carieră, fost subsecretar general ONU), trecerea de la echilibru static la echilibru dinamic și poziționarea ca putere medie regională cu ambiții globale.

Testul ucrainean a fost decisiv: astfel, la Forumul de la Sankt Petersburg (din iunie 2022), în prezența lui V.Putin, președintele Tokayev a refuzat public recunoașterea „republicilor populare" Donețk și Luhansk și a invocat explicit principiile suveranității teritoriale „inclusiv în cazul Crimeii". În 2025, Astana a aplicat un control vamal crescut pe reexporturile către Rusia și a blocat la frontieră peste 5.000 de camioane încărcate cu bunuri cu dublă utilizare. Simultan, însă, nu a rupt relația cu Moscova: astfel, în iunie 2025, a atribuit Rosatom contractul pentru prima centrală nucleară kazahă, iar a doua va fi probabil construită de CNNC.

Ilustrarea cea mai clară a doctrinei multi-vector 2.0 a venit în noiembrie 2025, atunci când președinții kazah și american au supravegheat semnarea a 29 de acorduri, în valoare de 17 miliarde USD (energie, tungsten, IT, etc.)[22], iar la 48 de ore distanță Tokayev a semnat la Moscova,

împreună cu Putin, o declarație de „parteneriat strategic și alianță”. Pe de altă parte, în prima jumătate a anului 2025, Kazahstanul a primit 23 miliarde USD prin investiții legate de proiectul chinez BRI[23] și 12 miliarde EUR prin pachetul Global Gateway al UE. Capacitatea de a converti simultan aceste patru fluxuri (american, chinez, rusesc și european) în concesii bilaterale definește multi-vectorialismul 2.0.

Limitele autonomiei rămân însă semnificative și sunt evidențiate prin dependența infrastructurală de CPC, apartenența la CSTO[24] și EAEU[25] (organizații conduse de F.Rusă) și capacitatea limitată a unui stat de 20 de milioane de locuitori de a susține o rețea diplomatică extinsă.

VULNERABILITĂȚI SISTEMICE

Cinci categorii de riscuri fac din fereastra strategică una temporară, nu permanentă. Prima este vulnerabilitatea infrastructurală relevată prin dependența de 80% a exporturilor petroliere față de CPC, expusă deja de patru ori în perioada 2022–2025. Reducerea acestei dependențe va dura cel puțin un deceniu.

A doua este vulnerabilitatea succesorală. Președintele Tokayev a anunțat că nu va candida la un nou mandat după 2029, iar Constituția modificată în 2022 limitează președinția la un singur mandat de șapte ani. Modelul kazah de tranziție pașnică (de la Nazarbayev la Tokayev, 2019) a fost contestat sever în ianuarie 2022, când protestele au escaladat aproape până la o lovitură de stat, iar invocarea Articolului 4 CSTO a permis intervenția trupelor rusești, care a generat o datorie politică tacită față de Moscova[26].

A treia este vulnerabilitatea climatică. O scădere a nivelului Mării Caspice cu până la 6,5 m până în 2045 ar lăsa porturile Aktau și Kuryk practic la uscat, ar impune investiții de 5–10 miliarde USD în terminale *offshore deep-water* și ar întârzia cu un deceniu funcționarea coridorului în parametri actuali. Este cea mai subevaluată vulnerabilitate, întrucât acționează pe orizonturi temporale care depășesc planificarea bugetară clasică.

A patra este vulnerabilitatea etno-demografică. Aproximativ 15% dintre locuitorii Kazahstanului sunt etnici ruși, concentrați istoric în nordul țării (în scădere de la 38% în 1989, dar încă semnificativi în regiunile de frontieră). Este o vulnerabilitate de tip „Donbas”, atenuată parțial de migrație.

A cincea este vulnerabilitatea de tip „capturare economică”. Investițiile chineze de 23 miliarde USD doar în prima jumătate a lui 2025, cumulate cu participațiile în câmpul petrolier Kashagan (CNPC), uraniu (CNNC), infrastructură feroviară și telecomunicații, generează un risc de transformare graduală în „dependență chineză” funcțională. Răspunsul kazah, diversificarea agresivă a investitorilor și impunerea de cerințe de procesare locală reduc riscul, fără să-l elimine.

SCENARII PROSPECTIVE 2026–2035

Patru scenarii, cu probabilități estimative, acoperă spațiul posibilităților relevante.

Scenariul A: Kazahstan – pivot strategic occidental (probabilitate 30%)/ tendințele din 2025 se consolidează; cota CPC scade sub 60%; investițiile occidentale în CRM le depășesc pe cele chineze; succesiunea produce un lider tehnocrat orientat occidental; Coridorul Median trece de 12 milioane de tone anual până în 2030.

Scenariul B: echilibru susținut (~ 45%, cel mai probabil)/ doctrina multi-vector 2.0 continuă; Kazahstanul extrage concesii simultane fără identificare exclusivă; dependența de CPC scade gradual; cooperarea cu UE pe CRM progresează, fără a atinge ambiția de 40% din importurile europene. Este scenariul cel mai stabil, dar și cel mai puțin transformator.

Scenariul C: capturare externă (~20%, divizat 10% rusă/10% chineză)/ slăbiciunea politică prelungită combinată cu presiunea externă consistentă conduce la realiniere fundamentală; sub-scenariul rus presupune crize succesorale, etnice sau economice exploatate de Moscova, iar sub-scenariul chinez implică adâncirea dependenței BRI dincolo de pragul reversibilității, cu acces preferențial chinez la toate resursele

critice. Ambele variante sunt catastrofale pentru autonomia strategică europeană.

Scenariul D: fragmentare internă (~5%)/ presupune destabilizare semnificativă pe linie etnică, politică sau economică, posibil cu intervenții externe. Probabilitate cumulativă redusă, impact sistemic disproporționat.

Indicatorii cheie de monitorizat sunt următorii: (1) ponderea exporturilor de țiței prin rute non-rusești; (2) volumele și prețul mediu per FEU pe Coridorul Median; (3) procentul de procesare locală a uraniului și CRM; (4) valoarea contractelor non-rusești și non-chineze în sectorul CRM; (5) tonul declarațiilor publice ale Astanei pe teme strategice (Ucraina, Taiwan, sancțiuni).

CONCLUZII

Pe scurt, Kazahstanul poate exercita o influență sistemică globală reală în fereastra de timp 2026–2035, însă aceasta este o influență funcțională, nu hegemonică. Astana nu propune un proiect civilizațional alternativ și nu inițiază blocuri ideologice. Rolul ei este acela de nod sistemic care condiționează, prin pârghii concrete, funcționarea unor lanțuri globale critice. Aceste pârghii sunt: poziția geografică unică (singurul stat dublu-vecin cu F.Rusă și R.P.Chineză), monopolul funcțional pe uraniu (39% din producția mondială), ponderea în CRM (19 din 34 produse, 21 din 34 cu rezerve), controlul fizic al Coridorului Trans-Caspic și doctrina multi-vectorială 2.0.

Vulnerabilitățile (CPC, succesiune, Marea Caspică, etnicitate, capturare economică) determină ca fereastra de oportunitate să fie una temporară. După 2035, pârghiile actuale își pot pierde semnificația maximă prin epuizare, substituție tehnologică sau reorganizarea ordinii internaționale. Implicația pentru UE și pentru România este că angajamentul cu Kazahstanul nu este o simplă opțiune tactică, ci o investiție în propria autonomie strategică. Costul reacției la o eventuală „capturare” rusească sau chineză ar fi exponențial mai mare decât costul unui parteneriat preventiv consolidat acum. Pentru România, în mod specific, se conturează trei priorități: contractele Nuclearelectrica – Kazatomprom pentru uraniu; poziționarea portului Constanța ca terminal european al variantei nordice a Coridorului Trans-Caspic; prelucrarea CPC Blend la rafinăriile Petromidia și Petrobrazi.

Dincolo de cazul specific, observația sugerează că „puterea de nod” (capacitatea de a condiționa fluxuri sistemice prin poziționare structurală) merită tratată în secolul al XXI-lea ca o categorie analitică separată de puterea agregată tradițională. Ordinea internațională contemporană se construiește atât prin centrele de putere, cât și prin nodurile care le conectează.

BIBLIOGRAFIE

1. BRZEZINSKI Zbigniew, *The Grand Chessboard: American Primacy and Its Geostrategic Imperatives*, Basic Books, New York, 1997.
2. CHASE Robert, Emily Hill, Paul Kennedy, ”Pivotal States and U.S. Strategy”, *Foreign Affairs*, vol. 75, no. 1, Council on Foreign Relations, 1996, pp 33–51.
3. Comisia Europeană – DG NEAR, ”Trans-Caspian Transport Corridor and Connectivity Investors Forum”, 27 nov. 2025; https://enlargement.ec.europa.eu/news/trans-caspian-transport-corridor-and-connectivity-investors-forum-eu-advances-cross-regional-2025-11-27_en.
4. CONRADI Friedrich, ”The Much-Touted Middle Corridor Transport Route Could Prove a Dead End”, Carnegie Endowment for International Peace, Russia Eurasia Center, Apr. 29, 2026; https://carnegieendowment.org/russia-eurasia/politika/2026/04/middle-corridor-transport-prospect.
5. DOLBAIA Tina, Amanda Southfield, ”Kazakhstan's Emerging Civilian Nuclear Energy Industry: Implications for U.S. Strategic Interests”, Podcast Episode, Center for Strategic and International Studies, Washington DC, September 2025; https://www.csis.org/analysis/kazakhstans-emerging-civilian-nuclear-energy-industry-implications-us-strategic-interests.
6. GRANTSEVA Vera, Rakhimbek Abdrakhmanov, *Kazakhstan After the Double Shock of 2022. Political, Economic and Military Consequences*”, IFRI Papers, Russie. Eurasie.Visions, no. 140, The French Institute of International Relations, Oct. 2025, 32 p.
7. INDEO Fabio, ”EU–Central Asia Cooperation on Critical Minerals within a Global Geopolitical Race”, Trends Group, 19 Oct. 2025; https://trendsresearch.org/insight/eu-central-asia-cooperation-on-critical-minerals-within-a-global-geopolitical-race/
8. KIM Alexander, ”Kazakhstan Reinforces Multivector Foreign Policy”, Jamestown Foundation, 07.09.2025; https://jamestown.org/kazakhstan-reinforces-multivector-foreign-policy/.
9. KUBAIZHANOV Askar, ”Kazakhstan on Europe's Oil Podium, but for How Long?”, *The Times of Central Asia*, 16 April 2026; https://timesca.com/kazakhstan-on-europes-oil-podium-but-for-how-long/
10. MACKINDER J. Halford, ”The Geographical Pivot of History”, *The Geographical Journal*, vol. 23, no. 4, 1904, pp. 421-437.
11. SEIDALIYEVA Sabina, ”The geopolitics of residual dependence: Kazakhstan`s multivector foreign policy and strategic realignment in the post-Soviet era”, Global Affairs, Universidad de Navarra, March 3, 2026.
12. VANDERHILL Rachel, Sandra Joireman, Roza Tulepbayeva, ”Between the Bear and the Dragon: Multivectorism in Kazakhstan as a Model Strategy for Secondary Powers”, *International Affairs*, vol. 96, no. 4, The Royal Institute of International Affairs, London, 2020, pp. 975-993.
13. ZIPATOLLA Shyngys, *Rethinking EU Strategy in Central Asia*, DGAP Policy Brief, no. 12, German Council on Foreign Relations, May 2025, 4 p.; https://dgap.org/en/research/publications/rethinking-eu-strategy-central-asia.
14. *** ”Opinion: Multi-Vectorism 2.0 – Kazakhstan Seeks Balance in a Shifting Geopolitical Landscape”, *The Times of Central Asia*, 19 nov. 2025; https://timesca.com/opinion-multi-vectorism-2-0-kazakhstan-seeks-balance-in-a-shifting-geopolitical-landscape/
15. *** International Energy Agency, *Kazakhstan-EU Strategic Partnership on Raw Materials*, 15.10.2025; https://www.iea.org/policies/17664-kazakhstan-eu-strategic-partnership-on-raw-materials.
16. *** Îndrumar pentru afaceri – Republica Kazahstan (iulie 2025), realizat de Agenția Română pentru Investiții și Comerț Exterior; https://arice.gov.ro/1/wp-content/uploads/2025/07/a/Indrumar-de-afaceri-KZ.pdf.
17. *** World Nuclear Association, ”World Uranium Mining Production”, 20 January 2026;. https://world-nuclear.org/information-library/nuclear-fuel-cycle/mining-of-uranium/world-uranium-mining-production.

[1] *Îndrumar pentru afaceri – Republica Kazahstan* (iulie 2025), realizat de Agenția Română pentru Investiții și Comerț Exterior; https://arice.gov.ro/1/wp-content/uploads/2025/07/a/Indrumar-de-afaceri-KZ.pdf

[2] Halford J. Mackinder, ”The Geographical Pivot of History”, *The Geographical Journal*, vol. 23, no. 4, 1904, pp 421–437.

[3] Zbigniew Brzezinski, *The Grand Chessboard: American Primacy and Its Geostrategic Imperatives*, Basic Books, New York, 1997, cap. 5 („The Eurasian Balkans"), pp 559-563.

[4] Robert Chase, Emily Hill și Paul Kennedy, ”Pivotal States and U.S. Strategy”, *Foreign Affairs*, vol. 75, no. 1, 1996, pp 33–51.

[5] Rachel Vanderhill, Sandra Joireman și Roza Tulepbayeva, ”Between the Bear and the Dragon: Multivectorism in Kazakhstan as a Model Strategy for Secondary Powers”, *International Affairs*, vol. 96, no. 4, The Royal Institute of International Affairs, London, 2020, pp 975-993.

[6] Un bazin endoreic reprezintă o zonă hidrografică închisă, din care apele curgătoare nu au legătură cu oceanul planetar sau cu marea, acumulându-se de obicei în lacuri interne, mlaștini sau pierzându-se prin evaporare/infiltrare. Aceste zone sunt tipice pentru regiunile aride sau aride-semideșertice.

[7] Belt and Road Initiative/BRI este programul strategic global al Chinei de finanțare a infrastructurii (porturi, căi ferate, conducte, autostrăzi, centrale energetice, rețele digitale) în peste 150 de țări. În taxonomia geopolitică, BRI este considerată instrumentul principal de proiecție a puterii economice chineze și concurentul direct al strategiei europene Global Gateway (12 miliarde EUR anunțate pentru Asia Centrală în aprilie 2025), pe care studiul o discută în paralel.

[8] Global Gateway este strategia oficială de conectivitate globală a Uniunii Europene, lansată la 1 decembrie 2021 de Comisia Europeană împreună cu Înaltul Reprezentant pentru Afaceri Externe și Politica de Securitate. Își propune să mobilizeze până la 300 de miliarde EUR în investiții, între 2021 și 2027, prin abordarea „Team Europe“ (Comisia, statele membre, BEI, BERD, instituțiile de finanțare a dezvoltării și capital privat), cu cinci domenii prioritare: digital, climă și energie, transport, sănătate, educație și cercetare. În taxonomia geopolitică, Global Gateway este răspunsul european direct la Belt and Road Initiative, construit pe standarde democratice, transparență financiară și sustenabilitate. Pachetul dedicat Asiei Centrale, anunțat în aprilie 2025, la summitul UE–Asia Centrală, însumează 12 miliarde EUR.

[9] C5+1 este platforma diplomatică regională a Statelor Unite cu cele cinci republici din Asia Centrală (Kazahstan, Kârgâzstan, Tadjikistan, Turkmenistan, Uzbekistan), lansată la întâlnirea inaugurală a miniștrilor de externe de la Samarkand, în 2015, sub Administrația Obama (secretar de stat John Kerry). Are trei grupuri tematice de lucru: economie, energie și mediu, securitate. În 2022 s-a constituit un Secretariat permanent, iar în septembrie 2023 platforma a fost ridicată la nivel prezidențial: prima reuniune a liderilor s-a desfășurat cu prilejul Adunării Generale ONU, sub președintele Biden — prima dată când un președinte american se întâlnea cu liderii Asiei Centrale în acest format. A doua reuniune la nivel de lideri a fost găzduită la Casa Albă, pe 6 noiembrie 2025, de președintele Trump, ocazie cu care au fost semnate cele 29 de acorduri Tokayev–Trump, discutate în acest studiu. C5+1 este principalul instrument al politicii americane față de regiune și concurentul direct, la nivelul angajamentului diplomatic, al cadrelor rusești (CSTO/EAEU) și chineze (BRI).

[10] World Nuclear Association (2025), World Uranium Mining Production – Producția pe anul 2024: Kazahstan 39%, Canada 24%, Namibia 12%; https://world-nuclear.org/information-library/nuclear-fuel-cycle/mining-of-uranium/world-uranium-mining-production, accesat la 24.04.2026.

[11] *In-Situ Recovery* (ISR), cunoscută și sub numele de *in-situ leaching* (ISL) sau minerit prin soluții, este o metodă modernă de extracție a mineralelor care implică dizolvarea acestora direct în zăcământ, în subteran, fără a fi nevoie de excavarea rocilor sau de construirea unor mine convenționale la suprafață.

[12] Tina Dolbaia, Amanda Southfield, ”Kazakhstan's Emerging Civilian Nuclear Energy Industry: Implications for U.S. Strategic Interests”, Podcast Episode, Center for Strategic and International Studies, Washington DC, September 2025; https://www.csis.org/analysis/kazakhstans-emerging-civilian-nuclear-energy-industry-implications-us-strategic-interests, accesat la 12.05.2026.

[13] SMR (Small Modular Reactor): reactor nuclear modular sub 300 MWe per modul. Proiectul-pilot românesc, o centrală VOYGR-6 cu șase module NuScale de 77 MWe (462 MWe total), este planificat la Doicești (Dâmbovița), prin joint-venture-ul RoPower Nuclear (Nuclearelectrica și Nova Power & Gas). Exploatarea este prognozată pentru începutul anilor 2030.

[14] Askar Kubaizhanov, ”Kazakhstan on Europe's Oil Podium, but for How Long?”, *The Times of Central Asia*, 16 April 2026; https://timesca.com/kazakhstan-on-europes-oil-podium-but-for-how-long/, accesat la 02.05.2026.

[15] Wikipedia – Caspian Pipeline Consortium, consolidare a datelor primare OPEC, EIA și CPC. Trend.az (feb. 2026): CPC a transportat 70,52 milioane de tone în 2025; https://en.wikipedia.org/wiki/Caspian_Pipeline_Consortium, accesat la 27.04.2026.

[16] Fabio Indeo, ”EU–Central Asia Cooperation on Critical Minerals within a Global Geopolitical Race”, Trends Group, 19 Oct. 2025; https://trendsresearch.org/insight/eu-central-asia-cooperation-on-critical-minerals-within-a-global-geopolitical-race/, accesat la 19.04.2026.

[17] *** IEA Policies Database, ”Kazakhstan-EU Strategic Partnership on Raw Materials”; https://www.iea.org/policies/17664-kazakhstan-eu-strategic-partnership-on-raw-materials, accesat la 03.05.2026.

[18] Comisia Europeană – DG NEAR, ”Trans-Caspian Transport Corridor and Connectivity Investors Forum”, 27 nov. 2025; https://enlargement.ec.europa.eu/news/trans-caspian-transport-corridor-and-connectivity-investors-forum-eu-advances-cross-regional-2025-11-27_en, accesat la 27.03.2026.

[19] Friedrich Conradi, ”The Much-Touted Middle Corridor Transport Route Could Prove a Dead End”, Carnegie Endowment for International Peace, Russia Eurasia Center, Apr. 29, 2026 (analiză critică a bottlenecks-urilor); https://carnegieendowment.org/russia-eurasia/politika/2026/04/middle-corridor-transport-prospect, accesat la 02.04.2026.

[20] FEU — *Forty-foot Equivalent Unit*: este unitatea standard de măsură pentru containerele maritime și pentru capacitatea de transport. Un FEU corespunde unui container de 40 de picioare lungime (~12 metri) — containerul „mare”, clasic, care poate fi văzut pe trenuri marfare, camioane lungi și nave port-container.

[21] Alexander Kim, *”Kazakhstan Reinforces Multivector Foreign Policy”,* Jamestown Foundation, 07.09.2025; https://jamestown.org/kazakhstan-reinforces-multivector-foreign-policy/, accesat la 30.03.2026.

[22] *** ”Opinion: Multi-Vectorism 2.0 – Kazakhstan Seeks Balance in a Shifting Geopolitical Landscape”, *The Times of Central Asia*, 19 nov. 2025 (documentează 29 de acorduri Tokayev-Trump, în valoare de aprox. 17 miliarde USD); https://timesca.com/opinion-multi-vectorism-2-0-kazakhstan-seeks-balance-in-a-shifting-geopolitical-landscape/, accesat la 07.04.2026.

[23] Sabina Seidaliyeva, ”The geopolitics of residual dependence: Kazakhstan`s multivector foreign policy and strategic realignment in the post-Soviet era”, Global Affairs, Universidad de Navarra, March 3, 2026; https://en.unav.edu/web/global-affairs/kazakhstan-s-multivector-foreign-policy, accesat la 15.05.2026.

[24] CSTO — Collective Security Treaty Organization (Organizația Tratatului de Securitate Colectivă/OTSC) este o alianță militară condusă de F.Rusă, gândită ca un fel de „NATO post-sovietic”. Membri actuali: Rusia, Belarus, Armenia (suspendată de facto), Kazahstan, Kîrgîzstan, Tadjikistan. Articolul 4 al tratatului este echivalentul Articolului 5 din NATO — atacul împotriva unui membru este considerat atac împotriva tuturor. În acest articol apare în legătură cu criza din ianuarie 2022: Tokayev a invocat Articolul 4 pentru a obține intervenția trupelor rusești care au stabilizat protestele, creând „o datorie politică tacită față de Moscova” și o limită clară a autonomiei kazahe.

[25] Este echivalentul economic al CSTO — o uniune vamală și piață comună condusă tot de Rusia, fondată în 2015. Membri: Rusia, Belarus, Kazahstan, Armenia, Kîrgîzstan. Funcționează ca o versiune mult mai mică și asimetrică a Uniunii Europene: liberă circulație a mărfurilor, tarif vamal extern comun. În lucrare apare ca a doua componentă a constrângerii ruse asupra Kazahstanului — împreună cu CSTO, ele delimitează cât de departe poate merge Astana în doctrina multi-vector înainte să rupă cadrul instituțional moștenit din zona post-sovietică. Logica de ansamblu din acest articol: CPC = lanț infrastructural rus, CSTO = lanț militar rus, EAEU = lanț economic rus/ toate trei formează „plafonul” autonomiei kazahe — explică de ce, oricât de mult ar deschide președintele Tokayev relațiile cu SUA, UE și China, nu poate rupe complet relația cu Moscova.

[26] Vera Grantseva, Rakhimbek Abdrakhmanov, *Kazakhstan After the Double Shock of 2022. Political, Economic and Military Consequences*”, IFRI Papers, Russie.Eurasie.Visions, no. 140, The French Institute of International Relations, Oct. 2025, 32 p.; https://www.ifri.org/en/papers/kazakhstan-after-double-shock-2022-political-economic-and-military-consequences, accesat la 17.04.2026.

CRIZA DE SECURITATE DIN EUROPA DE EST: DINAMICI GEOPOLITICE ȘI TEHNICE ÎN CONFLICTUL RUSO-UCRAINEAN

Andreea-Amalia POPESCU-STĂNICĂ*
Mihai-Laurențiu ZARIA**

Abstract

The Russo-Ukrainian conflict highlights the accelerated transformation of the European security environment, with the effects of instability spreading at regional, continental and international levels. This article analyzes the multisectoral impact of the conflict conducted during the 2022–2026 period on the regional security architecture, using the Regional Security Complex Theory as the theoretical foundation of the research. Through a focus on understanding regional geopolitics, the study examines the course of the Russo-Ukrainian conflict from the perspective of the Russian Federation's aggression and the measures adopted by the international community, reflected within the political, economic, societal, and ecological dimensions of security. Subsequently, by addressing the military dimension of security, the paper highlights how the use of autonomous systems, the integration of artificial intelligence and the digitalization of the battlefield have significantly transformed operational dynamics and military decision-making processes.

In order to understand the resilience architecture developed by NATO and the European Union in the context of the conflict, the study also examines the actions and mechanisms aimed at strengthening the Eastern Flank. The conclusions emphasize that the Russo-Ukrainian war generates significant transformations within the security architecture spectrum, producing effects with extended implications.

Keywords: *Russo-Ukrainian conflict; regional security complex; dimensions of security; hybrid warfare; NATO; EU; autonomous systems; artificial intelligence; electronic warfare; electromagnetic spectrum; strengthening of the Eastern Flank.*

* ***Doctorand la Școala Națională de Studii Politice și Administrative (SNSPA).***
** ***Doctorand la Universitatea Națională de Știință și Tehnologie Politehnica din București (UNSTPB).***

NOȚIUNI INTRODUCTIVE

Izbucnirea războiului ruso-ucrainean a determinat o serie de schimbări semnificative ale dinamicii de securitate regională, identificate la nivel multisectorial. Astfel, focalizarea unitară a eforturilor de echilibrare a climatului de securitate, realizată de către statele europene și de către Statele Unite ale Americii, pentru a contracara acțiunile Federației Ruse, a condus la înregistrarea unor evoluții accelerate atât în domeniul militar, cât și în domenii precum cel economic, cel politic și cel societal.

CONTEXTUALIZARE ȘI ORIENTARE TEORETICĂ

În acest sens, pornind de la evoluțiile menționate anterior, studiul va fi ancorat din punct de vedere teoretic pe tema „complexului de securitate regională", formulată (în anul 1983) de către Barry Buzan. Conform cadrului teoretic, securitatea internațională presupune analizarea subdiviziunilor regionale din punct de vedere securitar, luând astfel naștere complexul de securitate, format din mai multe entități cu probleme aflate în relație de interdependență, respectiv de congruență, „*securitatea lor națională neputând fi examinată în mod legitim separat una de cealaltă*[1]".

Teoria complexului de securitate regională a fost extinsă în cadrul cercetării publicate în 2003 de Barry Buzan și Ole Waever (cei mai importanți reprezentanți ai „Școlii de la Copenhaga"), fiind o abordare care are la bază, cumulate, atât viziuni constructiviste, cât și neo-realiste[2]. În acest sens, există o aplecare atât asupra proceselor culturale și politice, cât și asupra limitelor teritoriale și nivelului de putere, care pot genera probleme de securitate[3].

Conform cercetătorilor Școlii de la Copenhaga, care au dezvoltat și au rafinat atât conceptele teoriei securitizării în termeni de funcționalitate multi-sectorială, precum și conceptele teoriei complexului de securitate regională, concluzia asupra securității la nivel macro a fost că problemele viitoare de securitate vor fi generate de conflicte în plan regional sau intra-regional[4]. Astfel, au fost dezvoltate nouă complexe regionale de securitate, care cuprind întreaga dimensiune globală, respectiv: Cr[5]1 - America de Nord, Cr2 - America de Sud, Cr3 - Europa, Cr4 - Zona Post-Sovietică (integrează alte patru subregiuni Cs[6]1 - Asia Centrală, Cs2 - Caucazul, Cs3 - Statele Baltice, Cs4 - Ucraina și Belarus), Cr5 - Orientul Mijlociu, Cr6 - Africa de Sud, Cr7 - Africa Centrală, Cr8-Asia de Sud, Cr9 - Asia de Est[7].

