Anul XVII nr. 1/2025

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

Direcția Generală de Informații a Apărării

CUPRINS

PERSPECTIVE GEOPOLITICE ȘI GEOSTRATEGICE

RĂZBOAIELE SECOLULUI XXI

SECURITATE ȘI TEHNOLOGII EMERGENTE

INTELLIGENCE

PREMISE ȘI PRELIMINARII LA NOUA DOCTRINĂ TRUMP

Iulian CHIFU*

Abstract

The new mandate of President Trump begins with an important change in spin, force and planning comparing to the first one. If we could have talked about a pragmatic realism in the first term, the premises and preliminaries of a Trump Doctrine 2.0. lean more on the concept of peace/negotiations through strength and divisive negotiations than integrative negotiations, multilateralism and understanding of the interdependences of trade, politics and security bases, at the global level.

Fighting globalism with ideology and decoupling could be harmful on the long run, if "America First" means ignoring the interests of potential allies in the days before a possible global war outbreak. America might be made Great Again only if other international actors are on board and their own interests are observed and respected, especially when it is not about big players, but about allies and partners.

Keywords: *peace through strength; pragmatic realism; transactionalism; divisive negotiations; unilateral symbolic victory.*

INTRODUCERE

A discuta despre cum va arăta o doctrină "Trump 2.0." pare prematur având în vedere timpul scurt scurs de la preluarea mandatului de președinte de către Donald Trump. Totuși, bogăția de acte executive, exprimări și poziții publice conturează deja trăsăturile noii Administrații Trump și abordările sale, principalele caracteristici ce pot fi plasate sub semnul premiselor și preliminariilor, urmând ca adaptarea la lumea turbulentă în evoluție și schimbare să determine ajustări, reveniri, rescrieri și, cel mai probabil, teme și termene de aplicare a unei baze ideatice atât de largi.

Am avut ocazia de a studia și scrie pe îndelete despre mandatul Trump în lumina unei abordări a realismului pragmatic[1] și în siajul unor gânditori, autori și practicieni care coboară până în timpul președintelui Ronald Reagan, influență asumată de D.Trump în primul mandat. Apoi, influențe de continuitate ale politicii neoconservatoare a lui George Bush Jr. și neoconservatorilor americani (a se vedea întreaga pleiadă de teorii aparținând lui Robert Kagan, teoretician și apărător al curentului). De exemplu, R.Kagan abordează postura de hiperputere a SUA și aparenta ruptură din interiorul Occidentului[2] de pe pozițiile criticismului la adresa europenilor, o postură îmbrățișată de către Donald Trump în primul mandat la Casa Albă[3]. Dacă neoconservatorii au păstrat principiile și valorile comune, cu accent pe importanța și necesitatea NATO, precum și a relațiilor transatlantice[4], Kagan introduce și

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

tema unei lipse de respect și recunoaștere față de puterea americană, punând în discuție postura și rolul SUA în lume[5].

Pe dimensiunile populismului și naționalismului, devine relevant studiul lui Francis Fukuyama despre identitate, politici identitare contemporane, dorința de demnitate și lupta pentru recunoaștere[6], deși autorul nu are neapărat curajul să meargă și să identifice radicalismele liberal-democratice, de natură progresistă, care generează crizele identitare contemporane și fac loc politicilor identitare cu tendințe naționaliste, pe scară largă. În schimb, Fukuyama sesizează corect nevoia de identitate individuală și de identitate de grup, care este inerent legată de ființa umană și explicabilă psihologic, dar și istoric, cu nevoia profundă de a avea rădăcini, de a veni de undeva, de a crea o continuitate/ legătură cu trecutul[7]. Triada identitate - demnitate - respect este baza mecanismului care generează interesul general pentru participare, chiar neprofesionistă, la decizii, precum și apetitul pentru lideri mesianici, care discută direct cu poporul, ne spune Fukuyama.

Pentru a putea aduce în prim-plan analiza doctrinei Trump 2.0. am utilizat cadrul pe care l-am mai aplicat o dată, chiar în paginile acestei reviste, față de doctrina Trump originară, din primul mandat[8]. Apoi am analizat declarațiile de campanie și pe cele de la preluarea mandatului (primele discursuri publice în calitate de președinte, postările pe *Truth Social* și pe rețelele sociale). Am luat în considerare și declarațiile și răspunsurile din audierile de confirmare și pozițiile membrilor echipei Trump (de la Secretarul de Stat, Marco Rubio, și cel al Pentagonului, Pete Hegseth, la consilierul pentru securitate națională și șeful desemnat al CIA, ca și la alți membri implicați în politica externă, de securitate și apărare[9]).

Analiza vizează și literatura de specialitate deja publicată, organizată pe câteva teme pe care le-am considerat relevante, introduse și de adepții președintelui, de analiștii independenți, dar și de criticii actualului președinte american: Trump și naționalismul, Trump și oligarhia, Trump și libertarianismul, Trump și tranzacționalismul, elementele teoretice și practice din toată sfera conceptelor de negociere, pace, presiune cu forța/ în forță, prin forță, doctrina Monroe (amintită ca referențial pentru retragerea SUA din lume), dar și temele surprizei, impredictibilității (alții o numesc chiar *bullying* sau *Mad Man Theory*/ Teoria Omului Nebun), respectiv postura împrumutată pentru jocul de actor, comunicator și personaj histrionic a lui Donald Trump.

Desigur, nu puteam evita temele legate de politica de putere și cea de Mare Putere, teme studiate deja în contextul primului mandat Trump[10], dar cu impact sporit în cel de-al doilea mandat. Am adăugat și pozițiile Administrației Trump din primul mandat, precum și din cel curent, pe teme precum globalizarea sau naționalismul economic (de la obsesia echilibrării schimburilor de mărfuri și a balanței de plăți până la securitatea și securizarea lanțurilor de producție). Desigur, personalitatea histrionică a lui Donald Trump și interesul său pentru imagine au justificat și analiza acelor elemente de detaliu, de tipul elementelor de comunicare publică (pronunțări mai apăsate, vocabular direct și dur[11]), în raport cu evoluțiile curente[12].

DE LA REALISM PRAGMATIC LA TRANZACȚIONALISM ȘI NEGOCIERI CU SUMĂ NULĂ

Realismul pragmatic din primul mandat Trump a fost decantat, la acea vreme, pe baza evaluării unui număr semnificativ de documente definitorii, cu precădere cele două discursuri la ONU[13] și Strategia de Securitate Națională a SUA[14], dar și prin identificarea de elemente specifice[15] în acțiunile administrației, respectiv în deciziile concrete în relațiile cu Arabia Saudită, poziția față de combaterea terorismului, mutarea ambasadei SUA la Ierusalim și strategia privind Afganistanul[16].

Conceptul a fost determinat de limitarea realismului clasic, prin motivații morale, la ideile lui James Madison (1751-1836)[17] și adăugarea elementelor statului de drept la nivel global (respectiv nevoia extinderii justiției în lume) la Teddy Roosevelt (1858-1919), plus elementele

neoconservatoare ale exportului de democrație în lume și justificarea, astfel, a intervenționismului american. Putem realiza lesne, astăzi, elementele care disociază finalul de mandat Trump 1.0 și începutul celui curent de realismul principial clasic[18] și nuanțele introduse de accentul pronunțat pe interese naționale[19]. În niciun caz nu este vorba despre vreo apropiere cu înțelesurile date de echipa Trump realismului principial.

Am descoperit, firește[20], că sursa reală este Jeane J. Kirkpatrick,[21] în scrierile din 1980, prin ideile legate de **politica în forță**, respingerea destinderii și dorința de a câștiga Războiul Rece, rezistență în asumarea responsabilităților globale, dar și îmbrățișarea fundamentelor democrației liberale și a lumii bazate pe reguli și drepturile omului[22] (acestea din urmă lipsind astăzi din limbajul actualei Administrații Trump). Aduceam atunci ca argumente criticile lui Trump de la tribuna ONU[23] și multe elemente de putere și drept natural, îmbrățișate de către președintele american[24].

În evaluarea modului în care s-a transformat Doctrina Trump, în noul mandat, avem elemente de noutate care se regăsesc în discursurile din timpul campaniei electorale, atunci când a abordat teme de politică externă, securitate și apărare. Iar comentariile și analizele la zi ale profesioniștilor în relații internaționale și studii de securitate din Statele Unite sunt edificatoare în legătură cu aceste **schimbări tectonice**, dramatice. Chiar dacă analiza acestora poate fi lesne pusă pe seama unor eventuale influențe resimțite în plan personal (fapt ce ar putea justifica și limbajul folosit, care uneori atinge diatribe deranjante pentru spațiul tradițional al analizei științifice), logica și argumentele sunt corecte.

POSIBILE EFECTE ALE POLITICII DE MARE PUTERE

Principala caracteristică identificată în politica lui Donald Trump, chiar nedeclarată ca atare, este abandonarea lumii bazate pe reguli și înclinația de a îmbrățișa **revenirea la politica de putere**[25] și **politica de Mare Putere**[26]. Prima se referă la utilizarea forței, amenințarea cu utilizarea forței și exercitarea de constrângeri de toate tipurile pentru a atinge obiectivele de politică externă, iar cea de-a doua la „**marile înțelegeri”**[27] pe seama statelor mai mici și înclinația spre recrearea sferelor de influență. Tot aici se adaugă o revenire la naționalism, cu precădere la naționalismul economic, dar și la confruntările directe dintre marile puteri, evitate aproape complet după cel de-al Doilea Război Mondial.

Contestarea ordinii mondiale, pe motiv că nu mai servește intereselor Statelor Unite, a început în primul mandat Trump, dar cu mai puțină vigoare și mai degrabă pe tonul unor ajustări decât revoluții sau chiar distrugeri globale. Heterodoxia lui Trump și **distrugerea Pax Americana** se face pe considerentele președintelui că ordinea mondială actuală ar dezavantaja SUA, împinsă în rolul de polițist global, și ar permite aliaților să fugă de responsabilitățile propriei apărări[28]. Iar verdictul l-a dat Secretarul de Stat Marco Rubio, în audierea sa din Congres: „Ordinea globală post-război este depășită. A devenit azi o armă utilizată împotriva noastră”[29].

Aceste afirmații marchează revizionismul Administrației Trump 2.0. – tendință susținută și de Rusia și China de ani de zile, din cu totul alte motive, respectiv ambițiile geopolitice proprii și dorințele de dominație și restabilire a sferelor de influență sau de interese privilegiate – o gură de aer ce a justificat susținerea actualului președinte în alegeri. Revenirea la politicile de putere specifice secolului al 19-lea sau la sferele de influență adjudecate în timpul Războiului Rece este întărită de politica de putere asumată prin **impunerea păcii în forță sau cu forța**[30] (anunțată și practicată deja de Donald Trump), prin anunțurile și acțiunile care vizează obținerea supremației în imediata vecinătate (referințele la Panama, Mexic, Canada, Groenlanda[31]) și prin abordarea dominației în locul diplomației, din cauza impulsivității[32] și a temperamentului președintelui american, înclinat către tranșarea rapidă a temelor/ situațiilor complexe și dificile (varianta tăierii „nodului gordian”)[33].

Realismul actualei administrații este de netăgăduit odată ce renunță la partea pozitivă adusă lumii de Pax Americana – descurajarea comunismului, îndiguirea URSS și a regimului său, prosperitate globală fără precedent și pace relativă. Războaiele din Afganistan și Irak, precum și umilințele retragerii și risipirii unor investiții enorme în aceste operațiuni bipartizane au contat enorm. Revenirea la Tucidide și la lumea în care „*cel puternic face ceea ce vrea și cel slab suferă ceea ce trebuie să îndure*" este o altă notă a realismului dur și pur al lui Trump[34]. Diferența este că, astăzi, competiția între marile puteri a revenit în prim-plan, iar războiul între puteri majore comparabile, precum SUA și China, este tot mai probabil[35], de unde nevoia de a reîntări relațiile de importanță strategică existente și de a construi altele noi în regiunile cu relevanță pentru Statele Unite și care amenință să explodeze în confruntarea Marilor Puteri. De unde și nevoia reechilibrării obiectivelor economice, care au ocupat agenda politică în primele săptămâni ale Administrației Trump, cu cele de securitate și **maximizare de putere**.

Totuși, ipoteticele „**mari înțelegeri**", cum ar fi cea cu China, prin care Trump ar propune cedarea predominanței către Beijing în Asia (inclusiv asupra Taiwanului), și cea cu Rusia, prin care oferă o Ucrainăă demilitarizată și fără garanții de securitate pe viitor, sunt considerate improbabile[36], pentru că ar echivala cu un semn de slăbiciune sau chiar de recunoaștere a unei înfrângeri din partea președintelui american, fapt inacceptabil și de neconceput. Nici perspectiva sferelor de influență în Asia și Europa nu există, chiar dacă mecanismul de constrângere a lui Trump va genera mai multă asumare de către aliații europeni și asiatici a propriei apărări; astfel, pasul unei echilibrări de costuri nu se va face prin abandonarea fără apărare, pe termen scurt, a acestor regiuni de interes strategic și pentru viitor.

Însă, tentația utilizării forței și agresiunii asupra vecinilor, impunitatea beligeranților împotriva civililor și legea celui mai puternic vor fi prezente[37], ca și instabilitatea și impredictibilitatea globală. Așa cum nici scenariile extreme, precum războiul în Asia sau războiul revenit în Europa, nu pot fi excluse[38].

Realismul dur este confirmat prin maniera tranzacționistă în care Trump abordează soluționarea problemelor politico-diplomatice; această modalitate preferată de negociere este descrisă pe larg în cartea sa, *The Art of the Deal („Arta unei înțelegeri")*, acolo unde „inexplicabilitatea distructivă a proceselor de negociere"[39] este explicată prin recursul la „*distributive bargaining*", succesul fiind cel al învingătorului în fața înfrântului, și nu varianta negocierilor integrative, de tip *win-win*. Asistăm acum la o revenire strictă la jocurile de sumă nulă. La capitolul tranzacționism, este relevantă referirea președintelui Trump la o posibilă înțelegere vizând exploatarea resurselor de metale rare ale Ucrainei de către SUA contra asigurării securității și apărării acestui stat în fața Rusiei lui Putin[40].

Revenirea lumii la naționalism a devenit o tendință evidentă după criza financiară globală din 2008 și criza datoriilor suverane din Europa[41], tendință care s-a accentuat după pandemie și expunerea dificultăților și limitelor comerțului liber global, precum și a amenințărilor la adresa lanțurilor de furnizori de produse strategice. Noua eră naționalistă poate fi definită prin creșterea **preeminenței securității față de economie**[42] și nevoia de balansare între obiective contradictorii și în conflicte de valori economice și de securitate, teme pe care noua Administrație Trump 2.0. trebuie să le decanteze și să le învețe.

Competiția dintre Marile Puteri se manifestă cu preponderență pe palierele politico-strategic și economic. În perioada primului mandat Trump abordările economice au fost axate pe crearea de formule de îndiguire *soft*, pe principiile echilibrului de putere din partea aliaților, și au avut drept rezultat privarea administrației americane de posibilitatea construcției propriei coaliții pentru redesenarea unei viitoare ordini globale în competiția cu China și formulele sale de organisme internaționale ce acoperă Sudul Global și țările în curs de dezvoltare, cu influență preponderent economică, dar insidios militară în subtext[43].

Donald Trump dorește să se impună ca un **lider care a schimbat istoria**, pe modelul foștilor președinți – Franklin W. Roosevelt (care a redefinit rolul guvernului) și Ronald Reagan (care a luat măsuri pentru maximizarea puterii economice și militare a Statelor Unite, fapt ce a înclinat balanța în favoarea Washingtonului la finalul Războiului Rece, copleșind dușmanul în spirala înarmării). În momentul de față (februarie a.c.), politica Administrației Trump este, încă, contradictorie, iar echilibrele sunt de regăsit, fiind evident faptul că la vârful ierarhiei se află o persoană căreia îi place să experimenteze, care lansează teme disruptive pentru a obliga propria administrație și terțe state să gândească critic sau neconvențional (”out of the box”) și să întrerupă ritmul blocant al soluțiilor ineficiente la conflictele sau temele politice mari[44]. **Guvernarea prin criză**, pentru a obliga la soluții novatoare, pare să fie formula preferată. Din nou, această abordare nu este altceva decât un recurs la tăierea „nodului gordian”, ca soluție tranșantă și radicală a forței ce ocolește diplomația.

Cu toate acestea, regulile relațiilor internaționale se aplică, în cele din urmă, și „uraganului” Trump, iar politicile sale asertive au efecte secundare relevante. Pentru că politica de putere și politica de „mare putere” dau naștere, automat, la abordări de reechilibrare, respectiv **echilibrul de putere** și **balanța amenințărilor**, care presupun asocierea statelor sub presiune pentru a îndigui recalcitrantul din sistem, mai direct și dur sau mai *soft*, vezi varianta formatului BRICS extins, în primul caz, sau relația strategică China-Rusia versus acțiunile *soft* ale aliaților europeni și asiatici în primul mandat Trump.

Iar acest drum competițional/ confruntațional se manifestă mai ales când dispare elementul de atractivitate din politica „bunurilor comune globale”, apărate multilateral de toate statele (și întărită de SUA), și apare tentația părăsirii organizațiilor internaționale (pe motiv că limitează manifestarea politicii de putere, în mod individual, a actorilor). Și dacă Beijingul și Moscova nu au făcut-o până acum din cauza costurilor de imagine, pașii lui Donald Trump amenință să deschidă „cutia Pandorei” și în această direcție[45].

Atitudinea majorității statelor lumii, după Războiul Rece, de a se alinia la politica/ viziunea SUA și de a îmbrățișa valori comune[46] a fost contestată de unele puteri regionale și numită chiar o anomalie a politicilor globale. Încercările de balansare post-Război Rece, de până astăzi, au fost limitate și regionale, de exemplu Iranul și „axa rezistenței” în Orientul Mijlociu (mai ales post-Irak și Afghanistan) sau politicile economice antiamericane ale BRICS. În ceea ce-i privește pe vecinii direcți ai SUA, recentele politici de control lansate de D.Trump ar putea avea efecte contrare pentru interesele americane, de tipul tendinței de a rezista actualei administrații sau coalizării pentru blocarea acțiunilor distructive, chiar în cadrul spațiului occidental.

CONCLUZII PRELIMINARE PRIVIND DOCTRINA TRUMP

Din start trebuie precizat că am utilizat/ studiat în acest articol doar marile tendințe identificate la nivel global referitoare la doctrina „Trump 2.0”. De altfel, am avut la dispoziție doar elementele incipiente din primele săptămâni, nicidecum o perioadă substanțială de mandat și o administrație așezată, ale cărei politici ar fi fost predictibile, lesne de anticipat. Lipsesc din enumerarea de până acum abordări mai mult sau mai puțin partizane, la nivelul oponenților politici sau al unor analiști/ editorialiști, care vin, totuși, cu argumente importante, care merită menționate într-o dezbatere despre preliminariile la doctrina „Trump 2.0”. Până acum, unilateralismul agresiv și tentația de *bullying* și constrângere la nivel global sunt principalele elemente subliniate în analizele criticilor asumați ai lui Donald Trump.

Testul de stres pe care-l aplică lumii Donald Trump, cu instrumente de tip *bullying* și constrângeri pe baza amenințării cu taxe, tarife și sancțiuni, precum și tranzacționalismul *quid pro quo*, riscă să creeze probleme pe termen mediu și lung, chiar dacă, aparent, satisface nevoia de victorie clamată imediat, ca și de îndeplinire a promisiunilor făcute de către președinte și administrația sa[47]. Abordările tranzacționale și unilaterale ale lui Trump, în afara instituțiilor

internaționale, sunt de asemenea semnale ale politicii de putere *sic volo*, ca și recursul la amenințări formulate bombastic și referiri directe la preluare, cucerire și achiziție de diferite teritorii – de la Canada al 51-lea stat, Groenlanda de cumpărat, Canalul Panama de luat înapoi (prin denunțarea tratatului prin care a fost transferat noului stat) și Fâșia Gaza de preluat și transformat în Riviera Mediteranei de Est.