De asemenea, ancorând studiul în cadrul cercetării realizate de B.Buzan, este important de menționat perspectiva extinsă a analizării dinamicii unui complex de securitate, prin prisma a cinci dimensiuni: militară, economică, politică, societală și ecologică[8]. Luând în considerare că în contextul războiului ruso-ucrainean sunt vizibile evoluții la nivel multisectorial, în continuare vom realiza o analiză a impactului asupra dimensiunilor politică, economică, societală și ecologică ale securității, subliniind obiectivele F.Ruse de a destabiliza statul ucrainean, precum și măsurile care au fost adoptate la nivel internațional pentru a reduce efectele în plan regional. Ulterior, studiul va fi focalizat asupra sectorului militar și evoluțiilor în plan tehnologic, punând de asemenea accentul pe întărirea flancului estic, inclusiv prin prisma evoluțiilor identificate la nivelul UE și NATO, respectiv nivelul accelerat de integrare și cooperare din cadrul celor două organizații internaționale.

SINTEZĂ ANALITICĂ P(OLITIC)-E(CONOMIC)-S(OCIETAL)-E(COLOGIC)

Dimensiunea Securității			
Politică	**Economică**	**Societală**	**Ecologică**
Obiectivele F. Ruse de a destabiliza suveranitatea statului ucrainean, viziunea pro-occidentală, dezideratele de a accesa UE și NATO, încrederea populației în instituțiile statului.	Obiectivele F. Ruse de a destabiliza infrastructura critică (energetică și de transporturi), economia prin limitarea exporturilor de grâne și necesitatea de a continua cursa înarmării.	Obiectivele F. Ruse de a destabiliza populația civilă în plan psihologic, utilizând dezinformare profundă pentru a menține sfera de influență rusă.	Obiectivele F. Ruse de a destabiliza mediul înconjurător prin producerea de incendii și inundații, respectiv contaminarea solului.
Măsuri: -asigurarea de asistență militară prin misiunea EUMAM din Ucraina; -asigurarea răspunderii juridice asupra crimelor de război prin implicarea organismelor juridice internaționale; -excluderea F. Ruse din organizații internaționale (Consiliul Europei); -dezvoltarea programului „*Ukraine Facility*”, cu scopul de a sprijini procesul de integrare în UE; -punerea la dispoziție de către NATO a Pachetelor de Asistență Cuprinzătoare (CAP).	**Măsuri:** -impunerea de sancțiuni asupra F. Ruse (în domenii precum: financiar, energetic, apărare, transporturi, etc.) cu scopul de a slăbi capacitatea de înarmare; -crearea de noi coridoare, rute terestre și maritime pentru a asigura capacitatea de export și import; -reducerea dependenței de resursele energetice furnizate de F. Rusă, prin cuplarea statului ucrainean la rețeaua europeană.	**Măsuri:** -asigurarea de asistență umanitară prin furnizarea de medicamente, alimente, combustibil și surse de producere a energiei electrice; -acordarea de protecție civilă temporară pe teritoriul statelor membre UE; -dezvoltarea unor rețele de voluntari și organizații non-guvernamentale care acționează pentru a oferi sprijin.	**Măsuri:** -implicarea Agenției Internaționale pentru Energie Atomică în acțiuni de prevenție a unui posibil accident nuclear; -acordarea de sprijin în vederea deminării terenurilor agricole; -dezvoltarea unor programe de reciclare a materialelor și utilizarea acestora în procesul de reconstrucție; -dezvoltarea unor grupuri de lucru la nivelul UE pentru constatarea daunelor ecologice și orientarea acțiunilor de sprijin.

DIMENSIUNEA SECURITĂȚII ÎN DOMENIUL MILITAR

Pe lângă dimensiunile securității prezentate anterior sub formă tabelară, prezintă un interes deosebit și dimensiunea securității din domeniul militar sau al apărării, care se evidențiază în principal prin transformarea câmpului de luptă într-un spațiu profund digitalizat, în care sistemele fără pilot și fluxurile informaționale influențează direct modul de desfășurare al operațiilor militare[9]. În Ucraina, dronele au devenit un element central al acțiunii militare, fiind utilizate pe scară largă pentru recunoaștere, identificarea țintelor și ghidarea focului de artilerie. Această utilizare intensivă a UAV[10]-urilor a modificat semnificativ dinamica operațională, reducând necesitatea contactului direct și crescând precizia intervențiilor pe câmpul de luptă.

Astfel, conflictul dintre Ucraina și Federația Rusă reprezintă un exemplu relevant al transformării războiului clasic într-un sistem complex, în care dimensiunea geopolitică se intersectează direct cu evoluțiile tehnologice accelerate[11]. Acesta se înscrie în logica războiului hibrid, caracterizat de utilizarea simultană a instrumentelor militare, informaționale și digitale, cu efecte extinse inclusiv asupra populației civile[12].

În acest context, utilizarea sistemelor fără pilot de tip UAV, UAS[13] și UGV[14] a redefinit dinamica operațională a câmpului de luptă, contribuind la extinderea capacității de supraveghere, recunoaștere și colectare de informații în vederea coordonării acțiunilor militare[15]. Aceste echipamente nu sunt doar instrumente de atac, ci surse esențiale de date, furnizând informații în timp real despre evoluțiile din teren[16]. Integrarea inteligenței artificiale amplifică aceste capacități prin procesarea rapidă a datelor și sprijinirea procesului decizional[17].

În paralel, spectrul electromagnetic devine un spațiu esențial de confruntare, în care controlul comunicațiilor și al fluxurilor de informație influențează direct coordonarea operațiilor[18]. Dependența de infrastructuri digitale amplifică vulnerabilitățile acestora, iar capacitatea de integrare și adaptare tehnologică rapidă devine un factor esențial al eficienței operaționale[19]. În acest cadru, analiza conflictului necesită o abordare integrată, care să coreleze dimensiunea geopolitică cu evoluțiile tehnologice și rolul acestora în redefinirea conflictului modern[20].

Integrarea inteligenței artificiale amplifică această transformare prin capacitatea de a procesa volume mari de date provenite din surse multiple, precum drone, sateliți sau senzori terești. În conflictul din Ucraina aceste sisteme permit corelarea rapidă a informațiilor și sprijină procesul decizional în timp real, contribuind la creșterea vitezei de reacție și la optimizarea acțiunilor militare, în vederea evitării surprinderii strategice. Platformele digitale de tip „*battlespace management*” integrează aceste fluxuri informaționale într-un sistem interconectat, în care informația devine resursa centrală a superiorității operaționale[21]. Cu toate acestea, evoluțiile recente trebuie interpretate ca parte a unei transformări progresive, deoarece tehnologiile autonome și inteligența artificială nu au generat, în mod independent, schimbări decisive la nivel strategic și nu au înlocuit rolul forțelor convenționale[22].

Un element distinctiv al conflictului ruso-ucrainean îl constituie modul inovator de acces și integrare a tehnologiilor militare direct la nivel tactic și chiar individual, în funcție de nevoile din teren. Militarii ucraineni utilizează aplicații digitale instalate pe dispozitive inteligente personale, prin intermediul cărora pot selecta și comanda sisteme autonome, în special drone, de la contractori privați acreditați. Aceste achiziții sunt realizate pe baza unor credite puse la dispoziție de stat, ceea ce permite o flexibilizare semnificativă a procesului de aprovizionare militară. Livrarea acestor sisteme se realizează într-un interval scurt, de regulă între 3 și 5 zile, reducând drastic timpul dintre identificarea unei necesități operaționale și utilizarea efectivă a tehnologiei pe câmpul de luptă[23].

Această dinamică evidențiază faptul că automatizarea câmpului de luptă nu se limitează la utilizarea tehnologiilor avansate, ci presupune

existența unui ecosistem militar flexibil și adaptiv. În conflictul din Ucraina, avantajul operațional nu este determinat exclusiv de performanța sistemelor autonome, ci de capacitatea de integrare rapidă a acestora în structuri organizaționale, logistice și informaționale eficiente. Astfel, digitalizarea și automatizarea generează avantaje tactice semnificative, însă eficiența lor depinde de modul în care sunt utilizate în cadrul unui sistem coerent de operare[24].

În acest context, utilizarea sistemelor autonome și a inteligenței artificiale creează o dependență directă de comunicații și de fluxurile de date, ceea ce conduce inevitabil către o competiție pentru controlul mediului informațional[25]. În conflictul ruso-ucrainean, această interdependență evidențiază faptul că eficiența tehnologiilor emergente este strâns legată de capacitatea de a menține funcționalitatea infrastructurilor digitale într-un mediu contestat[26].

În conflictul dintre F.Rusă și Ucraina, spectrul electromagnetic s-a constatat a fi un domeniu operațional esențial, influențând direct capacitatea de coordonare, comunicare și execuție a acțiunilor militare[27]. Utilizarea intensivă a sistemelor digitale și a platformelor fără pilot a transformat controlul frecvențelor radio într-un factor esențial al eficienței operaționale, în special în condițiile unui câmp de luptă interconectat. În Ucraina, această dependență este evidentă prin integrarea continuă a datelor provenite din drone, senzori și comunicații în procesele de comandă și control, ceea ce face ca pierderea accesului la spectru să afecteze direct capacitatea de reacție a forțelor[28].

Războiul electronic reprezintă principalul instrument prin care acest spațiu este contestat și controlat. În conflictul din Ucraina, forțele ruse au utilizat sisteme dedicate de bruiaj, precum cele din familia „*Krasukha*” sau „*Zhitel*”, pentru a perturba comunicațiile și semnalele GPS, afectând funcționarea dronelor și a sistemelor de navigație. Aceste acțiuni au redus precizia operațiilor militare și au obligat forțele ucrainene să adopte soluții alternative, inclusiv control manual, sisteme redundante și navigație bazată pe repere vizuale. În paralel, tehnicile de „*spoofing*” au fost utilizate pentru a induce erori de poziționare, afectând atât platformele autonome, cât și procesele de coordonare operațională[29].

Un exemplu relevant al importanței spectrului electromagnetic în conflictul ruso-ucrainean îl constituie utilizarea comunicațiilor satelitare. În condițiile distrugerii infrastructurii terestre, rețelele satelitare, inclusiv cele comerciale, au devenit esențiale pentru menținerea comunicațiilor și coordonarea acțiunilor. Sistemele de tip Starlink au permis transmiterea continuă a datelor și integrarea rapidă a informațiilor din teren, însă au devenit simultan ținte ale acțiunilor de război electronic. Această interdependență evidențiază faptul că eficiența tehnologiilor moderne este condiționată de capacitatea de a menține funcționalitatea comunicațiilor[30].

În conflictul din Ucraina, utilizarea simultană a unui număr mare de sisteme moderne a condus la o congestie semnificativă a spectrului electromagnetic. Această suprasolicitare generează interferențe și pierderi de semnal, afectând performanța sistemelor și obligând unitățile să gestioneze dinamic frecvențele disponibile. În aceste condiții, spectrul electromagnetic devine un spațiu activ de competiție, în care fiecare actor încearcă să maximizeze utilizarea propriilor frecvențe și să limiteze accesul adversarului[31]. Unitățile ucrainene sunt nevoite să schimbe frecvențele de operare, să utilizeze comunicații criptate și să implementeze sisteme redundante pentru a evita bruiajul și interceptarea. În cazul dronelor, dezvoltarea unor moduri autonome de funcționare sau a unor sisteme de revenire automată în cazul pierderii semnalului reflectă această adaptare constantă la condițiile din teren.

Interdependența dintre războiul electronic și sistemele autonome este deosebit de evidentă în conflictul ruso-ucrainean. Dronele, devenite esențiale pentru operațiuni, sunt simultan dependente de spectrul electromagnetic și vulnerabile la perturbarea acestuia. Această dependență generează o cursă tehnologică continuă, în care fiecare parte dezvoltă soluții pentru protejarea propriilor sisteme și pentru

exploatarea vulnerabilităților adversarului. În acest context, utilizarea frecvențelor alternative, a comunicațiilor securizate și a sistemelor hibride de control reflectă adaptarea la un mediu operațional instabil și competitiv[32].

Pe lângă dimensiunea tactică, controlul spectrului electromagnetic are implicații strategice majore. Limitarea accesului adversarului la comunicații sau perturbarea sistemelor de detecție reduce capacitatea acestuia de a coordona operațiile și de a reacționa eficient la schimbările din teren[33]. În conflictul ruso-ucrainean, aceste acțiuni contribuie la modificarea echilibrului de putere, fără a implica neapărat distrugeri fizice directe[34].

În plan tehnologic, cercetările privind controlul propagării undelor electromagnetice indică direcții emergente relevante pentru dezvoltarea sistemelor militare[35], cu accent pe concepte precum benzile interzise de frecvență, care permit blocarea selectivă a propagării undelor în anumite intervale, contribuind la filtrarea și protejarea semnalelor, respectiv metamaterialele, care oferă posibilitatea controlului avansat al interacțiunii dintre unde și mediu, cu aplicații potențiale în optimizarea comunicațiilor, reducerea vibrațiilor nedorite și a detectabilității[36].

EVOLUȚII ALE ARHITECTURII DE REZILIENȚĂ

Principalele dinamici geopolitice identificate în contextul războiului ruso-ucrainean sunt strâns legate de consolidarea flancului estic din punct de vedere al revitalizării NATO, atât prin prisma cooperării între statele membre, cât și prin atragerea de noi state partenere, care anterior declaraseră o poziție neutră. În acest sens, NATO a desfășurat, încă din anul 2016, patru grupuri de luptă multinaționale în Estonia, Letonia, Lituania și Polonia, sub umbrela programului de Prezență Înaintată Consolidată, drept răspuns la anexarea Peninsulei Crimeea. În urma invaziei ruse din anul 2022, NATO a suplimentat eforturile defensive, desfășurând alte patru grupuri de luptă în Bulgaria, Ungaria, România și Slovacia[37].

De asemenea, pentru a putea facilita mișcarea trupelor, a echipamentelor și a tehnicii militare, luând în considerare limitările existente din punct de vedere al infrastructurii, în anul 2024 Germania, Olanda și Polonia au decis dezvoltarea unui coridor militar, evitând astfel limitări precum incapacitatea de a tranzita anumite puncte cheie ale infrastructurii civile deja existente[38]. În cadrul inițiativei s-au implicat, ulterior, Belgia, Cehia, Lituania, Luxemburg și Slovacia, dezvoltându-se astfel zona de mobilitate militară nord-centrală[39].

De impact pentru dezvoltarea organizației au fost cele două aderări, din perioada 2023-2024, ale Finlandei și Suediei, riscurile și amenințările generate de războiul ruso-ucrainean determinând cele două state să își reorienteze politica de neutralitate[40]. Astfel, prin înaintarea de către cele două state a solicitării de aderare, din iunie 2022, a fost reconfirmat succesul pilonului de securitate nord-atlantic[41].

Revenind la spectrul infrastructurii, în anul 2024 au fost înregistrate mai multe inițiative, precum dezvoltarea altor două coridoare militare pe axa Bulgaria - Grecia - România, respectiv pe axa Danemarca - Finlanda - Islanda - Norvegia - Suedia[42]. Pentru a susține proiectele de mobilitate, un sprijin semnificativ a fost furnizat de către UE, prin intermediul implementării Mecanismului de Interconectare a Europei (MIE) și alocării a aproximativ 800 mil. Euro[43], identificând totodată patru axe de mobilitate militară și proiecte de transport cu valențe strategice hibride (utilizare dual), care necesită implementare rapidă[44].

Din punct de vedere strategic, NATO a dezvoltat un program de exerciții militare, urmărind prin intermediul acestora creșterea capacității de răspuns în caz de amenințare, respectiv testarea unor parametri precum mobilitatea și ritmul de acțiune al trupelor. Analizând principiile care au stat la baza organizării și derulării exercițiilor militare din perioada 2024-2025, identificăm obiectivele de întărire regională susținută pe trei direcții, care cuprind flancul estic, respectiv Axa de Nord (Finlanda - Statele Baltice), Axa Centrală (Polonia - Cehia - Slovacia - Ungaria) și Axa de Sud (Ungaria-România-Bulgaria)[45].

2024

- STEADFAST DEFENDER 24 (32 națiuni implicate)
- NORDIC RESPONSE 24 (14 națiuni implicate)
- DRAGON 24 (10 națiuni implicate)
- GRAND QUADRIGA 24 (10 națiuni implicate)
- TROJAN FOOTPRINT 24 (10 națiuni implicate)
- SLOVAK SHIELD 24 (7 națiuni implicate)

2025

- IRON DEFENDER 25 (20 de națiuni implicate)
- HEDGEHOG 25 (11 națiuni implicate)
- DACIAN FALL 25 (10 națiuni implicate)
- STEADFAST DART 25 (9 națiuni implicate)
- ADAPTIVE HUSSARS 25 (8 națiuni implicate)
- TOXIC VALLEY 25 (8 națiuni implicate)
- BLACK SWAN 25 (5 națiuni implicate)

În ceea ce privește accelerarea procesului de integrare în cadrul UE, începând cu anul 2022 au fost înregistrate o serie de progrese, statele aliniindu-și interesele și strategiile de politică externă la viziunea comună europeană. În acest sens, în iunie 2022, Ucraina și Republica Moldova au obținut statutul de țări candidate la integrarea în UE, fiind urmate de Bosnia și Herțegovina în luna decembrie, apoi de Georgia în decembrie 2023[46]. În contextul obținerii statutului de candidați la aderare, până în prezent au fost deschise discuții de negociere cu cele patru state, viziunea aderării și a extinderii cooperării în cadrul UE fiind tratată cu atenție sporită. Astfel, având în vedere procesul de durată prin care trec statele care și-au manifestat interesul accederii în UE, în anul 2022 a fost lansată Comunitatea Politică Europeană (CPE), un nou forum de cooperare care reunește atât statele membre UE, cât și statele care doresc să se alinieze la viziunea europeană[47].

De asemenea, în anul 2025, UE a lansat planul strategic „*Defence Readiness Roadmap 2030*[48]”, care presupune atingerea, până în anul 2030, a obiectivelor formulate în cadrul proiectelor principale cunoscute drept Supravegherea Flancului Estic, Inițiativa Europeană de Apărare Împotriva Dronelor, Scutul Aerian European și Scutul Spațial European, toate acestea fiind aliniate cu viziunea NATO[49].

CONCLUZII ȘI EVALUARE

Conflictul ruso-ucrainean a determinat instabilitate în plan securitar, atât la nivel intern, cât și la nivel regional, fiind identificate în relație de interdependență multiple efecte și măsuri adoptate de către comunitatea internațională pentru a atinge dezideratul recalibrării securității. Amenințarea manifestată multi-sectorial în urma acțiunilor derulate de Federația Rusă continuă să reprezinte o provocare pentru statele partenere în cadrul NATO și UE, fiind adoptate și implementate în contrapartidă multiple măsuri atât la nivel regional, cât și la nivel continental.

Propagarea efectelor războiului secvențial din plan regional în plan continental și, mai apoi, în plan internațional, reflectă necesitatea abordării etapizate a problemelor de securitate, pornind de la cooperarea statelor vecine în cadrul inițiativelor regionale de cooperare, urmată de extensia cooperării statelor în cadrul organizațiilor internaționale. În prezent, crearea unor mecanisme de răspuns etapizat în caz de agresiune, precum și însușirea lecțiilor învățate rezultate din derularea războiului ruso-ucrainean reprezintă direcții fundamentale pentru întreaga comunitate internațională, provocarea aplicabilității acestora urmând a fi testată în viitor, în funcție de dinamica geopolitică regională.

Mai mult, conflictul ruso-ucrainean confirmă faptul că natura războiului modern este redefinită de integrarea tehnologiilor emergente în arhitectura operațională. Sistemele autonome, inteligența artificială și digitalizarea nu mai reprezintă simple instrumente de sprijin, ci elemente structurale care influențează direct viteza decizională, precizia acțiunilor și capacitatea de adaptare în timp real. În paralel, spectrul electromagnetic se consolidează ca un domeniu esențial de confruntare, în care controlul comunicațiilor și al fluxurilor de informație devine determinant pentru coordonarea și eficiența operațiilor[50].

În acest cadru, avantajul strategic nu mai derivă din superioritatea unei tehnologii izolate, ci din capacitatea de integrare a sistemelor într-un ecosistem interconectat și flexibil. Interdependența dintre războiul electronic, platformele autonome și infrastructura informațională evidențiază caracterul multidomeniu al conflictului contemporan. Astfel, controlul spectrului electromagnetic și valorificarea tehnologiilor emergente devin factori decisivi în configurarea echilibrului de putere[51].

BIBLIOGRAFIE

1. AKGÜL Pinar, "The impact of the Russia-Ukraine war on the Black Sea Economic Cooperation: adapting economic cooperation to security challenges", *Southeast European and Black Sea Studies*, March 2026; https://doi.org/10.1080/14683857.2026.2641309.
2. AVIV Itzhak, Ferri Uri, "Russian-Ukraine armed conflict: Lessons learned on the digital ecosystem", *International Journal of Critical Infrastructure Protection*, vol. 43, 2023; https://doi.org/10.1016/j.ijcip.2023.100637.
3. BACHMANN Sascha-Dominik Dov, Putter Dries, Duczynski Guy, "Hybrid warfare and disinformation: A Ukraine war perspective", *Global Policy*, vol. 14, 2023, pp. 858-869; https://doi.org/10.1111/1758-5899.13257.
4. BALTA Evren, Celik Wiltse Evren, *Introduction to Global Politics*, Iletisim Yayincilik, Istanbul, 2015, pp. 250-251.
5. BI Mengyi, He Yunze, Guo Cai, Deng Baoyuan, He Zhiyi, Yang Ruizhen, Zhang Hong, Chen Zhi, She Saibo, Wu Haoxuan, "Advances, challenges, and future directions of UAV/drone-based active non-destructive testing", *Nondestructive Testing and Evaluation*, vol. 41, January 2026; https://doi.org/10.1080/10589759.2025.2601323.
6. BUZAN Barry, *People, States and Fear: The National Security Problem in International Relations*, University of North Carolina Press, Brighton, 1983.
7. BUZAN Barry, Waever Ole, *Regions and Powers: The Structure of International Security*, Cambridge University Press, Cambridge, 2003.
8. BUZAN Barry, "New Patterns of Global Security in the Twenty-First Century", *International Affairs*, vol. 67, nr. 3, 1991, pp. 431-451; https://doi.org/10.2307/2621945.
9. CLAPP Sebastian, ENGEL Darius, CHAHRI Samry, *European Defence Readiness Roadmap*, Parlamentul European, 2026.
10. COTTEY Andrew, Cladi Lorenzo, Ewers-Peters Nele Marianne, "Introduction: the 2022 Russian invasion of Ukraine and the re-making of the European security order",

Defence Studies, vol. 25, nr. 4, 2025, pp. 759-778; https://doi.org/10.1080/14702436.2025.2577333.

11. DITRYCH Ondřej, Laryš Martin, "What can European security architecture look like in the wake of Russia's war on Ukraine?", *European Security*, vol. 34, nr. 1, 2025, pp. 44-64; https://doi.org/10.1080/09662839.2024.2347221.
12. FABBRINI Federico, "The Impact of the War in Ukraine on the Enlargement of the European Union: Securing the Blessings of Liberty and its Challenges", *International & Comparative Law Quarterly*, vol. 74, no.1, Cambridge University Press, January 2025, p. 123-146.
13. GHEȚU Caroline Raluca, "Comunitatea Politică Europeană: oportunități și provocări", Institutul European din România, Working Paper nr. 48, București, 2023.
14. HAGER Robert P., "History and Culture in Russia and Ukraine: How to Complicate a Crisis of European Security", *Democracy and Security*, vol. 12, nr. 3, 2016, pp. 211-218; https://doi.org/10.1080/17419166.2016.1205335.
15. HE Yunze, Liu Zhaoyan, Guo Yike, Zhu Qijia, Fang Yu, Yin Yong, Wang Yang, Zhang Bei, Liu Zhaohua, "UAV based sensing and imaging technologies for power system detection, monitoring and inspection: A review", *Nondestructive Testing and Evaluation*, vol. 40, nr. 12, 2025, pp. 5681-5748; https://doi.org/10.1080/10589759.2024.2421938.
16. HYNEK Nik, Šenk Michal, "Ukraine–Russia peace plans: historical lessons, operationalising criteria, and comparative assessment", *Peacebuilding*, november 2025; https://doi.org/10.1080/21647259.2025.2585235.
17. JOZWIAK Rikard, "Wider Europe Briefing: Will the EU Be Able to Create a 'Military Schengen'?", *Radio Free Europe/ Radio Liberty*, Praga, November 18, 2025; https://rferl.org/a/wider-europe-jozviak-military-schengen-eu/33593920.html.
18. KAUNERT Christian, De Deus Pereira Joana, "EU Eastern Partnership, Ontological Security and EU-Ukraine/Russian warfare", *Journal of Contemporary European Studies*, vol. 31, nr. 4, 2023, pp. 1135-1146; https://doi.org/10.1080/14782804.2023.2183182.
19. LI Lei, Meng Wei, Bao Yulin, "Bandgap metamaterials for vibration control: Theories, design, fabrication, and applications", *Engineering Structures*, vol. 347, 2026; https://doi.org/10.1016/j.engstruct.2025.121746.
20. LIPPERT William E., "How conventional arms control failures caused the Russo-Ukraine War", *Defense & Security Analysis*, vol. 40, nr. 1, 2024, pp. 138-160; https://doi.org/10.1080/14751798.2024.2300889.
21. MAKARYCHEV Andrey, Wicaksana I Gede Wahyu, "Multilateralism at War: Russia's Invasion of Ukraine, the G20 and World Order", *Global Society*, vol. 39, nr. 2, 2025, pp. 181-202; https://doi.org/10.1080/13600826.2024.2359969.
22. MANDLE J. Layton, "Consider the longbow: RMAs, evolutionary technology, and uncrewed systems", *Defense & Security Analysis*, online, January 2026; https://doi.org/10.1080/14751798.2025.2611454.
23. MARINESCU Antonio, Monu Ion, *Admiterea Suediei și Finlandei în NATO*, Centrul Euro-Atlantic pentru Reziliență, București, 2022; https://e-arc.ro/2022/05/27/admiterea-suediei-si-finlandei-in-nato/.
24. 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.
25. PYNNÖNIEMI Katri, Parppei Kati, "Understanding Russia's war against Ukraine: Political, eschatological and cataclysmic dimensions", *Journal of Strategic Studies*, vol. 47, nr. 6-7, 2024, pp. 832-859; https://doi.org/10.1080/01402390.2024.2379395.
26. ROSSITER Ash, "Bots on the ground: an impending UGV revolution in military affairs?", *Small Wars & Insurgencies*, vol. 31,

nr. 4, 2020, pp. 851-873; https://doi.org/10.1080/09592318.2020.1743484.
27. RUITENBERG Rudy, "Europeans set up corridor for rushing NATO troops eastward", *Defense News*, January 31, 2024; https://www.defensenews.com/global/europe/2024/01/31/europeans-set-up-corridor-for-rushing- nato-troops-eastward/
28. SIDDI Marco, "The partnership that failed: EU-Russia relations and the war in Ukraine", *Journal of European Integration*, vol. 44, nr. 6, 2022, pp. 893-898; https://doi.org/10.1080/07036337.2022.2109651.
29. SOLMAZ Tarik, "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.
30. SUN Jian, Zhou Jing, "Metamaterials: The art in materials science", *Engineering*, 2024; https://doi.org/10.1016/j.eng.2024.12.011.
31. TSYGANKOV P. Andrei, "Russia, Ukraine, and the West: from Mistrust to Conflict", *The Journal of Slavic Military Studies*, vol. 37, nr. 3-4, 2024, pp. 287-309; https://doi.org/10.1080/13518046.2024.2418231.
32. 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.
33. *** GLOBSEC, *Annual Battle Readiness on the Eastern Flank – 2026*, Praga, 2026, 139 p.; https://www.globsec.org/sites/default/files/2026-04/Annual%20Battle%20Readiness%20on%20the%20Eastern%20Flank%202026.pdf.
34. *** The Luxembourg Government, Directorate of Defence, "Military Mobility", 2025; https://defense.gouvernement.lu/en/la-defense/mobilite.html
35. *** European Commission, "Joint Report to the European Parliament and the Council on the implementation of the Action Plan on Military Mobility 2.0", Bruxelles, 2025; https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025JC0011
36. *** Directorate-General for Mobility and Transport, "Commission supports military mobility projects with €807 million", European Commission, 2024; https://transport.ec.europa.eu/news-events/news/commission-supports-military-mobility-projects-eu807-million-2024-01-24_en
37. *** European Commission, "Joint Communication to the European Parliament, The European Council and the Council: Preserving Peace – Defence Readiness Roadmap 2030", Bruxelles, 2025.
38. *** "A Choice of Deadly Drones Is Only a few Clicks Away for Ukrainian Troops", *The New York Times*, March 23, 2026; https://www.nytimes.com/2026/03/23/world/europe/ukraine-drones-marketplace-military-russia.html.