Nu lipsită de interes este și ideea legată de o revenire la o agendă de politică externă expansionistă – cu utilizarea constrângerilor economice sau a forței militare pentru cucerirea de noi teritorii – acțiune care contrazice retragerea în problemele interne, izolaționism sau o reformulare a Doctrinei Monroe (cu controlul regional în cele două Americi). Referirile dinaintea preluării mandatului, reluate după intrarea la Casa Albă, care vizează Groenlanda, Canada și Panama nu sunt o soluție pentru noile provocări ale lumii secolului 21, redesenată de creșterea influenței Chinei (dincolo de tot ce a fost vreodată Uniunea Sovietică la nivel global din punct de vedere militar, strategic, inovativ, tehnologic și, mai ales, economic), de inegalitățile globalizării (ce duc la dezindustrializare și pierderea locurilor de muncă în regiunile necompetitive) și de topirea calotei glaciare în Nord, cu amenințările de securitate și oportunitățile economice deschise de acest fenomen, dublat de instabilitatea echilibrelor între marile puteri - SUA și China[48].

Politica de putere se reflectă și aici prin coerciția impusă micilor actori, o abordare care creează imediat reacții, și, în timp, ar putea da naștere unor efecte secundare majore, respectiv alianțe de îndiguire sau soluții alternative de contracarare a constrângerii. Aceleași efecte din politică și reașezări strategice se regăsesc în formulele de naționalism economic, deja testate ca efect în creșteri de prețuri, a inflației, pierderi de piețe și scăderea eficienței economice în competiția globală a marilor puteri, purtată cu China. Putem adăuga la abordările critice deglobalizarea forțată, unilateralismul simbolic, dar și nevoia de reglobalizare dirijată[49]. După deconstructivism, revitalizarea bazelor de acțiune și a instrumentarului american, vedem renașterea la D.Trump a unei forme de constructivism ideologizat, care ar putea fi gândit la limită, prin exegeții săi, drept premisă de creare a unei internaționale naționaliste/ suveraniste.

O zonă pe care nu am putut-o decripta în manifestările începutului de mandat, deși s-au conturat unele elemente, este relația democrație-oligarhie pe care o introduce doctrina „Trump 2.0". D.Trump provine el însuși din zona oamenilor de afaceri, optează pentru statul minimal instituțional, care să constrângă marginal activitățile proprii și ale oricăror investitori, pe bazele libertății absolute clamate, cu precădere în zonele tehnologice. Unii au invocat o hegemonie a marilor corporații tehnologice ca bază a pragmatismului lui Trump – dacă nu chiar origine a puterii actualului lider de la Casa Albă -, iar rolul lui Elon Musk în administrație și impactul altor lideri multimiliardari și patroni ai giganților tehnologici în evoluția actuală pot ridica semne de întrebare legate de infuzia de tehno-utopism[50] în politica americană, dacă nu chiar un semnal de alarmă asupra căderii într-o epocă a oligarhiei tehnologice digitale și a preeminenței algoritmilor care au demolat și alterat deja substanțial democrația tradițională și au favorizat populismul[51]. Aceasta reprezintă o pistă de studiat în viitor.

BIBLIOGRAFIE

1. BRENES Michael, Jackson Van, ”Trump and the New Age of Nationalism. A Dangerous Combination for America and the World”, *Foreign Affairs*, 28 ianuarie 2025, https://www.foreignaffairs.com/united-states/trump-and-new-age-nationalism.
2. CHIFU Iulian, Frunzeti Teodor, „Doctrina Trump. Realismul principial”, în *Strategic Impact/ Impact Strategic* (engleză/ română), nr. 3/4 2019, ISSN 1582-6511; ISSN 1842-810X (on-line).
3. CHIFU Iulian, *„It's the security stupid!”. Alterarea pieței libere și liberului schimb în economie în condiții de război și stres securitar*, Adevărul, 25.08.2023, la https://adevarul.ro/blogurile-adevarul/its-the-security-stupid-alterarea-pietei-2294505.html.
4. CHIFU Iulian, *Actori, relații și politică de putere în secolul 21*, Editura RAO, București, 2022, ISBN 978-606-006-817-4, volumul 1 al tetralogiei „Reconfigurarea securității și a relațiilor internaționale în secolul 21”.
5. CHIFU Iulian, *Administrația Trump 2025 și Ucraina*, Calea Europeană, 27 ianuarie 2025, la https://www.caleaeuropeana.ro/iulian-chifu-administratia-trump-2025-si-ucraina/.
6. CHIFU Iulian, *Dezastrul sirian pentru Rusia lui Putin. Ce rol au avut Turcia și Ucraina?*, Calea Europeană, 31 ianuarie 2025, la https://www.caleaeuropeana.ro/iulian-chifu-dezastrul-sirian-pentru-rusia-lui-putin-ce-rol-au-avut-turcia-si-ucraina/.
7. CHIFU Iulian, „Doctrina Trump la apogeu: naționalism și realism dur și pur cu numele de „realism principial”, *Infosfera*, anul XI, nr.2/2019, ISSN 2065-3395.
8. CHIFU Iulian, *Donald Trump la Casa Albă 2025*, Calea Europeană, 21 ianuarie 2025, https://www.caleaeuropeana.ro/iulian-chifu-donald-trump-la-casa-alba-2025/.
9. CHIFU Iulian, *Lumea lui Trump – deconstrucție și reconstrucție pe baza oligarhiei conservatoare globalizante*, Calea Europeană, 24 ianuarie 2025, https://www.caleaeuropeana.ro/iulian-chifu-lumea-lui-trump-deconstructie-si-reconstructie-pe-baza-oligarhiei-conservatoare-globalizante/.
10. CHIFU Iulian, „Premise, preliminarii și perspective pentru o doctrină Trump: Revenirea la politica de putere”, *Infosfera*, anul XI, nr.1/2019, ISSN 2065-3395.
11. CHIFU Iulian, *Reconfigurarea securității și relațiilor internaționale în secolul XXI,* Editura Institutului de Științe Politice și Relații Internaționale, București, 2022, ISBN 978-630-6523-01-6.
12. CHIFU Iulian, Savu Lavinia, *The Impact of Technology on Human Being, Society and Politics,* Editura Institutului de Științe Politice și Relații Internaționale „Ion I. C. Brătianu” al Academiei Române, București, 2020, ISBN 978-606-8656-91-5, 398 p.
13. CHIFU Iulian, Simons Greg, *Rethinking warfare in the 21-st Century. The influence and effects of the Politics, Information and Communication Mix,* 2023, Cambridge University Press, 2023, ISBN:9781009355247.
14. CHIFU Iulian, *Strategia de Securitate Trump: realism dur şi pur, naţionalism şi excepţionalism american, cu Europa partener transatlantic puternic,* Adevărul blog, 22 Decembrie 2017, la https://adevarul.ro/international/statele-unite/strategia-securitate-trump-realism-dur-pur-nationalism-exceptionalism-american-europa-partener-transatlantic-puternic-1_5a3ccb25d7af743f8d9bb5c1/index.html.
15. CHIFU Iulian, ”When technology and social media are meeting Covid-19. Relativization of the truth and the fate of social media”, *Romanian Intelligence Studies Review,* nr. 25/2021.
16. COLLINSON Stephen, ”Trump's threats to Greenland, Canada and Panama explain everything about America First”, *CNN,* 8 ianuarie 2025, https://edition.cnn.com/2025/01/08/politics/trump-greenland-canada-panama-analysis/index.html.

17. DAALDER H. Ivo, Lindsay James M., ”The Price of Trump’s Power Politics. Why China and Russia Stand to Win in a Might-Makes-Right World”, *Foreign Affairs*, 30 Ianuarie 2025, https://www.foreignaffairs.com/united-states/price-trumps-power-politics.
18. DREZNER W. Daniel, ”Does the Madman Theory Actually Works?”, *Foreign Policy*, 7 ianuarie 2025, https://foreignpolicy.com/2025/01/07/madman-theory-international-relations-unpredictability/.
19. FERGUSON W. Roger Jr., Hippold F. Maximilian, ”The Case for Reglobalization. Turning Inward Won’t Secure America’s Interests”, *Foreign Affairs*, 30 ianuarie 2025, https://www.foreignaffairs.com/case-reglobalization-america-roger-ferguson-maximilian-hippold.
20. FUKUYAMA Francis, *Identity. Contemporary Identity Politics and the Struggle for Recognition*, Profilebooks Ltd, Londra, 2018, ISBN 978 1 78125 9801, 218 p.
21. GREENSPAN Allan, *The Age of Turbulence*, Penguin Books, 2008, ISBN 978-0-141-02991-7, 563 p.
22. HAGEL Chuck, ”Principles and interests”, *The National Interest*, 1 iunie 2006, https://nationalinterest.org/article/principles-and-interests-797.
23. HONIG David, ”Wonky Stuff”, 2 februarie 2025, https://www.newsfromme.com/2025/02/02/wonky-stuff/.
24. KAGAN Robert, ”Power and Weakness”, *Policy Review*, nr. 113, 2002, https://www.ies.be/files/documents/JMCdepository/Robert%20Kagan,%20Power%20and%20Weakness,%20Policy%20Review,%20No.%20113.pdf.
25. KAGAN Robert, *The Jungle Grows Back. American and Our Imperiled World*, Alfred A. Knopf, New York, 2018.
26. KIRKEY Sharon, ”Is Donald Trump’s, principled realism’ a real doctrine?”, *National Post*, 26 septembrie 2018, https://nationalpost.com/news/world/is-donald-trumps-principled-realism-a-real-doctrine.
27. MEHEUT Constant, ”Trump Urges Trading Ukraine’s Critical Minerals for More U.S. Aid”, *The New York Times*, 3 februarie 2025, https://www.nytimes.com/2025/02/03/world/europe/trump-ukraine-rare-earth-minerals.html.
28. RICHARDSON Bill, ”A new Realism. A realistic and principled foreign policy”, *Foreign Affairs*, nr. 1 (Ianuarie/Februarie), 2008, https://www.foreignaffairs.com/articles/2008-01-01/new-realism.
29. ROLLO Stuart, *The Perils of Tech-Utopian Thinking*, Observer Research Foundation, 17 mai 2023, at https://www.orfonline.org/research/the-perils-of-tech-utopian-thinking.
30. RUSSELL Greg, ”Madison’s Realism and the Role of Domestic Ideals in Foreign Affairs”, *Presidential Studies Quarterly*, vol. 25, nr. 4, Perceptions of the Presidency (Fall, 1995).
31. RUSSELL Greg, ”Theodore Roosevelt, Geopolitics, and Cosmopolitan Ideals”, *Review of International Studies,* vol. 32, nr. 3, 2006.
32. SIMONS Greg, Chifu Iulian, ”Information Warfare as a Theoretical Construct and an Operational practice”, în SAMOILENKO Sergei, Solon Simmons (eds.), *Handbook of Social and Political Conflict*, Wiley & Sons Ltd., 2025.
33. SIMONS Greg, Chifu Iulian, *The Changing Face of Warfare in the 21st Century*, Routledge, London and New York, 2017, ISBN 978-1-472-48212-9, 278 p.
34. TRUMP J. Donald, *Great Again. How to Fix Our Crippled America*, Threashold Editions, New York, 2015, ISBN 978-1-5011-3800-3, 193 p.
35. TRUMP J. Donald, *The Inaugural Address Remarks*, The White House, 20 ianuarie 2025, at https://www.whitehouse.gov/remarks/2025/01/the-inaugural-address/.
36. TRUMP J. Donald, *Imposing Sanctions on the International Criminal Court*, Executive Order, 6 februarie 2025, at https://www.whitehouse.gov/presidential-actions/2025/02/imposing-sanctions-on-the-international-criminal-court/.

37. TRUMP J. Donald, *Peace through strength*, Truth Social, 27 noiembrie 2024, at https://truthsocial.com/@realDonaldTrump/posts/113556157032343210.
38. WALT M. Stephen, ”Trump Can’t Bully the Entire World. Loudly making threats doesn’t amount to a foreign policy”, *Foreign Policy*, 30 decembrie 2024, https://foreignpolicy.com/2024/12/30/trump-bully-world-america-foreign-policy/.
39. WALT M. Stephen, ”What IR Theory Predicts About Trump 2.0. An academic assessment of the U.S. president’s foreign-policy revolution”, *Foreign Policy*, 3 februarie 2025, https://foreignpolicy.com/2025/02/03/ir-theory-trump-balance-power/.
40. WEBSTER Graham, Sherman Justin, ”The Fall and Rise of Techno-Globalism. Democracies Should Not Let the Dream of the Open Internet Die”*, Foreign Affairs*, 28 octombrie 2021, at https://www.foreignaffairs.com/articles/world/2021-10-28/fall-and-rise-techno-globalism.
41. *** Crisis Group, *10 Conflicts in 2025*, 01.01.2025, https://www.crisisgroup.org/global/10-conflicts-watch-2025.
42. *** Encyclopedia Britannica, *The Gordian Knot*, https://www.britannica.com/topic/Gordian-knot.
43. *** ”Musk backing for European far-right, threatens democracy,’ says German Chancellor Scholz”, *Le Monde,* 17 ianuarie 2025, https://www.lemonde.fr/en/germany/article/2025/01/17/musk-backing-for-european-far-right-threatens-democracy-says-scholz_6737138_146.html.
44. *** President Trump Donald J., *Press conference*, 11 ianuarie 2025, at https://www.youtube.com/watch?v=7AmMmYhJLZA.
45. *** *President Trump’s Speech to the Arab Islamic American Summit*, 21 mai 2017, https://www.whitehouse.gov/briefings-statements/president-trumps-speech-arab-islamic-american-summit/.
46. *** *Remarks by President Trump on the Strategy in Afghanistan and South Asia*, 21 august 2017, https://www.whitehouse.gov/briefings-statements/remarks-president-trump-strategy-afghanistan-south-asia/.
47. *** *Remarks by President Trump to the 73rd Session of the United Nations General Assembly*, 25 septembrie 2018, https://www.whitehouse.gov/briefings-statements/remarks-president-trump-73rd-session-united-nations-general-assembly-new-york-ny/.
48. *** Senate Foreign Relations Committee, *Hearings to examine the expected nomination of Marco A. Rubio, of Florida, to be Secretary of State*, 119th Congress (2025-2026), 15.01.2025, https://www.congress.gov/event/119th-congress/senate-event/336501.
49. ****A Keynote Speech by U.S. Secretary of State Michael R. Pompeo*, 4 decembrie 2018, http://www.gmfus.org/events/keynote-speech-us-secretary-state-michael-r-pompeo.
50. ***Mars and Venus, Ten Years Latter. Essays on the US and Europe a Decade after Robert Kagan’s Power and Weakness, *Policy Review*, 172/2012, Hoover Institution, Stanford University, ISSN 0146-5945, 144 p.
51. ****Remarks made by President Trump at the 72nd Session of the United Nations General Assembly*, 19 septembrie 2017, https://www.whitehouse.gov/briefings-statements/remarks-president-trump-72nd-session-united-nations-general-assembly/.
52. *** *President Donald Trump’s UN General Assembly Speech,* în *National Post*, 26 septembrie 2018, at https://nationalpost.com/news/world/trump-un-speech.
53. *** *US National Security Strategy*,*“A New National Security Strategy for a New Era”*, 18 decembrie 18, 2017, https://www.whitehouse.gov/articles/new-national-security-strategy-new-era/.

[1] Iulian Chifu, *Reconfigurarea securității și relațiilor internaționale în secolul XXI*, Editura Institutului de Științe Politice și Relații Internaționale, București, 2022, ISBN 978-630-6523-01-6; Iulian Chifu, *Actori, relații și politică de putere în secolul 21*, Editura RAO, București, 2022, ISBN 978-606-006-817-4, volumul 1 al tetralogiei „Reconfigurarea securității și a relațiilor internaționale în secolul 21".

[2] Robert Kagan, "Power and Weakness", *Policy Review*, nr. 113, 2002, https://www.ies.be/files/documents/JMCdepository/Robert%20Kagan,%20Power%20and%20Weakness,%20Policy%20Review,%20No.%20113.pdf.

[3] Iulian Chifu, Teodor Frunzeti, „Doctrina Trump. Realismul principial", în *Strategic Impact/ Impact Strategic* (engleză/ română), nr. 3/4 2019, ISSN 1582-6511; ISSN 1842-810X (on-line), p. 7-18.

[4] *** „Mars and Venus, 10 years latter. Essays on the US and Europe a Decade after Robert Kagan's Power and Weakness", *Policy Review*, 172/2012, Hoover Institution, Stanford University, ISSN 0146-5945, 144 p.

[5] Robert Kagan, *The Jungle Grows Back. American and Our Imperiled World*, Alfred A. Knopf, New York, 2018.

[6] Francis Fukuyama, *Identity. Contemporary Identity Politics and the Struggle for Recognition*, Profile Books Ltd, Londra, 2018, ISBN 978 1 78125 9801, 218 p.

[7] Ibidem.

[8] Iulian Chifu, „Premise, preliminarii și perspective pentru o doctrină Trump: Revenirea la politica de putere", în *Infosfera*, anul XI, nr.1/2019, ISSN 2065-3395, p. 3-12; Iulian Chifu, „Doctrina Trump la apogeu: naționalism și realism dur și pur cu numele de „realism principial", în *Infosfera*, anul XI, nr.2/2019, ISSN 2065-3395, p.3-15.

[9] Iulian Chifu, „Administrația Trump 2025 *și* Ucraina", *Calea Europeană*, 27 ianuarie 2025, la https://www.caleaeuropeana.ro/iulian-chifu-administratia-trump-2025-si-ucraina/; Iulian Chifu, „Lumea lui Trump – deconstrucție și reconstrucție pe baza oligarhiei conservatoare globalizante", *Calea Europeană*, 24 ianuarie 2025, la https://www.caleaeuropeana.ro/iulian-chifu-lumea-lui-trump-deconstructie-si-reconstructie-pe-baza-oligarhiei-conservatoare-globalizante/; Iulian Chifu, „Donald Trump la Casa Albă 2025", *Calea Europeană*, 21 ianuarie, la https://www.caleaeuropeana.ro/iulian-chifu-donald-trump-la-casa-alba-2025/.

[10] Greg Simons, Iulian Chifu, *The Changing Face of Warfare in the 21st Century*, Routledge, London and New York, 2017, ISBN 978-1-472-48212-9, 278 p.; Iulian Chifu, *Actori, relații și politică de putere în secolul 21*.

[11] Iulian Chifu, Greg Simons, *Rethinking warfare in the 21-st Century. The influence and effects of the Politics, Information and Communication Mix*, 2023, Cambridge University Press, 2023, ISBN:9781009355247.

[12] Vezi și Greg Simons, Iulian Chifu, "Information Warfare as a Theoretical Construct and an Operational practice", în Sergei Samoilenko, Solon Simmons, *Handbook of Social and Political Conflict*, Wiley & Sons Ltd, 2025.

[13] *** *Remarks made by President Trump at the 72nd Session of the United Nations General Assembly*, 19 septembrie, 2017, https://www.whitehouse.gov/briefings-statements/remarks-president-trump-72nd-session-united-nations-general-assembly/; transcriptul complet al declarației *President Donald Trump's UN General Assembly Speech* în *National Post*, 26 septembrie 2018, at https://nationalpost.com/news/world/trump-un-speech.

[14] *US National Security Strategy*, *"A New National Security Strategy for a New Era"*, 18 decembrie 2017, https://www.whitehouse.gov/articles/new-national-security-strategy-new-era/.

[15] Iulian, Chifu, Teodor, Frunzeti, *Op. cit.*

[16] *President Trump's Speech to the Arab Islamic American Summit*, 21 mai 2017, https://www.whitehouse.gov/briefings-statements/president-trumps-speech-arab-islamic-american-summit/; *Remarks by President Trump on the Strategy in Afghanistan and South Asia*, 21 august 2017, https://www.whitehouse.gov/briefings-statements/remarks-president-trump-strategy-afghanistan-south-asia/; vezi și Sharon Kirkey, "Is Donald Trump's 'principled realism' a real doctrine?", 26 septembrie, 2018, *National Post*, https://nationalpost.com/news/world/is-donald-trumps-principled-realism-a-real-doctrine.