[1] Barry Buzan, *People, States and Fear: The National Security Problem in International Relations*, Brighton, University of North Carolina Press, 1983, p. 190.
[2] Barry Buzan și Ole Waever, *Regions and Powers: The Structure of International Security*, Cambridge University Press, 2003, p. 4.
[3] *Ibidem*.
[4] Evren Balta, *Introduction to Global Politic*s, Iletisim Yayincilik, Istanbul, 2015, p. 250-251.
[5] Cr - Complex de securitate regional.
[6] Cs - Complex de securitate subregional.
[7] Balta, *Op.cit.*.
[8] Barry Buzan, ”New Patterns of Global Security in the Twenty-First Century”, *International Affairs*, 1991, p. 433.
[9] 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; https://www.proquest.com/scholarly-journals/battlefield-evidence-age-artificial-intelligence/docview/3235035015/se-2, accesat la 15.03.2026.
[10] *Unmanned Aerial Vehicle.*
[11] Tarik 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.
[12] Sascha-Dominik Dov Bachmann, Dries Putter, Guy Duczynski, ”Hybrid warfare and disinformation: A Ukraine war perspective”, *Global Policy*, vol. 14, 2023, pp. 858-869; https://doi.org/10.1111/1758-5899.13257.
[13] *Unmanned Aerial System.*
[14] *Unmanned Ground Vehicle.*
[15] Winthrop Wells, *Op.cit.*
[16] *Ibidem.*
[17] Ash Rossiter, ”Bots on the ground: an impending UGV revolution in military affairs”, *Small Wars & Insurgencies*, vol. 31, nr. 4, 2020, pp. 851-873.
[18] Itzhak Aviv, Uri Ferri, ”Russian-Ukraine armed conflict: Lessons learned on the digital ecosystem”, *International Journal of Critical Infrastructure Protection*, vol. 43, 2023.
[19] *Ibidem.*
[20] Andrei P. Tsygankov, ”Russia, Ukraine, and the West: from Mistrust to Conflict”, *The Journal of Slavic Military Studies*, vol. 37, nr. 3-4, 2024, pp. 287-309.
[21] *Ibidem.*
[22] Layton J. Mandle, ”Consider the longbow: RMAs, evolutionary technology, and uncrewed systems”, *Defense & Security Analysis*, online, January 9, 2026.
[23] *** ”A Choice of Deadly Drones Is Only a few Clicks Away for Ukrainian Troops”, *The New York Times*, March 23, 2026; https://www.nytimes.com/2026/03/23/world/europe/ukraine-drones-marketplace-military-russia.html, accesat la 17.05.2026.
[24] Layton J. Mandle, *Op. cit.*
[25] Winthrop Wells, *Op. cit.*
[26] Itzhak Aviv, Uri Ferri, *Op. cit.*
[27] Andrei P. Tsygankov, *Op. cit.*
[28] Itzhak Aviv, Uri Ferri, *Op. cit.*
[29] Winthrop Wells, *Op. cit.*
[30] *Ibidem.*
[31] Tarik Solmaz, *Op. cit.*
[32] Layton J. Mandle, *Op. cit.*
[33] Andrey Makarychev, I Gede Wahyu Wicaksana, ”Multilateralism at War: Russia’s Invasion of Ukraine, the G20 and World Order”, *Global Society*, vol. 39, nr. 2, 2025, pp. 181-202.
[34] Katri Pynnöniemi, Kati Parppei, ”Understanding Russia’s war against Ukraine: Political, eschatological and cataclysmic dimensions”, *Journal of Strategic Studies*, vol. 47, nr. 6-7, 2024, pp. 832-859.
[35] Jian Sun, Jing Zhou, ”Metamaterials: The art in materials science”, *Engineering*, 2024.
[36] Lei Li, Wei Meng, Yulin Bao, ”Bandgap metamaterials for vibration control: Theories, design, fabrication, and applications”, *Engineering Structures*, vol. 347, 2026.
[37] *** GLOBSEC, *Annual Battle Readiness on the Eastern Flank - 2026*, Praga, p. 16; https://www.globsec.org/sites/default/files/2026-04/Annual%20Battle%20Readiness%20on%20the%20Eastern%20Flank%202026.pdf., accesat la 12.05.2026.
[38] Rudy Ruitenberg, ”Europeans set up corridor for rushing NATO troops eastward”, *Defense News*, January 31, 2024; https://www.defensenews.com/global/europe/2024/01/31/europeans-set-up-corridor-for-rushing-nato-troops-eastward/, accesat la 21.05.2026.
[39] *** *Military mobility*, The Luxembourg Government, Directorate of Defence, 2025; https://defense.gouvernement.lu/en/la-defense/mobilite.html.

[40] Antonio Marinescu, Ion Monu, *Admiterea Suediei și Finlandei în NATO*, Centrul Euro-Atlantic pentru Reziliență, 2022; https://e-arc.ro/2022/05/27/admiterea-suediei-si-finlandei-in-nato/, accesat la 02.05.2026.

[41] *Ibidem.*

[42] *** European Commission, *Joint Report to the European Parliament and the Council on the implementation of the Action Plan on Military Mobility 2.0*, Bruxelles, 2025; https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025JC0011, accesat la 21.04.2026.

[43] *** Directoratul General pentru Mobilitate și Transport, *Commission supports military mobility project with 807 mil. Euro*, Comisia Europeană, 2024; https://transport.ec.europa.eu/news-events/news/commission-supports-military-mobility-projects-eu807-million-2024-01-24_en., accesat la 29.04.2026.

[44] Rikard Jozwiak, "Wider Europe Briefing: Will the EU Be Able to Create A 'Military Schengen'?", *RadioFreeEurope/RadioLiberty*, Praga, November 18, 2025; https://rferl.org/a/wider-europe-jozviak-military-schengen-eu/33593920.html., accesat la 11.04.2026.

[45] *** GLOBSEC, *Op.cit.*, p. 52.

[46] Federico Fabbrini, "The Impact of the War in Ukraine on the Enlargement of the European Union: Securing the Blessings of Liberty and its Challenges", *International & Comparative Law Quarterly*, vol. 74, no.1, Cambridge University Press, January 2025, p. 123-146.

[47] Caroline Raluca Ghețu, *Comunitatea Politică Europeană, oportunități și provocări*, Institutul European din România, Working Paper nr. 48, București, 2023.

[48] *** Comisia Europeană, *Joint Communication to the European Parliament, The European Council and the Council, Preserving Peace- Defence Readiness Roadmap 2030*, Bruxelles, 2025.

[49] Sebastian Clapp, Darius Engel, Samry Chahri, *European defence readiness roadmap*, Parlamentul European, 2026.

[50] Andrei P. Tsygankov, *Op. cit.*

[51] Katri Pynnöniemi, Kati Parppei, *Op. cit.*

OPERAȚIILE UAS ÎN ARMATA UCRAINEANĂ ȘI TRANSFORMAREA RĂZBOIULUI ÎNTR-UN JOC VIDEO – „ARMATA DE DRONE”

Ciprian-Constantin VOINEA*

Abstract

The Russo-Ukrainian war has become a pivotal case study for understanding the transformation of contemporary warfare and the expanding role of uncrewed systems on the modern battlefield. The widespread employment of Unmanned Air Systems/Vehicles (UAS/UAV) across ISR (Intelligence, Surveillance and Reconnaissance) and strike missions has demonstrated how relatively accessible technologies can be rapidly adapted to generate significant military advantages, on tactical, operational and even strategic levels. In particular, the use of commercially available and improvised platforms has highlighted the growing importance of the aerial dimension in land operations/multi-domain operations, enabling enhanced situational awareness, precision engagement and cost-effective force multiplication in high-intensity conflict environments. The small, cheap FPV (First Person-View) drone has taken to the stage and consolidated its reputation as one of the most fearsome weapons of the war for soldiers on the ground. In the context of the war in Ukraine, the Army of Drones Bonus (ADB) initiative has often been portrayed as an example of the so-called "game-ification of war," as drone units receive digital reward points for successful strikes that can later be exchanged for equipment and operational resources.

Keywords: *Unmanned Air Systems/Vehicles (UAS/UAV); drone warfare; Russia–Ukraine war; Army of Drones; multi-domain operations; military innovation; doctrine development; force adaptation.*

INTRODUCERE

Utilizarea dronelor în războiul din Ucraina reprezintă prima situație din istoria recentă în care sistemele fără pilot au fost integrate masiv într-un conflict convențional între state, fiind utilizate simultan pentru o gamă largă de misiuni, precum recunoaștere, supraveghere, corectarea focului de artilerie, executarea loviturilor de precizie, sprijinul logistic și evaluarea efectelor acțiunilor militare. Această diversitate funcțională evidențiază rolul tot mai important al operațiilor multidomeniu și necesitatea adaptării structurilor militare la un mediu operațional caracterizat de interconectivitate și dinamism. În prezent, sistemele fără pilot sunt utilizate nu doar în mediul aerian, ci și în mediul terestru și maritim, contribuind la extinderea spectrului de acțiune al forțelor armate și la creșterea flexibilității operaționale. Ca perspectivă de viitor, dezvoltarea și cercetarea în domeniul inteligenței artificiale

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

promite inovații majore în operațiile cu sisteme autonome și modificări în fizionomia acțiunilor militare multidomeniu.

Caracterul de uzură al războiului din Ucraina și ritmul accelerat al inovării tehnologice au evidențiat necesitatea ca forțele armate să își adapteze rapid sistemele de achiziții și logistică, astfel încât echipamentele adecvate să ajungă la unitățile operative în cel mai scurt timp. În acest context, crearea programului ucrainean ***„Army of Drones" (Armata de Drone)***, bazat pe un sistem de puncte inspirat din mecanisme specifice mediului digital, a generat dezbateri intense privind posibila „*game-ificare* a războiului" (apropierea acestuia de un joc video). Programul reprezintă o inițiativă inovatoare prin care unitățile de drone primesc puncte electronice pentru lovituri confirmate asupra țintelor inamice.

PROGRAMUL „ARMATA DE DRONE"

La începutul ofensivei ruse, în februarie 2022, primele sisteme UAS (drone comerciale DJI Mavic) erau percepute de către armata ucraineană ca niște simple „jucării"[1] și sprijineau efortul ISR doar prin oferirea imaginilor în timp real către comandamente, spre înțelegerea mai bună a situației tactice. Patru ani mai târziu, în armata ucraineană sunt folosite aproape 300 de modele diferite de UAS, construite de peste 200 de companii diferite (de la 7 înainte de război)[2] – de supraveghere, de lovire, kamikaze sau cu muniții de tip *loitering.*

Notorietatea aproape mitică a sistemelor FPV, eficiența și versatilitatea nou-identificată a capabilităților oferite de către dronele comerciale modificate și militarizate au condus la schimbări doctrinare semnificative, precum ridicarea în statut și formalizarea forțelor UAS în 2024, prin înființarea Forțelor Sistemelor fără Pilot (USF), Ucraina devenind astfel prima țară cu o categorie de forțe dedicată sistemelor fără pilot[3].

Ulterior, Guvernul Ucrainei a lansat proiectul comun *„Armata de Drone/ Army of Drones"* al Statului Major General al Forțelor Armate cu scopul cercetării și dezvoltării în domeniul UAS militar, al obținerii de fonduri internaționale pentru achiziția dronelor, precum și pentru donații (monetare sau în materie de echipament). De o importanță esențială în cadrul proiectului regăsim formatul „*e-points*", debutând în 2025, odată cu introducerea „Army of Drones Bonus" (ADB), care atribuie un punctaj acțiunilor întreprinse pe câmpul de luptă dovedite prin înregistrări video, transpunând într-un clasament acțiunile militarilor din cadrul Forțelor Sistemelor fără Pilot; militarii cu cele mai multe puncte primesc diverse recompense, ce pot fi ulterior utilizate pentru achiziționarea de echipamente și resurse operaționale prin intermediul platformei virtuale Brave1 Market.

Obiectivele de pe câmpul de luptă au fost aranjate în funcție de importanța acestora în vederea oferirii punctelor: astfel, neutralizarea confirmată video atribuia, la început, 6 puncte pentru un militar inamic, 20 de puncte pentru avarierea unui tanc, 40 de puncte pentru distrugerea unui tanc, 50 de puncte pentru un sistem de rachete autopropulsat[4], în timp ce capturarea unui militar inamic (convingerea acestuia să se predea unei drone) oferă jackpot-ul: 120 de puncte. Așadar, ADB pare să fie un sistem implementat la nivel tactic, dar cu potențial impact la nivel strategic – conform nevoilor forțelor armate ale Ucrainei, capturarea unui număr mai mare de militari ruși ar putea consolida poziția politică a Ucrainei în cadrul negocierilor privind schimburile de prizonieri și în eventualitatea unor discuții de pace. În plus, dacă livrarea accelerată a echipamentelor prin intermediul ADB contribuie la creșterea capacității de acțiune a unităților de drone ucrainene, acestea pot exercita o presiune mai mare asupra capacității forțelor ruse de a-și apăra pozițiile sau de a proteja tehnica blindată.

Chiar dacă avantajele tactice generate de programul ADB nu sunt susceptibile să producă efecte strategice imediate în forma sa actuală, este posibil ca acestea să contribuie, pe termen mai lung, la atingerea unor obiective și interese strategice mai ample ale Ucrainei. De exemplu, odată cu introducerea unor drone cu autonomie mai mare pe piața Brave1, se dorește stabilirea unui punctaj în funcție de distanță și pentru obiective de infrastructură critică aflate în

adâncime[5], în scopul distrugerii depozitelor de muniție, nodurilor logistice sau aeroporturilor militare care găzduiesc aviația strategică, ceea ce deja se întâmplă[6], dar la o scară mult mai mare. Mai mult decât atât, în funcție de intensitatea luptelor, Ministerul Apărării poate modifica temporar punctajul atribuit fiecărei ținte – de exemplu, în cazul unei ofensive cu forțe numeroase de infanterie, punctajul pentru neutralizarea unui inamic poate crește până la 12 puncte, pentru a determina operatorii de drone aflați la distanțe mari de front (aproximativ 20 km) să nu ignore asaltul iminent în favoarea avarierii unui vehicul blindat izolat, în altă parte a frontului[7] (prezența acestor vehicule, devenite ținte rare, aproape garantează „*o linie de drone care așteaptă să le lovească*”[8]).

Succesul a fost evident, în urma introducerii sistemului, în anul 2025: asfel, au fost confirmate 819.737 de lovituri independente înregistrate video, dintre care 240.000 asupra personalului forțelor ruse, 62.000 asupra vehiculelor ușoare, 29.000 asupra vehiculelor blindate, și 32.000 împotriva UAS inamice, ceea ce denotă, cel puțin la prima vedere și în faza incipientă, dovada că acest concept unic și deosebit de practic sprijină semnificativ efortul de război. Conform postării de pe Telegram a președintelui ucrainean, Volodymr Zelenskiy (5 ianuarie 2026), peste 90.000 de lovituri asupra militarilor ruși au fost înregistrate și verificate de către Delta în lunile octombrie-noiembrie 2025, iar, conform Ministerului Apărării, există o traiectorie crescândă, de la lună la lună, a loviturilor înregistrate – momentan, 80% din ținte sunt distruse de către drone, luna decembrie 2025 stabilind un nou record[11].

Este important de notat faptul că, deși astfel de inițiative monetare pentru performanță nu constituie un element de noutate, modul de aplicare este inedit. Un alt exemplu îl regăsim chiar în cadrul aceluiași război: militarii ruși pot fi recompensați pecuniar în cazul distrugerii vehiculelor construite în state NATO (de exemplu MLI Bradley sau tancul Leopard) cu suma de 50.000 de ruble pentru MLI/TBT (~$596) și 100.000 ruble pentru tancuri (~$1200), precum și cu distincția „Eroul Rusiei Steaua de Aur”[13].

Diferența fundamentală este constituită de starea finală a procesului – conform Fig.1, militarii ucraineni neutralizează o țintă, încarcă dovada în format video pentru a fi verificată de către entitatea responsabilă (Delta), apoi unitatea din care face parte militarul primește punctele; la nivelul unității se depune o comandă pe piața Brave1, iar cu ajutorul sistemului *DOT-chain Defence* echipamentul ajunge la unitățile solicitante în termen de doar 5 zile[14], prin contracte realizate automat de către aplicație, securizate prin semnături electronice, eliminând o parte semnificativă a birocrației necesare achiziției de echipament. Practic, unitățile primesc întotdeauna exact ceea ce au nevoie și exact atunci când au nevoie, în concordanță cu cerințele câmpului de luptă la acel moment de timp.

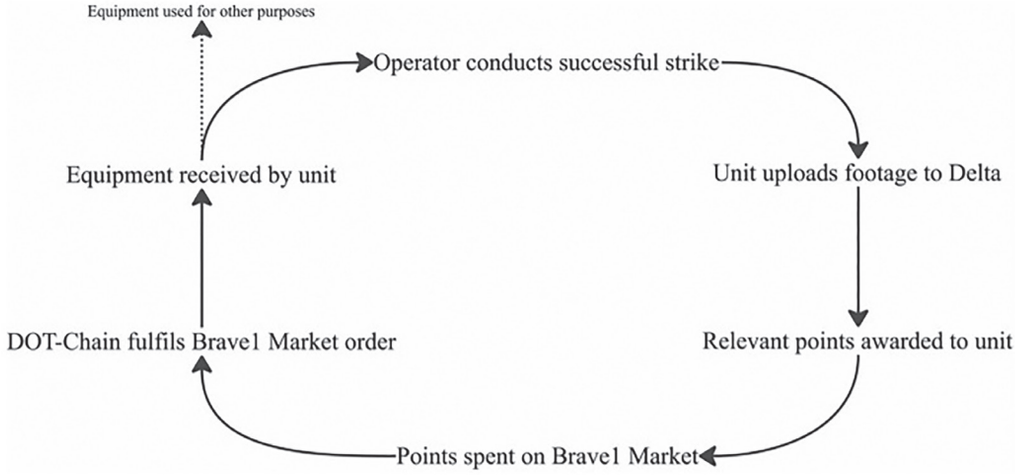

Fig.1: *Procesul de întrebuințare a punctelor pentru procurarea echipamentului*[12]

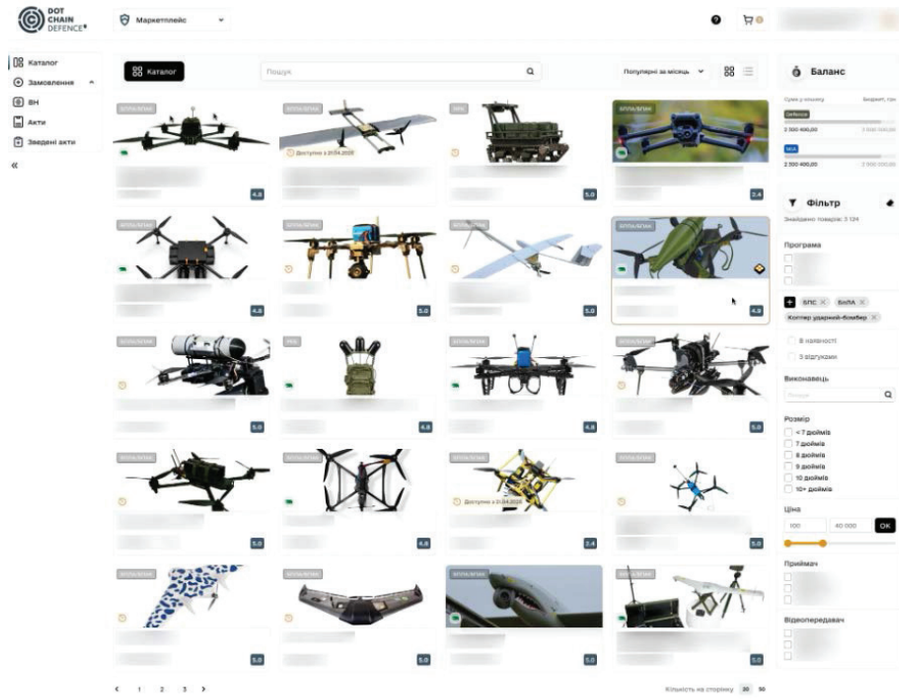

Fig.2: *Interfața sistemului DOT-Chain Defence*[15]

Din punct de vedere al securității operațiilor, un mare accent a fost pus pe oferirea doar a strictului necesar de informații pentru vânzător, în scopul protecției forței luptătoare. Pentru a definitiva livrarea, structura abilitată a Ministerului Apărării definește trei entități separate: cel care plasează comanda, cel care primește bunurile și cel care semnează nota de livrare – această diviziune limitează accesul unui singur individ la informațiile lanțului de aprovizionare și creează un strat în plus de securitate[16]. Livrarea este, de asemenea, organizată pe principiul minimizării riscurilor: platforma nu indică vânzătorului locația exactă în care trebuie să livreze, doar regiunea sau o unitate administrativă, iar livrarea în sine este realizată de către o companie diferită, care se află în contact cu unitatea militară și la nivelul căreia se agreează adresa exactă și data livrării[17].

ADB îndeplinește, așadar, un scop dublu: oferă motivație suplimentară operatorilor pentru a lovi ținte de valoare mare cu frecvență ridicată și oferă direcționări indirecte de la nivelul strategic la tactic. Prin acumularea de puncte pentru lovituri confirmate asupra țintelor inamice, unitățile militare pot fi clasate într-un sistem comparativ, ceea ce creează o ierarhie bazată pe performanță. Cu cât o unitate obține mai multe puncte, cu atât poziția sa în clasament devine mai favorabilă, iar prestigiul profesional crește în interiorul organizației militare. Unitățile de drone încarcă, în timp real, obiectivele neutralizate pe un „*online killboard*” (Fig.3), dând naștere astfel unei competiții vii și publice între acestea, prin promisiunea echipamentului mai bun și a recunoașterii performanțelor acestora într-un clasament în care, la final de an, cele mai bune unități sunt premiate.

Totuși, dincolo de aceste asemănări formale cu logica jocurilor video, elementul cu adevărat relevant al programului ADB nu este dimensiunea simbolică a competiției, ci transformarea procesului de achiziție și distribuție a echipamentelor militare. În trecut, unitățile combatante s-au confruntat cu proceduri de achiziție lente și complexe, caracterizate de un nivel ridicat de birocratizare și de o transparență limitată. Acum, în contextul conflictului actual, Ucraina a inițiat un proces gradual de reformă, orientat către integrarea sectorului comercial și a industriei private în sistemul de aprovizionare militară, cu scopul de a accelera dezvoltarea și livrarea tehnologiilor necesare pe front.

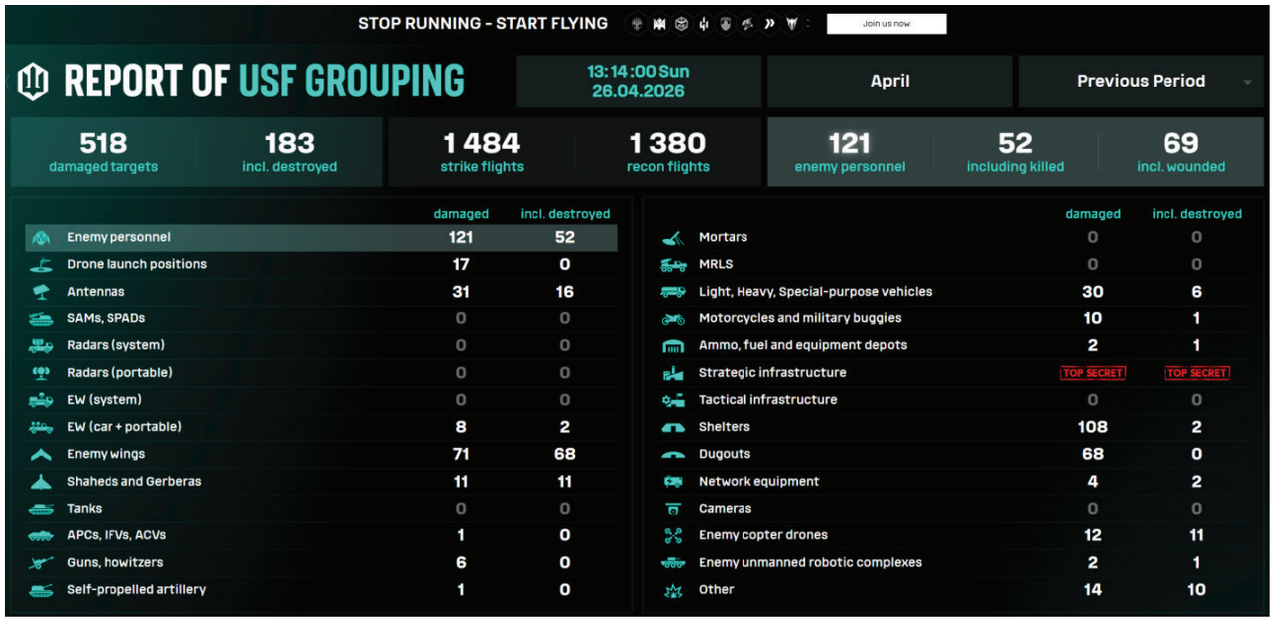

Fig. 3: *Lista țintelor distruse de către o unitate a Forțele Sistemelor fără Pilot în luna Aprilie 2026 (autodeclarate, pe site-ul oficial https://sbs-group.army/en/)*

Mecanismul de stimulare bazat pe performanță creează, de asemenea, un interes direct pentru îmbunătățirea acurateței loviturilor și pentru documentarea rezultatelor operaționale. Necesitatea de a demonstra eficiența acțiunilor prin înregistrarea și validarea loviturilor conduce la acumularea unui volum semnificativ de date și imagini din teren. Aceste materiale pot fi utilizate ulterior pentru instruirea operatorilor, analizarea modului de ducere a luptei și dezvoltarea unor noi tactici, tehnici și proceduri. În acest sens, sistemul de recompensare nu contribuie doar la optimizarea utilizării resurselor, ci și la stimularea inovării în domeniul apărării.

Este cert totuși că sistemul nu este perfect. S-au semnalat atât îngrijorări la nivel etic, cât și la nivel procedural. Pe site-ul Ministerului Apărării ucrainean, se deosebesc șase astfel de posibile impedimente de natură economică:

1. Procesul funcționează pe sistemul livrării inițiale și plății ulterioare;
2. Există un termen de maxim 60 de zile de la comandă până la livrare, în timp ce ciclul de producție durează mult mai mult;
3. Din punct de vedere al recenziilor, unitățile obișnuiesc să nu le ofere, deoarece doar utilizatorul cumpărător o poate face, nu militarii care comandă produsele;
4. Există o anumită înclinație pentru produse populare, iar militarii sunt reticenți să încerce și alte produse;
5. Nu există posibilitatea ca militarii să creeze la nivel conceptual o dronă specifică situației lor, care să poată fi ulterior construită;
6. Deoarece platforma este una de piață liberă, Ministerul Apărării nu poate impune specificații și condiții asupra producătorilor, precum abandonarea folosirii componentelor chinezești în favoarea celor naționale[18].