[17] Greg Russell, "Madison's Realism and the Role of Domestic Ideals in Foreign Affairs", *Presidential Studies Quarterly*, vol. 25, nr. 4 (Perceptions of the Presidency/ Fall, 1995), p. 711-723.

[18] Greg Russell, "Theodore Roosevelt, Geopolitics, and Cosmopolitan Ideals", *Review of International Studies,* vol. 32, nr. 3, 2006, p. 541-559.

[19] Chuck Hagel, "Principles and interests", *The National Interest*, 1 iunie 2006, https://nationalinterest.org/article/principles-and-interests-797.

[20] Iulian Chifu, *Premise, preliminarii* și *perspective pentru o Doctrină Trump: revenirea la politica de putere;* Iulian Chifu, *Actori, relații și politică de putere în secolul 21.*

[21] Bill Richardson, "A new Realism. A realistic and principled foreign policy", *Foreign Affairs*, nr. 1 (ianuarie/februarie), 2008, https://www.foreignaffairs.com/articles/2008-01-01/new-realism.

[22] *Ibidem*.

[23] ***, *Remarks by President Trump to the 73rd Session of the United Nations General Assembly*, 25 Septembrie, 2018, https://www.whitehouse.gov/briefings-statements/remarks-president-trump-73rd-session-united-nations-general-assembly-new-york-ny/.

[24] *** *A Keynote Speech by U.S. Secretary of State Michael R. Pompeo*, 4 decembrie 2018, http://www.gmfus.org/events/keynote-speech-us-secretary-state-michael-r-pompeo.

[25] Iulian Chifu, *Strategia de Securitate Trump: realism dur şi pur, naţionalism şi excepţionalism american, cu Europa partener transatlantic puternic*, Adevărul blog, 22 decembrie 2017, la https://adevarul.ro/international/statele-unite/strategia-securitate-trump-realism-dur-pur-nationalism-exceptionalism-american-europa-partener-transatlantic-puternic-1_5a3ccb25d7af743f8d9bb5c1/index.html; Iulian Chifu, *Premise, preliminarii* și *perspective pentru o Doctrină Trump: revenirea la politica de putere*.

[26] Donald J. Trump, *Great Again. How to Fix Our Crippled America*, Threashold Editions, New York, 2015, ISBN 978-1-5011-3800-3, 193 p.

[27] Iulian Chifu, *Actori, relații și politică de putere în secolul 21.*

[28] Donald J. Trump, *The Inaugural Address Remarks*, The White House, 20 ianuarie 2025, la https://www.whitehouse.gov/remarks/2025/01/the-inaugural-address/.

[29] Senate Foreign Relations Committee, *Hearings to examine the expected nomination of Marco A. Rubio, of Florida, to be Secretary of State*, 119th Congress (2025-2026), 15.01.2025, https://www.congress.gov/event/119th-congress/senate-event/336501.

[30] Donald J. Trump, *Peace through strength*, Truth Social, 27 noiembrie, 2024, https://truthsocial.com/@realDonaldTrump/posts/113556157032343210.

[31] President Donald Trump, *Press conference*, 11 ianuarie 2025, https://www.youtube.com/watch?v=7AmMmYhJLZA.

[32] Ivo H. Daalder, James M. Lindsay, "The Price of Trump's Power Politics. Why China and Russia Stand to Win in a Might-Makes-Right World", *Foreign Affairs*, 30 Ianuarie 2025, https://www.foreignaffairs.com/united-states/price-trumps-power-politics.

[33] Encyclopedia Britannica, *The Gordian Knot*, https://www.britannica.com/topic/Gordian-knot.

[34] Iulian Chifu, *Doctrina Trump la apogeu: naționalism și realism dur și pur cu numele de „realism principial"*.

[35] Roger W. Ferguson, Jr., Maximilian F. Hippold, "The Case for Reglobalization. Turning Inward Won't Secure America's Interests"*, Foreign Affairs*, 30 ianuarie 2025, https://www.foreignaffairs.com/case-reglobalization-america-roger-ferguson-maximilian-hippold.

[36] Crisis Group, *10 Conflicts in 2025*, https://www.crisisgroup.org/global/10-conflicts-watch-2025.

[37] Donald J. Trump, *Imposing Sanctions on the International Criminal Court*, Executive Order, 6 februarie 2025, at https://www.whitehouse.gov/presidential-actions/2025/02/imposing-sanctions-on-the-international-criminal-court/.

[38] Crisis Group, *Op.cit.*

[39] David Honig, *Wonky Stuff*, 2 Februarie 2025, https://www.newsfromme.com/2025/02/02/wonky-stuff/.

[40] Constant Meheut, "Trump Urges Trading Ukraine's Critical Minerals for More U.S. Aid"*, The New York Times*, 3 februarie 2025, at https://www.nytimes.com/2025/02/03/world/europe/trump-ukraine-rare-earth-minerals.html.

[41] Allan Greenspan, *The Age of Turbulence*, Penguin Books, 2008, ISBN 978-0-141-02991-7, 563 p.

[42] Iulian Chifu, *„It's the security stupid!". Alterarea pieței libere și liberului schimb în economie în condiții de război și stres securitar*, Adevărul, 25.08.2023, la https://adevarul.ro/blogurile-adevarul/its-the-security-stupid-alterarea-pietei-2294505.html.

[43] Michael Brenes, Van Jackson, "Trump and the New Age of Nationalism. A Dangerous Combination for America and the World", *Foreign Affairs*, 28 ianuarie 2025, https://www.foreignaffairs.com/united-states/trump-and-new-age-nationalism.

[44] Iulian Chifu, *Dezastrul sirian pentru Rusia lui Putin. Ce rol au avut Turcia și Ucraina?*, Calea Europeană, 31 ianuarie 2025, la https://www.caleaeuropeana.ro/iulian-chifu-dezastrul-sirian-pentru-rusia-lui-putin-ce-rol-au-avut-turcia-si-ucraina/.

[45] Stephen M. Walt, "What IR Theory Predicts About Trump 2.0. An academic assessment of the U.S. president's foreign-policy revolution", *Foreign Policy*, 3 februarie 2025, https://foreignpolicy.com/2025/02/03/ir-theory-trump-balance-power/.

[46] Francis Fukuyama, *Op. cit*.

[47] Stephen M. Walt, "Trump Can't Bully the Entire World. Loudly making threats doesn't amount to a foreign policy"*, Foreign Policy*, 30 decembrie 2024, https://foreignpolicy.com/2024/12/30/trump-bully-world-america-foreign-policy/.

[48] Stephen Collinson, *Trump's threats to Greenland, Canada and Panama explain everything about America First,* CNN, 8 ianuarie 2025, https://edition.cnn.com/2025/01/08/politics/trump-greenland-canada-panama-analysis/index.html.

[49] Roger W. Ferguson Jr., Maximilian F. Hippold, *Op.cit.*

[50] Stuart Rollo, *The perils of Tech-Utopian Thinking*, Observer Research Foundation, 17 mai 2023, https://www.orfonline.org/research/the-perils-of-tech-utopian-thinking; Graham Webster, Justin Sherman, "The Fall and Rise of Techno-Globalism. Democracies Should Not Let the Dream of the Open Internet Die"*, Foreign Affairs*, 28 octombrie 2021, https://www.foreignaffairs.com/articles/world/2021-10-28/fall-and-rise-techno-globalism.

[51] Iulian Chifu, "When technology and social media are meeting Covid-19. Relativization of the truth and the fate of social media"*,* în *Romanian Intelligence Studies Review*, nr. 25/2021, p.101-113; Iulian Chifu, Lavinia Savu, *The Impact of Technology on Human Being, Society and Politics,* Editura Institutului de Științe Politice și Relații Internaționale „Ion I. C. Brătianu" al Academiei Române, București, 2020, ISBN 978-606-8656-91-5, 398 p.

EPOCA XI JINPING

Isabela ANCUȚ*

Motto: „Orice epocă socială are nevoie de propria personalitate și dacă nu există o astfel de personalitate atunci o creează”.

Karl Marx

Abstract

Starting from the ideea that the years 2016-2017 marked the beginning of the crystallization of new forms of „democratic centralism”[1], this article explores how China's current president, Xi Jinping, has sought to consolidate his power in relation to traditional political factions.

Power struggles intensified following the 19th Congress of the Chinese Communist Party/ CCP[2], and Xi's strengthened position led to shifts in how the authoritarian leader interacts with the ruling party.

Across his three terms[3], Xi's leadership has been defined by extensive political and military purges, alongside significant social and economic challenges, both domestically and internationally.

Keywords: *authoritarian leadership; power struggles; military control; political purges; one-party rule; China's global influence; state surveillance; political loyalty.*

XI JINPING – PRIMELE DOUĂ MANDATE (2012 – 2022)

Anul 2024 s-a încheiat pentru China în aceeași notă caracteristică din ultima perioadă, de consolidare și centralizare a puterii președintelui Xi Jinping, de creștere a controlului său asupra Partidului Comunist Chinez (PCC) și instituțiilor statului, eforturi considerabile întreprinse pentru marginalizarea oricăror potențiali rivali, promovarea în poziții guvernamentale cheie a aliaților agreați, gestionarea tuturor aspectelor sociale sau economice care ar putea amenința îndeplinirea obiectivelor politice propuse. Acțiunile directe și vizibile ale lui Xi Jinping, mai ales în domeniul campaniei anticorupție la nivel național (inițiată în 2012 și vocalizată puternic în anii următori), au continuat să se subscrie, la un anumit nivel, într-o manieră indirectă, setului de măsuri care vizează înlăturarea rivalilor și amenințărilor la adresa puterii sale[4].

Însă, manevrele politice ale lui Xi Jinping au adus atingere planului inițial de reforme economice (un sistem național de taxe pe proprietate și înregistrarea proprietăților, modernizarea și liberalizarea industriilor grele), periclitând semnificativ și stabilitatea socială și economică (creșterea șomajului, supra-îndatorarea companiilor, intervenţia constantă a statului pe pieţele monetare, creșterea tarifelor aplicate importurilor şi subvenţionarea unei părţi considerabile a economiei, intervenția în piața liberă și în activitatea firmelor private din domeniul IT etc.).

În plus, politica externă a lui Xi Jinping – de „renaștere a națiunii chineze” – a adus tensiuni în relațiile cu alți actori statali, tensiuni materializate

Autoarea este doctor în Științe Militare și Informații.

într-o serie de politici restrictive și sancțiuni la adresa companiilor chineze. Toate acestea au avut un impact major asupra evoluțiilor interne, în pofida politicilor de securitate extrem de dure și restrictive, demonstrațiile și grevele de la nivelul anului 2022/2023 fiind în creștere față de cele înregistrate în anii anteriori. Vom păstra concluziile menționate în articolul nostru din 2017, respectiv afirmațiile fostului președinte american, Barack Obama, cum că președintele chinez „și-a consolidat puterea mai repede și mai eficient decât oricine altcineva de la Deng Xiaoping încoace": Xi Jinping s-a dovedit capabil să promoveze reforme economice, sociale și militare ambițioase, să „transforme" procesul decizional la vârful PCC și să elimine o multitudine de oficiali de rang înalt și foarte înalt (utilizând cea mai mare campanie anticorupție cunoscută de China). Prin înființarea de structuri paralele, de dimensiuni mici și mai eficiente, prin aplicarea de noi reguli sau prin încălcarea celor existente, Xi Jinping a evitat orice conflict sau opoziție în procesul decizional.

Etapa în care succesul s-a datorat carismei sale, abilității deosebite de a manipula, dar și intuiției/flerului său de a profita de circumstanțele geoeconomice și geopolitice, de tradiții și tendințele reformatoare de la nivel intern, de jocurile complexe de putere și de dificultatea obținerii consensului între membrii elitei asupra unor probleme importante s-a încheiat. Președintele chinez se află acum în vârful puterii și profită din plin de această poziție[6]. Orgoliile și vanitățile unor personalități, idealismul și pragmatismul facțiunilor politice existente anterior epocii lui Xi Jinping în interiorul PCC au dispărut, autodistrugându-se cu ajutorul nemijlocit al acestuia. De asemenea, trimiterile sale[7] la citate din Mao Zedong, din scrierile tradiționale chinezești, din Deng Xiaoping și Confucius, din istoricii din timpul dinastiei Qing și filozofii din timpul dinastiei Song, din scrierile lui Adam Smith, Marx, Engels, Lenin, Jiang, Hu, Chen Yun, Han Feizi și Mengzi au dispărut și ele[8]. Afirmația din dialectica lui Marx precum că „fără trecut nu ar fi fost prezent, astfel încât nu putem nega complet toate lucrurile din trecut"[9] nu mai există. Toate acestea au fost reformate în accepțiunea lui Xi Jinping și prezentate în lucrarea „Gândirea lui Xi Jinping asupra socialismului cu caracteristici chinezești pentru o nouă eră". În prezent, ideologia politică promovată de liderul chinez este cuprinsă în următoarele documente: „Visul chinezesc", „Esența celor mai importante serii de remarci ale Secretarului General Xi Jinping", „Conceptele, gândurile și strategiile noii guvernanțe a Secretarului general Xi Jinping", „Cele patru înțelepciuni", „Cele patru autoconvingeri" și „Cele patru examene".

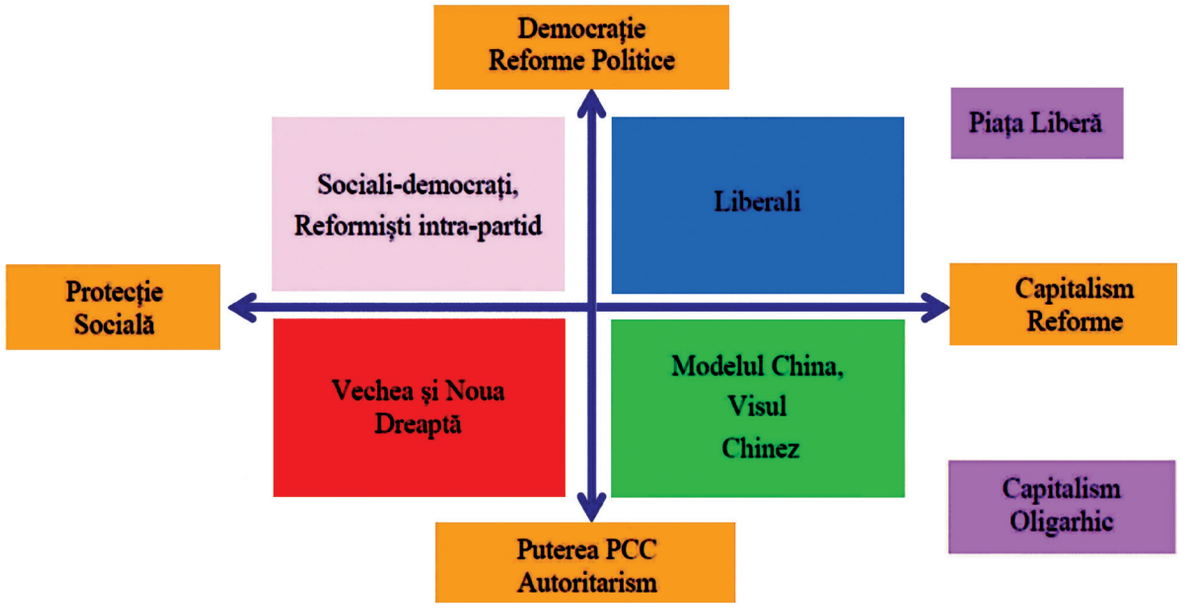


Figura nr. 1: *Spectrul politic chinez în perioada 2014-2016*[5]

Așa cum menționam și în articolul din 2017, Xi Jinping a avut nevoie de persoane/ grupuri loiale pentru a derula proiectul său de reformă. De altfel, liderul chinez a demonstrat deja faptul că nu respectă regulile – formale sau informale – stabilite de predecesorii săi, în special de Deng Xiaoping, pentru a-și pune în practică ideile reformatoare. De exemplu, regula că oficialii cu vârsta de 68 de ani (sau mai mult) trebuie să se retragă se respectă doar „în general", existând și destule excepții. Această regulă este importantă pentru stabilirea echilibrului de putere în cadrul Comitetului Permanent al Biroului Politic (PBSC[10]), locul de decizie finală asupra politicilor care trebuie urmate, dar și locul unde se presupune că se va stabili cine va fi succesorul președintelui în exercițiu (de regulă, acesta este ales dintre membrii PBSC). În plus, un control strâns asupra PBSC înseamnă, implicit, și un control al altor organe ale PCC și al instrumentelor-cheie din cadrul sistemului PCC. Erodarea normelor Partidului l-a ajutat pe Xi Jinping să reducă importanța rolului unor structuri de putere consacrate, precum Consiliul de Stat, la cea de simple organe de punere în execuție a politicilor sub directul control al PBSC, reducând la minim capacitatea acestora de a realiza/ implementa politici în aproape toate domeniile vieții. Totodată, modul său de acțiune i-a adus sub control personal structurile de securitate, campania de luptă anticorupție eliminând mare parte din cei care nu erau de acord cu ideile sale sau care aveau propriile rețele de influență (ierarhic, pe verticală și pe orizontală).

Primele mandate au adus dominația lui Xi asupra Armatei Populare de Eliberare (APE) și, mai important, asupra oficialilor de rang înalt din PBSC. Astfel, au fost eliminați generalii Fang Fenghui – șef al departamentului Stat Major Întrunit/ Comisia Militară Centrală (CMC) și Zhang Yang – director al departamentului Muncă Politică din cadrul CMC[11]. În perioada 2020-2022, Xi Jinping a reușit să controleze nu numai conducerile Ministerului Securității Statului (MSS) și Ministerului Securității Publice (MPS), dar și conducerile de nivel doi și trei din aceste structuri și conducerile polițiilor locale/ provinciale, totul culminând cu condamnarea la moarte a fostului ministru al justiției, Fu Zhenghua, și a fostului vice-ministru al Securității Publice, Sun Lijun. În paralel cu demiterile a existat și o politică a numirii în funcții cheie a persoanelor agreate, astfel a fost cazul protejaților săi, Wang Xiaohong (în MPS), Chen Yixin (CPLAC) și Ying Yong[12].

Rezultatul a fost că Xi Jinping s-a înconjurat de persoane loiale și în cadrul mecanismului birocratic care există în APE, în agențiile executive ale PBSC (cu accent pe Secretariatul PCC și Biroul/ Oficiul General – structura administrativă a PBSC), respectiv în toate structurile care controlează ideologia și disciplina de partid.

La nivel practic, structura PBSC reprezintă instrumentul prin care președintele chinez controlează sistemul politic de partid, dar și scena politică internă, în general, miza fiind influențarea luptelor pentru stabilirea succesorului său[13], precum și a celor ce vor ocupa poziții cheie în cadrul administrației[14]. Deși într-o primă fază Xi și-a instaurat în poziții-cheie aliații și susținătorii, există și oficiali care nu se aflau în cercul intim de prieteni, dar care, prin acțiuni, au putut fi considerați loiali lui Xi Jinping, așa cum au fost cazurile lui Miao Hua și Zhang Shengmin (membrii ai CMC în 2022).

De-a lungul mandatelor liderului de la Beijing se poate observa o constanță în doctrina politică aprobată și impusă (necesitatea măsurilor de reformă, întărirea disciplinei la nivel de partid şi la nivel regional, administrativ statal)[15]. În prezent, cel de-al treilea mandat i-a permis lui Xi Jinping să-și consolideze poziția de la vârful ierarhiei politice, să elimine o foarte mare parte a elementelor aparținând facţiunilor politice tradiționale și să „producă" constant noi instituţii şi reguli pentru asigurarea susţinerii sale necondiționate. Cu alte cuvinte, a eliminat principiul diviziunii puterii între diverse birocraţii aflate la vârful statului, renunțând la ideea conducerii colective și instaurând conducerea unui lider suprem unic.

Congresele 18 și 19 (și, ulterior, chiar 20) ale PCC au reprezentat pentru liderul chinez momente adecvate, pregătite cu minuțiozitate, de lansare a reformelor politice (și nu numai) la nivelul structurilor de conducere ale PCC (Comitetul

Central/ CC al PCC, Biroul Politic/ BP[16] şi PBSC), de recalibrare a platformelor ideologică şi politică ale PCC în favoarea intereselor sale. Structura politică și ideologică din perioada 2014 – 2017 a dispărut în mare parte, subsumată intereselor lui Xi Jinping[17]. Acea structură presupunea existența următoarelor grupări: promotorii „Modelului China" - dominau PCC şi forțele armate, „prinţişorii" şi administraţiile de stat; „Stânga" – compusă atât din nostalgicii erei Mao (Vechea Stângă), cât și din reprezentanți ai lumii academice, critici ai Occidentului/ capitalismului şi partizani ai unui stat puternic (Noua Stângă); social-democraţii (membri ai clasei intelectualilor şi foşti reformatori ai nucleului PCC) și liberalii (aparțin, cu precădere, mediei „metropolitane" semi-private, avocaţilor, populaţiei urbane şi mediului economic privat).

Începând cu 2017 a fost impusă și legitimată legislativ modalitatea de conducere practicată de Mao Zedong. Printre primele măsuri adoptate s-a numărat detașarea de tradițiile instaurate sub conducerea lui Mao Zedong[18] (schimbarea datelor plenarelor, de pildă, în 2018, PCC a desfășurat cea de a 3-a Plenară a Comitetului Central în luna februarie și nu în toamnă, așa cum se derula din anii 90) și amendarea Constituției, în scopul eliminării limitelor mandatului prezidențial. În acest mod, liderul chinez a obținut cel de-al treilea mandat la conducerea țării (ca secretar general al PCC și comandant suprem al Armatei Populare de Eliberare - APE).

Anul 2023 a reprezentat un punct de cotitură, semnificative fiind schimbările care au avut loc la nivel înalt: premierul Li Keqiang (decedat), ministrul de externe Qin Gang (demis) și ministrul apărării (acuzat de corupție). Acești oficiali erau parte a birocrației chineze care oferea susținere necondiționată lui Xi Jinping. Dar, în fapt, impunerea controlului statului asupra sectorului privat și trecerea de la sistemul autoritar bazat pe consens spre cel al conducerii unice – dictatoriale au început încă din 2022. Președintele Xi Jinping a impus creșterea implicării statului în sectorul privat, cea mai productivă parte a economiei chineze, fapt ce a condus treptat la estomparea imaginii PCC.

Dacă existaseră așteptări ca stilul de conducere a lui Xi Jinping să fie asemănător cu cel al lui Hu Jintao sau Jiang Zemin – acel *primus inter pares* –, din punct de vedere economic lucrurile au evoluat diferit. Astfel, predecesorii săi au lăsat economia să evolueze „liber", considerând că prosperitatea acesteia susține însăși dezvoltarea PCC și, implicit, a țării. Odată cu lansarea programelor chineze internaționale (precum Inițiativele Centurii și Drumului Mătăsii) s-a mizat pe faptul că se va reduce supracapacitatea de producție din China, că va exista un influx masiv de capital către firmele de stat și că se vor susține programele de ajutorare a populației cu venituri mici. Nu s-a reușit decât inducerea de probleme unor companii de renume internațional (vezi cazului companiei Alibaba[19]), îndepărtarea investitorilor străini din cauza legilor privind securitatea informațiilor etc. Cu alte cuvinte, implicarea statului în sectorul privat a determinat încetinirea ritmului de creștere economică, acesta atingând un nivel îngrijorător[20]. În plan social, Xi Jinping a impus o politică prin care au fost afectate drastic drepturile omului, în special în ceea ce privește drepturile religioase și drepturile minorităților naționale.

Președintele Xi a generat o nouă revoluție culturală, dar nu în sensul promovat de Mao. Există doctrina naționalismului chinez, unde etnia Han reprezintă nucleul culturii. În 2024 a apărut un nou manual de studiu – O introducere în comunitatea etniei Zhonghua[21], care explică gândirea lui Xi Jinping în ceea ce privește guvernarea PCC asupra „statului multietnic unificat"[22]. Președintele chinez pleacă de la paradigma „comunismului multicultural" și ajunge la un naționalism centrat pe etnia Han. Deși Constituția revizuită în 2018 reitera promisiunea Chinei de a recunoaște oficial cele 125 de milioane de etnici ai minorităților naționale ca fiind „egali" cu majoritatea de peste un miliard a etnicilor Han, noua doctrină a impus subordonarea și adaptarea culturii minorităților la normele etniei dominante. În realitate, aceste idei se cristalizaseră deja în 2014, în politicile „minzu" ale PCC, menționate de Xi Jinping în discursurile sale despre guvernanța unită și controlul regiunilor autonome/ provinciilor de graniță.

Dintre vectorii „gândirii” lui Xi (reîntinerirea Chinei; reforma instituțiilor și eliminarea corupției; modernizarea APE; promovarea naționalismului și „întregirea” țării cu Taiwanul), restaurarea rolului PCC în țară și în lume este cel mai bine prezentată în doctrina „Gândirea lui Xi Jinping”[23]. La nivelul acestor vectori, o anume semnificație specială a căpătat-o, după 2018, modalitatea de implementare. În prezent, aceasta înseamnă modernizarea militară a țării în paralel cu represiunea minorităților prin instaurarea unei singure etnii, Han, și controlul statului asupra companiilor private.

FACȚIUNI POLITICE ȘI GRUPURI DE INTERESE

Dacă în timpul primelor două mandate ale lui Xi Jinping mai existau facțiuni și grupuri de interese independente, odată cu cel de-al treilea mandat acestea au fost restructurate/reorganizate sau chiar desființate, în funcție de interesele politicii promovate de liderul suprem[24]:

1. *„Prinților”* (taizidang) sau moștenitorii primei generații de revoluționari[25], grup format, inițial, din Xi Jinping, Yu Zhengsheng (președintele CPCPC), Wang Qishan (fostul șef al Comisiei Centrale pentru Inspecția Disciplinei de Partid - CCID) și Zhang Dejiang (președintele CNP), a ajuns în prezent să cuprindă „prinți” din altă generație (cei născuți în perioada anilor '50 – '70).

2. *Facțiunea Liga Tinerilor Comuniști/ LTC* (tuanpai), prima dintre facțiunile politice esențiale ale PCC (fostul președinte Hu Jintao și fostul premier Li Keqiang au făcut parte din rândurile sale[26]). În momentul de față această facțiune se află în „moarte clinică”, iar motivele distrugerii sale se regăsesc în politicile duse de către Xi Jinping (deși, la celebrarea centenarului acestei structuri, în 2022, liderul chinez a menționat că o respectă și o consideră *un partener important, o forță de rezervă* pentru PCC). Bugetul LTC a scăzut cu peste 50%, la fel și numărul adepților săi, iar Xi a „închis” Școala Centrală a LTC prin încorporarea sa într-o structură nouă, Academia de Științe Sociale. Criticile aduse de Xi Jinping la adresa guvernării rutinate și precaute ale lui Jiang Zemin și Hu Jintao au determinat eliminarea acestora de la conducere (în cadrul celei de-a 6-a Plenare din cel de-al 19-lea Comitet Central), precum și modificarea regulilor prin care oficialii pot fi înlăturați din funcții importante.

Foștii membrii ai PBSC, Wang Yang și Hu Chunhua, deși parte a LTC, au aderat la ideile lui Xi Jinping. Moartea lui Li Keqiang i-a permis lui Xi Jinping să-și impună aliații în cadrul PBSC (Ding Xuexiang și/sau Li Qiang). De altfel, președintele a reușit eliminarea tuturor celor aflați în rețelele de influență ale lui Hu Jintao[27], determinând diminuarea drastică a influenței LTC, iar faptul că Wang Yang și Hu Chunhua au mai rămas în structurile de conducere nu reprezintă o garanție a resuscitării LTC și nici a supraviețuirii acestei structuri. Acești lideri se află în siguranță doar în măsura în care susțin politica lui Xi Jinping, iar președintele chinez consideră că ideile lor privind stabilizarea economiei chineze pot servi politicii sale de „prosperitate comună”[28].

3. *Grupul reformatorilor neoliberali* (gaigepai), format din persoane care susțin o mai mare libertate economică și politică, în marea lor majoritate din provincia Guangdong, s-a diminuat substanțial, pentru moment una dintre personalitățile marcante ale grupului este Wang Yang. Conceptul de libertate economică promovat de Deng Xiaoping a fost modificat de Xi Jinping pentru a servi ideilor sale de „prosperitate comună”.

4. *Neomaoiștii* (baoshoupai), care susțin consolidarea puterii statului și au puternice tendințe naționaliste, au supraviețuit deoarece ideile promovate de aceștia sunt în concordanță cu politica lui Xi Jinping. Similar pare a fi și cazul *neoconfucianiștilor,* care deplâng pierderea vechilor valori morale și susțin întoarcerea către o politică a Chinei mai puțin agresivă atât la nivel intern, cât și extern.

Menționam, în articolul din 2017[29], că Xi Jinping a început să-și creeze propria facțiune de suporteri în conducerea PCC, „demolând” încet, dar sigur, facțiunile tradiționale și creând centre de putere politică loiale. Ian Johnson subliniază faptul[30] că există și o serie de demnitari de rang înalt (precum Wang Yang, Li Xi și Hu Chunhua)

care și-au creat propriile facțiuni separate de facțiunea lui Xi Jinping.

5. *Facțiunea Fujian* – reprezintă un grup format din persoanele de încredere cu care Xi Jinping a lucrat pe timpul activității sale în provincia Fujian (1985 – 2002). Această facțiune este una dintre cele două grupări pe care se bazează administrația lui Xi (în ascensiune față de *cealaltă grupare, Zhejiang*). Printre numele marcante ale acestei facțiuni îi regăsim pe Wang Xiaohong, Deng Weiping, He Weidong, Zhuang Rongwen, Miao Hua, Zhao Keshi, Cai Yingting și, nu în ultimul rând, Cai Qi, care a avut o ascensiune politică fulminantă în ierarhia de putere a PCC.

6. *Facțiunea Zhejiang,* supranumită și „Armata noului Zhijiang". Figuri reprezentative sunt Huang Kunming, Chen Derong, Lou Yangsheng, Xia Baolong, Li Qiang, Chen Min`er, Yin Yong, Li Xi, Chen Xi, He Lifeng, Shu Guozeng.

7. *Facțiunea Shanghai* a reunit cadrele care au lucrat/ lucrează în Administrația Municipiului Shanghai sub conducerea lui Jiang Zemin sau a unor asociați ai acestuia și care dețin poziții marcante în politica chineză. Personalități precum Yu Zhengsheng, Liu Yunshan, Zhang Gaoli și Zhang Dejiang aparțin acestui grup. Facțiunea a susținut ascensiunea lui Xi Jinping (prin intermediul soției sale, Peng Liyuan). Deși facțiunea a jucat un rol important în politica chineză în trecut, în prezent influența sa a fost considerabil redusă, iar structura de putere din China este acum dominată de cercul de aliați ai lui Xi Jinping.

8. *Politicieni fără legături personale cu Xi Jinping, dar aparținând tehnocrației chineze* - această categorie s-a dovedit extrem de utilă lui Xi Jinping, în perioada celui de-al treilea mandat. Prin recunoașterea importanței acestei categorii, președintele Xi Jinping a admis indirect că abordarea adoptată pe timpul primelor mandate – de instaurare a protejaților, aliaților și susținătorilor săi în funcții cheie – a fost utilă pentru acapararea puterii, dar nu și pentru succesul politicilor sale. În context, este de așteptat ca liderul chinez să continue să pună pe primul plan legăturile personale și loialitatea, dar, totodată, să valorizeze și criteriul competenței[31]. Au existat situații în care chiar dacă persoanele în cauză făceau parte din anturajul apropiat președintelui, precum premierul Li Qiang sau vice-premierul Ding Xuexiang, au fost marginalizate de către acesta.

9. *Facțiunea Xi Jinping* - a luat naștere ca parte a eforturilor de subminare a facțiunilor rivale și ca urmare a interferențelor repetate ale președintelui chiar și în numirile de nivel mediu și inferior, fapt ce a condus treptat la erodarea rolului conducerii colective, alterând în mod semnificativ mecanismul de recrutare a liderilor în cadrul PCC. Totodată, eforturile acestuia de modificare a ideologiei, a regulilor/ normelor existente ca documentație de partid a afectat și încadrarea politicienilor de elită în diferite facțiuni. Tacticile folosite pentru descurajarea/ stoparea încadrărilor în diferite grupări au îmbrăcat forme diverse, mergând de la acuzații de înființare de grupuri de interese opuse intereselor PCC (cazul Sun Lijun, fost vice-ministru al MPS) la cele de corupție (cazurile lui Ling Jihua și Zhou Yongkang). Pentru Xi Jinping important este nu medierea conflictelor de interese ale diverselor facțiuni, ci controlul absolut asupra PCC. Acest lucru s-a reflectat direct asupra acestor grupuri, care, treptat, din 2015 și până în prezent, par a cunoaște o reformare, o nouă taxonomie centrată pe susținerea politicilor lui Xi Jinping.

Cu alte cuvinte, conceptul de facționalism în politica chineză a dispărut în sensul cunoscut până acum, transformându-se în funcție de gradul de susținere a politicii liderului suprem în paralel cu măsura în care meritele personale pot și servesc politica președintelui. Prin urmare, apartenența la diferite facțiuni nu va mai constitui unicul criteriu pentru avansarea în cariera politică[32]. Este evident că Xi Jinping a impus o politică de înlocuire a structurilor formale, conduse de reguli solide de autoritate politică, cu structuri informale, care respectă în principal direcțiile de acțiune agreate de liderul suprem. O astfel de abordare a generat, deja, cristalizarea unei conduceri de tip maoist. Este evident că Xi Jinping și-a creat și consolidat propria facțiune, aliații și susținătorii

săi provenind din orașul său natal, din provinciile unde și-a desfășurat activitatea și unde a repurtat succese în campania sa de reformă economică, politică și de luptă anticorupție – Fujian și Zhejiang și în municipiile Shanghai, Tianjin, Chongqing și Beijing (astfel apar numele lui Huang Kunming, Li Xi și Cai Qi).

Tradiția lungă a lui Xi Jinping de a încălca regulile și convențiile PCC a făcut ca, la Congresul al 20-lea al PCC, să-și însușească titulatura de „nucleu al partidului pe viață", revizuind Carta PCC și consolidându-și poziția prin „ocuparea" CC și a BP cu membrii propriei facțiuni[33]. Drept urmare, nu se întrevăd probleme în ceea ce privește apariția unui potențial rival real la Congresul al 22-lea al PCC din 2032[34]. Cei numiți în PBSC au legături strânse în plan personal sau profesional cu Xi. Membrii mai tineri aleși în BP sau PBSC - Ding Xuexiang (1962), Yuan Jiajun (1962), Chen Min'er (1962), Liu Guozhong (1962), Li Shulei (1964), Chen Jining (1964) – vor atinge/ depăși vârsta de 68 de ani în 2032, ceea ce va determina eliminarea lor din cursa pentru menținerea în PBSC, respectiv de a fi propozabili ca succesori ai lui Xi. Rămân în atenție, totuși, reprezentanții din generația a 6-a: Huang Kunming (1956), Chen Xi (1953), Ding Xuexiang (1962), Liu He (1952), He Lifeng (1955), Zhong Shan (1955), Shu Guozeng (1956), Ying Yong (1957), Li Hongzhong (1956), Li Qiang (1959), Gong Zheng (1960), Lou Yangsheng (1959), Hu Heping (1962), Chen Yixin (1959), Liu Qi (1957)[35].

După Congresul al 19-lea, Xi Jinping a numit, la nivel regional, în funcții cheie – secretari de partid, guvernatori și primari în cele mai importante provincii și orașe – din rândul Facțiunii Xi Jinping. Numiri au avut loc și la nivel de vice-guvernatori sau rang echivalent în 31 districte administrative importante[36]. Aceste numiri demonstrează faptul că *Facțiunea Xi Jinping* domină eșaloanele superioare de conducere ale administrațiilor regionale: Li Qiang (1959), Li Xi (1956), Wang Dongfeng (1958), Yu Weiguo (1955), Tang Yijun (1961), Hu Huping (1962). În afară de protejații și susținătorii lui Xi, există și membri care aparțin clasei tehnocrate și care, prin activitatea lor, susțin politicile lui Xi – denumită *Facțiunea Apărării Aerospațiale*[37] - de exemplu, Zhang Guoqing (1964), inginer electrician, desfășurându-și cariera în cadrul „China North Industries Group Corp" (Norinco). „Tânărul mareșal al industriei de apărare" a devenit conducătorul Norinco în 1996 (avea 32 de ani). La fel este și cazul lui Chen Qiufa (1954) sau cel al lui Lou Qinjian (1956)[38].

Figura 2: *Facțiunea XI JINPING*
Sus (de la stânga): Chen Xi, He Lifeng, Wang Xiaohong
Jos (de la stânga): Chen Min'er, Cai Qi, Li Qiang,
Ding Huexiang

10. *Aripa militară* - o situație specială în cadrul politicii sale de numiri în funcții o reprezintă promovarea soției Peng Liyuan într-o funcție importantă din cadrul CMC, și anume în *Comitetul de evaluare a cadrelor*[39]. Unii analiști consideră că ascensiunea lui Peng Liyuan se datorează temerilor lui Xi generate de aparenta lipsă de fidelitate din partea conducerii APE. Astfel, deși armata chineză a fost întotdeauna sub controlul Partidului, implicarea directă a familiei liderului în procesul de vetting[40] face ca deciziile militare să fie influențate și mai mult de considerente politice/ se creează o rețea de loialitate față de Xi Jinping, reducând posibilitatea opoziției interne.

Deși așa-zisa „Armata Familiei Xi"[41] cuprinde oficiali de rang înalt din conducerea APE, aceasta se confruntă deja cu tensiuni, personalități precum gl.lt. Zhong Shaojun fiind înlăturate din funcție, chiar dacă se numărau

printre protejații președintelui chinez. Se cunoaște faptul că Xi a reușit să-și impună influența asupra APE abia în 2017, la sfârșitul primului mandat, prin exploatarea la maxim a reformelor impuse acesteia. În articolul din 2017, am afirmat că, după prima fază a reformei APE decisă de Xi Jinping, a avut loc promovarea în eșaloanele superioare a unor cadre militare prin „saltul" peste anumite poziții/ funcții sau acumulare de experiență în anumite garnizoane. Schimbările decise la acel moment s-au derulat atât la nivelul fostelor regiuni militare (RM), cât și la nivelul categoriilor de forțe, dorindu-se distrugerea grupurilor de interese de pe anumite niveluri de ierarhie militară, unde corupția era mai mult decât vizibilă, și eliminarea rezistenței față de reforme. Decizia lui Xi Jinping era de a constitui o nouă „facțiune" – *Facțiunea (fostei RM) Nanjing* – ca bază de dezvoltare a puterii sale în cadrul APE și susținere viitoare pentru programul de reformă militară[42].