La nivel individual, deși opinia generală este favorabilă, militarii ucraineni au identificat și probleme de altă natură: „*Problema fundamentală a motivației nu este rezolvată de către acest sistem*”, „*Punctele nu vor opri oamenii din a dezerta*”, „*Unitățile petrec prea mult timp certându-se despre cine a lovit ce, sau atacă în mod deliberat vehicule deja avariate pentru a obține mai multe puncte*”, unii afirmând chiar că „*Acest sistem este doar un rezultat al obiceiului nostru mental greșit de a obține profit din orice, chiar și din moarte*”[19].

CONCLUZII

Expunerea acestui fenomen evidențiază faptul că percepția privind transformarea într-un joc video a războiului trebuie evaluată cu prudență și în raport cu realitățile concrete ale conflictului contemporan. Digitalizarea accelerată a câmpului de luptă a introdus noi forme de organizare și motivare a personalului militar, iar sistemele bazate pe performanță pot reprezenta mai degrabă soluții pragmatice pentru gestionarea resurselor într-un conflict de lungă durată decât o transformare a actului militar într-o activitate ludică. În același timp, aceste evoluții ridică întrebări legitime privind moralitatea acțiunilor militare, impactul psihologic asupra operatorilor și respectarea normelor dreptului internațional umanitar.

Deși analogiile cu jocurile video sunt ușor de identificat la nivel conceptual, impactul real al programului ADB trebuie privit, în primul rând, din perspectiva eficienței operaționale și logistice. Programul reprezintă mai degrabă o soluție instituțională adaptată la cerințele unui conflict de uzură, caracterizat de un ritm rapid de inovare și necesitatea unei reacții logistice imediate, decât o transformare simbolică a războiului într-o activitate de natură ludică, iar la momentul de față pare un succes răsunător.

Printre cele mai bune caracteristici ale sistemului se evidențiază posibilitatea unităților de a comanda exact ceea ce au nevoie și de a primi produsul într-un timp foarte scurt, o mai bună înțelegere de către individ a intenției strategice prin prioritizarea anumitor ținte de valoare ridicată, feedback-ul primit de către Statul Major General (oferit de unitățile participante care alcătuiesc 90-95% din toate unitățile luptătoare al forțelor armate), precum și un impuls pentru moralul militarilor și al unităților.

Prin urmare, programul ADB merită analizat dincolo de simpla critică referitoare la fenomenul de transformare într-un joc video a războiului. Implementarea acestui sistem ridică, fără îndoială, o serie de preocupări legitime, precum: tendința de a cuantifica rezultatele militare în termeni numerici, care poate sugera o reducere a valorii vieții umane la indicatori de performanță; impactul psihologic asupra operatorilor implicați direct în executarea loviturilor; riscul diminuării barierelor morale în utilizarea forței.

Totuși, aceste aspecte trebuie evaluate în paralel cu avantajele practice pe care programul le oferă din punct de vedere operațional și logistic, precum și în contextul particular al unui război defensiv purtat în condiții de presiune existențială. Realitățile conflictului impun soluții rapide și adaptative, iar instrumente precum ADB pot reprezenta răspunsuri instituționale la cerințele unui mediu de securitate caracterizat de un ritm accelerat al schimbării tehnologice.

Indiferent dacă viitorul războiului va integra sau nu mecanisme similare celor din mediul digital, este cert că acesta va fi profund influențat de digitalizare, de utilizarea extensivă a datelor și de creșterea nivelului de autonomie al sistemelor militare. În acest sens, programul ADB poate fi interpretat ca un exemplu timpuriu al modului în care organizațiile militare își pot adapta structurile și procesele interne pentru a face față provocărilor generate de noile tehnologii și de transformările rapide ale mediului operațional.

BIBLIOGRAFIE

1. ADAMS Paul, ”Kill Russian soldiers, win points: Is Ukraine’s new drone scheme gamifying war?”, *BBC*, bbc.com, 18 July, 2025; https://www.bbc.com/news/articles/c80p9k1r1dlo.
2. BARKER Kim, Oleksandra Mykolyshyn, ”Ukraine Gamifies the War: 40 Points to Destroy a Tank, 12 to Kill a Soldier”, *The New York Times*, 31.10.2025; https://www.nytimes.com/2025/10/31/world/europe/ukraine-war-drone-game.html.
3. GRESSEL Gustav, *Beyond the counter-offensive: Attrition, stalemate and the future of the war in Ukraine*, Policy Brief, European Council on Foreign Relations, January 2024, 30 p.; https://ecfr.eu/wp-content/uploads/2024/01/Beyond-the-counter-offensive-Attrition-stalemate-and-the-future-of-the-war-in-Ukraine-v2.pdf.
4. KHOMENKO Ivan, ”Ukraine Launches Point-Based Rewards for Drone Operators”, *United24Media*, April 30 2025; https://united24media.com/latest-news/ukraines-launches-point-based-rewards-for-drone-operators-8002.
5. KHREBET Alexander, ” `We set a precedent`. Ukraine officially presents Unmanned Systems Forces”, *Kyiv Independent,* June 11, 2024; https://kyivindependent.com/we-set-a-precedent-ukraine-officially-presents-unmanned-systems-forces/
6. MIROSHNYCHENKO Bohdan, Volynskyi Illia, ”Less corruption, more competition: how Ukraine is building a digital arms procurement system now being adopted by NATO”, *Ukrainska Pravda*, May 1, 2026; https://pravda.com.ua/eng/articles/2026/05/01/8032647/
7. MOLLOY Oleksandra, *Drones in Modern Warfare: Lessons Learnt from the War in Ukraine*, Australian Army Research Centre, Australian Army Occasional Paper, no. 29, 2024, 106 p.
8. MURPHY Joe, ”Gamifying Ukraine’s army of drones: strategic or moral(e) destruction?”, *International Politics,* on-line, 1 March, 2026; https://link.springer.com/article/10.1057/s41311-026-00753-w.
9. ROMANIUK Roman, ”They Set Targets Deep Inside Russia on Fire”, *Ukrainska Pravda*, March 17, 2025; https://www.pravda.com.ua/eng/articles/2025/03/17/7503165/;
10. ZELENSKIY Volodymyr, *Postare pe Telegram*, 5 ianuarie 2026; https://t.me/V_Zelenskiy_official/17571.
11. *** Biroul de presă al Ministerului Apărării ucrainean, *Nou record: în decembrie, Forțele de Apărare au eliminat 33,000 de ocupanți folosind drone*, 2026; https://thedigital.gov.ua/news/army/novyy-rekord-za-hruden-syly-oborony-likviduvaly-33-000-okupantiv-za-dopomohoiu-droniv.
12. *** Ministerul Apărării al Ucrainei, *”Army of Drones Bonus” program delivers results: nearly 820,000 russian targets hit in 2025, says Mykhailo Fedorov*, 2026; https://mod.gov.ua/en/news/army-of-drones-bonus-program-delivers-results-nearly-820-000-russian-targets-hit-in-2025-says-mykhailo-fedorov.
13. *** Reuters, ”Russian troops get bonuses for destroying Western tanks”, June 16, 2013; https://www.reuters.com/world/europe/russian-troops-get-bonuses-destroying-western-tanks-2023-06-16/

[1] Oleksandra Molloy, *Drones in Modern Warfare: Lessons Learnt from the War in Ukraine,* Australian Army Research Centre, Australian Army Occasional Paper, no.29, 2024, p. 9.

[2] Gustav Gressel, *Beyond the counter-offensive: Attrition, stalemate and the future of the war in Ukraine,* Policy Brief, European Council on Foreign Relations, 18 ianuarie 2024; https://ecfr.eu/wp-content/uploads/2024/01/Beyond-the-counter-offensive-Attrition-stalemate-and-the-future-of-the-war-in-Ukraine-v2.pdf.

[3] Alexander Khrebet, " `We set a precedent`. Ukraine officially presents Unmanned Systems Forces", *Kyiv Independent,* 11 iunie 2024, https://kyivindependent.com/we-set-a-precedent-ukraine-officially-presents-unmanned-systems-forces/

[4] Ivan Khomenko, "Ukraine Launches Point-Based Rewards for Drone Operators", *United24Media,* 30 aprilie 2025; https://united24media.com/latest-news/ukraines-launches-point-based-rewards-for-drone-operators-8002.

[5] Ministerul Apărării al Ucrainei, "Army of Drones Bonus" program delivers results: nearly 820,000 russian targets hit in 2025, says Mykhailo Fedorov, 26 ianuarie 2026; https://mod.gov.ua/en/news/army-of-drones-bonus-program-delivers-results-nearly-820-000-russian-targets-hit-in-2025-says-mykhailo-fedorov.

[6] Roman Romaniuk, "They set Targets Deep Inside Russia on Fire", *Ukrainska Pravda,* 17 martie 2025; https://www.pravda.com.ua/eng/articles/2025/03/17/7503165/

[7] Kim Barker, Oleksandra Mykolyshyn, "Ukraine Gamifies the War: 40 Points to Destroy a Tank, 12 to Kill a Soldier", *The New York Times,* 31 octombrie 2025; https://www.nytimes.com/2025/10/31/world/europe/ukraine-war-drone-game.html.

[8] *Ibidem.*

[9] Ministerul Apărării al Ucrainei, "Army of Drones Bonus" program delivers results: nearly 820,000 russian targets hit in 2025, says Mykhailo Fedorov, 26 ianuarie 2026; https://mod.gov.ua/en/news/army-of-drones-bonus-program-delivers-results-nearly-820-000-russian-targets-hit-in-2025-says-mykhailo-fedorov.

[10] Volodymyr Zelenskiy, Postare pe Telegram, 5 ianuarie 2026; https://t.me/V_Zelenskiy_official/17571.

[11] Biroul de presă al Ministerului, „Nou record: în decembrie, Forțele de Apărare au eliminat 33,000 de ocupanți folosind drone", 5 ianuarie 2026; https://thedigital.gov.ua/news/army/novyy-rekord-za-hruden-syly-oborony-likviduvaly-33-000-okupantiv-za-dopomohoiu-droniv.

[12] Joe Murphy, "Gamifying Ukraine's army of drones: strategic or moral(e) destruction?", *International Politics,* on-line, 1 martie 2026, p. 6.

[13] Reuters, "Russian troops get bonuses for destroying Western tanks", 16 iunie 2013; https://www.reuters.com/world/europe/russian-troops-get-bonuses-destroying-western-tanks-2023-06-16/.

[14] Joe Murphy, *Op.cit.,* p.9.

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

[16] Bogdan Miroshnychenko, Illia Volynskyi, "Less corruption, more competition: how Ukraine is building a digital arms procurement system now being adopted by NATO", *Ukrainska Pravda,* May 1, 2026; https://pravda.com.ua/eng/articles/2026/05/01/8032647/

[17] *Ibidem.*

[18] *Ibidem.*

[19] Paul Adams, "Kill Russian soldiers, win points: Is Ukraine's new drone scheme gamifying war?", *BBC,* 18 iulie 2025; https://www.bbc.com/news/articles/c80p9k1r1dlo.

CRIMINALITATEA INFORMATICĂ ÎN UE: EVOLUȚIA AMENINȚĂRILOR CIBERNETICE ÎN CONTEXTUL CONFLICTULUI F.RUSĂ-UCRAINA

Cosmin CÎRLAN*

Abstract

The last decade has been marked by innovation, as the dependence on technology rises. The cyberspace has become an essential component of modern life by providing ways to communicate, access information and work. It has also become an extension for modern conflicts, the war in Ukraine being one of the most relevant examples of how important the cyber tools are. Through cyberattacks, hacker groups can affect critical infrastructure, institutions, economy, politics and civilians. The situation of the war and the actions carried by Russian cyber groups are influencing each other, affecting not only the countries that are directly involved, but also having global repercussions. The conflict has accelerated the development of cyber threats, forcing bigger investments in cybersecurity. Since the war gives a significant boost to the race between cyber threats and cybersecurity, creating instability in the cyberspace, this volatile, borderless environment gains much more importance.

Keywords*: cyberspace; cybersecurity; cyberattack; hackers; APT28; APT29; Sandworm; Russian hacker groups; Russia; Ukraine; war; conflict; Unified Kill Chain.*

INTRODUCERE

Creșterea accelerată a datelor din spațiul digital, a numărului și tipurilor de dispozitive conectate la Internet, contribuie la evoluția experienței și diversificarea interacțiunilor din mediul online. Un mediu atât de vast, aflat în continuă expansiune, generează provocări pentru cei care asigură securitatea cibernetică, amenințările devenind tot mai complexe și mai greu de detectat. În cadrul acestui articol ne propunem să urmărim dinamica spațiului cibernetic în ultimul deceniu, cu accentul pus pe influența pe care o are conflictul dintre F.Rusă și Ucraina asupra evoluției amenințărilor cibernetice. Pentru înțelegerea în profunzime a subiectului, atenția se va îndrepta asupra activității cibernetice a celor mai importante *trei grupări* de hackeri afiliate Moscovei: APT28 (Fancy Bear), APT29 (Cozy Bear) și APT44 (Sandworm).

Când vorbim despre spațiul cibernetic, punem accentul pe dinamica acestui mediu.

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

Fiecare nouă inovație contribuie la procesul de evoluție, schimbare a parametrilor și a regulilor care guvernează acest domeniu. Dacă la început spațiul cibernetic se deosebea de cel fizic, pe măsură ce tehnologia a evoluat, statele și-au impus autoritatea prin manipularea ecosistemelor de internet, stabilind, mai mult sau mai puțin, granițe virtuale în acest mediu[1].

Atacurile cibernetice reprezintă mijlocul prin care sunt îndeplinite anumite scopuri într-un război cibernetic, precum dezinformarea, propaganda, spionajul și afectarea infrastructurii critice a unui stat[2]. Operațiunile desfășurate în mediul virtual sunt organizate de structuri guvernamentale, actori non-statali, grupări teroriste și alte entități/„hackerii" sunt persoane care posedă cunoștințe informatice avansate. Deseori acțiunile acestor grupări au implicații politice, militare, economice, fiind finanțate și protejate de actori statali[3].

Securitatea cibernetică este reprezentată de totalitatea de măsuri, tehnologii și instrumente folosite pentru a proteja utilizatorii, datele acestora, sistemele informatice și rețelele de internet de agresiuni cibernetice. Cele mai multe vulnerabilități ale domeniului virtual sunt cauzate de neatenția utilizatorilor, neactualizarea sistemelor de operare folosite pe stații, introducerea stick-urilor infectate în dispozitive, lipsa programelor antivirus și accesarea site-urilor sau mail-urilor suspicioase.

ABORDAREA F.RUSE ASUPRA DOMENIULUI CIBERNETIC

F.Rusă pune accentul pe importanța calității de lider mondial în diverse domenii, pe influența și rolul în spațiul internațional, precum și pe competiția continuă în care principalul adversar este Occidentul. Există o contradicție între principiile pe care Rusia le promovează și acțiunile cibernetice pe care grupările ruse le întreprind. În „Strategia de securitate națională a Federației Ruse" se susține că amenințările cibernetice care pun în pericol suveranitatea statelor sau intervin în afacerile interne sunt în creștere, cu un impact puternic asupra păcii și siguranței internaționale, principii promovate și de către liderul rus, Vladimir Putin[4]. Totuși, o mare parte a operațiunilor cibernetice ofensive la nivel internațional sunt efectuate de către grupări finanțate de guvernul rus și coordonate de serviciile de informații ruse.

Grupările cibernetice ruse

Operațiunile cibernetice desfășurate vizează structuri critice, companii private, guverne sau indivizi. Entități precum Cozy Bear, Fancy Bear, Killnet, NoName057(16), Play, Sandworm, Turla, Anonymous Sudan, Conti sau Wizard Spider sunt recunoscute pentru utilizarea de tehnici avansate, precum: DDoS[5] (atacuri de tipul refuz-serviciu "Distributed Denial-of-Service"), phishing[6], spearphishing[7], atacuri ce utilizează malware[8], ransomware[9], spyware[10] și atacuri ce vizează exploatarea vulnerabilităților. Țintele sunt adesea reprezentate de site-uri guvernamentale, rețele de instituții publice, organizații și companii multinaționale, sisteme informatice ale forțelor armate, dar și diferite personalități. Unul dintre scopurile bine cunoscute ale grupărilor ruse este influențarea mediului politic din alte state.

APT28 (Fancy Bear)

Fancy Bear este un grup de hackeri cu originea în Rusia, asociat cu serviciul de informații al armatei (GRU), activ din anul 2004[11], care întreprinde acțiuni de spionaj și sabotaj. Operațiunile desfășurate de APT28 vizează domenii precum mass-media, sectorul guvernamental, apărare, energie și altele, utilizând phishing și colectare de date prin autentificarea pe site-uri false[12]. De asemenea, gruparea își bazează o parte din operațiuni pe exploatarea vulnerabilităților de tip zero-day. Termenul "zero-day" se referă la numărul (0) de zile în care victima este conștientă de o vulnerabilitate a sistemului[13]. Cu timpul, gruparea și-a extins aria de acțiuni întreprinse pentru guvernul rus, de la spionaj și sabotaj până la utilizarea mass-media și social-media pentru influențarea maselor prin dezinformare și propagandă (răspândirea de știri false, acuzații false), tehnici de manipulare a opiniei publice și influențarea politicilor interne sau externe ale unui stat. APT28 este,

spre deosebire de alte grupări de hackeri, slab interesată de posibilitatea deconspirării în cadrul atacurilor întreprinse[14].

Gruparea a derulat o serie de operațiuni notabile. În 2015, APT28 a lansat un atac printr-un virus de tip „cal troian" asupra Parlamentului german. Daunele provocate au constat în 16 GB de date trimise mai multor adrese suspecte, cu locații diferite pe glob (există posibilitatea ca numeroase mail-uri din perioada 2012-2015 să fi fost furate)[15]. Momentele preferate pentru lansarea de atacuri sunt reprezentate de perioadele electorale, precum cele din SUA și Franța, în anul 2016, respectiv 2017. În acel context au fost demarate de către grupare operațiuni ofensive constând în accesarea neautorizată de fișiere, documente, date personale, informații clasificate, pentru exploatare prin publicare. De asemenea, s-a recurs și la metoda conturilor false[16], prin care erau reprezentate diferite oficialități, fiind construite narative care să susțină interesele Moscovei[17].

APT29 (Cozy Bear)

Spre deosebire de Fancy Bear, APT29, grupare asociată serviciului extern de informații al Federației Ruse (SVR), are o abordare mai discretă. Astfel, membrii Cozy Bear reușesc să rămână conectați în cadrul unei rețele, cu acces constant la date, fără a trezi suspiciuni. Tehnicile utilizate includ: manipularea datelor de autentificare a conturilor, a privilegiilor și permisiunilor în sistem, achiziționarea de domenii web prin intermediul cărora se pot transmite sau stoca date obținute, încercarea repetată a posibile parole la multiple conturi, redirecționarea mail-urilor, spearphishing și phishing[18].

Aceștia folosesc malware personalizat pentru garantarea accesului, împreună cu platforme utilizate de publicul larg, ceea ce le oferă deschidere într-un mediu în care totul este interconectat. Totodată, perseverența atacurilor lansate de grupare este dată de faptul că nu se limitează la o singură secvență care să le ofere acces în sistem, ci încarcă componente care pot funcționa și garanta acces independent[19], reprezentând o adevărată provocare pentru companiile de securitate cibernetică.

Gruparea a atacat Comitetul Național Democrat în anul 2016, alături de Fancy Bear, și a obținut acces la mai multe informații, unele fiind folosite pentru favorizarea unui candidat în campania sa electorală[20]. Un alt eveniment major este reprezentat de atacul asupra unei companii americane, SolarWinds, furnizor de software. În urma atacului, un pachet de actualizare infectat a fost introdus în codul sursă al programului descărcat de peste 18.000 clienți. Pachetul a trecut de verificările de securitate, iar CozyBear au obținut acces la nenumărate rețele[21].

SANDWORM

APT44 este o grupare de hackeri ruși afiliată GRU, sponsorizată de Federația Rusă pentru a desfășura atacuri cibernetice, cu precădere împotriva țărilor din fostul bloc sovietic[22]. Gruparea desfășoară preponderent operațiuni de sabotaj, atacând în repetate rânduri componente ale rețelei electrice, în special în Ucraina. Astfel, în 2015, atacurile asupra unor regiuni (inclusiv Kiev) au afectat sute de mii de cetățeni ucraineni, provocând o pană de curent ce a durat până la 6 ore[23]. Instrumentul folosit în cadrul atacului este un malware din familia BlackEnergy, care utilizează internetul pentru a livra atacuri de tipul DDoS[24]. În cadrul atacului a fost folosit și malware-ul KillDisk (capabil să șteargă fișiere esențiale) prin care atacatorii au reușit să aducă sistemele informatice în stare de inoperabilitate[25].

Un atac asemănător celui din 2015 a avut loc anul următor cauzând întreruperea curentului electric pe o porțiune egală cu o cincime din dimensiunea capitalei, timp de o oră. În 2017 au fost publicate rapoarte de către două firme de securitate cibernetică, ESET și Dragos, prima denumind malware-ul folosit drept Industroyer, iar a doua drept Crashoverride[26].

Considerat cel mai distructiv atac din istoria spațiului cibernetic, cu pagube estimate la 10 mld. de dolari, NotPetya a fost un malware lansat de Sandworm în 2017, prin care Rusia urmărea să destabilizeze Ucraina prin afectarea sistemelor informatice a zeci de companii. Ecranele calculatoarelor infectate afișau un mesaj care crea impresia de ransomware, cerându-se victimei suma de 300$ (în bitcoin) în schimbul obținerii unei chei de decriptare a datelor, însă NotPetya a

fost construit pentru a șterge datele. Infrastructura critică a Ucrainei a fost grav afectată, însă nu a fost singura care a avut de suferit, companii multinaționale ca FedEx și Merck pierzând sute de milioane de dolari în urma contactului cu virusul[27].

Aplicabilitatea modelului *Unified Kill Chain* (UKC)

Pentru a putea înțelege modul de operare al atacatorilor cibernetici, este necesară existența unei reprezentări schematice a amenințării, un model în baza căruia să poată fi identificat atacatorul, etapa în care se află atacul și tehnicile folosite. Paul Pols, expert în securitate cibernetică, a dezvoltat și publicat în anul 2017 un model exhaustiv, intitulat The Unified Kill Chain (UKC). Autorul a utilizat detalii privind gruparea Fancy Bear pentru a putea crea modelul UKC, care conține mai multe etape.

1. ***Cercetarea țintei:*** În timp ce APT28 folosește, în general, informațiile din surse deschise pentru a putea lansa atacuri *spearphishing*[28], CozyBear preferă trimiterea în masă de email-uri folosind metoda phishing-ului, după care este analizat statutul țintei. Gruparea Sandworm atacă cu precădere sisteme industriale, etapa de cercetare constând în analiza detaliată a codurilor sursă ale programelor folosite pentru sistemele informatice industriale.
2. ***Accesul inițial:*** Cele trei grupări se folosesc de phishing, spearphishing și exploatarea vulnerabilităților de tip 0-day, APT29 deosebindu-se prin atacarea de producători software, ca în cazul Solarwinds[29].
3. ***Evitarea mecanismelor de apărare****:* Fancy Bear nu pune accentul pe discreție când vine vorba de evitarea sistemelor de apărare[30]. La polul opus, APT29 pune accentul pe mascarea activităților malițioase și păstrarea anonimității[31]. Sandworm utilizează diferite aplicații pentru evitarea mecanismelor de detecție și apărare, prin care se șterg date sau se obțin privilegii cu acest scop[32].
4. Pentru ***comandă și control*****,** APT28 utilizează diferite metode de stabilire a conexiunii cu stația infectată, în primă fază încercându-se crearea unei legături prin Internet[33]. Cozy Bear în schimb își pregătește viitoarele conexiuni chiar cu un an înainte de efectuarea atacului[34]. Sandworm folosește instrumente specifice pentru stabilirea prin Gmail a unui server și securizarea conexiunii cu acesta[35].
5. ***Etapa de descoperire***: În această etapă, atacatorul adună informații despre un sistem și rețeaua din care acesta face parte. APT29 și APT28 utilizează malware care trimite date despre sistemul infectat, iar gruparea folosește acele date pentru a stabili dacă victima este de interes[36]. Sandworm a obținut, în general, cunoștințele necesare operațiunilor desfășurate prin studierea programelor industriale open-source vechi, dar încă utilizate de multe companii.
6. ***În etapa de execuție*** APT29 încearcă inițial execuția prin inginerie socială, utilizatorul fiind păcălit de fișierele inserate în mail-uri. De asemenea, gruparea se mai folosește și de vulnerabilități sau capabilități de sistem. După prima execuție a malware-ului, Cozy Bear îl folosește pentru a rula alte componente adiționale. Sandworm utilizează, de asemenea, ingineria socială, faza incipientă a atacurilor asupra centralelor de energie constând în trimiterea de email-uri cu „fișiere Microsoft". Astfel, fișierul descărcat este, în fapt, un soft malițios.
7. ***Etapa mișcării laterale*** (*lateral movement)* presupune utilizarea anumitor tehnici de către atacator pentru a asigura controlul, transferul și comunicarea cu alte sisteme. Principala metodă utilizată de APT28, *pass-the-hash*, se referă la folosirea amprentei digitale a utilizatorului pentru accesarea altor domenii. Un alt mod de transfer poate fi facilitat de Xagent, malware-ul putând fi transmis prin USB[37]. Cozy Bear folosesc instrumente precum *Mimikatz, SMB beacon*, propriul malware dezvoltat, „*FatDuke*", având capabilități de deplasare laterală într-un sistem local. Sandworm nu arată interes față de

posibilitatea descoperirii instrumentelor, prin intermediul acestora transportând diferite programe, inclusiv de tip *wiper*[38].

8. APT28 ***colectează datele*** din email-uri și rețele prin *keylogging* (înregistrarea caracterelor introduse de utilizator), redirecționare, capturi de ecran și copii back-up. Cozy Bear folosește aceleași metode, însă filtrează căutarea după nume, dată, extensii sau mărimea fișierelor, colectând datele sub forma unor arhive 7-Zip.
9. ***Etapa Impactului***: Atât APT28, cât și APT29 au executat atacuri de tip DDoS și au folosit metode de ștergere a datelor, aducând sistemele în stare de inoperabilitate[39]. Sandworm a folosit KillDisk, un program care are capacitatea de a șterge date, metodă utilizată des de grupare, deoarece scopul principal până în 2022 a fost provocarea de daune industriei energetice. Un alt exemplu care include ștergerea datelor este NotPetya, virusul eliberat de grupare în Ucraina având un impact devastator la nivel global.
10. ***Etapa obiectivelor***: În timp ce APT29 se concentrează pe furtul de informații delicate, APT28 are în palmares și activități de sabotaj[40]. Cele mai multe operațiuni semnificative desfășurate de Sandworm au avut ca scop sabotajul, prin distrugerea capabilităților de operare a centralelor energetice sau eliberarea unui *wiper* la nivel global care să dea impresia de ransomware[41]. Trebuie menționat faptul că un scop comun îndeplinit de aceste grupări este cel al expunerii informațiilor confidențiale obținute.

DIMENSIUNEA CIBERNETICĂ A CONFLICTULUI

Deși inițial părea că nu există un factor cibernetic semnificativ în organizarea și desfășurarea atacului din 24 februarie 2022, pe măsură ce conflictul a progresat au apărut informații cu privire la implicarea grupărilor cibernetice, atât anterior invaziei din 2022 (P1), cât și de-a lungul conflictului (P2). Ofensiva cibernetică servește scopului F.Ruse de a controla atât spațiul cibernetic intern, cât și de a-l submina pe cel al celorlalte state. Statul rus își dezvoltă arsenalul informatic de cel puțin 15 ani, folosindu-l împotriva actorilor pe care îi consideră inamici. Cel mai bun exemplu de utilizare a operațiunilor cibernetice într-un mod coercitiv asupra unei națiuni, fără utilizarea forței armate, este reprezentat de campaniile desfășurate împotriva Ucrainei în perioada 2014 – 2022, menite să sprijine înlocuirea guvernului pro-occidental cu unul pro-rus[42].

APT44 (Sandworm): Abilitățile dezvoltate de hackerii grupului sunt valorificate în timpul războiului, Sandworm atacând cu o lună înainte de invazie mai multe site-uri web ale guvernului ucrainean. Între 13 și 15 ianuarie 2022, un set de componente malware, numit *WhisperGate*, a fost folosit împotriva mai multor site-uri web aparținând guvernului ucrainean. Pe ecranul unităților infectate apărea un mesaj care, asemeni cazului NotPetya, crea impresia de ransomware, fiind cerută o suma de 10.000$ în bitcoin pentru recuperare. În tot acest timp, datele de pe hard-ul sistemului sunt șterse printr-un *datawiper*.

```
Your hard drive has been corrupted.
In case you want to recover all hard drives
of your organization,
You should pay us  $10k via bitcoin wallet
1AVNM68gj6PGPFcJuftKATa4WLnzg8fpfv and send message via
tox ID 8BEDC411012A33BA34F49130D0F186993C6A32DAD8976F6A5D82C1ED23'
054C057ECED5496F65
with your organization name.
We will contact you to give further instructions.
```

Fig. 1: *Mesaj WhisperGate ce vrea să lase falsa impresie de ransomware, 2022.*
(Sursa : Crowdstrike Blog, Technical Analysis of the WhisperGate Malicious Bootloader)

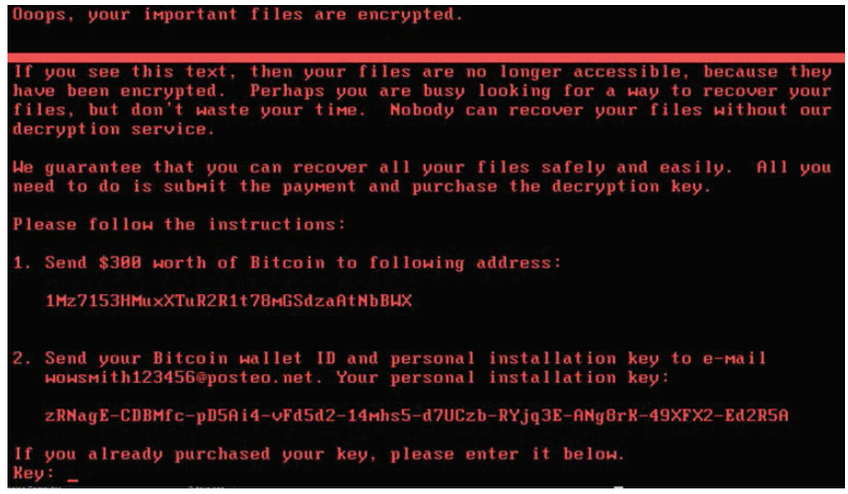

Fig. 2: *Mesaj NotPetya ce vrea să lase falsa impresie de ransomware, 2017.*
(Sursa: Crowdstrike Blog, NotPetya Technical Analysis -
A Triple Threat: File Encryption, MFT Encryption, Credential Theft)

Deși Crowdstrike se abține de la atribuirea WhisperGate vreunui actor cibernetic rus, declarând că cercetarea asupra problematicii continuă, alte surse indică Sandworm ca gruparea responsabilă de acest atac, mijloacele folosite fiind asemănătoare. Printre ținte se află și Ministerul Afacerilor Externe ucrainean și organizații IT, entitatea identificată fiind Centrul de Tehnologii Speciale al GRU (APT44)[43]. Alte acțiuni relevante sunt reprezentate de atacurile de tip DDoS, din perioada 15-16 februarie 2022, asupra sistemelor de apărare și bancare ucrainene; scopul atacurilor a fost acela de a slăbi încrederea populației în capacitatea autorităților de a răspunde amenințărilor provenite din spațiul cibernetic. Acțiunilor întreprinse le sunt atribuiți doi actori cibernetici, cel responsabil pentru atacurile DDoS fiind Sandworm[44].

Relevant este și atacul orchestrat de GRU în zilele de 23-24 februarie 2022. Operațiunea a constat în lansarea mai multor atacuri (majoritatea executate de Sandworm) de tip DDoS asupra Parlamentului unicameral al Ucrainei, Ministerului Afacerilor Externe și Serviciului de Securitate (SBU), ale căror site-uri web au fost scoase temporar din funcțiune. Gruparea a folosit malware-ul *FoxBlade*, denumit și *Hermetic Wiper*, pentru a distruge peste 300 de sisteme informatice din mai multe organizații guvernamentale, din industria energetică, IT, industria agriculturii și organizații financiare din Ucraina, Lituania și Letonia. În timp ce NotPetya era programat să infecteze și distrugă orice sistem informatic la care avea acces, FoxBlade avea ținte definite. O analiză tehnică asupra atacului relevă faptul că a fost plănuit cu câteva săptămâni înaintea eliberării FoxBlade, ceea ce indică alinierea cu invazia militară[45]. Conform companiei ESET, atacul din 23 februarie, ce a precedat invazia cu câteva ore, a conținut 3 componente: Hermetic Wiper – corupe datele sistemului, făcându-l imposibil de folosit; Hermetic Wizard – folosește diferite mijloace pentru a răspândi malware-ul într-un sistem; și Hermetic Ransom – ransomware folosit pentru a distrage atenția de la wiper[46].

APT29 (Cozy Bear): Din momentul contra-ofensivei ucrainene, operațiunile de tip phishing ale Cozy Bear s-au intensificat, fiind țintite în special ambasade din Kiev. Luând în considerare momentul și țintele alese, se poate concluziona că operațiunile întreprinse au rolul de a sprijini SVR în obținerea de informații. Pe lângă creșterea frecvenței acțiunilor, s-a putut observa și o evoluție a capabilităților cibernetice. Cozy Bear a îmbunătățit instrumentele și metodele folosite în trecut, punând accent în continuare pe discreție. Relevante sunt două operațiuni desfășurate în mai 2023, respectiv octombrie 2024, fiind folosite ROOTSAW pentru phishing sau deghizarea în ”servicii web Amazon”, cu scopul de obținere a datelor de acces și instalarea de soft, precum *backdoors*, ce permite controlul discret asupra sistemului[47].

APT28 (Fancy Bear): În contextul războiului, APT28 și-a extins arealul de ținte, monitorizând companii și entități implicate în livrarea de ajutor militar. Sectoarele țintite au fost cel al industriei de apărare, managementul traficului aerian, servicii IT, sectorul maritim și industria transportului[48]. Printre țările-țintă s-au aflat Bulgaria, Cehia, Franța, Germania, Grecia, Italia, R.Moldova, Țările de Jos, Polonia, România, Slovacia, Ucraina și Statele Unite. Metodele utilizate pentru a fi realizată intruziunea inițială în sistemele victimelor au inclus: spearphishing și phishing, atacuri de tip brute force, vulnerabilități, exploatarea infrastructurii web și a VPN-urilor. Atacatorii creșteau credibilitatea prin asocierea unor documente oficiale cu entități cunoscute și potrivite pentru subiectul abordat (ex.: atenționări cu privire la conturile bancare ale utilizatorilor și, uneori, conținut pornografic).

Campania aceasta a fost catalogată ca spearphishing deoarece victimele primeau mesaje personalizate, în limba lor nativă, de la conturi cunoscute (dar compromise de Fancy Bear). Un alt mijloc folosit de grupare pentru obținerea de credențiale sau coruperea sistemelor informatice este reprezentat de exploatarea vulnerabilităților. Una dintre acestea se afla în structura Microsoft Outlook, atacatorii creând fișiere care arătau ca invitații la programări calendaristice. În cazul în care este infectat un sistem informatic care nu poate furniza date de interes pentru grupare, operațiunea se sistează. Unul dintre scopurile principale ale Fancy Bear este monitorizarea ajutorului militar și economic primit de Ucraina, aceștia urmărind să obțină acces la informații privind transporturile de ajutoare, date despre expeditor, destinatar, conținutul pachetului, numerele de identificare ale mijlocului de transport, punctul de ridicare și ruta de călătorie. De asemenea, gruparea a atacat camere care transmiteau video în timp real, localizate în Ucraina, încă de la începutul lunii martie 2022, cu scopul de a supraveghea îndeaproape structurile militare și infrastructura critică a statului ucrainean[49].

Evoluția Fancy Bear: Evoluția tehnologică generală a permis APT28 să-și eficientizeze procesul de căutare și cercetare prin automatizare. De asemenea, tipurile de documente prin care se efectuează recunoașterea s-au schimbat, în loc de documente Microsoft atașate în email-uri phishing ce aveau ca scop atragerea victimelor, fiind folosite adițional și alte metode de cercetare, precum exploatarea platformei de mesagerie Signal, crearea de profiluri false și utilizarea de inginerie socială, phishing, user-agent filtering și altele. În P1, APT28 activa într-un areal mai extins, având ca ținte țările occidentale, în special SUA, partide politice, presă, în timp ce în P2 atenția se concentrează pe personalul militar ucrainean, ambasadele occidentale din Ucraina, administrații locale și furnizorii de echipamente militare și ajutor pentru război. Deși în P1 se urmărea asigurarea minimă a discreției, în P2 lucrurile se schimbă, Fancy Bear folosind noi metode pentru a evita mecanismele de apărare ale sistemelor informatice. Gruparea filtrează țintele după capabilitățile acestora de apărare sau sistemele de operare folosite, implementează tehnici de auto-ștergere și folosește browserul TOR. În majoritatea etapelor, instrumentele precizate anterior sunt înlocuite total sau parțial în P2 de utilizarea facilităților Windows pentru a îngreuna detectarea atacurilor sau a sursei. APT28 vizează planuri logistice, militare, documente strategice, drone, ce ar putea ajuta ofensiva rusă. A fost observată reducerea acțiunilor de tip sabotaj și focusarea pe spionaj militar.

Evoluția Cozy Bear: În P2 se face trecerea de la profilarea prin OSINT la utilizarea instrumentelor din arsenalul propriu, automatizându-se și procesul de colectare a datelor, fapt ce permite grupării să analizeze documente cu dimensiuni exponențial crescute. APT29 livra produsele malware preponderent prin spearphishing, însă a adăugat noi metode precum folosirea ROOTSAW, platformele alternative Signal, WhatsApp și Telegram și livrarea fileless prin exploatarea unei vulnerabilități din Outlook. Asemeni Fancy Bear, Cozy Bear a adaptat temele folosite la conflict, ingineria socială fiind tehnica nelipsită din cadrul

arsenalului grupării. În P2 modul de operare se schimbă, persistența fiind asigurată prin backdoors, OpenSSH și modificarea fișierelor legitime. APT29 a folosit diverse metode de evitare a detecției, precum utilizarea de conturi Twitter pentru livrarea de componente malware sub formă de cod sau folosirea steganografiei, cu mesaje criptate ascunse. Pentru pivotare, se folosea metoda SSH sau instrumentul FatDuke, acestea fiind înlocuite în prezent de abuzul de credențiale sau tuneluri prin TOR. Războiul din Ucraina și-a lăsat amprenta semnificativ în cadrul etapei de colectare, gruparea trecând la țintirea documentelor de interes din domeniul militar, mailuri diplomatice sau documente clasificate.

Evoluția Sandworm: Ținând cont de specificul atacurilor, Sandworm realizează cercetarea asupra codurilor sursă ale programelor folosite în sisteme industriale în ambele perioade, proces automatizat numai în P2. Pentru accesul inițial, APT44 trece de la metodele clasice, printre care și ingineria socială, la phishing cu tematici militare, politice, exploatarea infrastructurilor compromise și livrarea de malware prin DarkTortilla, CaddyWiper sau ArguePatch. Din punct de vedere al resurselor, Sandworm continuă utilizarea malware-ului dezvoltat intern (Industroyer, KillDisk), însă aduce multe îmbunătățiri (Industroyer2) și folosește TOR. Pentru livrare, APT44 trece de la emailuri phishing la folosirea vulnerabilităților OneNote și falsificări de actualizări software. Totodată, în P2 își modifică parțial strategia, organizând atacuri personalizate pentru evitarea detecției. În etapa de comandă și control, APT44 trece de la folosirea Gcat și GOSSIPFLOW (primul pentru stabilirea prin Gmail a unui server, iar al doilea pentru stabilirea conexiunii cu acesta) la servere TOR. În contextul conflictului, gruparea începe să activeze mai mult în sfera spionajului, colectând informații privind planuri militare, drone, rețele energetice, date despre interfața SCADA și documente confidențiale cu informații tehnice. Spre deosebire de APT28 și APT29, impactul acțiunilor Sandworm s-a diminuat drastic. Gruparea și-a aliniat obiectivele cu cele ale F.Ruse, executând, în locul atacurilor distructive, operațiuni de spionaj și eventual de sabotaj.

CONCLUZII

Argumentația acestui articol a pornit de la ipoteza conform căreia capabilitățile, modul de operare și direcțiile de acțiune ale actorilor cibernetici ruși sunt influențate de război, care intensifică ritmul de evoluție a instrumentelor și metodelor folosite, dezechilibrând și mai mult peisajul cibernetic, caracterizat oricum de o volatilitate crescută.

Au putut fi observate modificări prin analizarea schimbărilor în cadrul etapelor UKC, fiecare grupare având un parcurs similar, toate datele indicând îndreptarea către un scop comun: sprijinirea ofensivei ruse împotriva Ucrainei. Un aspect relevant, ce reiese din analiza comparativă, este reprezentat de intensificarea eforturilor grupărilor cibernetice de a acționa discret, fiind aduse îmbunătățiri semnificative asupra metodelor și instrumentelor utilizate.

Totodată, se poate observa cum APT28, APT29 și APT44 și-au direcționat atenția către Ucraina și aliații săi, cu accentul pe operațiuni de spionaj, în detrimentul acțiunilor distructive. Contextul actual a forțat extinderea relativ bruscă a arsenalului și obiectivelor pentru fiecare actor cibernetic implicat, dezechilibrând balanța dintre atac și apărare. Astfel, conflictul ruso-ucrainean dirijează și impulsionează dezvoltarea tehnologiei, atât din perspectiva atacatorului, cât și din perspectiva companiilor care se ocupă cu asigurarea securității cibernetice, care sunt astfel nevoite să răspundă corespunzător cu amploarea fenomenului.

BIBLIOGRAFIE

1. ABLON Lillian, Andy Bogart, *Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits*, RAND Corporation, March 2017.
2. BARANOVSKYI Oleksii, *How did NotPetya cost businesses over $10 Billion in damages?*, Cyber Ranges Corp.; https://www.cyberranges.com/how-did-notpetya-cost-businesses-over-10-billion-in-damages/
3. BENDIEK Annegret, Matthias Schulze, *Attribution: A Major Challenge for EU Cyber Sanctions. An Analysis of WannaCry, Not Petya, Cloud Hopper, Bundestag Hack and the Attack on the OPCW*, SWP Research Paper, German Institute for International and Security Affairs, no.11, 2021.
4. BRATTBERG Erik, Tim Maurer, *Russian Election Interference. Europe's Counter to Fake News and Cyber Attacks*, Carnegie Endowment for International Peace, May 2018, 45 p.
5. DAVID Cristian, „Războiul cibernetic - între ordine și haos", *Infosfera*, vol. XII, nr. 4, 2020, pp. 58-69.
6. DUTTA Subhash, *Cyber Operations Associated with the Ukraine-Russia Conflict: An Open-Source Assessment*, National Maritime Foundation, New Delhi, May 10, 2022; https://www.maritimeindia.org/cyber-operations-associated-with-the-ukraine-russia-conflict-an-open-source-assessment.
7. GJESVIK Lars, Kacper Szulecki, "Interpreting cyber-energy-security events: experts, social imaginaries, and policy discourses around the 2016 Ukraine blackout", *European Security*, vol. 32, no. 1, 2023, pp. 104-124.
8. GODWIN Zealous, Nidia Guadarrama, "The Effects of Nation Sponsored Cyber Attacks on all Stakeholders", April 2024; https://www.researchgate.net/publication/379988073_The_Effect_of_Nation_Sponsored_Cyber_Attacks_on_all_Stakeholders
9. HAGIOGLU Sila Ozeren, *APT29 Explained: Cozy Bear`s Evolution, Techniques and Notorious Cyber Attacks*, Picus Labs, www.picussecurity.com., April 06, 2026; https://www.picussecurity.com/resource/blog/apt29-cozy-bear-evolution-techniques.
10. JENKINS Luke, Josh Atkins, Dan Black, *Backchannel Diplomcy: APT29`s Rapidly Evolving Diplomatic Phishing Operations*, Mandiant, Google Cloud, September 21, 2023; https://cloud.google.com/blog/topics/threat-intelligence/apt29-evolving-diplomatic-phishing.
11. KUBBA Sama, Sim Sayer, Newaz Rahman, Syed Ahmed, Andrew Lu, "Russian Cyber Capabilities and Vulnerabilities: Analyzing the Cyberoperations of the Russian Government", 2021.
12. LAM Christina, "A Slap on the Wrist: Combatting Russia's Cyber Attack on the 2016 U.S. Presidential Election", *Boston College Law Review*, vol. 59, no. 6, 2018, pp. 2167-2201.
13. LAMBACH Daniel, „The Territorialization of Cyberspace", *International Studies Review*, vol. 22, no. 3, 2019, pp. 482-506.
14. LEHMAN Gary, *Cyber-Attack Against Ukrainian Power Plants. Lessons Learned, Implementations Considerations*, Contemporary Issues in Security Management, PMT 754, March 20, 2016; https://www.garylehman.net/wp-content/uploads/2016/01/Cyber-Attack-Against-Ukrainian-Power-Grid-Implications.pdf.
15. MARTÍNEZ Jeferson, Javier M. Durán, "Software Supply Chain Attacks, a Threat to Global Cybersecurity: SolarWinds' Case Study", *International Journal of Safety and Security Engineering*, vol. 11, no. 5, October 2021, pp. 537-545.
16. NAZARIO Jose, "BlackEnergy DDoS Bot Analysis", Arbor Networks, October 2007, 11 p.; https://www.hndanesh.github.io/sandworm/BlackEnergy+DDoS+Bot+Analysis.pdf

17. OLLI Hönö, *From Moonlight Maze to Solarwinds: How Russian APT Groups Operate?*, Master Thesis, Faculty of Information Technology, University of Jyvaskyla, 2023, 131 p.
18. PARZYAN Anahit, Doctoral Student, Nanjing University, School of International Studies, 2017, „Cyberspace – A Manmade Domain for Wars", *«21st CENTURY»*, no. 1 (20), 2017, pp. 42-57.
19. POLS Paul, *Modeling Fancy Bear Cyber Attacks - Designing a Unified Kill Chain for Analyzing, Comparing and Defending Against Cyber Attacks*, Executive Master Thesis, Cyber Security Academy, Leiden University, December 7, 2017, 104 p.; https://hdl.handle.net/1887/64569.
20. RONCONE Gabby, Dan Black, John Wolfram, Tyler McLellan, Nick Simonian, Ryan Hall, Anton Prokopenkov, Dan Perez, Lexie Aytes, Alden Wahlstrom, *Unearthing APT44: Russia`s Notorious Cyber Sabotage Unit Sandworm*, Mandiant, Google Cloud, April 17, 2024; https://cloud.google.com/blog/topics/threat-intelligence/apt44-unearthing-sandworm.
21. SAM Jeffrey, *A Research Report on Advanced Persistent Threat Fancy Bear (APT28) Threat Actor*, May 2024, 19 p.
22. SENEWIRATHNA Amith Nilupul, *Evolution and Impact of Malware: A Comprehensive Analysis from the First Known Malware to Modern-Day Cyber Threats*, Sri Lanka Institute of Information Technology, August 2024, 7 p.; DOI:10.13140/RG.2.2.21647.60325.
23. STAHIE Silviu, *Russian Hackers Target Ukrainian Military and Organizations with RDP Phishing Campaign*, Bitdefender, www.bitdefender.com., 25 Octombrie 2024; https://www.bitdefender.com/en-au/blog/hotforsecurity/russian-hackers-ukrainian-rdp-phishing-aws.
24. YOUNG Norman, "The Blame Game. Attribution in the 2016 Elections", December 15, 2016, 8 p.; https://www.cs.tufts.edu/comp/116/archive/fall2016/nyoung.pdf.
25. WHITEHEAD E. David, Kevin Owens, Dennis Gammel, Jess Smith, *Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies*, Conference paper, 70th Annual Conference for Protective Relay Engineers, Texas A&M University, April 2017; https://www.ieeexplore.ieee.org/document/8090056.
26. WILLETT Marcus, "The Cyber Dimension of the Russia–Ukraine War", în *Cyber Operations and Their Responsible Use,* The Adelphi Series, vol. 64, no. 511-513, The International Institute for Strategic Studies, London, 2024, pp. 105-124.
27. *** *Threat Actor Profiles: Sandworm*, Cyble.com., March 18, 2026; https://cyble.com/threat-actor-profiles/sandworm/
28. *** *Technical Analysis of the WhisperGate Malicious Bootloader*, CrowdStrike Intelligence Team, January 19, 2022; https://www.crowdstrike.com/en-us/blog/technical-analysis-of-whispergate-malware/
29. *** US Cybersecurity & Infrastructure Security Agency, *Russian GRU Targeting Western Logistics Entities and Technology Companies*, April 17, 2026, 33 p.; https://www.cisa.gov/news-events/cybersecurity-advisories/aa25141a.
30. *** ESET Research, *IsaacWiper and HermeticWizard: New Wiper and Worm Targeting Ukraine*, March 1, 2022; https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/
31. *** *Report on Cyber Lessons Learned During the War in Ukraine*, The Regional Cyber Defence Centre, Ministry of National Defence of the Republic of Lithuania, Vilnius, 2023, 61 p.
32. *** *Strategia de securitate națională a Federației Ruse*, 2 iulie 2021.

[1] Daniel Lambach, „The Territorialization of Cyberspace", *International Studies Review*, vol. 22, no. 3, 2019, pp. 482-506.
[2] Anahit Parzyan, Doctoral Student, Nanjing University, School of International Studies, 2017, „Cyberspace – A Manmade Domain for Wars", *«21st CENTURY»*, no. 1 (20), 2017, pp. 42-57.
[3] Cristian David, „Războiul cibernetic - între ordine și haos", *Infosfera*, vol. XII , nr. 4, 2020, pp. 58-69.
[4] Strategia de securitate națională a Federației Ruse, 2021.
[5] Supraîncărcarea unui site web prin accesări multiple, care conduc la încetarea temporară a funcționării.
[6] Folosirea unui paravan oficial pentru obținerea de parole, informații.
[7] Phishing targetat, atacul fiind construit pe profilul țintei.
[8] Software rău-intenționat.
[9] Criptează datele și cere o taxă pentru decriptare.
[10] Se infiltrează subtil și execută doar transmiterea de informații către atacator.
[11] Jeffrey Sam, *A Research Report on Advanced Persistent Threat Fancy Bear (APT28) Threat Actor*, May 2024, 19 p.
[12] Amith Nilupul Senewirathna, "Evolution and Impact of Malware: A Comprehensive Analysis from the First Known Malware to Modern-Day Cyber Threats", Sri Lanka Institute of Information Technology, August 2024, 7 p.; DOI:10.13140/RG.2.2.21647.60325, accesat la 23.05.2026.
[13] Lillian Ablon, Andy Bogart, *Zero Days, Thousands of Nights : The Life and Times of Zero-Day Vulnerabilities and Their Exploits*, RAND Corporation, March 2017, p. 132.
[14] *** *Report on Cyber Lessons Learned During the War in Ukraine*, The Regional Cyber Defence Centre, Ministry of National Defence of the Republic of Lithuania, Vilnius, 2023, 61 p.
[15] Annegret Bendiek, Matthias Schulze, *Attribution: A Major Challenge for EU Cyber Sanctions. An Analysis of WannaCry, Not Petya, Cloud Hopper, Bundestag Hack and the Attack on the OPCW*, SWP Research Paper, German Institute for International and Security Affairs, no.11, 2021, p.11.
[16] Christina Lam, "A Slap on the Wrist: Combatting Russia's Cyber Attack on the 2016 U.S. Presidential Election", *Boston College Law Review*, vol. 59, no. 6, 2018, pp. 2167-2201.
[17] Erik Brattberg, Tim Maurer, *Russian Election Interference. Europe's Counter to Fake News and Cyber Attacks*, Carnegie Endowment for International Peace, May 2018, 45 p.
[18] Sama Kubba, Sim Sayer, Newaz Rahman, Syed Ahmed, Andrew Lu, "Russian Cyber Capabilities and Vulnerabilities: Analyzing the Cyberoperations of the Russian Government", 2021.
[19] Sila Ozeren Hagioglu, *APT29 Explained: Cozy Bear`s Evolution, Techniques and Notorious Cyber Attacks*, Picus Labs, www.picussecurity.com., April 06, 2026; https://www.picussecurity.com/resource/blog/apt29-cozy-bear-evolution-techniques, accesat la 08.04.2026.
[20] Norman Young, "The Blame Game. Attribution in the 2016 Elections", December 15, 2016, 8 p.; https://www.cs.tufts.edu/comp/116/archive/fall2016/nyoung.pdf., accesat la 15.03.2026.
[21] Jeferson Martínez, Javier M. Durán, "Software Supply Chain Attacks, a Threat to Global Cybersecurity: SolarWinds' Case Study", *International Journal of Safety and Security Engineering*, vol. 11, no. 5, October 2021, pp.537-545.
[22] Zealous Godwin, Nidia Guadarrama, "The Effects of Nation Sponsored Cyber Attacks on all Stakeholders", April 2024; https://www.researchgate.net/publication/379988073_The_Effect_of_Nation_Sponsored_Cyber_Attacks_on_all_Stakeholders, accesat la 21.04.2026.
[23] Gary Lehman, *Cyber-Attack Against Ukrainian Power Plants*. *Lessons Learned, Implementations Considerations*, Contemporary Issues in Security Management, PMT 754, March 20, 2016; https://www.garylehman.net/wp-content/uploads/2016/01/Cyber-Attack-Against-Ukrainian-Power-Grid-Implications.pdf., accesat la 27.04.2026.
[24] Jose Nazario, "BlackEnergy DDoS Bot Analysis", Arbor Networks, October 2007, 11 p.; https://www.hndanesh.github.io/sandworm/BlackEnergy+DDoS+Bot+Analysis.pdf, accesat la 15.03.2026.
[25] David E. Whitehead, Kevin Owens, Dennis Gammel, Jess Smith, "Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies", Conference paper, 70th Annual Conference for Protective Relay Engineers, Texas A&M University, April 2017; https://www.ieeexplore.ieee.org/document/8090056, accesat la 03.04.2026.
[26] Lars Gjesvik, Kacper Szulecki, "Interpreting cyber-energy-security events: experts, social imaginaries, and policy discourses around the 2016 Ukraine blackout", *European Security*, vol. 32, no. 1, 2023, pp. 104-124.
[27] Oleksii Baranovskyi, *How did NotPetya cost businesses over $10 Billion in damages?*, Cyber Ranges Corp.; https://www.cyberranges.com/how-did-notpetya-cost-businesses-over-10-billion-in-damages/, accesat la 29.03.2026.
[28] Paul Pols, *Modeling Fancy Bear Cyber Attacks - Designing a Unified Kill Chain for Analyzing, Comparing and Defending Against Cyber Attacks*, Executive Master Thesis, Cyber Security Academy, Leiden University, December 7, 2017, 104 p.; https://hdl.handle.net/1887/64569, accesat la 25.04.2016.
[29] Hönö Olli, *From Moonlight Maze to Solarwinds: How Russian APT Groups Operate?*, Master Thesis, Faculty of Information Technology, University of Jyvaskyla, 2023, 131 p.
[30] Paul Pols, *Op.cit.*
[31] Hönö Olli, *Op.cit.*
[32] *** *Threat Actor Profiles: Sandworm*, Cyble.com., March 18, 2026.; https://cyble.com/threat-actor-profiles/sandworm/,

accesat la 01.05.2026.