În prezent, așa-zisa „Armata Familiei Xi" se confruntă cu probleme, acestea devenind „vizibile" odată cu dispariția ministrului apărării, generalul Li Shangfu, și a generalului Wei Fenghe. Ulterior au apărut o multitudine de acuzații de corupție la adresa unor oficiali de rang înalt, precum și decizia de a se reforma, încă o dată, structura de forțe a APE. Se presupune[43] și că înlăturarea protejaților și aliaților din APE exprimă temerea lui Xi Jinping la adresa propriei securități, fapt discutabil[44]. În plus, dimensiunea și scopul/ importanța CMC s-a redus semnificativ[45], unii specialiști afirmând că după Congresul al 21-lea al PCC, din 2027, schimbările în aripa militară vor și mai dramatice: nouă din cei 23 lideri ai APE vor fi schimbați, iar un alt lot de 11 este sub semnul întrebării. Normele aplicabile anterior „Epocii Xi Jinping"[46] prevedeau retragerea la 65 de ani pentru liderii din APE și la 70 - 72 de ani pentru liderii militari care fac parte din CMC, excepție făcând vicepreședinții CMC, pentru care nu exista limită de vârstă. În 2012, CMC era alcătuit din 11 membri (Xi Jinping, doi vicepreședinți și opt alți membri), în 2017 numărul s-a redus la șapte (Xi Jinping, doi vicepreședinți, patru membri), număr păstrat și în 2022. În prezent, după înlăturarea ministrului apărării și a directorului Departamentului Muncă Politică, CMC are doar cinci membri. Schimbările continuă să se deruleze nu numai în structurile de putere ale APE, dar și în ceea ce privește procedurile de avansare în grad, așa cum este cazul promovării la gradul de general cu trei stele, și în construirea carierei militare[47].

XI JINPING - AL TREILEA MANDAT LA CONDUCEREA PCC

Modalitatea în care Xi Jinping a menținut distanța față orice fel de facțiune, reformatoare sau conservatoare, chiar și față de unii dintre aliații și susținătorii săi, demonstrează abilitatea și duritatea politică ale acestuia. Acțiunile sale continuă să meargă pe vectorii politic și militar, dar planul intern are întâietate față de cel extern. Numeroasele reforme implementate demonstrează că liderul chinez urmărește păstrarea și consolidarea controlului asupra organelor de putere, dar și asupra populației, fiind extrem de „deranjat" de eventualele întârzieri/ tergiversări în implementarea politicilor sale, în ansamblul lor.

O măsură destinată consolidării controlului prezidențial o reprezintă și trecerea sub controlul organelor de partid a unor departamente și atribuții ce-i revin Consiliului de Stat. Astfel, Departamentul Frontul Unit al Muncii a asimilat trei dintre organele Consiliului de Stat: Comisia de Stat pentru probleme etnice, Administrația de Stat pentru Probleme religioase și Departamentul de supraveghere a muncii depuse de diaspora chineză. Este evident că Xi Jinping va continua să-și consolideze, respectiv să-și legitimeze, la nivel popular, poziția. Pandemia Covid-19, politicile de securitate extrem de dure, amestecul în economie și declinul acesteia, alături de vocile critice ale „seniorilor" din clasa politică (câți au mai rămas), reprezintă provocări la adresa puterii sale. Chiar dacă Biroul/ Oficiul General al CC al PCC a emis o directivă de atenționare la adresa acestor seniori, pentru nu mai exprima opinii „inadecvate" la adresa conducerii, acest lucru nu înseamnă că situația s-a rezolvat, că nu mai transpare în spațiul public vreun comentariu nedorit. Facțiunile care

par a „comenta” tot mai vocal și incisiv sunt: „prințișorii” aflați în afara granițelor statului, lideri din APE (Zhang Youxia) și o parte a tehnocraților. La aceștia se adaugă moștenitorii direcți ai foștilor lideri (precum Deng Pufang - primul fiu al lui Deng Xiaoping sau Hu Deping și Hu Dehua – fiii fostului secretar General al PCC, Hu Yaobang), foști membri ai PBSC, Zhu Rongji (fost premier) și Wen Jiabao, foști consilieri ai predecesorilor lui Xi Jinping[48].

Din acest punct de vedere, în pofida diverselor acte normative emise de conducerea PCC, Xi Jinping este conștient că trebuie să ducă o politică de compromis între politica de promovare a ideilor sale și politicile sociale și economice oficiale, cel puțin până când o parte dintre indicatorii economici esențiali se redresează. Acesta ar fi și motivul pentru care, în acest al treilea mandat, campania sa anticorupție a vizat o parte dintre susținătorii, aliații și chiar protejații săi. Astfel, se pot observa modificări și provocări în ceea ce privește existența Façțiunii Xi Jinping; deja s-a văzut că unii dintre prietenii lui Xi, precum Li Qiang, Ying Yong, Zhou Jianyong și Xu Liyi au avut de suferit, la nivel de importanță politică, din cauza unor evenimente de natură socială, economico-financiară sau a acuzațiilor de corupție/ mită. Pentru a reuși să-și impună ideile reformatoare, Xi Jinping nu poate avea în jurul său decât persoane integre, în adevăratul sens al cuvântului[49]. Chiar și eliminarea generalului Miao Hua, director al Departamentului de Muncă Politică și membru al CMC, un apropiat al președintelui chinez, arată cât de incisivă este atitudinea lui Xi Jinping în cadrul campaniei sale anticorupție.

Alți oficiali militari de rang înalt care au fost eliminați în 2024/ 2025 prin intermediul campaniei anticorupție au fost generalii Li Qiaoming (63 de ani), Qin Shutong (61 de ani) și Wang Chunning (61 de ani), membri ai celui de-al 20-lea CC al PCC. Au mai fost eliminați, din cadrul CNCNP, gl.lt. You Haitao (66 de ani) și vice-amiralul Li Pengcheng (61 de ani). Doisprezece dintre cei 56 de oficiali reținuți în anul 2024 (au fost 87 la nivelul anului 2023) au ocupat funcții în structurile centrale ale PCC și cele de stat: Wu Cunrong (61 de ani) – fost șef al Organismului Consultativ Politic Provincial din Shanxi, Tang Yijun - fost ministru al justiției, Tang Renjian- fost ministru al agriculturii, Tan Ruisong – fost președinte al corporației Industriei de Aviație etc.

Deși puterea politică a lui Xi Jinping s-a consolidat după Congresul 20 al PCC, China continuă să se confrunte cu o perioadă dificilă de redresare post-pandemică, înregistrându-se, în principal, un *pesimism economic, un consumerism lent și o acută criză imobiliară.* Se pare că anul 2025 va continua să înregistreze o creștere a decalajului dintre puterea personală a lui Xi Jinping și abilitatea sa de a obține rezultate concrete în cadrul guvernării. Deja procesul decizional a devenit un pic mai flexibil, acest lucru dovedind, încă o dată, adaptabilitatea ideologică a președintelui atunci când se pune problema atingerii intereselor politice concomitent cu reducerea volatilității politicilor publice și a incertitudinii economice și sociale. Este evident că rezultatele obținute rapid nu înseamnă mereu și rezultate de calitate, iar acest fapt rămâne dificil de acceptat de către liderul chinez atunci când se referă la politica sa de „dezvoltare egalitară, ecologică, inovatoare și deschisă”. Din păcate, această politică include altă viziune esențială a lui Xi Jinping, aceea că statul trebuie să joace un rol mai puternic în orientarea capitalului și a întreprinderilor (private) către obiective strategice, viziune care se dovedește că afectează creșterea economică a țării. Această abordare are un impact negativ direct asupra bugetelor administrațiilor locale și a încrederii antreprenorilor.

În timpul celei de-a Treia Plenare a CC a PCC, din 2024, au fost menționate reforme fiscale (consolidarea bazei de impozitare, stabilizarea economiei și reducerea inegalităților) necesare soluționării problemelor generate de creșterea limitărilor bugetare ale administrațiilor locale și, implicit, a ineficienței sistemului fiscal. Acest sistem a fost conceput pentru a centraliza veniturile, motiv pentru care, în prezent, a devenit inadecvat. O reformă în acest domeniu trebuie să

fie etapizată (cinci ani) și trebuie să aibă în vedere restructurarea datoriilor administrațiilor locale, pentru evitarea intrării în incapacitate de plată.

Un aspect pozitiv al politicilor lui Xi Jinping îl reprezintă introducerea conceptului de „noi forțe productive de calitate", o altă exprimare pentru promovarea inovărilor locale ca mijloc de diminuare a concurenței tehnologice externe. Xi Jinping a introdus conceptul în 2023, apreciind că acesta va viza înlocuirea modelului de creștere bazat pe investiții cu cel al inovării bazate pe productivitate, respectiv acționarea pe trei vectori: cercetare și descoperiri tehnologice, alocarea inovatoare a factorilor de producție și transformarea industriilor tradiționale. Creșterea prin inovare va avea nevoie, însă, de o modernizare/ îmbunătățire instituțională, de o alocare eficientă și adecvată a capitalului și de eliminarea protecționismului local. Toate aceste politici vor fi prezentate în viitorul Plan Cincinal (2026-2030).

În prezent, continuă să rămână problemele legate de tarifele pentru produsele chinezești, cererea internă redusă și supracapacitatea de producție. Nesiguranța economică, diminuarea încrederii publice și încetinirea ritmului de obținere a rezultatelor în implementarea reformelor au avut un efect profund asupra populației chineze. Deși aceste politici au fost bine primite, abandonarea acestora la sfârșitul lui 2022 a generat un sentiment puternic de neîncredere. Factori precum insecuritatea economică, scăderea prețurilor proprietăților și perspectivele limitate de angajare au determinat populația să economisească mai mult, fapt care a determinat scăderea creșterii economice. Este posibil ca dezamăgirea populației față de guvern să crească și să apară dorința de emigrare și reorientare către religie. Aceste evoluții sunt total contrare viziunii lui Xi Jinping privind dezvoltarea Chinei. Practicile religioase au crescut rapid în ultimii ani și, paradoxal, politicile restrictive ale PCC față de acestea au consolidat popularitatea lor. Cu alte cuvinte, președintele chinez se va confrunta, în 2025, nu numai cu recrudescența tensiunilor pe baze etnice, ci și cu cele generate de creșterea exprimărilor religioase, în disociere crescândă de idealurile PCC (a se înțelege cu doctrinele emanate de către Xi Jinping).

Doctrina Xi Jinping consideră că „cele trei forțe diabolice" care amenință securitatea Chinei sunt terorismul, extremismul și separatismul, ultimul devenind și jutificarea actualei doctrine oficiale. Prin urmare, Epoca Xi Jinping s-ar putea să vină cu diminuarea libertăților minorităților, deși, oficial, acestea nu sunt specificate în nici un document oficial al conducerii.

Dacă, la nivelul elitei politice, spațiul de manevră în ceea ce privește contestarea politicilor lui Xi Jinping este limitat, la nivelul clasei militare acest spațiu aproape că nu există. Campania anticorupție implementată de liderul chinez de la începutul activității sale a vizat cazurile foarte evidente de corupție și comportament inadecvat. În prezent, lipsa de transparență a acțiunilor a început să afecteze conducerea militară, respectiv eficiența operațională și încrederea personalului APE în conducerea militară chineză. Incisivitatea extremă a campaniei anticorupție ne arată, în mod clar, nivelul de control politic al PCC asupra conducerilor structurilor APE. Xi Jinping ne demonstrează că pentru implementarea tuturor ideilor sale de politică externă, de dezvoltare socială și, mai ales, militară, APE trebuie să devină un exemplu. În fapt, orice instituție sau organ care joacă un rol în scenariul de dezvoltare a ambițiilor conducerii supreme chineze trebuie să funcționeze fără greș.

În acest context, nu suntem de acord cu opiniile unor analiști care consideră că, în 2025, deși Xi Jinping va continua să domine jocul politic și elitele chineze, rivalitățile dintre diferitele curente și facțiuni se vor intensifica, mai ales în perspectiva stabilirii succesorului acestuia, generând un anumit nivel de instabilitate politică. Președintele chinez și-a demonstrat deja hotărârea de a controla cu mână de fier orice mișcare și orice voce contrară deciziilor sale. Politica sa autoritară de tip maoist („cine nu este cu mine, este împotriva mea") va continua să se se consolideze cel puțin la nivel ideologic și politic.

Un alt lucru care se așteaptă de la Xi Jinping este construcția unui *echilibru între controlul politic și stimulentele oferite elitelor pentru a contribui la dezvoltarea economiei, respectiv la realizarea unei guvernări eficiente.* La acestea se va adăuga și stabilirea unui control adecvat al noilor clase politice, respectiv a limitării/ eliminării de facțiuni și grupuri de interes. Liderul de la Beijing va continua campania anticorupție, țintele sale fiind persoanele care ocupă funcții de rang foarte înalt, dar și cele care apar/ se impun în competiția diferitelor rivalități între noile generații de cadre. Concentrarea puterii în mâinile lui Xi Jinping a consolidat disciplina în PCC și a redus autonomia cadrelor, tensiunile care s-ar putea manifesta fiind cele generate de incapacitatea acestora de a-și îndeplini responsabilitățile conform fișei postului.

EXISTĂ UN „APOI" DUPĂ EPOCA XI JINPING ?

Ne vom menține afirmația din articolul din 2017 cum că există suficient de multe variabile care trebuie luate în considerare atunci când se analizează principalele organe politice chineze. La fel de dificil va fi demersul de identificare a unui mecanism regulat care să explice operaţiunile din interiorul PCC, în special în ceea ce privește previziunea schimbărilor de personal, în contextul multiplicării deciziilor informale şi ale practicilor opace, cu reguli dificil de determinat, din sistemul politic chinez. Încă din 2015, evoluțiile de pe scena politică și socială au arătat că Xi Jinping dorește să fie cel mai influent om din stat, cel puțin până la Congresul al 21-lea al PCC (2027), când acesta va avea 74 de ani. În sprijinul acestei afirmații vine decizia acestuia de a numi oficiali din cadrul celei de-a șasea generații în organele importante ale PCC.

Aproape toți analiștii politici occidentali apreciază că una dintre prioritățile lui Xi Jinping pentru pregătirea Congresului 21 va fi stabilirea unui mecanism de alegere a succesorului său. Este evident că actualul președinte are intenția de a conduce până la Congresul 22 al PCC (în 2032), bazându-se pe numeroși oficiali ai 6G – Li Qiang, Chen Min'er, Ding Xuexiang etc. – dar care nu vor mai respecta criteriul de eligibilitate începând cu anul 2030. În mod normal, Xi Jinping va trebui să ia în considerare oficiali din generația a 7-a (7G), care sunt destul de numeroși[50]. Pentru 7G vor trebui să fie libere, în principalele organe de conducere politică, următoarele locuri: în CC - 30 oficiali/ 171 de locuri, CCDI - cinci oficiali/ 131 poziții. Pentru aceasta sunt oficiali precum Zhuge Yujie și Shi Guanghui, ca membri supleanți în CC. Propozabili pentru eșaloanele superioare în CC mai sunt și Liu Jie (1970), Yang Jinbo (1973), Liu Qiang (1971), Huang Zhiqiang (1970), Fei Gaoyun (1971), Guo Ningning (1970), Cui Yonghui (1970), Lu Dongliang (1973), Yang Fasen (1971), Liu Hongjian (1973) și Wei Tao (1970). Câțiva membri ai 7G, numiți ca supleanți în CC, vor putea fi tehnocrați, cu experiență în inginerie și managementul unităților din industria metalurgică, energetică și facilităților portuare, a activităților unităților bancare. Liu Qiang și Guo Ningning sunt exemple de tehnocrați ai domeniului financiar. Printre membrii 7G ai CCDI, Li Xinran (1972) pare a avea cele mai bune referințe – master în domeniul juridic și o carieră petrecută în totalitate în departamenetele CCDI[51].

Cu toate acestea, nici în 2024 nu am regăsit un succesor „desemnat" al lui Xi Jinping. Calculele care s-au făcut anterior luau în considerare regula privind limita de vârstă în PCC și faptul că o astfel de persoană va conduce pentru 10 ani, aceste premise impunând concluzia ca respectiva persoană care trebuie să intre în componența PBSC să aibă maxim 50 de ani. Până în prezent, în niciuna dintre structurile de putere nu găsim o astfel de persoană, majoritatea oficialilor apropiindu-se de vârsta de 60, respectiv 70 de ani, ceea ce înseamnă că se vor retrage în 5-10 ani din funcții, deci nu sunt opțiuni viabile pentru rolul de succesor al lui Xi Jinping.

Prin modificarea Constituției PCC - dar nu și a R.P. Chineze - și prin controlul său asupra votului în PBSC, Xi Jinping ar putea, *de facto*, să aibă suficientă putere politică pentru a manipula situația, putând obține un alt mandat fără invocarea unor situații de extremă criză (internă

sau externă). Acest fapt, însă, este puțin probabil în opinia majorității analiștilor, unii apreciind și că Xi Jinping nu va dori să rămână la vârful puterii politice, chiar dacă va instaura la conducerea țării un protejat, și nici nu va păstra conducerea CMC (așa cum au făcut unii dintre predecesorii săi) după încheierea mandatului.

În articolul din 2017 menționam faptul că, în ceea ce privește nominalizarea unui *succesor al lui Xi Jinping*, ar exista două posibilități: Chen *Min'er* (1960) sau *Li Qiang* (1959), amândoi fiind apropiați ai lui Xi. După 2022, ascensiunea lui *Cai Qi* pe scena politică îl face propozabil poziției de succesor al lui Xi Jinping.

Luând în considerare puterea acumulată de Xi Jinping până în prezent, dar și demersurile sale pe plan ideologic, de politică internă și externă, putem afirma că acesta dorește să-și vadă îndeplinită măcar una din previziunile sale – cea mai ardentă fiind unificarea cu Taiwanul. Aceasta ar implica faptul că actualul lider de la Beijing nu va numi un succesor nici pe timpul Congresului 21 al PCC, în 2027. Totuși, din componența PBSC, a BP și a CC al PCC am putea afla propozabilul cu cele mai mari șanse la funcția de Secretar General al PCC și președinte al R.P. Chineze. La nivelul anului 2024, președintele PBSC era Zhao Leji (numit în 10.03.2023), vicepreședinți ai PBSC erau Li Hongzhong, Wang Dongming, Xiao Jie, Zheng Jianbang, Ding Zhongli, Hao Mingjin, Cai Dafeng, He Wei, Wu Weihua, Tie Ning, Peng Qinghua, Zhang Qingwei, Losang Jamcan, Shohrat Zakir, Secretar general al PBSC este Liu Qi (numit în 10.03.2023), iar Prim-secretar al PCC este Cai Qi.

Consolidarea puterii lui Xi Jinping a redefinit echilibrul politic din cadrul elitei chineze, subordonând facțiunile tradiționale și întărind controlul centralizat al PCC. Pe fondul epurărilor politice și al provocărilor economice, viitorul regimului său va depinde de capacitatea de a menține stabilitatea internă și de a gestiona presiunile internaționale.