[33] Paul Pols, *Op.cit.*

[34] Hönö Olli, *Op.cit.*

[35] *** *Threat Actor Profiles: Sandworm*, Cyble.com.,. *Op.cit.*

[36] Hönö Olli, *Op.cit.*; a se vedea și Paul Pols, *Op.cit.*

[37] Ibidem.

[38] Gabby Roncone, Dan Black, John Wolfram, Tyler McLellan, Nick Simonian, Ryan Hall, Anton Prokopenkov, Dan Perez, Lexie Aytes, Alden Wahlstrom, *Unearthing APT44: Russia`s Notorious Cyber Sabotage Unit Sandworm*, Mandiant, Google Cloud, April 17, 2024; https://cloud.google.com/blog/topics/threat-intelligence/apt44-unearthing-sandworm, accesat la 29.04.2026.

[39] Hönö Olli, *Op.cit.*

[40] *Ibidem.*

[41] Gabby Roncone et al., *Op.cit.*

[42] Marcus Willett, ”The Cyber Dimension of the Russia–Ukraine War”, în *Cyber Operations and Their Responsible Use,* The Adelphi Series, vol. 64, no. 511-513, The International Institute for Strategic Studies, London, 2024, pp. 105-124.

[43] *** *Technical Analysis of the WhisperGate Malicious Bootloader*, CrowdStrike Intelligence Team, January 19, 2022; https://www.crowdstrike.com/en-us/blog/technical-analysis-of-whispergate-malware/, accesat la 13.04.2026. A se vedea și Subhash Dutta, *Cyber Operations Associated with the Ukraine-Russia Conflict: An Open-Source Assessment*, National Maritime Foundation, New Delhi, May 10, 2022; https://www.maritimeindia.org/cyber-operations-associated-with-the-ukraine-russia-conflict-an-open-source-assessment, accesat la 11.04.2026.

[44] *** *Report on Cyber Lessons Learned During the War in Ukraine*, The Regional Cyber Defence Centre, Ministry of National Defence of the Republic of Lithuania, Vilnius, 2023, 61 p.

[45] *Ibidem.*

[46] *** ESET Research, *IsaacWiper and HermeticWizard: New wiper and worm targeting Ukraine,* March 1, 2022; https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/, accesat la 09.03.2026.

[47] Luke Jenkins, Josh Atkins, Dan Black, *Backchannel Diplomcy: APT29`s Rapidly Evolving Diplomatic Phishing Operations*, Mandiant, Google Cloud, September 21, 2023; https://cloud.google.com/blog/topics/threat-intelligence/apt29-evolving-diplomatic-phishing, accesat la 23.05.2026. A se vedea și Silviu Stahie, *Russian Hackers Target Ukrainian Military and Organizations with RDP Phishing Campaign*, Bitdefender, www.bitdefender.com., 25 Octombrie 2024; https://www.bitdefender.com/en-au/blog/hotforsecurity/russian-hackers-ukrainian-rdp-phishing-aws, accesat la 15.05.2026.

[48] *** US Cybersecurity & Infrastructure Security Agency, *Russian GRU Targeting Western Logistics Entities and Technology Companies*, April 17, 2026, 33 p.; https://www.cisa.gov/news-events/cybersecurity-advisories/aa25141a, accesat la 29.05.2026.

[49] *Ibidem.*

DILEMA CONTROL–INIȚIATIVĂ ÎN CONDUCEREA OPERAȚIILOR: CONDIȚIONĂRI ORGANIZAȚIONALE ALE COMENZII PRIN MISIUNE

Radu PRIOTEASA*

Abstract

Within this article we examine the control–initiative dilemma in the conduct of military operations within the context of the evolving contemporary security environment. Building on the transition from expeditionary operations in Iraq and Afghanistan to the return of industrial-style warfare as demonstrated by the conflict in Ukraine, the study argues that the effectiveness of mission command cannot be understood as a universal solution, but must be assessed in relation to specific organizational conditions. The analysis highlights that, although mission command is often promoted as a means to enhance flexibility and adaptability, its successful implementation depends on factors such as the level of professionalization, organizational culture, and the use of technology. In this regard, the article explores the tension between centralized control and decentralized initiative, outlining the strengths and limitations of each approach.

Furthermore, the paper discusses the implications of technological development for command processes, emphasizing a key paradox: while modern technologies provide improved situational awareness, they may also lead to excessive recentralization of decision-making. In conclusion, the article argues that the effectiveness of operational leadership does not derive from the rigid application of a doctrinal model, but from the ability to dynamically balance control and initiative in accordance with the operational context and the characteristics of the military organization.

Keywords: *mission command; control and initiative; operational leadership; adaptive planning; Ukraine conflict; organizational culture; military professionalization; command and technology.*

INTRODUCERE

Conflictele militare au reprezentat dintotdeauna un aspect de netăgăduit al realităților sociale, iar modalitatea de a învinge într-un conflict a reprezentat, cu certitudine, un aspect esențial pentru cei care au purtat aceste războaie. Conducătorii și teoreticienii militari au fost fascinați de posibilitatea obținerii unor victorii răsunătoare folosind resurse limitate, identificând situații, factori, elemente punctuale care ar fi putut contribui la simplificarea conflictului. În acest sens, experiența conflictelor recente, în special războiul dintre F.Rusă și Ucraina, dar și

*[*] **Student doctorand, Universitatea Națională de Apărare „Carol I”***

conflictele din Irak și Afganistan, au evidențiat, încă o dată, că factorul cantitativ nu prevalează întotdeauna în fața celui calitativ, astfel că victoria poate fi, de multe ori, de partea celor curajoși și nu doar a celor mulți.

În contextul activităților militare, modul în care sunt gestionate și coordonate acțiunile forțelor implicate într-un conflict sau într-o misiune este esențial pentru succesul acestora. O metodă de conducere care a câștigat recunoaștere și aplicabilitate pe scară largă în rândul forțelor armate moderne este ***comanda prin misiune*** (*mission command*). Aceasta reprezintă un model de conducere care se bazează pe delegarea autorității și responsabilității decizionale către nivelurile inferioare ale structurii de comandă, încurajând inițiativa și autonomia, menținând, în același timp, claritate în ceea ce privește obiectivele și scopul general al acțiunii.

Modelul *comenzii prin misiune* promovează un tip de conducere care nu se centrează pe micro-management, ci pe crearea unui cadru flexibil în care liderii și subordonații sunt încurajați să își asume responsabilitatea pentru îndeplinirea misiunilor stabilite. În această abordare, se pune un accent deosebit pe încrederea reciprocă între comandanți și subordonați, pe transmiterea unui obiectiv comun clar și pe capacitatea de adaptare rapidă la situații imprevizibile, caracteristice oricărei acțiuni militare.

Scopul acestui articol este de a analiza conceptul de *comandă prin misiune*, explorând unele dintre principiile fundamentale care o definesc, avantajele și provocările pe care le implică aplicarea acestui model în cadrul structurilor militare contemporane. Ne vom referi, de asemenea, la modul în care acest tip de conducere poate fi considerat o metodă eficientă pentru coordonarea forțelor în acțiuni complexe și dinamice, precum și impactul său asupra performanței generale a unităților militare.

Într-o eră în care tehnologia, informațiile și ritmul schimbărilor pot influența semnificativ dinamica unui conflict, comanda prin misiune devine un instrument de conducere indispensabil. Aceasta încurajează eficiența operațională prin decizii luate rapid la nivelurile inferioare, care pot răspunde mai bine și mai prompt la schimbările de pe teren. La rândul lor, aceste decizii locale pot contribui la succesul unui obiectiv mai larg, având în vedere faptul că cei care sunt direct implicați în acțiuni au cea mai mare înțelegere a contextului și pot evalua mai bine opțiunile disponibile.

Un alt aspect important al comenzii prin misiune este eficiența în gestionarea resurselor și a timpului. Într-un conflict militar, timpul este un factor crucial, iar întârzierea luării deciziilor poate avea consecințe grave. Modelul de comandă susține un cadru de autonomie care reduce dependența de ordinele centrale și permite comandanților locali să își alinieze resursele și forțele la cerințele specifice ale misiunii, fără a aștepta aprobări sau instrucțiuni suplimentare. Acest lucru conduce la o reacție mai rapidă și o mai mare flexibilitate în fața schimbărilor din câmpul de luptă.

Cu toate acestea, adoptarea comenzii prin misiune presupune și unele provocări. Un astfel de model de conducere necesită un nivel înalt de instruire și pregătire a tuturor membrilor structurii ierarhice, precum și o cultură a încrederii care să permită delegarea eficientă a responsabilităților. Lipsa unei coordonări centralizate ar putea duce la conflicte sau la interpretarea greșită a obiectivelor, iar în astfel de cazuri misiunea ar putea eșua. De aceea, implementarea cu succes a comenzii prin misiune depinde de maturitatea organizațională și de capacitatea de a evalua riscurile și beneficiile asociate acestei forme de conducere.

Dincolo de importanța generală a procesului de planificare, a unui cadru unanim recunoscut la nivelul unei organizații, precum cea militară, pentru standardizarea unui mod de gândire este imperios necesar să adaptăm cadrul științific la dezvoltările tehnologice și la experiența ultimelor conflicte. Astfel, putem spune fără putință de tăgadă, susținuți de realitatea războiului din Ucraina și de eforturile de înzestrare militară de pe întreg continentul european, că paradigma ”războiului antiterorist” este depășită, iar ”războiul clasic este aici”. Din acest motiv, trebuie să dezgropăm vechile instrumente, tactice

și strategice, de câștigare a acestuia. În tot mai mare măsură, aceasta depinde de capacitatea forțelor armate și a întregului sistem care le susține de a se adapta rapid și de a lua decizii eficiente în condiții de incertitudine[1].

O provocare importantă în conducerea operațiilor este menținerea unui echilibru funcțional între control și inițiativă. În mod tradițional, controlul centralizat a fost perceput ca un factor de stabilitate, asigurând coerența și predictibilitatea acțiunilor, în special în cadrul organizațiilor extinse sau eterogene. Cu toate acestea, experiența practică evidențiază că un nivel excesiv de rigiditate poate afecta capacitatea de reacție și poate limita exploatarea oportunităților apărute pe câmpul de luptă. Simultan, promovarea inițiativei implică propriile riscuri, mai ales în situațiile în care nivelul de pregătire sau gradul de coeziune al structurilor nu susține asumarea responsabilității în mod eficient.

O serie de exemple recente sunt relevante pentru această discuție. Astfel, modalitatea în care forțele ucrainene au reușit să acționeze într-un mod descentralizat, valorificând inițiativa la nivel tactic, este într-un contrast evident cu dificultățile întâmpinate de unități/ subunități care au rămas dependente de un control strict[2]. Simultan, dezvoltarea în domeniul tehnologiilor emergente/ inovative, pe câmpul de luptă, reprezintă o provocare suplimentară pentru această relație. Accesul comandanților și comandamentelor la informații, în timp real, asigură o imagine mult mai detaliată a situației locale, dar în același timp creează și o tentație de a se implica direct în execuție, limitând astfel autonomia subordonaților[3].

În acest context, devine evident că eficiența comenzii prin misiune nu poate fi evaluată în mod abstract sau aplicată uniform. Funcționarea sa este condiționată de factori concreți, precum nivelul de profesionalizare, cultura organizațională, gradul de încredere între eșaloanele de comandă și experiența operațională acumulată. În absența acestor elemente, delegarea autorității riscă să genereze mai degrabă incertitudine decât flexibilitate.

Având în atenție aceste observații, ne propunem să abordăm dilema control–inițiativă dintr-o perspectivă pragmatică, concentrându-ne asupra condiționărilor organizaționale ale *comenzii prin misiune*. Demersul nostru nu urmărește să valideze un model în detrimentul altuia, ci să evidențieze faptul că raportul dintre control și autonomie trebuie ajustat în funcție de context. În acest sens, analiza vizează atât identificarea limitelor, dar și a condițiilor în care *comanda prin misiune* poate contribui efectiv la creșterea eficienței în conducerea operațiilor și, în ultimă instanță, la obținerea victoriei.

NECESITATEA ADAPTĂRII PROCESULUI DE PLANIFICARE

Comanda prin misiune reprezintă un concept pe cât de vechi pe atât de redescoperit cu fiecare generaţie sau nou tip de război. Strategi şi gânditori militari, de la Sun Tzî la Napoleon, de la Pericle la generalul Joffre, au subliniat importanţa „împuternicirii” subordonaţilor/ a descentralizării deciziei. 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.

Dincolo de argumentele istorice, am descoperit, pe parcursul carierei militare, empiric, că structurile, respectiv micii comandanți, cărora li se acorda încredere în rezolvarea sarcinilor aveau un grad de coeziune ridicat, îndeplineau sarcinile şi, deloc de neglijat, stârneau invidia celorlalți. Mai departe, pe parcursul variilor misiuni externe, în context multinaţional, am identificat aceeași tendință, de această dată generalizată, mai ales la membrii aparţinând armatelor anglo-saxone. Cu diferenţa că, de data aceasta, cadrul era normat prin conceptul „*comanda prin misiune*”. Şi cum, pentru o forţă militară precum armata noastră, în cadrul geopolitic actual, perspectiva unei evoluţii accelerate, care nu ţine neapărat de factorul bugetar, era foarte atrăgătoare, am decis că un studiu atent al acestui concept, identificarea punctelor forte şi a perspectivelor

de implementare poate contribui la crearea unor premise care să faciliteze succesul pe câmpul de bătălie.

Având în vedere importanța și necesitatea adaptării procedurilor naționale, în contextul apartenenţei la structurile euro-atlantice, la tipologia noilor conflicte, motivarea alegerii temei pare relativ simplă. Implementarea conceptului „*comanda prin misiune*" înseamnă, de fapt, implementarea unei filosofii de comandă bazate pe descentralizarea deciziei, responsabilitate augmentată pentru comandanţii de pe toate treptele ierarhice subordonate, concomitent cu un tip de audit, un sistem de control al rezultatelor. Dincolo de exotismul expresiei *comanda prin misiune* se găsesc, de fapt, două ipoteze atrăgătoare pentru orice comandant militar: prima este ipoteza victoriei, iar cea de-a doua este ipoteza desfășurării de către structurile subordonate a unui proces de planificare abreviat, în lipsa unei direcţionări actualizate a comandantului. Esenţial, comanda prin misiune înseamnă o victorie, a se înţelege aici atingerea obiectivului stabilit de comandant, prin destratificarea deciziei şi, deci, a comenzii.

Considerăm că adoptarea conceptului comenzii prin misiune, la nivelul Armatei României, va sprijini, în mod decisiv, derularea cu succes a unor eventuale acțiuni militare în care ţara noastră ar fi implicată şi, de asemenea, va modela lideri şi subordonaţi care vor sprijini naţiunea, în orice domeniu vor activa. În Introducerea la Strategia militară a României-2021, fostul şef al Statului Major al Apărării, menţiona că „..... strategia oferă astfel direcționările necesare unei noi generații de lideri militari, îndemnând la flexibilitate conceptuală și eficiență acțională în parcurgerea etapelor procesului de transformare a Armatei României până în anul 2040....". Deci, această flexibilitate conceptuală, care duce la eficienţa acţională, reprezintă domeniul de manifestare al comenzii prin misiune. „În plan operațional, acțiunile militare executate simultan, în multiple medii de confruntare, și integrarea acestora în strategii hibride vor deveni un standard de acțiune şi vor genera efecte superioare la țintă, ceea ce va influența modul de angajare a structurilor militare. Este posibil ca operațiile hibride, care în trecut erau clasificate ca operații de modelare, să devină decisive, un potențial adversar urmărind realizarea paraliziei multidimensionale a statului țintă ".

Dacă *incertitudinea*, care a fost dintotdeauna o caracteristică a afacerilor militare, este potenţată de prevalenţa unui mediu de confruntare aflat la limita normării, devine imperativă şi implementarea în arsenalul comandanţilor, de pe toate treptele ierarhice, a unui arsenal care să le ofere un avantaj decisiv asupra adversarilor. Acest arsenal, dincolo de gadget-uri şi sisteme „last generation", este reprezentat de modificări la nivel cognitiv, de încurajarea şi crearea unui mediu în care „iniţiativa disciplinată" să fie un atribut al tuturor comandanţilor de pe toate treptele ierarhice.

Comanda prin misiune, ca metodologie recunoscută, își are rădăcinile în concepţiile generalilor prusaci Johann David von Scharnhorst, August Graf Neidhardt von Gneisenau și Carl von Clausewitz. În urma înfrângerilor în bătăliile de la Jena și Auerstedt, 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". 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*”, încearcă, dar într-un mod destul de neconvingător, să argumenteze dezastrul încercuirii Armatei 6 germane la Stalingrad. În cadrul argumentaţiei sale, acesta prezintă nucleul funcţiunii de comandă şi control a armatei germane şi anume: „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”.

Controlul și inițiativa, echivalente până la un anumit nivel cu nucleul activităților militare, și ne referim aici la sistemul de comandă și control, reprezintă o parte esențială a planificării operațiilor militare. Este evident că „niciun plan nu supraviețuiește primului contact cu inamicul”, dar implementarea unor metodologii care să ofere atât comandanților, cât și subordonaților un avantaj pe câmpul de luptă, sunt esențiale în cadrul proceselor de planificare a operațiilor. În acest sens, planificarea nu poate fi privită ca un produs finit, ci ca un cadru de orientare care trebuie permanent adaptat[4].

Este evident, atât din punct de vedere istoric, cât mai ales logic, că planificarea operațiilor într-un cadru tradițional, care implică conflicte de tip tradițional, este diferită de cea a unor conflicte reduse ca mărime și intensitate, de tipul războiului antiterorist. Operațiile desfășurate în Irak și Afganistan au fost, în cea mai mare măsură, caracterizate de existența unui tip de adversar inferior atât din punct de vedere tehnologic, cât și organizațional, precum și de un ritm al operațiilor relativ diferit față de conflictele convenționale de mare intensitate, astfel că mediul operațional a permis, în majoritatea situațiilor, menținerea de către puterea dominantă a unui grad ridicat de control asupra acțiunilor. Coroborat cu avantajul tehnologic, superioritatea informațională și, mai ales, libertatea de mișcare (cu accent pe avantajul aerian), au oferit posibilitatea comandanților de a executa o planificare detaliată și o supraveghere extinsă a execuției.

Procesul de planificare a operațiilor, grevat de o stratificare a lanțurilor de comandă multiple, era totuși destul de liniar, permițând parcurgerea în totalitate a cadrului doctrinar existent la nivelul armatei respective. Totodată, existența unor situații relativ stabile la nivel strategic, cu comandamentele amplasate relativ sigur, în afara unor zone de risc și în absența unor amenințări constante și credibile, dublate de existența unor sisteme de armament superioare, au permis desfășurarea acestor procese de planificare într-un mod liniar.

Situația s-a modificat în cazul conflictului din Ucraina, care marchează o revenire la ceea ce poate fi descris drept război de tip industrial: utilizarea pe scară largă a forțelor convenționale, prin intensitatea ridicată a operațiilor și prin implicarea unor sisteme de armament avansate de ambele părți; adversari relativ comparabili ca dotare; dispariția, pentru moment, a avantajului numeric al unuia dintre adversari în fața tehnologiilor utilizate de celălalt; ritmul operațional accelerat de utilizarea extensivă a tehnologiilor moderne (precum dronele, sistemele de recunoaștere în timp real și integrarea informațiilor din surse multiple) a reprezentat o întoarcere la tipul de conflicte experimentat de bunicii noștri și învățat în academiile militare.

Un adversar care are aceeași vizibilitate asupra câmpului de luptă ca și forțele proprii, aceleași capabilități, anumite avantaje atât tehnologice, cât și operaționale, este infinit mai dificil în a fi combătut, adică învins, decât unul inferior tehnologic. În astfel de situații, identificarea unor factori particulari, care să exploateze oportunități sau să ofere avantaje operaționale forțelor, este esențială. Planurile nu mai pot fi concepute ca secvențe rigide de acțiuni, ci trebuie să ofere direcții generale, bazate pe intenția comandantului, lăsând spațiu pentru inițiativa subordonaților. În același timp, această abordare presupune acceptarea unui anumit nivel de incertitudine și risc.

Prin urmare, diferența dintre tipurile de conflict analizate nu este doar una de intensitate, ci

și una de logică a conducerii. În timp ce conflictele din Irak și Afganistan au permis, într-o anumită măsură, menținerea unui model mai apropiat de controlul centralizat, conflictul din Ucraina evidențiază limitele acestuia și necesitatea unei adaptări către forme mai flexibile de conducere. În acest sens, comanda prin misiune nu mai apare doar ca o opțiune doctrinară, ci ca o consecință a realităților operaționale contemporane.

DILEMA CONTROL–INIȚIATIVĂ ÎN CONDUCEREA OPERAȚIILOR

Sistemul militar este centrat în mod tradițional pe disciplină, aceasta însemnând respectarea ordinelor primite de la comandanții ierarhici și îndeplinirea acestora, în spiritul și litera lor. Aparatul militar este construit pe această axiomă, disciplina fiind sinonimă cu tot ceea ce înseamnă sistemul de relații între militari, activitățile desfășurate, și, într-un cuvânt, tot ce ține de armată. Dar, având în vedere limitările evidente de control (un comandant nu poate supraveghea tot timpul toți subordonații săi), rezultă o nevoie de a armoniza ordinul comandantului cu tipul execuției. Aceasta este transpusă într-o relație de comandă și control în care este necesară integrarea elementului de inițiativă. Această relație dintre control și inițiativă reprezintă una dintre cele mai persistente și dificil de gestionat tensiuni în conducerea operațiilor militare. Cu toate că doctrina modernă tratează cele două aspecte ca fiind complementare, practica arată că echilibrul dintre ele este instabil și dependent de context. În esență, problema nu constă în alegerea între control sau inițiativă, ci în determinarea nivelului adecvat al fiecăreia în funcție de situație.

Controlul centralizat este elementul principal asociat, în mod tradițional, cu eficiența în organizații complexe, cum este și sistemul militar. Un amalgam, organizat, de oameni, sisteme și echipamente nu poate funcționa decât prin existența unor proceduri/ ordine bine definite și respectarea/ controlul acestora de către toți cei implicați. Controlul asigură atât coordonarea resurselor (umane, materiale, financiare, informaționale), sincronizarea acțiunilor, cât și menținerea unei direcții unitare. În special în structuri extinse sau eterogene, controlul oferă un grad de predictibilitate necesar pentru evitarea fragmentării. Din acest motiv, în multe situații, conducerea militară tinde să privilegieze controlul, mai ales atunci când există incertitudini legate de nivelul de pregătire sau de coeziunea forțelor[5].

Cu toate acestea, avantajele controlului centralizat sunt însoțite de limitări evidente. Procesele decizionale devin mai lente, iar reacția la schimbările din teren este întârziată. Într-un mediu operațional caracterizat prin ritm accelerat și interacțiuni complexe, această întârziere poate conduce la pierderea inițiativei. Suplimentar, dependența ridicată de nivelurile superioare de comandă reduce capacitatea subordonaților de a acționa individual, aspect problematic în situații de criză sau în care comunicațiile sunt reduse/ inexistente. În contrast, inițiativa descentralizată oferă o multitudine de avantaje care devin atrăgătoare pentru comandanți, mai ales în conflictele contemporane. Posibilitatea de a lua decizii la nivel tactic permite adaptarea rapidă la situații neprevăzute și exploatarea oportunităților ivite. Conceptul de comandă prin misiune se bazează tocmai pe această idee, încurajând subordonații să acționeze în conformitate cu intenția comandantului, chiar și în absența unor ordine detaliate.

Totuși, această abordare nu este lipsită de riscuri; acestea trebuie să fie luate în considerare și reduse, pe toate nivelurile de comandă. Autonomia presupune existența unor structuri capabile să interpreteze corect intenția și să ia decizii adecvate. În absența unui nivel suficient de instruire sau a unei culturi organizaționale bazate pe încredere, inițiativa poate conduce la incoerență sau la acțiuni divergente. Din acest motiv, implementarea comenzii prin misiune nu poate fi realizată doar prin schimbări doctrinare, ci necesită transformări la nivel organizațional și cultural. Experiența conflictului din Ucraina oferă exemple relevante în acest sens. Capacitatea forțelor ucrainene de a acționa descentralizat, adaptându-se rapid la schimbările din teren, a fost frecvent asociată cu utilizarea eficientă

a inițiativei la nivel tactic. În același timp, dificultățile întâmpinate de structuri caracterizate prin control rigid au evidențiat limitele unui model excesiv centralizat[6].

Pe lângă dimensiunea doctrinară, dilema control–inițiativă are și o componentă psihologică importantă. Asumarea inițiativei implică acceptarea riscului de a greși, iar acest lucru este influențat direct de cultura organizațională. În organizațiile în care greșelile sunt sancționate sever, există o tendință de evitare a responsabilității, ceea ce limitează inițiativa. În schimb, în mediile în care există toleranță pentru erori și accent pe învățare, subordonații sunt mai dispuși să acționeze autonom[7].

Această relație dintre încredere, inițiativă și conducere nu este specifică doar contextului modern. Ea poate fi observată încă din relatările clasice privind conducerea în condiții de incertitudine. În lucrarea antică *Anabasis*, Xenofon descrie modul în care, în absența unei structuri de comandă stabile, liderii sunt obligați să stimuleze inițiativa și responsabilitatea individuală pentru a asigura supraviețuirea și coeziunea grupului[8]. Decizia și acțiunea nu mai pot fi amânate în așteptarea unor ordine superioare, iar capacitatea de a interpreta situația și de a acționa devine esențială.

CONDIȚIONĂRI ORGANIZAȚIONALE ALE COMENZII PRIN MISIUNE

Comanda prin misiune este, în mod tradițional, asociată cu o eficiență ridicată a proceselor de planificare a operațiilor, cu un ritm operațional mai alert, cu idei operaționale și inițiativă care, în mod inevitabil, vor duce la succes pe câmpul de luptă. Exemple nenumărate, atât în literatura de specialitate, dar și în opere literare, subliniază nu doar avantajele, ci și dependența succesului de adoptarea acestui concept.

Cu toate acestea, experiența din practică arată că eficiența acestui model este determinată, în mare măsură, de tipul de organizație și condițiile specifice în care este implementat. Altfel spus, comanda prin misiune nu funcționează în mod automat, ci presupune adaptarea la factori precum nivelul de profesionalizare și instruire, cultura organizațională și încrederea, structura forței și eterogenitatea organizațională, tehnologia și dimensiunea psihologică a inițiativei, care să îi susțină aplicarea.