BIBLIOGRAFIE

1. ANCUȚ Isabela, „Jocuri de Putere: Noua elită politică chineză în perspectiva Congresului al 19-lea al Partidului Comunist Chinez”, revista *Infosfera*, nr. 2, 2017.
2. BRAZIL Matthew, *The Qin Gang Saga Reveals Security Gaps*, Jamestown Foundation, China Brief, vol. 24, nr. 19, 04.10.2024.
3. DOTSON John, *Year-End CCP Politburo Meetings Stress Political Loyalty—and Hint at Potential Shake-Ups in the Party Bureaucracy,* Jamestown Foundation, China Brief, vol. 21, nr. 1, 13.01.2020.
4. ECONOMY Elizabeth C., *The Third Revolution: Xi Jinping and the New Chinese State*, Council on Foreign Relations, 17.05.2018, https://www.cfr.org/event/third-revolution-xi-jinping-and-new-chinese-state-elizabeth-c-economy.
5. JOHNSON Ian, *Xi Jinping Exposed*, Council on Foreign Relations, 23.10.2022; https://www.cfr.org/blog/xi-jinping-exposed.
6. JOHNSON Ian, *Qin Gang's Removal Puts the Focus on Xi Jinping's Leadership*, Council on Foreign Relations, 26.07.2023, https://www.cfr.org/blog/qin-gangs-removal-puts-focus-xi-jinpings-leadership.
7. KENNETH W. Allen, *Assessment of PLA Leaders at the End of 2024*, Jamestown Foundation, China Brief, vol. 25, nr. 1, 17.01.2025.
8. KURLANTZICK Joshua, *My Previous Book on State Capitalism in China: Right Idea, Wildly Underestimated*, Council on Foreign Relations, China Studies, 17.10.2022.
9. LAM Willy Wo-Lap, *Xi Jinping Consolidates Power by Promoting Alumni of the Nanjing Military Region*, Jamestown Foundation, China Brief, vol. 15, nr. 1, 09.01.2015.
10. LAM Willy Wo-Lap, *The Irresistible Rise of the "Xi Family Army"*, Jamestown Foundation, China Brief, vol. 17, nr. 13, 20.10.2017.
11. LAM Willy Wo-Lap, *The Xi Jinping Faction Dominates Regional Appointments After the 19th Party Congress*, Jamestown Foundation, China Brief, vol. 18, nr. 2, 13.02.2018.
12. LAM Willy Wo-Lap, *Xi Jinping Steers China back to the Days of Mao Zedong*, Jamestown Foundation, China Brief, vol. 18, nr. 4, 12.03.2018.
13. LAM Willy Wo-Lap, *Who are Xi Jinping's Enemies?*, Jamestown Foundation, China Brief, vol. 19, nr. 1, 04.12.2018.
14. LAM Willy Wo-Lap, *Xi Jinping Boosts the Party's Control and His Own Authority,* Jamestown Foundation, China Brief, vol. 21, nr. 1, 13.01.2020.
15. LAM Willy Wo-Lap, *"Helmsman" Xi Jinping primed to rule at least until the early 2030s,* Jamestown Foundation, China Brief, vol. 20, nr. 20, 13.11.2020.
16. LAM Willy Wo-Lap, *Early Warning Brief: Xi Jinping Issues Tough Warnings to Enemies Within the Party*, Jamestown Foundation, China Brief, vol. 21, nr. 15, 23.07.2021.
17. LAM Willy Wo-Lap, *Xi Jinping is Poised to Become "Leader for Life" in Exchange for Sharing Politburo Seats with Rivals,* Jamestown Foundation, China Brief, vol. 22, nr. 10, 27.05.2022.
18. LAM Willy Wo-Lap, *Will the Xi Jinping Leadership Take up Reformist Policies After the 20th Party Congress?*, Jamestown Foundation, China Brief, vol. 22, nr. 16, 09.09.2022.
19. LAM Willy Wo-Lap, *Will a Successor to Xi Jinping Emerge from the Party's Seventh-Generation Leadership?*, Jamestown Foundation, China Brief, vol.22, nr. 23, 16.12.2022.
20. LAM Willy Wo-Lap, *The National People's Congress Exposes Xi Jinping's Problems*, Jamestown Foundation, China Brief, vol. 24, nr. 6, 15.03.2024.
21. LAM Willy Wo-Lap, *Peng Liyuan Rises Up the Ranks: Implications for Xi's Despotic Rule*, Jamestown Foundation, China Brief, vol. 24, nr. 11, 24.05.2024.
22. LAM Willy Wo-Lap, *Xi Sets Out 2029 Vision*

at Third Plenum, Jamestown Foundation, China Brief, vol. 24, nr. 15, 26.07.2024.
23. LEIBOLD James, *New Textbook Reveals Xi Jinping's Doctrine of Han-Centric Nation-Building,* Jamestown Foundation, China Brief, vol. 24, nr. 11, 24.05.2024.
24. MINZNER Carl, *What direction for legal reform under Xi Jinping?,* Jamestown Foundation, China Brief, vol. XII, nr. 24, 14.12.2012.
25. MITCHELL Tom, "Speculation Grows Xi Jinping will Defy China Rule on Leadership Retirement", *Financial Times,* modificat 11.10.2016; https://www.ft.com/content/09cc1044-8f77-11e6-a72e-b428cb934b78; http://chinafocus.us/2016/10/24/getting-ahead-in-the-politburo-predicting-who-will-be-enthroned-in-chinas-19th-party-congress/
26. PURBRICK Martin, *All the President's Men – Corruption in the Xi Jinping Era*, Jamestown Foundation, China Brief, vol. 22, nr 17, 20.09.2022.
27. VEG Sebastian, "China`s Political Spectrum under Xi Jinping", 11.08.2014, în *The Diplomat*, www.thediplomat.com/2014/china-s-political-spectrum-under-xi-jinping/11.08.2014.
28. ZHIYUE Bo, *[Party and the man] Factions and fence-sitters in Xi Jinping's China,* ThinkChina Forum, Bo Zhiyue China Institute, 27.09.2022, https://www.thinkchina.sg/politics/party-and-man-factions-and-fence-sitters-xi-jinpings-china, Singapore Press Holdings.
29. ZHOU Chutian, "Who will be enthroned at China`19th Party Congress", în *The Diplomat,* http://Thediplomat.Com/2016/10/Who-Will-Be-Enthroned-At-Chinas-19th-Party-Congress/ 26.10.2016.

[1] Această idee am enunțat-o și analizat-o pe larg în cadrul unui alt articol, „Jocuri de Putere: Noua elită politică chineză în perspectiva Congresului al 19-lea al Partidului Comunist Chinez", în *Infosfera,* nr. 2, 2017.

[2] Zhou Chutian, "Who will be enthroned at China`19th Party Congress", în *The Diplomat,* http://thediplomat.com/2016/10/Who-Will-Be-Enthroned-At-Chinas-19th-Party-Congress/ 26.10.2016.

[3] 2012-2017, 2017-2022 și 2022-2027.

[4] Carl Minzner, "What direction for legal reform under Xi Jinping?", Jamestown Foundation, China Brief, vol. XII, nr. 24, 14.12.2012.

[5] Veg Sebastian, "China`s Political Spectrum under Xi Jinping", 11.08.2014, în *The Diplomat,* www.thediplomat.com/2014/china-s-political-spectrum-under-xi-jinping/11.08.2014.

[6] Tom Mitchell, "Speculation Grows Xi Jinping Will Defy China Rule on Leadership Retirement", *Financial Times,* modificat 11.10.2016; https://www.ft.com/content/09cc1044-8f77-11e6-a72e-b428cb934b78; http://chinafocus.us/2016/10/24/getting-ahead-in-the-politburo-predicting-who-will-be-enthroned-in-chinas-19th-party-congress/; Colecția online 2012 – 2016 a China Brief/Jamestownfoundation.

[7] Xi Jinping, *Work on Real Things,* p. 440–453.

[8] Lam Willy Wo-Lap, "Xi Jinping Steers China back to the Days of Mao Zedong", Jamestown Foundation, China Brief, vol. 18, nr. 4, 12.03.2018.

[9] Xi Jinping, Op.cit., p. 421.

[10] PBSC este cel mai înalt organism decizional din China. Anterior regimului lui Xi Jinping, fiecare dintre cei șapte membri ai CPBP aveau câte un portofoliu: numărul 1 era secretarul general al PCC și președinte al PCC și al Comisiei Militare Centrale de Stat, persoana care superviza politica externă și avea responsabilitatea de a prezida întâlnirile extinse ale PBSC și ale Biroului Politic, precum și lucrările Secretariatului PCC; numărul 2 - premierul, responsabil de managementul sistemul birocratic al statului; numărul 3 - președintele Comitetului Permanent al CNP; numărul 4 - președintele organului politic consultativ, CPCPC, responsabil pentru legătura cu grupurile non-comuniste, cu cele opt partide politice ale minorităților din China și asociațiile religioase; numărul 5 - Secretarul PCC, responsabil și de activitățile privind ideologia și propaganda comunistă; numărul 6 - șeful Comisiei Centrale de Inspecție privind Disciplina de Partid/CCID, cu competențe legate de investigarea cazurilor de corupție, alte forme de abuz, la nivelul

conducerii partidului; numărul 7 - prim vice-premierul Consiliului de Stat. Principiul conducerii colective presupunea, în general, că deciziile majore ale secretarului general al PCC erau unanim aprobate de ceilalţi membri ai PBSC.

[11] În plus, au fost eliminați și susținătorii și discipolii lui Guo Boxiong (precum generalul Du Jincai) și Xu Caihou, oficiali din fosta CMC. Similar au fost înlăturați toți susținătorii și discipolii lui Jiang Zemin, respectiv ai lui Zeng Qinghong (vice-președintele lui Ziang Zemin): Meng Jianzhu (fost șef al Comisiei Centrale pentru Probleme Juridice și Politice ale PCC (CPLAC), Gua Shengkun (fost șef al Ministerului Securității Publice - MPS), Geng Huichang (fost șef al Ministerului Securității Statului – MSS).

[12] Lam Willy Wo-Lap, "The Xi Jinping Faction Dominates Regional Appointments After the 19th Party Congress", Jamestown Foundation, China Brief, vol. 18, nr. 2, 13.02.2018.

[13] Lam Willy Wo-Lap, "Will a Successor to Xi Jinping Emerge from the Party's Seventh-Generation Leadership?", Jamestown Foundation, China Brief, vol. 22, nr. 23, 16.12.2022.

[14] În acest sens, exemple relevante sunt Huang Kunming - a ocupat funcția de șef CPLAC, Ding Xuexiang – șef CCDI, Li Shulei – șef al Departamentului Propagandă.

[15] Isabela Ancuț, Op.cit..

[16] BP include 25 de membri. În structura sa sunt cuprinși reprezentanţi ai conducerii PCC, ai conducerii de stat, ai provinciilor, ai conducerii militare, ai Parlamentului (Congresul Naţional al Poporului/CNP) şi un reprezentant al unui organism politic consultativ (Comitetul Naţional al Conferinţei Politice Consultative a Poporului Chinez – CPCPC). Printre membrii a căror responsabilitate vizează activitatea PCC, trei conduc portofolii sensibile, fiecare dintre acestea fiind considerate, de către PCC, cruciale pentru menţinerea conducerii PCC: şeful Departamentului Organizare/DO, structură responsabilă de recrutarea membrilor de partid şi repartizarea sarcinilor pentru aceştia; șeful Departamentului Propagandă/DP, structură responsabilă de transmiterea mesajelor PCC, controlul mass-media şi ideologie; şeful Comisiei Centrale pentru Politici şi Legislaţie, structură care supraveghează aparatul de securitate, inclusiv tribunalele, birourile procurorilor, birocraţia securităţii de stat interne şi externe şi, împreună cu Comisia Militară Centrală şi Consiliul de Stat, supraveghează forţele paramilitare.

[17] Carl Minzner, "Delay in China's Annual Fall Party Plenum Meeting: A Sign of Deepening Institutional Erosion?", Council on Foreign Relations, China Studies, 27.11.2023.

[18] Congresul 8 a avut loc în 1950, iar Congresul 9 în 1969.

[19] Lam Willy Wo-Lap, "Xi Jinping Boosts the Party's Control and His Own Authority", Jamestown Foundation, China Brief, vol. 21, nr 1, 13.01.2020.

[20] Joshua Kurlantzick, "My Previous Book on State Capitalism in China: Right Idea, Wildly Underestimated", Council on Foreign Relations, China Studies, 17.10.2022.

[21] Manualul a fost realizat sub îndrumarea lui Pan Yue, locțiitorul șefului Departamentului Frontul Unit de Muncă, responsabil de politicile minzu, și director al Comisiei privind problemele naționale etnice.

[22] James Leibold, "New Textbook Reveals Xi Jinping's Doctrine of Han-Centric Nation-Building", Jamestown Foundation, China Brief, vol. 24, nr. 11, 24.05.2024.

[23] Lam Willy Wo-Lap, op.cit.

[24] Bo Zhiyue, "[Party and the man] Factions and fence-sitters in Xi Jinping's China", ThinkChina Forum, Bo Zhiyue China Institute, Singapore Press Holdings, 27.09.2022, https://www.thinkchina.sg/politics/party-and-man-factions-and-fence-sitters-xi-jinpings-china.

[25] Prima generație (1949-1976) - lider Mao Zedong, a doua generație (1976-1989) - lider Deng Xiaoping, a treia generație (1992-2003) - lider Jiang Zemin, a patra generație (2003-2012) - lider Hu Jintao, a cincea generație (2012-probabil 2022) - lider XI Jinping. Sub mandatul lui Xi Jinping a apărut și a șasea generație de prinților (cei născuți în anii 50-60) și cei din generația a șaptea (cei născuți în anii 70).

[26] Membrii LTC sunt influenți cu precădere în regiuni/provincii, urmând politica lui Hu – „regiunile înconjoară centrul" – care dorea să contracareze tendințele autoritariste ale șefului său, fostul președinte Jiang Zemin, care a condus Grupul Shanghai, influent cu precădere în metropolă (Voice Of America, 12.01.2016; Oriental Daily/Hong Kong, 04.07.2015).

[27] Precum Ling Jihua – fost director al Biroului/ Oficiului General al PCC, Qin Yizhi – șef al LTC în 2017, Li Yuanchao – fost vice-președinte, Liu Qibao – fost șef al Departamentului Propagandă sau Lu Hao

[28] Lam Willy Wo-Lap, "Xi Jinping Boosts the Party's Control and His Own Authority", Jamestown Foundation, China Brief, vol. 21, nr. 1, 13.01.2020.

[29] Isabela Ancuț, Op.cit.

[30] Ian Johnson, "How Xi Will Consolidate Power at China's Twentieth Party Congress", China Studies, Council on Foreign Relations, 05.10.2022; Johnson Ian, Qin Gang's Removal Puts the Focus on Xi Jinping's Leadership, China Studies, Council on Foreign Relations, 26.07.2023.

[31] Lam Willy Wo-Lap, "Xi Jinping Boosts the Party's Control and His Own Authority", Jamestown Foundation, China Brief, vol. 21, nr.1, 13.01.2020.

[32] Lam Willy Wo-Lap, "Helmsman" Xi Jinping primed to rule at least until the early 2030s", Jamestown Foundation, China Brief, vol. 20, nr. 20, 13.11.2020.

[33] Lam Willy Wo-Lap, "At China's 'Two Sessions', Xi Jinping Leaves His Mark on the Party State", Jamestown Foundation, China Brief, vol. XVIII, nr. 5, 26.03.2018.
[34] Lam Willy Wo-Lap, "Helmsman" Xi Jinping primed to rule at least until the early 2030s", Jamestown Foundation, China Brief, vol. 20, nr. 20, 13.11.2020.
[35] John Dotson, "Year-End CCP Politburo Meetings Stress Political Loyalty – and Hint at Potential Shake-Ups in the Party Bureaucracy", Jamestown Foundation, China Brief, vol. 21, nr. 1, 13.01.2020.
[36] Lam Willy Wo-Lap, "Xi Jinping Boosts the Party's Control and His Own Authority", Jamestown Foundation, China Brief, vol. 21, nr. 1, 13.01.2020; Zhiyue Bo, [Party and the man] Factions and fence-sitters in Xi Jinping's China, ThinkChina, Bo Zhiyue China Institute, 27.09.2022, https://www.thinkchina.sg/politics/party-and-man-factions-and-fence-sitters-xi-jinpings-china.
[37] Lam Willy Wo-Lap, "The Xi Jinping Faction Dominates Regional Appointments After the 19th Party Congress", Jamestown Foundation, China Brief, vol. 18, nr. 2, 13.02.2018.
[38] Lam Willy Wo-Lap, "Xi Jinping is Poised to Become "Leader for Life" in Exchange for Sharing Politburo Seats with Rivals", Jamestown Foundation, China Brief, vol. 22, nr. 10, 27.05.2022.
[39] Lam Willy Wo-Lap, "Peng Liyuan Rises Up the Ranks: Implications for Xi's Despotic Rule", Jamestown Foundation, China Brief, vol. 24, nr. 11, 24.05.2024.
[40] În perioada 2015 – 2016, procesul de vetting al cadrelor era realizat de către Departamentul General de Politică, dar prin reorganizarea unităților CMC problemele disciplinare și de loialitate au fost preluate de Comitetul menționat mai sus, înființat la sfârșitul lui 2022.
[41] Lam Willy Wo-Lap, "The Irresistible Rise of the "Xi Family Army", Jamestown Foundation, China Brief, vol. 17, nr. 13, 20.10.2017.
[42] Jamestown Foundation, China Brief, vol. 16, nr. 1, 12.01.2016.
[43] Idem.
[44] Idem.
[45] Allen W. Kenneth, "Assessment of PLA Leaders at the End of 2024", Jamestown Foundation, China Brief, vol. 25, nr. 1, 17.01.2025.
[46] Retragerea la 65 de ani pentru liderii din APE și la 70/72 de ani pentru liderii militari care fac parte din CMC, excepție făcând vice-președinții CMC pentru care nu există limită de vârstă.
[47] Allen W. Kenneth, "Assessment of PLA Leaders at the End of 2024", Jamestown Foundation, China Brief, vol. 25, nr. 1, 17.01.2025.
[48] Lam Willy Wo-Lap, "Who are Xi Jinping's Enemies?", Jamestown Foundation, China Brief, vol. 19, nr. 1, 04.12.2018.
[49] Lam Willy Wo-Lap, "Will the Xi Jinping Leadership Take up Reformist Policies After the 20th Party Congress?", Jamestown Foundation, China Brief, vol. 22, nr. 16, 09.09.2022.
[50] Lam Willy Wo-Lap, "Xi Jinping is Poised to Become "Leader for Life" in Exchange for Sharing Politburo Seats with Rivals", Jamestown Foundation, China Brief, vol. 22, nr. 10, 27.05.2022.
[51] Lam Willy Wo-Lap, "The Xi Jinping Faction Dominates Regional Appointments After the 19th Party Congress", Jamestown Foundation, China Brief, vol. 18, nr. 2, 13.02.2018; Lam Willy Wo-Lap, "Xi Jinping Boosts the Party's Control and His Own Authority", Jamestown Foundation, China Brief, vol. 21, nr. 1, 13.01.2020.

PERSPECTIVE ASUPRA TENSIUNILOR DIN STRÂMTOAREA TAIWAN

*Mihai VIDESCU**

Abstract

The Taiwan Strait has always been a region characterized by high tensions, both military and political, drawing global attention due to its geopolitical importance. This paper examines the different perspectives on the possibility of war in the Taiwan Strait, focusing on Taiwan's military power and the possible implications of a conflict in the area. The paper briefly explores the historical relationship between Taiwan and China and the significance of Taiwan in terms of security and global trade. The role of external powers, especially the United States, is also discussed, looking at military support and diplomatic policies towards Taiwan. The paper analyzes four scenarios (with different degrees of plausibility) regarding the potential war and it concludes by suggesting that dialogue and international cooperation might be the key to maintaining peace and avoiding conflict in the Taiwan Strait.

***Keywords**: Taiwan Strait; war; geopolitical tensions; military support; global powers; United States; economic impact; regional organizations.*

ELEMENTE INTRODUCTIVE

Evoluând în ultimele două secole de la statutul de colonie până la stadiul de națiune democratică și prosperă, Taiwanul are astăzi un rol important în securitatea și economia din Asia de Sud-Est. După perioade precum colonizarea japoneză și retragerea pe insulă a guvernului Republicii Chineze, în 1949, Taiwanul a devenit un motor economic la nivel regional și global, evidențiindu-se în ultimele decenii prin industria semiconductorilor, relevantă pentru tehnologii avansate (de la dispozitive inteligente la tehnică militară). În plus, situarea sa la intersecția unor importante rute maritime consolidează dimensiunea strategică a insulei, făcând din Taiwan un actor economic și geopolitic de prim rang.[1]

Pe de altă parte, din perspectiva securității regionale, relația tensionată cu China continentală (R.P. Chineză) definește o mare parte a istoriei recente a Taiwanului. Beijingul continuă să revendice suveranitatea asupra Taiwanului, după separarea politică din 1949, menținând ridicate presiunile diplomatice și militare. Strâmtoarea Taiwan este adesea scena unor demonstrații de forță, incursiunile Beijingului în spațiul aerian și maritim taiwanez fiind frecvente. Totuși amenințările chineze nu au împiedicat Taiwanul

Autorul este expert în cadrul Ministerului Apărării Naționale.

din procesul de modernizare a forțele armate; astfel, insula și-a consolidat apărarea prin strategii defensive, dar și prin parteneriate (în special cel cu Statele Unite ale Americii) care susțin securitatea Taiwanului și stabilitatea regională[2].

Taiwanul contrastează cu regimul autoritar al R.P. Chineze, fiind perceput, în general, drept un simbol al democrației și libertăților civile în regiune. Prin reformele democratice și consolidarea propriei identități naționale, Taiwanul rezistă presiunilor Beijingului și, în același timp, continuă să aloce resurse pentru educație și inovație, iar firme de renume (ex.: Taiwan Semiconductor Manufacturing Company/ TSMC) favorizează progresul în domenii precum inteligența artificială și energiile regenerabile. Cu o economie robustă, o poziție strategică importantă și parteneriate internaționale solide, Taiwanul rămâne un actor cheie în menținerea echilibrului de putere în regiunea Indo-Pacific și în economia mondială[3].

CONTEXT GEOPOLITIC REGIONAL

Peisajul geopolitic din Asia de Sud-Est este legat de tensiunile militare din jurul Taiwanului, mulți actori statali și non-statali având propriile interese în zonă. R.P. Chineză consideră insula o problemă teritorială fundamentală, esențială pentru identitatea sa națională și obiectivele de securitate. Viziunea Beijingului are ecouri față de alte țări din regiune, influențate de proximitatea lor față de Taiwan și de relațiile economice și strategice atât cu R.P. Chineză, cât și cu SUA. Țări precum Filipine, Vietnam și Malaiezia se află în diferite forme de competiție maritimă cu China, fiind îngrijorate de creșterea prezenței militare a Beijingului în Marea Chinei de Est și Marea Chinei de Sud. Intensificarea militarizării celor două mări și rolul strategic al Taiwanului în a împiedica expansiunea R.P. Chineze în regiune complică situația de securitate[4].

Asociația Națiunilor din Asia de Sud-Est (ASEAN) se confruntă cu dificultăți în echilibrarea relațiilor SUA - R.P. Chineză și menținerea stabilității în regiune, având în vedere interesele naționale diferite și tensiunile internaționale crescute. Deși statele membre adoptă o poziție de neutralitate și promovează dialogul, pentru a evita escaladarea tensiunilor în strâmtoarea Taiwan, preocupările legate de politica externă asertivă a Beijingului, un partener economic major, determină aceste state să evite o poziție fermă privind statutul insulei. Totuși, tensiunile din strâmtoarea Taiwanului și comportamentele provocatoare ale forțelor armate chineze în Marea Chinei de Sud au determinat unele state, precum Filipine, să caute o colaborare mai strânsă cu autoritățile de la Taipei. În acest context, capacitatea statelor ASEAN de a menține acest echilibru va fi testată pe măsură ce rivalitatea dintre China și SUA se va intensifica[5].

Complementar, AUKUS și QUAD reprezintă alianțe importante în regiunea Asia-Pacific, influențând securitatea și echilibrul de putere. AUKUS (format de cooperare care include Australia, Regatul Unit și Statele Unite) se concentrează pe îmbunătățirea capacităților militare ale Australiei, inclusiv prin dezvoltarea de submarine cu propulsie nucleară, pentru a contracara influența R.P. Chineze în regiune. QUAD (SUA, Japonia, India și Australia), de asemenea, promovează colaborarea între cele patru state membre în domeniile securității maritime și economic pentru a menține echilibrul și a limita ambițiile regionale ale Beijingului. Taiwanul este un punct central al rivalităților din spațiul redefinit, în ultimii ani, cu denumirea de Indo-Pacific, în condițiile în care R.P. Chineză percepe crearea AUKUS și QUAD drept o amenințare față de ambițiile sale regionale[6].

În plus, actori non-statali, precum corporații internaționale și ONG-uri, influențează geopolitica Taiwanului, insula fiind esențială în lanțul global de aprovizionare, în special în industria semiconductorilor, vitală pentru economiile din Asia de Sud-Est. Aceste relații economice complică situația diplomatică și

militară, deoarece țările din regiune trebuie să facă față presiunilor R.P. Chineze, care își folosește influența economică pentru a modela politicile regionale. Într-o perioadă de mare dependență economică față de R.P. Chineză, entitățile non-statale joacă un rol tot mai activ în formularea de răspunsuri la problema Taiwanului[7].

POLITICA MILITARĂ A TAIWANULUI

Situația militară din jurul Taiwanului rămâne una dintre cele mai delicate și importante probleme geopolitice ale prezentului, tensiunile din zonă continuând să fie alimentate de poziția autorităților de la Beijing, care consideră Taiwanul parte a teritoriului chinez și au semnalat, în mod repetat, intenția de a folosi forța pentru a-l reintegra. Armata Populară de Eliberare (APE) a Chinei a avansat semnificativ în modernizarea sa, axându-se pe capabilități de atac la distanțe mari. Printre elementele cheie ale strategiei chineze se numără sistemele de rachete balistice cu rază lungă de acțiune DF-21D și DF-26, care pot viza portavioanele americane și bazele militare din regiunea Pacificului. În plus, avioanele de vânătoare chineze J-20 constituie o componentă esențială în competiția aeriană, oferindu-le chinezilor posibilitatea de a provoca forțele aeriene ale SUA[8].

Forțele armate taiwaneze sunt formate din forțe terestre, marină, forțe aeriene și un comandament cibernetic în curs de dezvoltare, fiecare având un rol esențial în apărarea insulei. Deși este semnificativ mai mică decât APE a Chinei, armata taiwaneză s-a concentrat pe modernizare, pregătire avansată și soluții inovatoare pentru a-și consolida capacitatea de apărare. Astfel, forțele terestre au misiunea de a proteja teritoriul, fiind dotate cu vehicule blindate modernizate, artilerie performantă și unități de infanterie bine antrenate. Printre echipamentele cheie se numără tancurile M1A2T Abrams, achiziționate recent din SUA[9], alături de modele modernizate pe plan local, precum CM-11 și CM-12. În plus, forțele taiwaneze sunt înzestrate cu sisteme mobile de rachete și apărare aeriană, cum ar fi Tien Kung (Sky Bow), concepute pentru a intercepta rachete balistice și de croazieră.

Forțele navale joacă un rol vital în protejarea frontierelor maritime și a rutelor comerciale, operând distrugătoare, fregate, corvete și ambarcațiuni rapide dotate cu rachete avansate. Pentru a contracara eventualele blocade și atacuri amfibii, industria de apărare a dezvoltat propriile sisteme de rachete anti-navă, precum Hsiung Feng II și III, și a demarat construcția unor submarine indigene. În ceea ce privește forțele aeriene, acestea dispun de o flotă diversificată de avioane de luptă, atât fabricate pe plan local, cât și achiziționate din străinătate. Printre tipurile de avioane deținute pot fi enumerate F-16V Viper modernizate, Mirage 2000-5 și AIDC F-CK-1 Ching-Kuo. Apărarea aeriană este susținută de baterii de rachete Patriot și Sky Bow, menite să intercepteze orice amenințare înainte de a ajunge pe teritoriul insulei [10].

Confruntându-se cu o putere militară net superioară, Taiwanul a adoptat o apărare bazată pe așa-numita strategie a „porcului spinos” (*porcupine defense*), care se axează pe mobilitate, structuri de comandă descentralizate și atacuri de precizie. Pentru a spori eficiența defensivă conducerea militară taiwaneză a investit în unități mobile de rachete, mine navale și tehnologii avansate de drone, capabile să monitorizeze și să contracareze activitățile APE din vecinătatea insulei.

Suplimentar componentei militare convenționale, Taiwanul acordă o importanță sporită securității cibernetice, luând în considerare faptul că se confruntă frecvent cu atacuri cibernetice asupra infrastructurii sale critice, în special din partea R.P. Chineze. Pentru a răspunde acestor amenințări, la nivelul forțelor armate taiwaneze a fost înființată o unitate specializată de apărare cibernetică și s-au dezvoltat capacități de război informațional, menite să combată dezinformarea și influențele externe asupra opiniei publice[11].

Pe fondul tensiunilor regionale, liderii de la Taipei au reintrodus serviciul militar obligatoriu

cu durata de un an, începând din 2024, ca parte a unui efort mai amplu de pregătire și creștere a efectivelor. De asemenea, autoritățile au extins programele de pregătire a rezerviștilor pentru a asigura o mobilizare eficientă[12]. În condițiile în care există premisele confruntării cu un adversar mult mai puternic, Taiwanul își adaptează permanent strategia militară, punând accent pe tehnologie, război asimetric și alianțe strategice. Din această perspectivă, prin investiții în echipamente indigene, exerciții militare comune și reforme în domeniul apărării, Taiwanul își menține o poziție defensivă solidă[13].

SUA sunt principalul partener al Taiwanului în domeniul apărării, oferind sprijin militar, instruire și echipamente moderne. Astfel, Washingtonul a aprobat mai multe contracte de livrare a unor sisteme de armament, printre care rachete Stinger, Harpoon și echipamente radar avansate, menite să îmbunătățească capacitățile defensive ale forțelor taiwaneze. Cu toate că nu face parte dintr-o alianță militară (precum NATO), Taiwanul menține relații de securitate strânse cu mai multe state democratice din regiune, inclusiv Japonia (care și-a exprimat dorința de a colabora mai mult în domeniul apărării regionale).

Deși SUA nu au un tratat formal de apărare cu Taiwanul, prezența forțelor militare americane în regiune este crucială pentru securitatea insulei, inclusiv prin sprijinul strategic acordat insulei. SUA dispun de numeroase forțe în Oceanul Pacific, inclusiv portavioane, submarine și avioane F-35, staționate în baze din Japonia și Coreea de Sud. De asemenea, au instalat sisteme de apărare antirachetă, precum THAAD, și distrugătoare dotate cu sisteme Aegis pentru a proteja regiunea de rachetele chineze. Aceste resurse sunt esențiale pentru a descuraja o agresiune din partea Beijingului, însă creșterea capacităților chineze de tip „anti-access/ area denial" (A2/AD) reprezintă o provocare permanentă pentru forțele americane[14].

Totodată, Japonia joacă un rol esențial în strategia de descurajare față de R.P. Chineză, pe fondul poziției sale geografice și a alianței cu SUA. Forțele de autoapărare ale Japoniei sunt dotate cu tehnologii avansate, cum ar fi sisteme de interceptare a rachetelor SM-3 și Aegis, precum și aeronave F-35. Datorită apropierii de Taiwan, Japonia ar fi un actor cheie într-un eventual conflict, oferind sprijin logistic și ajutând la restricționarea forțelor chineze la nord de „primul lanț de insule". Totuși, Constituția pacifistă a Japoniei limitează implicarea directă în conflicte externe[15].

SCENARII PRIVIND RELAȚIA TAIWAN – R.P. CHINEZĂ

Situația din jurul Taiwanului implică o dinamică complexă între capabilitățile militare ale R.P. Chineze, Taiwanului, SUA și Japoniei: Taiwanul se bazează pe o apărare asimetrică, susținută de sprijinul SUA și al Japoniei, dar creșterea puterii militare chineze, în special în domeniul rachetelor și aviației, reprezintă o amenințare semnificativă. Washingtonul continuă să mențină o prezență militară puternică în regiune, dar o serie de experți au evidențiat ideea potrivit căreia capabilitățile A2/AD ale Chinei ar putea pune în dificultate o intervenție americană într-un eventual conflict în Strâmtoarea Taiwan, care ar afecta întreaga regiune Indo-Pacific (crescând, totodată, semnificativ riscurile de escaladare[16]).

Având în vedere cele prezentate mai sus, pe termen scurt și mediu, ar putea avea loc următoarele evoluții în privința Taiwanului:

a) ***Cel mai bun scenariu*** *(din perspectivă occidentală):* tensiunile rămân la cotele actuale, gestionate prin descurajare și diplomație. Beijingul se abține de la agresiune militară, concentrându-se pe presiuni economice. Washingtonul și aliații regionali continuă să sprijine Taiwanul cu arme și prezență militară, asigurându-se că nu se ajunge la un conflict pe scară largă. Interesele de securitate ale Occidentului se vor concentra pe menținerea stabilității regionale, protejarea rutelor comerciale vitale și asigurarea rezilienței tehnologice a Taiwanului, în special în domeniul semiconductorilor[17].

b) ***Cel mai rău scenariu*** *(din perspectivă occidentală):* China va lansa o invazie pe scară largă a Taiwanului, ceea ce va duce la un conflict direct cu SUA și aliații regionali. Agresiunea escaladează în război regional, perturbând grav comerțul mondial, în special în domeniul tehnologiei și industriei. Agresiunile cibernetice și potențialele escaladări nucleare adaugă instabilitate. Pentru Occident, acest scenariu este cel mai puțin dezirabil din cauza implicațiilor severe asupra securității și comerțului global[18].

c) ***Cel mai probabil scenariu:*** Beijingul menține în ușoară creștere presiunea militară asupra Taiwanului, prin continuarea încălcării spațiului aerian și posibile blocade maritime. Vor avea loc atacuri cibernetice asupra Taiwanului, China vrând să mențină presiunea asupra insulei, fără a declanșa o invazie directă. SUA și aliații răspund cu descurajare militară, livrări de arme și măsuri diplomatice. Occidentul se va concentra pe menținerea păcii și susținerea capabilităților de apărare ale Taiwanului, astfel încât să continue descurajarea unei potențiale agresiuni chineze[19].

d) ***Cel mai puțin probabil scenariu:*** China optează pentru o rezolvare pașnică, posibil prin acordarea unui grad mai mare de independență Taiwanului, evitând confruntarea militară. Deși puțin probabil, un astfel de scenariu ar fi salutat de Occident deoarece ar păstra sistemul democratic al Taiwanului și ar evita conflictul. SUA și aliații s-ar concentra pe menținerea acestui *statu-quo* și pe sprijinirea normelor internaționale privind suveranitatea și disputele teritoriale[20].

IMPLICAȚIILE UNUI EVENTUAL CONFLICT CHINA-TAIWAN

Un eventual război între R.P. Chineză și Taiwan ar avea implicații profunde și complexe pe mai multe planuri, afectând nu doar regiunile vizate direct, dar și echilibrul geopolitic global, economia internațională și stabilitatea regională.

Începând cu dimensiunea economică, trebuie subliniat că Taiwanul joacă un rol esențial în industria semiconductorilor, care sunt fundamentali pentru tehnologii precum telefoanele mobile, computerele, autovehiculele electrice și echipamentele militare. Aproximativ 60% din semiconductorii de înaltă performanță la nivel global sunt produși în Taiwan, iar orice perturbare a acestui sector ar afecta întregul lanț de aprovizionare global. Economiile celor mai mari puteri economice ar urma să fie afectate, având în vedere dependența lor de aceste tehnologii.

De asemenea, conflictul ar influența în mod negativ și stabilitatea economiilor din regiunea Asia-Pacific. Strâmtoarea Taiwan, prin care trec numeroase rute comerciale internaționale, ar deveni un punct sensibil, iar blocarea acesteia ar perturba grav fluxurile comerciale globale. Transportul maritim, vital pentru comerțul internațional, ar suferi blocaje semnificative, iar navele comerciale ar fi puse în situația de a căuta rute alternative mult mai costisitoare și mai lente, ceea ce ar duce la o creștere a prețurilor și la o scădere a eficienței economice la nivel global.

În plan militar, implicarea directă a SUA și a altor aliați ai Taiwanului ar putea duce la o escaladare rapidă a conflictului, afectând nu doar Taiwanul și R.P. Chineză, ci și alte națiuni din regiune, precum Japonia, Coreea de Sud și Australia. Riscul unui război regional cu impact global ar crește considerabil, iar conflictele indirecte ar putea apărea în alte zone ale lumii.

Din punct de vedere umanitar, un război în această regiune ar avea consecințe devastatoare pentru populația civilă din Taiwan, dar și din China. Ar crește numărul victimelor, ar produce migrarea masivă a refugiaților și ar determina apariția unei crize umanitare, cu repercusiuni asupra sistemelor de sănătate, educație și infrastructură. Mai mult, o astfel de criză ar afecta grav securitatea regională și ar submina încrederea între marile puteri. În acest context, stabilitatea globală ar fi pusă la mare încercare, iar regiunile caracterizate deja de tensiuni în creștere, cum ar fi Europa de Est sau Orientul Mijlociu, ar putea deveni și mai volatile.

În concluzie, un conflict între R.P. Chineză și Taiwan nu ar fi doar un eveniment tragic pentru părțile implicate, ci și unul cu implicații profunde asupra securității internaționale, ordinii geopolitice și economiei globale. Prin urmare, rămâne esențial ca diplomația, dialogul și măsurile împotriva escaladării să primeze, pentru a evita un eveniment ce ar putea avea efecte catastrofale pentru întreaga lume.

CONCLUZII

Taiwanul rămâne un punct strategic important în Indo-Pacific, cu rol esențial în securitatea regională și globală. Economia sa, bazată pe producția de semiconductori, este vitală pentru asigurarea lanțurilor de aprovizionare în domeniul tehnologiilor avansate la nivel global, iar poziția geografică a insulei o face relevantă pentru rutele comerciale internaționale.

Pe de altă parte, liderii de la Taipei mențin o relație tensionată cu R.P. Chineză în condițiile în care conducerea de la Beijing consideră că insula este parte integrantă a statului și civilizației chineze, Xi Jinping afirmând că este dispus să folosească inclusiv forța (în viitor) pentru a o reintegra, fapt ce a determinat o accelerare a militarizării regiunii. În acest context, Taiwanul, conștient de superioritatea militară a Chinei, a optat pentru o apărare asimetrică bazată pe relațiile de cooperare cu SUA și Japonia.

Un eventual conflict deschis în Strâmtoarea Taiwan ar afecta întreaga regiune Indo-Pacific și echilibrul global de putere. Însă, în condițiile actuale, tensiunile dintre Taiwan și R.P. Chineză s-ar putea concretiza în escaladări limitate, precum blocade sau acțiuni cibernetice, situații ce ar destabiliza punctual unele economii din zonă.