Unul dintre atributele principale care leagă comanda prin misiune de succesul misiunii este nivelul de profesionalizare și instruire al forțelor. Este evident aici, atât din punct de vedere al experienței, cât mai ales al cadrului în care își desfășoară activitatea, că inițiativa, ca element central al comenzii prin misiune, nu poate fi impusă prin reglementări sau ordine, ci este rezultatul unui proces îndelungat de formare. Capacitatea de a lua decizii individuale în condiții de incertitudine presupune nu doar cunoștințe tehnice, ci și experiență operațională și judecată profesională, aspecte exersate îndelungat pe timpul activităților curente în care sunt implicați militarii. Simplist spus, una este situația unei unități profesionalizate, cu militari care își dedică tot timpul instruirii profesionale, spre deosebire de o structură care va fi augmentată sau constituită din rezerviști.

În organizațiile în care instruirea este consistentă și continuă, iar personalul este expus la scenarii variate, există o probabilitate mai mare ca subordonații să înțeleagă intenția comandantului și să acționeze în mod adecvat. În schimb, în structuri în care nivelul de pregătire este inegal sau insuficient, autonomia poate genera decizii incoerente sau chiar eronate. Din acest motiv, doctrina militară subliniază faptul că delegarea autorității trebuie să fie corelată cu nivelul de competență al celor care o primesc[9].

Dacă profesionalizarea oferă un cadru tehnic pentru exercitarea inițiativei, cultura organizațională reprezintă mediul în care aceasta poate fi sau nu pusă în practică. Comanda prin misiune presupune un nivel ridicat de încredere între comandant și subordonați. Fără această încredere, delegarea autorității devine formală, iar inițiativa este limitată de teama de a greși. O cultură organizațională care încurajează inițiativa, reduce controlul excesiv și nu se grăbește să sancționeze rapid erorile este mediul propice

pentru implementarea comenzii prin misiune. Elementul central al tuturor acestor acțiuni este încrederea. Încrederea între comandanți și subordonați, cât și între subordonați, nu este un element care poate fi construit rapid, ci se clădește în timp, prin interacțiuni repetate și prin experiențe comune. În lipsa acestui proces, comanda prin misiune riscă să rămână un ideal dificil de atins.

Un alt factor esențial pentru implementarea comenzii prin misiune îl reprezintă structura forței. Organizațiile militare nu sunt omogene, iar diferențele dintre unități pot influența semnificativ modul de conducere. În structurile omogene, cu nivel ridicat de coeziune și pregătire similară, inițiativa poate fi extinsă relativ ușor. În schimb, în organizațiile eterogene, unde există diferențe în nivelul de instruire sau experiență, este necesară o abordare diferită, mai nuanțată, aplicată la fiecare unitate și/sau structură în parte. Această realitate devine evidentă în situațiile în care forțele sunt extinse rapid (ex.: prin mobilizare sau integrate din surse diferite). În astfel de cazuri, aplicarea uniformă a comenzii prin misiune poate conduce la incoerență în acțiune și, pe cale de consecință, alterarea scopului pentru care intenționam, în primă instanță, aplicarea conceptului. În consecință, nivelul de descentralizare trebuie ajustat în funcție de caracteristicile fiecărei structuri.

Conectivitatea generală facilitată de tehnologia modernă reprezintă un alt factor care influențează în mod semnificativ modul în care este exercitată comanda prin misiune. Sistemele de comandă și control, precum și accesul la informații în timp real, oferă comandamentelor o imagine operațională mult mai detaliată decât în trecut. În teorie, acest lucru ar trebui să faciliteze procesul decizional și să sprijine coordonarea acțiunilor; în practică, însă, apare un fenomen paradoxal. Posibilitatea de a monitoriza în detaliu evoluția situației creează tentația de a interveni direct în execuție, chiar și la niveluri inferioare. Astfel, tehnologia poate conduce la o recentralizare a deciziei, limitând inițiativa subordonaților[10]. Această situație evidențiază necesitatea unui echilibru între utilizarea tehnologiei și menținerea capacității de acțiune autonomă. Tehnologia trebuie să sprijine decizia, nu să o înlocuiască sau să o concentreze excesiv la un singur nivel.

Pe lângă factorii structurali și organizaționali, comanda prin misiune are și o dimensiune profund umană. Inițiativa presupune nu doar competență, ci și disponibilitatea de a-ți asuma riscuri. Această disponibilitate este influențată de factori precum încrederea în sine, percepția asupra consecințelor și climatul organizațional. În mediile în care greșeala este percepută ca un eșec major, există o tendință de evitare a deciziei. În schimb, acolo unde există o abordare orientată spre învățare, subordonații sunt mai dispuși să acționeze. Această diferență este esențială pentru înțelegerea modului în care inițiativa poate fi încurajată sau, dimpotrivă, inhibată.

Exemplele istorice confirmă această observație. În situații de criză, în care structurile de comandă sunt afectate sau absente, capacitatea liderilor de a stimula inițiativa individuală devine decisivă pentru supraviețuire și succes.

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://usacac.army.mil/sites/default/files/documents/mccoe/TheEvolutionOfMissionCommandInArmyDoctrine.pdf.
2. GADY Franz-Stefan, "Ukraine's Army Must Shed Its Soviet Legacy, Says a Military Expert", *The Economist* (website), March 17, 2023; https://www.economist.com.
3. HEWSON Jack, Artem Starosiek, "Ukrainian Company Uses Social Media, Open Source Technology to Counter Russian Invasion", *PBS NewsHour* (website), April 19, 2023; https://www.pbs.org/newshour.
4. HERSZENHORN M. David, 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.
5. HOCKENHULL Jim, "How Open-Source Intelligence Has Shaped the Russia-Ukraine War", Speech, Members Webinar, Royal United Services Institute, London, December 9, 2022; www.gov.uk/government/speeches/how-open-source-intelligence-has-shaped-the-russia-ukraine-war.
6. (von) MANSTEIN Erich, *Victorii pierdute*, Editura Elit, Iași, 2005.
7. NAGL John, Crombe Katie (coord.), *A Call to Action: Lessons from Ukraine for the Future Force*, Strategic Studies Institute, US Army War College, USAWC Press, June 2024, 323 p.; https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=1964&context=monographs.
8. SHUSTER Simon, vera Bergengruen, "Inside the Ukrainian Counterstrike that Turned the Tide of War", *Time Magazine*, 26.09.2022; https://time.com/6216213/ukraine-military-valeriy-zaluzhny/
9. *** Headquarters, Department of the Army (HQDA), *Mission Command*: *Command and Control of Army Forces, Army Doctrine Publication 6-0* (Washington, DC: HQDA, July 2019).

[1] Department of the Army, *ADP 5-0: The Operations Process,* Headquarters, Department of the Army, Washington DC, 2019, 1-3.
[2] John A. Nagl și Katie Crombe, *A Call to Action: Lessons from Ukraine for the Future Force,* US Army War College Press, Carlisle Barracks, PA, 2024, xxv–xxvi.
[3] Department of the Army, *ADP 6-0: Mission Command: Command and Control of Army Forces,* Headquarters, Department of the Army, Washington DC, 2019, 1-11.
[4] *Ibidem.,* 24-27.
[5] *Ibidem.*
[6] *Ibidem,* 1-5.
[7] John A. Nagl și Katie Crombe, *Op.cit.,* xix–xx.
[8] Xenophon, *Anabasis* (trad. Carleton L. Brownson), Harvard University Press, Cambridge MA, 1922, III.1–2.
[9] Department of the Army, *ADP 6-0: Mission Command: Command and Control of Army Forces,* 2019.
[10] John A. Nagl și Katie Crombe, *Op.cit.,* xxiii–xxiv.

HOW ARTIFICIAL INTELLIGENCE COULD BENEFIT HUMINT

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

Abstract

For Romania, the inauguration of a new, pro-modernization administration, the activation of NATO DIANA test centers in Bucharest,[1] and the need for compliance with the EU AI Act[2] creates a unique window of opportunity for Romania's military to establish AI-enabled intelligence collection and analysis capabilities[3]. Over the past decade, artificial intelligence, or AI, has indisputably benefited technical intelligence collection disciplines. But how could AI be put to use supporting human intelligence, or HUMINT? A student research team at Mercyhurst University used open-source intelligence collection and analysis in an attempt to answer this question. They identified specific activities in the HUMINT operational cycle that could benefit from AI, and examined how six different AI-enabled platforms (Maltego, Babel Street, Videris, TrackLight, Neotas, and SpiderFoot) could be leveraged to support HUMINT. They identified concerns that could be associated with using AI to support HUMINT and examined how governments have attempted to mitigate those concerns.

Keywords*: Artificial Intelligence; human intelligence; tradecraft; machine learning; natural language processing.*

INTRODUCERE

What is artificial intelligence (AI)?

Artificial intelligence (AI) is a computer science field focused on creating machines and software that can simulate human intelligence to complete complex tasks. Unlike traditional software, AI systems use algorithms to learn from data, identify patterns, and make independent decisions[4]. Core AI technologies include *machine learning* (ML), where systems learn from experience; *deep learning* (DL), where computers use neural networks, computational structures inspired by the human brain, to solve complex problems; *natural language processing* (NLP), which enables computers to understand, interpret, and generate human language, and *computer vision*, which enables machines to see, interpret, and react to visual information, which is essential for medical imaging and self-driving cars[5].

How AI is impacting the intelligence profession

Currently, both friendly and adversarial governments around the world are in the process

****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.***

of integrating AI capabilities for a variety of intelligence purposes[6]. For example, the U.S. Air Force is currently experimenting with Palantir's Target Workbench as a means to reduce civilian casualties from air strikes[7]. During the first quarter of the 21st century, artificial intelligence (AI) has already made significant contributions to enhancing such technical intelligence collection disciplines as signals intelligence (SIGINT), geospatial intelligence (GEOINT), measurement and signature intelligence (MASINT), social media intelligence (SOCMINT), and open-source intelligence (OSINT)[8]. But what could AI do to enhance the world's oldest intelligence collection discipline, which is human intelligence (HUMINT)?

Why is AI limited in its ability to enhance HUMINT?

The very foundation of HUMINT is the *human* element – intuition, empathy, and the ability to build and sustain trust[9]. While AI excels at rapidly processing voluminous amounts of data and identifying patterns, successful HUMINT moves "at the speed of humans"[10], requiring the patient cultivation and sustainment of relationships based on cognitive skills that automated systems simply cannot replicate[11]. AI lacks the emotional intelligence (EQ) necessary to understand emotions, sarcasm, and nonverbals, all of which are essential for human cognition[12]. "The objective is not to replace human officers but to empower them and serve as force multipliers"[13].

HOW COULD AI ENHANCE HUMINT?

Although AI is limited in its ability to replace the human-on-human component of HUMINT, there are aspects of the HUMINT methodology that could definitely benefit from the application of AI. These include:

HUMINT targeting

One of the first steps in the HUMINT process is lead identification, or "spotting". Enabled by AI, HUMINT targeteers can now analyze massive datasets (social media, communication patterns, digital footprints) to identify possible leads and assess their access, motivations, and vulnerabilities[14]. "AI and machine learning (ML) can enhance HUMINT success by identifying potential intelligence sources (targeting, in intelligence parlance) or constructing digital patterns of life for prospective recruitment targets"[15].

Psychological profiling

AI systems can predict personality traits from social media content with high accuracy, helping case officers tailor their rapport-building strategy. Machine learning (ML) algorithms can assist case officers by creating detailed psychological profiles of targets, assessing where their grievances lie and identifying who may be susceptible to recruitment. AI tools can process voice inflections, facial micro-expressions, and textual cues in real-time to detect stress, deception, or shifting loyalties.

Simultaneous engagement with developmentals

Once prospective HUMINT sources have been identified, AI can manage hundreds of developmental conversations simultaneously, using hyper-realistic personas to establish and maintain rapport with potential sources[16]. This could be accomplished on a scale that would be impossible for a single HUMINT officer to achieve. While human-to-human engagement is not an activity that should be entirely delegated to AI, it is one where the addition of AI could greatly expand the reach and effectiveness of digital case officers.

Assessment & development

AI-driven behavioral analysis offers deep insights into a target's internal state, often with greater accuracy than human-only assessment[17]. In the HUMINT operational cycle, AI significantly enhances the assessment and development phases by converting vast amounts of digital footprint data into actionable psychological profiles, identifying precise windows of vulnerability for recruitment.

Developing and generating personalized recruitment pitches

Using AI to assess and recruit talent is already being used by headhunters in the commercial

sector[18]. "Modern recruitment intelligence leverages advanced AI – from sophisticated search algorithms to autonomous screening agents – to identify and engage exceptional candidates that might otherwise go unnoticed"[19]. Digital case officers can use AI to analyze massive datasets—including social media, professional history, and public records—to build detailed psychological profiles. Algorithms categorize potential assets based on the traditional *MICE* framework (Money, Ideology, Coercion, Ego) by detecting grievances, financial instability, or ideological shifts in their digital behavior. AI tools can evaluate traits such as risk tolerance, empathy, and attention through gamified assessments or linguistic patterns, helping recruiters understand how a target makes decisions. Machine learning models forecast when a target is most receptive to a new opportunity, identifying a "window of openness," such as after a professional setback or a period of increased online activity. This technique is known as *propensity modeling*, or uplift modeling, which has gained considerable interest thanks to machine learning[20].

No contact recruitment

In 2019, a *New York Times* article by Edward Wong reported "How China uses LinkedIn to recruit spies abroad"[21]. In this article, the director of the National Counterintelligence and Security Center explained that it is simply "more efficient" to sit behind a computer in China and target thousands of individuals oversea using fake profiles[22]. For a HUMINTer using the "no contact" approach technique, this methodology is also cost-effective, consumes far less resources than traditional approaches, and poses considerably less risk to the HUMINTer. As part of a 2019 plea deal he signed, former DIA Ron Rockwell Hansen admitted in writing that he had collected information on "several former and current DIA case officers" and passed this information to Chinese intelligence in 2015[23]. Add AI-enabled tools to the mix, and the volume, quality, and precision of such targeting efforts could be amplified considerably.

Passive online approaches

In addition to using social media to reach out and make contact with leads, a HUMINTer could also set up a fake social media profile in the name of a high-profile, actual person in the hope of receiving friend requests from unsuspecting individuals of operational interest. The *U.S. Naval Institute* reported how this had been done to Admiral Michael Gilday, the U.S. Navy's new Chief of Naval Operations (CNO) in 2019[24]. "Conducting human intelligence (HUMINT)-enabled cyberspace operations requires only a single, crafty cyber actor with an internet connection," Lieutenant Commander Raymond Dennis observed[25]. Here, too, the use of AI tools could significantly enhance the volume and effectiveness of such fake profiles.

Cybernetic HUMINT

Cybernetic HUMINT, also referred to as cyber-HUMINT or virtual HUMINT, is the application of traditional HUMINT tradecraft within the cyber domain[26]. Whereas traditional HUMINT relies on physical, face-to-face interactions, Cybernetic HUMINT moves the case officer-asset relationship to the world of encrypted messaging apps, dark web forums, and closed digital communities. HUMINT case officers can create highly detailed, believable online identities with backstories (legends) to infiltrate restricted online groups. Using these online personas[27], known as "sock puppets," operators engage directly with threat actors on platforms like *Telegram, Signal,* or darknet marketplaces to gather insights that automated tools cannot reach. Just like in the physical world, the goal of cybernetic HUMINT is to build rapport and trust to elicit information about a target's motivations, plans and intentions, or capabilities[28]. Cybernetic HUMINT differs from traditional, face-to-face HUMINT because the latter "involves people within a physical contact, intimate and direct, with an emotional language that fosters connection and closeness, beyond the shared interests"[29]. Cybernetic HUMINT, while useful, "is based on relationships that are not necessarily permanent, that have a lower degree of commitment and loyalty, which do not allow levels of depth in the management of relationships because they are not based on a direct human bond"[30].

Asset validation

AI improves the vetting process by cross-referencing information across multiple databases to detect inconsistencies, identify subtle indicators of deception, or anomalies in a source's historical patterns. Handlers cross-reference a source's claims against their digital pattern of life and geospatial data to ensure they are who they say they are. AI tools can also analyze shifts in a target's communication tone or response timing to flag potential double-agents or cases where a source has been compromised[31].

Translation

Natural language processing (NLP) could help HUMINTers grasp cultural nuances, idioms, and non-verbal cues in real time, reducing the risk of cultural *faux pas*, thus improving rapport-building.

Cover

AI can be used to create suitable online identities, known as sock puppets, with logical, consistent legends, matching time zones, and nuanced language to mitigate the risk of detection by platform administrators or foreign intelligence services[32]. "A sock puppet account is a clandestine method through which intelligence agencies conduct their business; due to the anonymity of the SIM card, the agents behind the operation are not easily identifiable as they penetrate the target group or demographic"[33].

Immersive training

In the private sector, "companies in virtually every business sector are increasingly leveraging virtual training as a strategic asset to boost employee engagement and differentiate themselves in a competitive marketplace"[34]. In similar fashion, AI is transforming HUMINT training by serving as an augmented intelligence partner that can simulate complex human behaviors and generate hyper-realistic operational scenarios. Instead of replacing human instruction, AI acts as a force multiplier that allows agents to practice high-stakes interactions in a safe, scalable environment[35].

Cognitive load reduction

By automating routine data collection and analysis, AI enables HUMINTers to shift their time, energy, and focus to high-level strategy, empathy, and the establishment and maintenance of complex human relationships that remain at the core of the HUMINT process. "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"[36].

The criticality of Meaningful Human Control

AI cannot completely replace human beings in conducting HUMINT. For certain key functions, at certain points in the HUMINT process, AI can serve as a force multiplier and provide insights that would not be otherwise attainable. However, other HUMINT functions are best left to human beings to conduct. The key to the successful use of AI to enhance HUMINT is the concept of *Meaningful Human Control*, or MHC. "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"[37].

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[38]. 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[39]. 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[40].

Application of project management principles

In this project, the student project team employed both project management principles and commonly used intelligence analysis team techniques[41]. 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"[42]. The kick-off meeting was followed by an initial client meeting at which the client elaborated on their interest in the research topic[43]. 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[44]. 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[45]. 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[46]. 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[47]. 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[48].

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 "involves observation or direct gathering of PAI from public events and spaces"[49]. 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[50].

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"[51]. 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"[52]. 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[53]. 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"[54]. 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[55].

Use of OSINT

In this study, the four members of the team conducted open-source intelligence (OSINT)

collection to address the following questions about six AI software products that could be used to support HUMINT operations: What does the product do? How could the product support HUMINT operations?

We also collected and aggregated information concerning the ethical and operational challenges of using AI-enabled platforms in support of HUMINT operations, and examined how U.S. government users have attempted to mitigate those challenges and concerns.

FINDINGS

Maltego

What does Maltego do?

Maltego "functions by parsing large amounts of publicly available information from various open source websites and visualizing the results in graphs"[56]. By integrating disparate data sets into actionable visual maps, Maltego can serve as a critical fusion-intelligence platform for human intelligence (HUMINT) operations. Maltego bridges the gap between digital footprints and real-world human networks, allowing analysts to transition from a "hunch" to a defensible investigative outcome within a single interface. Maltego can reveal relationships three or four degrees of separation apart, which are often missed in manual spreadsheets or traditional databases.

How could Maltego support HUMINT operations?

Maltego is a "data mining tool used for digital forensics and intelligence gathering"[57]. Maltego started off as a useful desktop tool for link analysis: Maltego could diagram associations between individuals, aliases, social media profiles, and physical locations[58]. However, the shift to a cloud-based ecosystem made Maltego viable for real-time fieldwork; Maltego now functions as a connected platform for live coordination between headquarters and field agents[59]. The standout feature for case officers is *Maltego Monitor*, whose use could directly impact safety during physical meets[60]. By using AI to scan social media streams, Maltego Monitor filters out the usual noise and flags actual risk signals like crowd agitation or police movements. This gives case officers the warning needed to adjust routes or abort when the environment turns hostile. Leveraging "real-time data" and "AI-powered sentiment analysis," *Maltego Monitor* provides live insights into social media activity and messenger communications, which is vital for tracking active human networks and sentiment[61].

Babel Street

What does Babel Street do?

Babel Street is a Virginia-based technology company that specializes in AI-powered *risk intelligence* and open-source intelligence (OSINT) solutions for government, defense, and law enforcement agencies. Their platform, formerly known as *Babel X*, provides several core capabilities: *Babel Street*[62], an AI-powered threat, identity, and risk intelligence tool, focuses on closing the risk confidence gap through its *Insights* engine[63]. Babel Street's primary utility remains its handling of diverse languages which is critical for monitoring Russian, Chinese, or other targets who hide behind transliteration. Babel Street's *Agentic AI* search is a significant upgrade because it removes the need for constant manual tweaking[64]. The system now performs self-guided queries based on initial results and digs deeper into the web to build a target profile with minimal prompting. For operations involving languages using something other than Latin script, the *Native Script Resolution*[65] is the most valuable capability. The *Name Match*[66] engine, which maps aliases across 200 languages so that Cyrillic or Chinese characters align with the same individual, prevents high risk targets from slipping through database checks simply by switching alphabets. We also see a shift in integration through *Insight APIs*[67]. Agencies can now pull these multilingual data streams directly into their own dashboards instead of treating Babel Street as a separate, standalone research tool. Babel Street uses advanced Natural Language Processing (NLP) to understand sentiment, intent, and context beyond simple translation.

How could Babel Street support HUMINT operations?

Babel Street supports human intelligence (HUMINT) operations by serving as a force-multiplier for analysts, bridging the gap between digital footprints and physical human activity. Its platform integrates massive open-source data streams to provide situational awareness and identity resolution that would be impossible to achieve manually. Babel Street benefits HUMINT operations through the following core functions:

Providing improved situational awareness. Analysts can use Babel Street to monitor real-time social media reports from conflict zones or areas of interest, which often provide faster, more anecdotal "ground truth" than traditional classified channels.

Identifying Key Influencers: By analyzing social media interactions and digital behavior, the platform identifies reliable authors and influential nodes within a target network, helping HUMINT officers determine who is worth monitoring or potentially engaging.

Offering multilingual nuance: AI trained for native linguistic context captures nuances and intent in over 200 languages that simple translation misses, essential for understanding the actual "voice" and sentiment of human targets.

Improved identity resolution. Babel Street uses AI-powered identity resolution to resolve names, aliases, and identifiers across 200+ languages. This helps operators identify persons of interest and perform deep background checks (vetting) for potential informants or threats. HUMINT targeteers are able to resolve names and aliases across disparate systems, to include the Deep and Dark web.

Counterintelligence and insider threat detection. Babel Street helps identify behavioral indicators of insider threats, such as public grievances, lifestyle changes, or unusual online activity, which are critical for helping to protect sensitive operations.

Continuous vetting. For asset validation purposes, the platform automates the monitoring of persons of interest for such vulnerabilities as financial distress or unauthorized foreign travel, which are indicators of potential problems of interest to counterintelligence.

Secure access. Using *Babel Street Secure Access* enables HUMINT operators to conduct sensitive research or digital investigations without leaving a trace[68]. "Secure Access goes beyond traditional privacy tools because it offers advanced anonymization, controlled attribution, and an isolated research environment. This means that users can appear to originate from virtually any location, avoid geo-restrictions, and customize their digital footprint to fit specific investigative requirements"[69].

Babel Street's data is often integrated via APIs (Application Programming Interface) into platforms like Maltego. This allows analysts to pull Babel Street's massive datasets—such as social media profiles and location signals—directly into Maltego's visual interface to map complex human networks and "connect the dots" during investigations. Babel Street integrates with other platforms (like Maltego) via APIs to enrich existing internal data with transparent open-source context, creating a single unified view of a threat actor.

Videris

What does Videris do?

Videris, developed by the firm Blackdot Solutions, is an enterprise OSINT platform used by government agencies, law enforcement, and financial institutions that consolidates data collection, analysis, and reporting into a "single pane of glass"[70]. In contrast to Maltego's manual pivot method, Videris focuses on automating the investigative workflow for high-volume screening and deep-dive risk detection[71]. For the *investigation of financial crimes*, Videris is useful for investigating money laundering, fraud, and sanctions evasion. It is also used for *Enhanced Due Diligence* (EDD) and *supply chain risk assessments*, identifying organized crime networks and terrorist threats, and for monitoring and investigating insider threats[72]. *Videris Automate* is an AI-powered platform meant to handle high-volume investigative tasks using Agentic AI[73]. It allows users to "deploy standardized, customizable 'playbooks' in

natural language for any use case"[74]. According to Blackdot Solutions, Videris Automate is useful for complex investigations, Enhanced Due Diligence, and screening and monitoring[75].

How could Videris support HUMINT operations?

As an AI-enabled OSINT platform, Videris could benefit HUMINTers in a number of ways. HUMINT targeting officers could use Videris to spot, assess, and validate prospective HUMINT sources by securely and anonymously researching persons and locations of interest without tipping off the investigation subjects or leaving digital footprints that could compromise an operation[76]. Videris could also be used to build comprehensive profiles of leads or other persons of interest "by tracing real-world identities from usernames, email addresses, and phone numbers across social media, blogs, and forums"[77].

TrackLight

What does TrackLight do?

TrackLight is an AI-powered platform primarily focused on *fraud detection and prevention* for government agencies and corporate enterprises. TrackLight fills the void between standard targeting and deep financial forensics[78]. Its core capability is *Ray the Parrot*[79], which acts as an automated financial analyst trained on fraud schemes and open-source records. For a targeting officer, Ray breaks down a subject's business footprint and debt exposure in seconds. This speed allows users to identify leverage points like hidden liabilities or shell companies much earlier in the operational cycle.

TrackLight was designed to modernize how organizations identify fraud, waste, and abuse (FWA) without slowing down the delivery of critical services like grants, benefits, and procurements. The platform specializes in moving from a "pay-and-chase" model to *proactive prevention* by analyzing risks before payments are disbursed. The TrackLight suite consists of four primary modules, all supported by Ray:

- *Due Diligence*: A real-time search tool that scans over *1 billion open-source intelligence (OSINT)* records to uncover risks related to individuals or businesses during the application process.
- *Social Network Analysis:* A visualization tool that identifies high-risk relationships and hidden connections through graph displays, helping to expose conflicts of interest or collusion.
- *Fraud Analytics*: Uses a library of over *3,000 known fraud schemes* to continuously monitor financial transactions and program behaviors for anomalies and suspicious patterns.
- *FLEX AI Agents*: Uses Large Language Models (LLMs) to automate the management of fraud allegations and background vetting, reducing processing times from hours to minutes.

How could TrackLight support HUMINT operations?

TrackLight could support human intelligence (HUMINT) operations by acting as an AI force-multiplier for *vetting, targeting*, and *insider threat detection*. While primarily used as a fraud prevention tool, its ability to fuse billions of records with real-time analytics provides a distinct advantage for intelligence officers managing human networks. TrackLight's Due Diligence module allows human intelligence officers to cross-reference potential assets against over one billion OSINT records (including criminal histories, financial statuses, and business registrations) to confirm identities in under 90 seconds. They could also use *AI-enhanced risk scoring* to flag inconsistencies in an asset's background, such as undisclosed foreign affiliations or financial distress, which are key indicators for both vulnerability and potential deception. TrackLight's *Social Network Analysis (SNA) tool* identifies high-risk relationships and the strength of connections between entities. This would be critical for uncovering collusion or criminal networks that a person of interest might be attempting to conceal.

The *TrackLight co-pilot, Ray,* translates complex network graphs into actionable insights, helping analysts pinpoint the most influential or vulnerable individuals within a human network for potential recruitment or monitoring. For

counterespionage use, TrackLight monitors for *behavioral indicators of insider threats*, such as IP theft, espionage, or sabotage within an organization. Instead of conducting one-time background checks, analysts can better ensure the reliability of human sources by using TrackLight to *conduct continuous vetting*, providing real-time alerts if a monitored subject's status changes (e.g., experiences legal trouble or is involved in suspicious financial activity).

TrackLight's *FLEX AI Agents* can generate *automated briefings*, reducing the time needed to process and summarize complex background intelligence from 15 hours to 15 minutes, allowing case officers to spend more time on other tasks critical for managing HUMINT assets. Because TrackLight offers *traceability and auditability*, every discovery includes full source attribution, ensuring that intelligence gathered is defensible and suitable for use in formal legal or military briefings.

Neotas

What does Neotas do?

Neotas is a risk intelligence company that provides an AI-driven SaaS platform specialized in *Enhanced Due Diligence* (EDD) and *Third-Party Risk Management*. The Neotas platform is used for anti-money laundering (AML) and know your customer (KYC) checks, designed to uncover risks beyond traditional structured watchlists by *global risk screening*, searching over 1.8 billion court records, over 198 million corporate records, and over 40,000 media sources from more than 100 countries[80]. Neotas is designed to uncover hidden risks by analyzing data far beyond standard credit or background checks; it uses AI and OSINT to scan over 600 billion archived web pages, social media footprints, and deep/dark web sources[81]. Neotas claims that it is "ideal" for "high-risk onboarding, executive vetting, and integrity-sensitive roles"[82]. Neotas is primarily built for risk, compliance, legal, and procurement teams in high-stakes industries, including financial services (banks, hedge funds), government, security, and aerospace.

How could Neotas support HUMINT operations?

The Neotas platform could support Human Intelligence (HUMINT) operations by providing an advanced Open-Source Intelligence (OSINT) capability that validates, contextualizes, and protects human-centered activities. While Neotas was originally developed and primarily marketed for corporate and government due diligence, its technical capabilities align with the ODNI's 2024–2026 OSINT strategy to integrate OSINT into all-source analysis and operational tradecraft: The OSINT Strategy calls for embracing "new technologies and tradecraft to collect and evaluate open source data"[83].

Specifically, Neotas could be used for a number of core HUMINT functions, to include source asset validation and vetting, HUMINT targeting, operational security (OPSEC). It would also be useful for counterintelligence purposes.

HUMINT targeting. Neotas assists in the pre-contact phase of HUMINT operations by building a comprehensive profile of a target of interest. *Digital Footprint Mapping* uncovers hidden social media profiles and digital breadcrumbs that traditional search engines miss. *Relationship Discovery* maps personal and corporate networks to identify the best entry points, or intermediaries, for approaching a target. Finally, *Contextual Intelligence* gathers local jurisdictional data—such as court records and corporate filings—to understand the target's legal and financial pressures[84].

Asset validation and vetting. The Neotas platform could be used to access 600 billion archived web pages and over 40,000 media sources to verify a lead's (or source's) background and claims. It could also be used to identify hidden affiliations with foreign governments or criminal networks via graph-based network analysis. To ensure a source does not pose an internal threat, it could also be used to screen for extremist content, violent behavior, or anti-democratic sentiments in over 200 languages[85].

Cover identify validation. Neotas could also be used to verify that a HUMINT officer's

cover identity is robust and has no linkage to the officer's true identity[86].

SpiderFoot

What does SpiderFoot do?

SpiderFoot is an open-source automation tool designed for conducting OSINT to identify and analyze such targets as IP addresses, domain names, usernames, and email addresses across hundreds of data sources to uncover digital footprints. It maps potential security risks, breaches, and connections, making it widely used for cybersecurity reconnaissance and threat intelligence[87]. Two of the advantages of SpiderFoot is that it is a "free, open-source tool with a user-friendly interface"[88]. SpiderFoot does not require a login or subscription, which permits user anonymity[89]. Users should note that SpiderFoot is only available through GitHub. Ideally, SpiderFoot should not be downloaded directly onto a user's computer; instead, it would be preferable to user SpiderFoot in a virtual environment, such as Google Cloud Shell Editor[90].

How could SpiderFoot support HUMINT operations?

SpiderFoot could support HUMINT operations by automating the collection of OSINT and gathering information from publicly available sources. This information could then be used to create profiles of individuals or organizations. By automating the discovery of publicly available information, SpiderFoot can perform *entity mapping*, identifying a target's names, aliases, and usernames across multiple social media platforms, providing a map of their online presence and affiliations. SpiderFoot is also useful for determining the physical or virtual whereabouts of persons of interest by analyzing such available data points as IP addresses and domain registrations. SpiderFoot can generate graphic visualizations and maps that show how different publicly identified entities (people, emails, domains) relate to each other. This can help identify connections or publicly known relationships within a social or professional network[91].

WHAT CONCERNS MIGHT BE ASSOCIATED WITH USING AI-ENABLED PRODUCTS FOR HUMINT OPERATIONS?

Algorithmic bias

Common challenges for AI tools include *algorithmic bias* and *misinterpretation*[92]. Algorithmic bias refers to systematic and repeatable errors in how software identifies, collects, or interprets public data, leading to skewed or discriminatory intelligence outcomes[93]. If the underlying algorithms are biased, certain demographic or political groups may be disproportionately flagged, leading to unfair targeting or "moral erosion" in how HUMINT targeteers assess those groups.

Collection & selection bias

AI tools may prioritize sources from certain geographic regions, languages, or platforms (e.g., focusing only on English-language Twitter/X, while missing niche forums), leading to a tunnel vision effect.

Language and cultural biases

Natural Language Processing (NLP) models may struggle with slang, dialects, or cultural nuances, causing them to misinterpret sentiment or miss critical threats in non-Western contexts.

Confirmation bias

Algorithms often surface content that aligns with a user's previous search history or an analyst's working theory, reinforcing existing assumptions rather than providing a neutral view.

Automation bias

Another challenge is *automation bias*, which refers to an analyst's over-reliance on a tool's output without applying sufficient human judgement. Analysts *might simply accept* the AI platform's conclusions without engaging in critical thinking, which could lead to the unfair flagging of innocent individuals.

Tool and platform bias

"The tools we use to collect and analyse data are not neutral. Search engines, social media platforms, and scraping tools all apply filters, ranking algorithms, and personalisation — often without the user's awareness. This can prioritise

certain types of content and bury others, skewing the analyst's perception of what is prevalent or important"[94].

Invasive digital profiling

Maltego's ability to aggregate data from disparate sources—including social media, public records, and the dark web—could lead to invasive digital profiling. Even if data is public, its consolidation into a single visual map could conceivably infringe on an individual's expectation of privacy.

Warrantless surveillance

For Babel Street, the most significant ethical and legal concern involves **Locate X**. By purchasing commercial advertising ID (ADID) data, agencies have the ability to track a device's location history without a warrant. Critics argue this bypasses Fourth Amendment protections, as it allows for "warrantless surveillance" of individuals' movements over months, or even years.

Lack of transparency

Lack of transparency could be a problem if the AI were to flag an actual or potential human asset as high risk; it might be difficult for the analyst to determine exactly why that score was generated. This lack of explainability for an AI product could conceivably lead to unfair treatment or even the dismissal of a valuable source due to an algorithmic error. A third challenge for Babel Street users is that because Babel Street is a private vendor, its proprietary algorithms are often "black boxes." Unlike government-built systems, the internal logic of how Babel Street matches names or flags risks is not always available for public or judicial audit, making it difficult to defend its findings in court.

False positives

Another challenge is the possible misinterpretation of sarcasm, slang, or cultural nuances, leading to "false positives," where even advanced NLP can misconstrue something a person says on social media. "*False positives*" in a HUMINT context could conceivably lead to a recruited source being unfairly flagged and possibly even terminated[95].

Guilt by association

In social network analysis, false positives, or *guilt by association*, are possible; a person might be flagged by the system simply because they share a digital or professional connection with a bad actor, even if they have no knowledge of, or involvement in, illicit activity.

Vulnerability to deception

Nation state adversaries (such as the Russian Federation and the People's Republic of China) have moved beyond experimental programs and now can deploy autonomous AI agents capable of executing cyber espionage and massive cyber warfare campaigns[96]. They can also use AI-enabled systems to disseminate *AI-generated disinformation and deepfakes*[97]. According to the Atlantic Council's Digital Forensics Lab, Russia's *Pravda* network has published millions of articles in over 80 countries for the express purpose of influencing what AI tells its users[98]. Web crawlers ingest this material, and AI software encodes these narratives as knowledge. As a result, when users query AI, they do not receive actual "knowledge" because their AI software has been fooled into serving as an amplification vector for laundered propaganda[99].

HOW HAVE GOVERNMENT USERS MITIGATED THESE CONCERNS?

Government users mitigate the ethical and privacy risks of Babel Street through a combination of structured policy frameworks, technical controls, and human-in-the-loop validation. These measures aim to balance the desire for high-speed intelligence with the need to protect civil liberties.

Integrate tools into AI governance frameworks

Government users at the Department of Homeland Security (DHS) mitigate ethical concerns regarding TrackLight in HUMINT and investigative operations by integrating the platform into rigorous federal AI governance frameworks that prioritize human accountability and transparency[100].

Human-in-the-loop

Given the AI shortcomings mentioned in the previous section, Neotas notes that while "an intelligence cycle that combines Open-Source Intelligence (OSINT), Natural Language Processing (NLP), and human analytics is powerful…a full switch to AI might not be favorable"[101]. For this reason, Neotas notes that, "Decisions made using AI can be fully automated or involve a 'human in the loop' "[102]. In this way, AI augments – rather than replaces – human judgement and ensures ethical boundaries are respected and known AI shortcomings are mitigated.

In the U.S., government users often employ a human-centered approach, ensuring that AI never makes final decisions in high-stakes situations. In fact, DHS prohibits analysts from relying on AI outputs as the sole basis for law enforcement activities like arrests, searches, or the denial of benefits[103], and the Office of the Director of National Intelligence (ODNI), which manages the other 17 entities in the U.S. intelligence community, asserted that AI should "Incorporate human judgment and accountability at appropriate stages to address risks across the lifecycle of the AI and inform decisions appropriately"[104]. The TrackLight company itself acknowledges that they "have designed (their) tools to augment, not replace, human efforts," acknowledging that there are situations where AI "falls short," and where "technology alone simply isn't enough"[105].

Interpret behavioral cues

Fraud investigations often rely on detecting inconsistencies in interviews, body language, and interactions—things AI simply cannot process. For example, a trained investigator can spot hesitation or inconsistencies in an interview that an algorithm might miss.

Investigative anomalies

AI can detect anomalies, but it can't always determine why they're happening. Unlike AI, humans can provide context, apply intuition, and make judgments. For example, an AI system might flag an unusually high number of unemployment claims in one area, but only a human investigator can recognize that a local factory shut down, leading to a legitimate spike in claims.

Conduct investigations and interviews

Fraud isn't confined to digital footprints—site visits and in-person interviews remain vital in confirming suspicions and gathering additional evidence. For example, AI might flag a suspicious business address, but only an in-person visit can confirm whether it is a real storefront or an abandoned building.

Limit AI use to trained and certified users

In the U.S., intelligence services and federal, state, and local law enforcement organizations commonly limit the use of AI-enabled OSINT platforms to individuals who have been properly trained and certified in its use. For example, in the city of Seattle, Washington, the Seattle Police Department (SPD) requires that "all authorized users of Maltego must be CJIS certified and must maintain Washington State ACCESS certification and trained directly in the use of the Maltego software, in addition to all standard SPD training and Directives"[106]. The SPD uses Maltego "to assist Seattle Police Department (SPD) to research publicly available data and diagram associations between individuals, devices, and networks"[107]. In the SPD, use of Maltego is limited to two users in the SPD's Technical and Electronic Support Unit, or TESU, who are "SPD's only trained and authorized users of Maltego"[108]. These authorized users are certified by the Criminal Justice Information Services (CJIS) and maintain Washington State ACCESS (A Centralized Computerized Enforcement Service System) certification[109]. To mitigate ethical risks, law enforcement agencies employ a combination of rigorous training, technical guardrails, and formalized investigative protocols to ensure that tools like Maltego are used within the bounds of law and human rights.

Require a "need to know" for data access

Tools like Babel Street Analytics use granular "atomization" of data, allowing only authorized personnel to view specific elements of information based on their role and security clearance. High-side classified platforms maintain robust activity tracking and auditing features to ensure transparency and accountability for every search performed.

Employ structured analytic techniques

To counter these risks, investigators can use Structured Analytic Techniques (SATs) to challenge their own findings, diversify their toolsets to avoid single-platform bias, and maintain a human-in-the-loop approach where AI recommendations are always manually verified[110]. "Structured Analytic Techniques are proven tools to help analysts explore alternative explanations, test assumptions, and reduce cognitive traps"[111].

CONCLUSIONS

AI may never reach the point where it can fully replicate human cognition and demonstrate the kind of interpersonal skills necessary for the human-to-human interactions that are so critical to HUMINT. However, AI platforms can serve as a force multiplier, helping case officers perform certain tasks in the human intelligence operations cycle more completely and rapidly than in the past. Through this contribution, AI enables case officers to shift their focus and energies to other high-priority HUMINT tasks that require interpersonal skills. The rise of digital case officers, made possibly by AI, represents a new and intriguing approach to conducting the world's second-oldest profession.

[1] NATO Industry Forum 2025, Bucharest, 6 November 2025, *Romania Journal*; https://www.romaniajournal.ro/politics/nato-industry-forum-2025-bucharest/

[2] EU AI Act: first regulation on artificial intelligence, 19 February 2025, European Parliament, https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

[3] Stefano Lovi, "How Disinformation Can Influence a Nation: The Case of Romania", *Studia i Analizy Nauk o Polityce*, no.1, Lublin, 2025, pp. 27-44.

[4] Adrian A. Hopgood, *Intelligent Systems for Engineers and Scientists*, Boca Raton, CRC Press, 2021.

[5] *Ibidem.*

[6] Too much data, too few analysts: How AI offers a 'force multiplier' for intelligence analysts, *DefenseScoop*, 12 November 2025; https://defensescoop.com/2025/11/12/too-much-data-too-few-analysts-how-ai-offers-a-force-multiplier-for-intelligence- analysts/

[7] Shaun Waterman, "Can AI help targeteers curb civilian casualties?", *Air & Space Forces*, 11 August 2025; https://www.airandspaceforces.com/can-ai-help-targeteers-curb-civilian-casualties/

[8] Yashwant A. Waykar and Sucheta Yambal, *AI and Geospatial Intelligence: Unlocking New Possibilities for the Future*, IGI Global, DOI: 10.4018/979-8-3693-8104-5.ch001.

[9] Htein Win, "Psychological dynamics of trust and deception in HUMINT: Balancing 'need to know' and 'right to know' in security information management", *Security and Intelligence*, 2025, pp. 1-27.

[10] Michael DeBolt, "Gaining the intelligence advantage with cyber HUMINT – Part one," *Intel471*, 14 May 2023; https://www.intel471.com/blog/gaining-the-intelligence-advantage-with-cyber-humint-part-one

[11] Kiran Krishnamurthy, "The evolution of HUMINT in the digital era", *Karve International*, 25 June 2024; https://www.karveinternational.com/insights/does-ai-signify-the-end-of-humint-as-we-know-it.

[12] Mykhailo Zhylin, Viktoriia Mendelo, Yuliia Chumaieva, Andrey Kernas, Yevhen Zaporozhtsev, "Analysis of contemporary methods of integrating emotional intelligence into artificial intelligence systems: Advantages, disadvantages, and perspectives", *Journal of Theoretical and Applied Information Technology*, vol. 102, no. 7, 2024, p. 2842 – 2853.

[13] Ylli Bajraktari, "The digital case officer: How AI is poised to transform espionage," *SCSP*, 29 October 2025; https://scsp222.substack.com/p/the-digital-case-officer-how-ai-is

[14] *Ibidem.*

[15] Jennifer Ewbank, *The role of artificial intelligence in the U.S. Intelligence Community: Current uses and future developments,* The Aspen Institute, 2024, 3 p.

[16] Ylli Bajraktari, *Op.cit.*

[17] Henan Flores and Andrea Luna, "AI for Psychological Profiles: Advances, Challenges, and Future Directions", *Ciencia Latina. Revista Cientifica Multidisciplinar*, vol. 8, no. 3, May-June 2024, pp. 10592-10609.

[18] Yuma Heymans, "Recruitment intelligence: Modern AI techniques to find the top 1% talent", *HeroHunt*, 22 September 2025; https://www.herohunt.ai/blog/recruitment-intelligence-modern-ai-techniques-to-find-the-top-1-talent

[19] *Ibidem.*

[20] "Here's what you need to know about propensity modeling," *Medium*, 28 August 2018; https://medium.com/the-official-integrate-ai-blog/heres-what-you-need-to-know-about-propensity-modeling-521ab660cb43

[21] Edward Wong, "How China uses LinkedIn to recruit spies abroad", *The New York Times*, 27 August 2019; https://www.nytimes.com/2019/08/27/world/asia/china-linkedin-spies.html

[22] *Ibidem.*

[23] Jeff Stone, "LinkedIn is becoming China's go-to platform for recruiting foreign spies", *CyberScoop*, March 26, 2019; https://cyberscoop.com/linkedin-china-spies-kevin-mallory-ron-hansen/

[24] Raymond Dennis, "Keep your friends close and your enemies closer? Not in cyberspace", U.S. Naval Institute, *Proceedings*, vol. 145, no.11, november 2019; https://www.usni.org/magazines/proceedings/2019/november/keep-your-friends-close-and-your-enemies-closer-not-cyberspace.

[25] *Ibidem.*

[26] Michael DeBolt, "Gaining the intelligence advantage with cyber HUMINT – Part one," *Intel471*, 14 May 2023; https://www.intel471.com/blog/gaining-the-intelligence-advantage-with-cyber-humint-part-one

[27] *Idem*., "What is cyber HUMINT?", *Authentic8*, 12 November 2025; https://youtu.be/reBbJBNSuCA?si=pUHp5LvmeZRrlLcp

[28] *Ibidem.*

[29] Antonio Teti, "From HUMINT to virtual HUMINT", *Cyber Defense*, 7 February 2019; https://www.cyberdefensemagazine.com/from-humint-to-virtual-humint/

[30] *Ibidem.*

[31] *Ibidem.*

[32] Vikas Chauhan, "Behind the digital curtain: Exposing the hidden world of sock puppets in cyber intelligence", *Medium*, 23 May 2024; https://osintteam.blog/behind-the-digital-curtain-exposing-the-hidden-world-of-sock-puppets-in-cyber-intelligence-f0ec94740f58

[33] *Ibidem.*

[34] Rob Porter, "How AI is shaping the future of corporate training in 2025", *Training Industry*, 18 February 2025; https://trainingindustry.com/articles/artificial-intelligence/how-ai-is-shaping-the-future-of-corporate-training-in-2025/#:~:text=For%20example%2C%20in%20the%20public,roles%20in%20safeguarding%20public%20health.

[35] *Ibidem..*

[36] Ylli Bajraktari, *Op.cit.*

[37] *Ibidem.*

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

[39] F. 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

[40] *Ibidem.*

[41] *Ibidem.*

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

[43] Hoffman, *Op.cit.*

[44] *Ibidem.*

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

[46] Hoffman, *Op.cit.*

[47] *Ibidem.*

[48] *Ibidem.*

[49] Practitioner Committee, "OSINT collection methodologies", *OSINT Foundation*, 20 November 2023, p. 2; https://www.osintfoundation.com/NewsBot.asp?MODE=VIEW&ID=31734.

[50] Fred Hoffman and Brian Fuller, "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.

[51] Richmond Thomason (ed.), *Philosophical Logic and Artificial Intelligence*, Springer, Klüver Academic Publisher, 1989; see also 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.

[52] Ralph H. Pherson and Richard J. Heuer, *Structured analytic techniques for intelligence analysis*, CQ Press, 2019, p. 21.

[53] Bjorn Gunnar Isaksen and 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.

[54] *Ibidem.*, p. 1.

[55] Jeffrey A. Friedman and Richard Zeckhauser, "Assessing Uncertainty in Intelligence", *Intelligence and National Security*, vol. 27, no. 6, 2012, pp. 824-847; DOI: 10.1080/02684527.2012.708275.

[56] "Link analysis software – Maltego", *Seattle Police Department*, 2021, p. 6.

[57] "7 top OSINT software tools", *Liferaft*, 17 January 2023; https://liferaftlabs.com/blog/7-top-osint-software-tools.

[58] "Link analysis software – Maltego," *Seattle Police Department*, 2021, p. 6.

[59] Maltego, "Monitor social media in real-time with AI-driven analysis of massive data volumes", *Maltego*, https://www.maltego.com/

[60] Maltego Monitor, https://www.maltego.com/monitor/

[61] "From data to intelligence – in minutes", *Maltego*, https://www.maltego.com/

[62] Babel Street, https://www.babelstreet.com/

[63] Babel Street, https://www.babelstreet.com/babel-street-insights.

[64] Andrew Alach, Three Guiding Principles for the Development of OSINT Agentic Systems, *Babel Street*, 2025; https://www.babelstreet.com/blog/designing-trustworthy-ai-for-osint?utm_source=google.com&utm_medium=Organic+Search&utm_campaign=Not+Provided.

[65] NativeScript is a framework for building truly native mobile apps with JavaScript/TypeScript, letting you access device APIs directly, while Babel Street itself is an AI-powered intelligence platform that uses advanced NLP and entity resolution to analyze massive, multilingual global data for risk, identity, and threat intelligence.

[66] "Name Match (RNI-RNT)", *Babel Street*; https://docs.babelstreet.com/Identity/en/name-match--rni-rnt-.html#-130544

[67] Harris Kevin, "Insights APIs connect any application with Babel Street's enhanced PAI", *Babel Street*, 2025.
https://www.babelstreet.com/blog/new-insight-apis-connect-any-application-with-babel-streets-enhanced-pai?utm_source=google.com&utm_medium=Organic+Search&utm_campaign=Not+Provided.

[68] Lexi Bowen, "Shielded online: How managed attribution empowers trust & safety teams", *Babel Street*.

[69] *Ibidem.*

[70] "FAQs", *Blackdot Solutions*, 2026, https://blackdotsolutions.com/faq.

[71] "Transform investigations with the power of AI", *Blackdot Solutions*, 2026; https://blackdotsolutions.com/blackdot-solutions-videris-automate.

[72] "Illuminate intelligence in open source data," *Blackdot Solutions*, 2026; https://blackdotsolutions.com/

[73] "Transform investigations with the power of AI," *Blackdot Solutions*, 2026; https://blackdotsolutions.com/blackdot-solutions-videris-automate.

[74] *Ibidem.*

[75] *Ibidem.*

[76] Stuart Clarke, "6 ways Videris augments your investigations", *Blackdot Solutions*, 2026; https://blackdotsolutions.com/blog/how-videris-augments-investigations.

[77] "Public sector OSINT solution", *Blackdot Solutions*, 2026; https://blackdotsolutions.com/public-sector.

[78] "Introducing TrackLight FLEX: Prevent, Monitor, and Manage Fraud with AI Agents", *TrackLight*, https://TrackLight/

[79] "TrackLight Raises $3M in Funding to Empower Government Agencies and Enterprises with an AI-Driven Fraud Prevention Solution; Launches AI Co-Pilot Ray the Parrot", TrackLight; https://TrackLight/news/tracklight-raises-3m-in-funding-to-empower-government-agencies-and-enterprises-with-an-ai-driven-fraud-prevention-solution-launches-ai-co-pilot-ray-the-parrot/

[80] "AML checks – Anti-money laundering regulations for identity assessment and verification process", *Neotas*, 2026; https://www.neotas.com/aml-checks/

[81] "About Neotas", *Neotas*, 2026; https://www.neotas.com/about-us/

[82] *Ibidem.*

[83] "The IC OSINT Strategy, 2024-2026", *Office of the Director of National Intelligence*, 2024, p. 2; https://www.dni.gov/files/ODNI/documents/IC_OSINT_Strategy.pdf

[84] "Smarter risk insights, faster decisions", *Neotas*, 2026; https://www.neotas.com/

[85] *Ibidem.*

[86] "OSINT background check", *Neotas*, 2026; https://www.neotas.com/why-are-neotas-expert-background-checks-different/

[87] Priscilla Pereira and others, "OSINT toolkit: SpiderFoot, a cyber-focused GitHub tool that automates data collection and maps digital footprints", *The Counterterrorism Group*, 15 April 2025; https://www.counterterrorismgroup.com/post/osint-toolkit-spiderfoot-a-cyber-focused-github-tool-that-automates-data-collection-and-maps-digit#:~:text=SpiderFoot%20is%20an%20OSINT%20tool,map%20a%20target's%20digital%20footprint.

[88] *Ibidem.*

[89] *Ibidem.*

[90] *Ibidem.*

[91] *Ibidem.*

[92] "Putting the 'intelligence' back into AI", *Neotas*, 2026; https://www.neotas.com/putting-the-intelligence-back-into-ai/

[93] "Strategies to defense against AI algorithmic bias," *Blue Ridge Risk Partners*, 11 April 2024; https://www.

blueridgeriskpartners.com/blog/strategies-to-defend-against-ai-algorithmic-bias .

[94] Daniel Collyer, "Seeing clearly: Understanding and addressing bias in OSINT", *SOS Intelligence*, 7 May 2025; https://sosintel.co.uk/seeing-clearly-understanding-and-addressing-bias-in-osint/

[95] Joseph Fitsanakis, "Spy agencies must regulate ethics of manipulation in HUMINT, researcher argues", *IntelNews.org*, 7 November 2022; https://intelnews.org/2022/11/07/01-3231/

[96] Turkel Nury, "The First Large-Scale Cyberattack by AI", *The Wall Street Journal*, 23 November 2025; https://www.wsj.com/opinion/the-first-large-scale-cyberattack-by-ai-4a1e1a30.

[97] "OSINT in 2026: Key trends and what to expect", *Blackdot Solutions*, 2026.

[98] "Research," DFRLab, 2026, https://dfrlab.org/research/

[99] "Research," DFRLab, 2026, https://dfrlab.org/research/

[100] "Ensuring AI is used responsibly", *Department of Homeland Security*, 29 September 2025; https://www.dhs.gov/ai/ensuring-ai-is-used-responsibly#:~:text=Directive%20139%2D08%20sets%20forth,systems%20to%20meet%20performance%20goals.

[101] "Putting the 'intelligence' back into AI", *Neotas*, 2026; https://www.neotas.com/putting-the-intelligence-back-into-ai/

[102] "Regulatory compliance in digital screening", *Neotas*, 2026; https://www.neotas.com/regulatory-compliance-in-digital-screening/

[103] *Ibidem*

[104] "Artificial intelligence ethics framework for the intelligence community", *Intelligence.gov*, June 2020; https://www.intelligence.gov/ai/ai-ethics-framework#:~:text=AI%20should:,identify%20issues%20for%20resolution;%20and%2C

[105] "TrackLight's approach: The best of both worlds", *Tracklight*, 2024; https://blog.TrackLight/blog/what-ai-cant-solve-in-fraud-detection-and-why-humans-still-matter#:~:text=TrackLight%20solutions%20are%20built%20by,at%20investigating%20and%20mitigating%20fraud.%22

[106] *Ibidem*., p. 8.

[107] "Link analysis software – Maltego", *Seattle Police Department*, 2021, p. 5.

[108] *Ibidem*., p. 7.

[109] *Ibidem.*

[110] Daniel Collyer, "Seeing clearly: Understanding and addressing bias in OSINT", *SOS Intelligence*, 7 M ay 2025; https://sosintel.co.uk/seeing-clearly-understanding-and-addressing-bias-in-osint/

[111] *Ibidem.*