BIBLIOGRAFIE

1. BARRANCO B. John, *Taiwan: The Key to Containing China in the Indo-Pacific. A Strategy of Deterrence to Maintain the US-Led, Rules-Based Global System*", Forward Defense Report, Atlantic Council, noiembrie 2022, 46 p.; disponibil la https://www.atlanticcouncil.org/in-depth-research-reports/report/taiwan-the-key-to-containing-china-in-the-indo-pacific/
2. BELLOCCHI P. Luke, "The Strategic Importance of Taiwan to the United States and Its Allies: Part Two", *Decisive Point*, Podcast Transcript, U.S. Department of Defense, 30 octombrie 2023, 5 p.; disponibil la https://media.defense.gov/2023/Oct/30/2003330634/-1/-1/0/DP-4-22_BELLOCCHI_TRANSCRIPT_TRATEGICIMPORTANCETAIWANPART2.PDF.
3. BO-JIUN Jing, "Taiwan's Regional Strategy in Southeast Asia: Kicking the New Southbound Policy into High Gear", *Briefs Series*, The National Bureau of Asian Research, 31 ianuarie 2018, 7 p.; disponibil la https://www.nbr.org/publication/taiwans-regional-strategy-in-southeast-asia-kicking-the-new-southbound-policy-into-high-gear/
4. BUSH C. Richard, "China-Taiwan: Recent Economic, Political, and Military Developments Across the Strait and Implications for the United States", *Commentary*, The Brookings Institution, 2010; disponibil la https://brookings.edu/articles/china-taiwan-recent-economic-political-and-military-developments-across-the-strait-and-implications-for-the-united-states/
5. deLISLE Jacques, „U.S.-Japan-Taiwan Dialogue: Deterrence, Defense, and Trilateral Cooperation", Strategic Trends Research Initiative Report, Foreign Policy Research Institute, octombrie 2022, 24 p.; disponibil la https://www.fpri.org/article/2022/12/u-s-japan-taiwan-dialogue-deterrence-defense-and-trilateral-cooperation/
6. DOTSON John, "Taiwan initiates its new one-year military conscription program", *Global Taiwan Brief,* Global Taiwan Institute, vol. 9, nr. 3, p. 4-8, 7 februarie 2024; https://globaltaiwan.org/2024/02/taiwan-initiates-its-new-one-year-military-conscription-program/
7. ENGMAN Mats, Larissa Stunkel, „Taiwan and the AUKUS: A Double-Edged Sword for Taipei", *ISDP Voices blog,* Institute for Security and Development Policy, 15.11.2021; disponibil la https://www.isdp.eu/taiwan-aukus-regional-implications/
8. GERSHANECK K. Kerry, „China and Taiwan: The Geopolitical Crisis Hiding in Plain Sight", *The Diplomat*, 13 octombrie 2022; disponibil la https://thediplomat.com/2022/10/china-and-taiwan-the-geopolitical-crisis-hiding-in-plain-sight/
9. MOVROYDIS Jonathan, „Scholars Consider Possible Scenarios in Preventing a Chinese Takeover of Taiwan", Hoover Institution, 16 aprilie 2021; disponibil la https://www.hoover.org/news/scholars-consider-possible-scenarios-preventing-chinese-takeover-taiwan.
10. SANG Huynh Tam, "The Taiwan Crisis Could Spill Over into Southeast Asia", *The Diplomat*, 11 august 2022; disponibil la https://thediplomat.com/2022/08/the-taiwan-crisis-could-spill-over-into-southeast-asia/
11. SANG Huynh Tam et al., "How Taiwan fights the disinformation war", *The Interpreter*, Lowy Institute, 20 iunie 2024; disponibl la https://lowyinstitute.org/the-interpreter/how-taiwan-fights-disinformation-war.
12. von SYDOW Alexis, "Most Experts Agree: China Isn't About to Invade Taiwan", *The Diplomat*, 23 februarie 2024; disponibil la https://thediplomat.com/2024/02/most-experts-agree-china-isnt-about-to-invade-taiwan/
13. YEO Mike, "China's missile and space tech is creating a defensive bubble difficult to penetrate", *Defense News*, 1 iunie 2020; disponibil la https://www.defensenews.com/global/asia-pacific/2020/06/01/chinas-missile-and-space-tech-is-creating-a-defensive-bubble-difficult-to-penetrate/
14. WANG Joyu, "Taiwan is getting its U.S. weaponry – but years behind schedule", *The Wall Street Journal*, 20 decembrie 2024; disponibil la https://www.wsj.com/world/asia/taiwan-is-getting-its-u-s-weaponrybut-years-behind-schedule-11c151b1.
15. *** France24, *Taiwan receives first batch of US-made Abrams tanks*, France24.com., 16 decembrie 2024; disponibil la https://www.france24.com/en/live-news/20241216-taiwan-receives-first-batch-of-us-made-abrams-tanks-1

[1] Luke P. Bellocchi, ”The Strategic Importance of Taiwan to the United States and Its Allies: Part Two”, *Decisive Point*, Podcast Transcript, U.S. Department of Defense, 30 octombrie 2023, 5 p.; disponibil la https://media.defense.gov/2023/Oct/30/2003330634/-1/-1/0/DP-4-22_BELLOCCHI_TRANSCRIPT_STRATEGICIMPORTANCETAIWANPART2.PDF și accesat în 04.12.2024.

[2] Richard C. Bush, ”China-Taiwan: Recent Economic, Political, and Military Developments Across the Strait and Implications for the United States”, *Commentary*, The Brookings Institution, 2010; disponibil la https://brookings.edu/articles/china-taiwan-recent-economic-political-and-military-developments-across-the-strait-and-implications-for-the-united-states/ și accesat în 04.12.2024.

[3] John B. Barranco, „Taiwan: The Key to Containing China in the Indo-Pacific. A Strategy of Deterrence to Maintain the US-Led, Rules-Based Global System”, Forward Defense Report, Atlantic Council, noiembrie 2022, 46 p.; disponibil la https://www.atlanticcouncil.org/in-depth-research-reports/report/taiwan-the-key-to-containing-china-in-the-indo-pacific/ și accesat în 04.12.2024.

[4] Kerry K. Gershaneck, „China and Taiwan: The Geopolitical Crisis Hiding in Plain Sight”, *The Diplomat*, 13 octombrie 2022; disponibil la https://thediplomat.com/2022/10/china-and-taiwan-the-geopolitical-crisis-hiding-in-plain-sight/ și accesat la 01.02.2025.

[5] Jing Bo-Jiun, ”Taiwan’s Regional Strategy in Southeast Asia: Kicking the New Southbound Policy into High Gear”, *Briefs Series*, The National Bureau of Asian Research, 31 ianuarie 2018, 7 p.; disponibil la https://www.nbr.org/publication/taiwans-regional-strategy-in-southeast-asia-kicking-the-new-southbound-policy-into-high-gear/ și accesat la 14.12.2024.

[6] Mats Engman, Larissa Stunkel, „Taiwan and the AUKUS: A Double-Edged Sword for Taipei”, *ISDP Voices blog,* Institute for Security and Development Policy, 15.11.2021; disponibil la https://www.isdp.eu/taiwan-aukus-regional-implications/ și accesat la accesat la 11.12.2024.

[7] Huynh Tam Sang, ”The Taiwan Crisis Could Spill Over into Southeast Asia”, *The Diplomat*, 11 august 2022; disponibil la https://thediplomat.com/2022/08/the-taiwan-crisis-could-spill-over-into-southeast-asia/ și accesat la 04.12.2024.

[8] Mike Yeo, ”China’s missile and space tech is creating a defensive bubble difficult to penetrate”, *Defense News*, 1 iunie 2020; disponibil la https://www.defensenews.com/global/asia-pacific/2020/06/01/chinas-missile-and-space-tech-is-creating-a-defensive-bubble-difficult-to-penetrate/ și accesat la 05.12.2024.

[9] *** France24, *Taiwan receives first batch of US-made Abrams tanks*, France24.com., 16 decembrie 2024; disponibil la https://www.france24.com/en/live-news/20241216-taiwan-receives-first-batch-of-us-made-abrams-tanks-1 și accesat la 19.02.2025.

[10] Joyu Wang, ”Taiwan is getting its U.S. weaponry – but years behind schedule”, *The Wall Street Journal*, 20 decembrie 2024; disponibil la https://www.wsj.com/world/asia/taiwan-is-getting-its-u-s-weaponrybut-years-behind-schedule-11c151b1 și accesat la 19.02.2025

[11] Huynh Tam Sang et al., ”How Taiwan fights the disinformation war”, *The Interpreter*, Lowy Institute, 20 iunie 2024; disponibil la https://lowyinstitute.org/the-interpreter/how-taiwan-fights-disinformation-war și accesat la 19.02.2025.

[12] John Dotson, ”Taiwan initiates its new one-year military conscription program”, *Global Taiwan Brief,* Global Taiwan Institute, vol. 9, nr. 3, p. 4-8, 7 februarie 2024; disponibil la https://globaltaiwan.org/2024/02/taiwan-initiates-its-new-one-year-military-conscription-program/ și accesat la 19.02.2025.

[13] Mike Yeo, *Op.cit.*

[14] Jacques deLisle, *U.S.-Japan-Taiwan Dialogue: Deterrence, Defense, and Trilateral Cooperation,* Strategic Trends Research Initiative Report, Foreign Policy Research Institute, octombrie 2022, 24 p.; disponibil la https://www.fpri.org/article/2022/12/u-s-japan-taiwan-dialogue-deterrence-defense-and-trilateral-cooperation/ și accesat la 05.12.2024.

[15] Ibid.

[16] Ibid.

[17] Alexis von Sydow, ”Most Experts Agree: China Isn’t About to Invade Taiwan”, *The Diplomat*, 23 februarie 2024; disponibil la https://thediplomat.com/2024/02/most-experts-agree-china-isnt-about-to-invade-taiwan/ și accesat la 05.12.2024.

[18] Ibid.

[19] Ibid.

[20] Jonathan Movroydis, „Scholars Consider Possible Scenarios in Preventing a Chinese Takeover of Taiwan”, Hoover Institution, 16 aprilie 2021; disponibil la https://www.hoover.org/news/scholars-consider-possible-scenarios-preventing-chinese-takeover-taiwan și accesat la 05.12.2024.

CĂDEREA REGIMULUI BASHAR AL-ASSAD ÎN SIRIA

Eugen-Nicolae BOGOVICI*

Motto: „Power is not a means; it is an end. One does not establish a dictatorship in order to safeguard a revolution; one makes the revolution in order to establish the dictatorship."

George Orwell

Abstract

The article examines the rise and fall of Bashar al-Assad's regime in Syria, tracing the historical, political and social dynamics that shaped his authoritarian rule. Beginning with a background of Syria's history, the study explores the rise of the Ba'ath Party and the Assad family's consolidation of power. Bashar's leadership, marked initially by promises of reform, is analyzed through his reliance on military control, secret services and ethnic-religious divisions to sustain his regime.

The eruption of the Syrian civil war in 2011 is discussed as a turning point, leading to mass repression, international involvement and a devastating humanitarian crisis.

The study concludes with an analysis of the consequences of Assad's fall, including Syria's ongoing challenges in achieving political transition, economic reconstruction and national reconciliation. Hypothetical scenarios are outlined, emphasizing the critical role of international cooperation in shaping a stable and democratic post-conflict Syria.

Keywords: *civil war; authoritarianism; regime collapse; political transition; humanitarian crisis; Middle East geopolitics; reconstruction.*

INTRODUCERE

De-a lungul istoriei sale, Siria a ocupat o poziție geostrategică de mare importanță, fiind situată la intersecția rutelor comerciale care leagă Europa, Africa și Asia. La începutul secolului al XX-lea, imediat după prăbușirea Imperiului Otoman, conform Acordului Sykes-Picot (din 1916) și deciziilor Ligii Națiunilor, Siria a intrat sub mandat de conducere francez. Perioada respectivă a fost marcată de lupte pentru câștigarea independenței și de tulburări la nivel politic care, în anul 1946, s-au finalizat cu obținerea suveranității.

Două decenii mai târziu, după numeroase lovituri de stat și instabilitate la nivel politic, a apărut partidul Ba'ath – o mișcare ce a inaugurat o epocă de guvernare autoritară în Siria, marcată de promovarea unității arabe, socialismului și secularismului. După mai puțin de un deceniu de guvernare autoritară, Hafez al-Assad, ofițer

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

alawit, a condus lovitura de stat care i-a permis să obțină funcția de președinte al Siriei. Aflată sub conducerea lui Hafez, Siria a suferit transformări radicale care i-au facilitat partidului aflat la conducere să domine toate aspectele politico-sociale. La rândul său, Bashar al-Assad, fiul lui Hafez, a fost integrat în puterea politică și a avut un puternic impact asupra structurilor statale și asupra modului de conducere a guvernării. Ascensiunea lui Bashar al-Assad la conducerea Siriei, în iunie 2000, a fost marcată de un optimism general din punct de vedere al sferei politice internaționale, cât și în rândul populației. „Primăvara de la Damasc", o scurtă perioadă de relaxare politico-culturală, lansată de Bashar, a fost rapid încheiată prin arestarea activiștilor și închiderea spațiului politic.

Relațiile externe ale Siriei au fost caracterizate de alianțe strategice cu Moscova, fiind marcate de poziția antagonistă față de Israel și implicarea activă în conflictele regionale.

PRELUAREA PUTERII ASUPRA STATULUI SIRIAN

Preluarea puterii politice de către Bashar al-Assad și cercul său de apropiați s-a bazat pe utilizarea forțelor de represiune împotriva opoziției. Imaginea pe care noul lider sirian a dorit s-o contureze/transmită a fost cea de lider omniprezent și omnipotent, asociat cu „părintele națiunii" (imaginea de lider protector a fost dezvoltată și promovată în rândul societății prin propagandă statală și de către tatăl său, Hafez al -Assad).

Regimul instaurat de familia Assad a manipulat diferențele etnice și religioase (Siria este împărțită din punct de vedere etnic în 70% arabi sunniți, 10% alawiți, 10% kurzi, 10% creștini și druzi), prezentând alawiții drept protectorii celor aflați în minoritate față de majoritatea sunnită, cultivând relațiile cu liderii creștini și druzi (le-a oferit protecție în schimbul loialității) și a marginalizat kurzii prin intermediul conflictelor de natură internă (folosindu-se de facțiunile acestora și împiedicându-i să se unifice din punct de vedere politic). Concret, în urma retoricii naționaliste instaurate pentru justificarea controlului său bazat pe secularism, Bashar al-Assad a prezentat unitatea statală ca fiind dependentă de conducerea sa, folosind discursurile politice dintr-o perspectivă narativă atent aleasă pentru înfricoșarea populației (prin propagarea ideii că o eventuală înlăturare a sa ar produce un haos inimaginabil).

Această politică s-a bazat pe principiul „*divide et impera*". Punând în aplicare acest pricipiu, Bashar al-Assad s-a asigurat că are controlul asupra instituțiilor-cheie, precum armata, serviciile de informații și structurile economice. Din perspectiva rolului armatei, instituția a fost unul dintre cei mai importanți piloni de susținere ai regimului: aceasta a fost restructurată pentru asigurarea protecției regimului, în detrimentul misiunilor principale de apărare națională, totalitatea pozițiilor de conducere fiind încadrate de alawiți, loiali regimului. Garda Republicană și Divizia 4 Blindată, unități militare de elită ale forțelor siriene, au fost conduse chiar de către membri ai familiei Bashar.

Un alt punct important al susținerii regimului a fost reprezentat de subordonarea atentă a serviciilor de informații, cunoscute sub numele de *„mukhabarat"*, care au avut în responsabilitate monitorizarea atentă a populației, identificarea și înlăturarea potențialelor amenințări asupra conducerii, dar și eliminarea opoziției interne și externe. GID (General Intelligence Directorate), principalul serviciu civil de informații al lui Bashar, a primit ca misiuni de bază interceptarea comunicațiilor și recrutarea din rândul populației civile. Prin intermediul MID (Military Intelligence Directorate), serviciul a condus numeroase operațiuni de suprimare a opoziției din zonele urbane, unde tensiunea de la nivel social atingea niveluri ridicate (ex.: manifestații și proteste frecvente).

AFID (Air Force Intelligence Directorate), considerat a fi un serviciu de informații cu acțiuni specifice în spațiul aerian și al operatorilor din câmpul aviației, și-a extins îndatoririle la nivel național prin asumarea de misiuni precum acțiunile îndreptate asupra rebelilor din timpul războiului civil. Un alt serviciu de informații

folosit de Bashar a fost cel care s-a specializat în monitorizarea tuturor activităților interne și care folosea tortura și interogatoriile violente, cu scopul de a obține informații în cadrul centrelor de detenție (cazurile documentate au scos la iveală recursul frecvent la metode inumane pentru extragerea informațiilor precum bătăi, șocuri electrice, abuzuri severe, indiferent dacă acestea se încheiau sau nu cu moartea victimei).

Un alt mediu în care serviciile de informații și-au desfășurat activitatea a fost reprezentat de mass-media, unde Internetul, rețelele de socializare, canalele radio și cele de televiziune au fost atent supravegheate și supuse cenzurii drastice pentru prevenirea și înlăturarea tuturor mesajelor de natură critică la adresa regimului; astfel, orice încercare de a comunica, liber sau codat, a fost sever pedepsită. De asemenea, pe timpul desfășurării războiului civil, serviciile de informații au fost acuzate, la nivel internațional, de crime împotriva umanității. *Amnesty International* și *Human Rights Watch* – organizații care se ocupă cu respectarea drepturilor omului – au documentat numeroase încălcări ale drepturilor omului (tortură, execuții judiciare, dispariții forțate ale celor care se poziționau împotriva regimului sau care erau bănuiți de trădare/jocuri duplicitare, indiferent dacă se aflau sau nu pe funcții de conducere). În consecință, toate aceste acțiuni, atent executate, au avut ca urmare menținerea unui climat bazat pe teamă și frică în rândul populației, descurajarea disidenței fiind scopul principal.

Din punct de vedere economico-social, regimul Bashar al-Assad a concentrat economia către structurile loiale de elită, sectoarele de la nivel strategic (instalațiile petroliere, serviciile de transport și cele de comunicații și date) fiind plasate sub atenta conducere a membrilor regimului. Drept urmare, patronajul instaurat a răsplătit loialitatea prin asigurarea resurselor necesare finanțării represive.

Totodată, regimul s-a orientat către colaborarea cu F.Rusă în domeniul militar, Moscova intervenind în sprijinul acestuia (inclusiv cu forțe aeriene în anul 2015). În plan extern, nu doar F.Rusă a jucat un rol important în menținerea regimului Bashar al-Assad, Iranul fiind celălalt aliat, furnizând miliții șiite și sprijinindu-l din punct de vedere economic. Toate aceste acțiuni iraniene au avut drept scop principal păstrarea coridorului teritorial de către aliatul libanez, Hezbollah. Mișcarea Hezbollah a colaborat cu serviciile de informații aflate sub conducerea lui Assad, contribuind la coordonarea și executarea a numeroase operațiuni militare împotriva rebelilor de pe teritoriul statului sirian. În același timp, Bashar al-Assad s-a folosit de conflictul cu statul israelian pentru a-și conferi legitimitate la nivel intern, poziționându-se în tabăra rezistenței arabe.

Regimul instaurat de Bashar al-Assad a produs efecte devastatoare atât pentru sirieni, cât și la nivel internațional. Astfel, din punct de vedere politic, fragmentarea teritorială a Siriei este marcată, pe axa timpului, de războiul civil izbucnit în anul 2011. Acest război a divizat statul sirian în mai multe entități controlate de regimul de la Damasc, ISIS, grupările rebele și milițiile kurde. Redobândirea controlului asupra tuturor diviziunilor a fost obiectivul prioritar al lui Bashar al-Assad, care a solicitat în acest sens sprijinul F.Ruse și al Iranului.

O altă consecință a dictaturii lui Bashar al-Assad, cu efecte devastatoare pentru națiune, a fost reprezentată de izolarea internațională a statului. În pofida tuturor sancțiunilor adoptate de către Liga Arabă și de statele occidentale, liderul sirian a reușit să se mențină la putere, fapt care a avut consecințe la nivel social, economic și geopolitic.

RĂZBOIUL CIVIL

În 2010, înainte de declanșarea războiului civil nemulțumirile sociale (lipsa de libertate politică, inegalitatea economică, nivelul ridicat al corupției) au creat tensiuni de amploare. Această situație a condus, în 2011, la amplificarea și generalizarea, la nivel național, a manifestațiilor de protest anti-regim, momentul zero fiind considerat protestul izbucnit în orașul Daraa (aflat în sudul Siriei), unde pentru prima dată populația

a cerut plecarea lui Bashar de la conducerea statului.

În acest context, regimul Assad a încercat să aplaneze nemulțumirile sociale cu un amalgam de promisiuni de reformă prin care se angaja să ofere mai multă libertate, dar care nu au atins rezultatele scontate, obligând autoritățile siriene să recurgă la acte de violență extremă, fapt ce a alimentat și ridicat nivelul crizei. Astfel, la nivel național, din proteste pașnice s-a ajuns la un conflict armat de amploare, cauzat de represiunea regimului și inexistența soluțiilor la nivel politic. Puși în fața violențelor, o parte din militari au dezertat și au format FSA (Armata Siriană Liberă), care a inițiat apoi lupte împotriva conducerii și a forțelor guvernamentale.

Pe măsură ce conflictul creștea în amploare, Arabia Saudită, Qatar și Turcia au venit în sprijinul opoziției, Rusia și Iranul implicându-și forțele și mijloacele orientate în susținerea regimului de la putere. De la proteste pașnice s-a ajuns la revolte cu urmări grave din punct de vedere al victimelor, Siria fiind în pragul unui război cu efecte majore interne, dar și globale.

La nivel regional, criza siriană a produs un efect de domino afectând stabilitatea politică și securitatea națională din mai multe state. În Irak, ascensiunea ISIS a fost facilitată de instabilitatea de la nivel politic, care a înlesnit (granițe slab controlate) ocuparea unor teritorii importante. În Liban, cu sprijinul iranienilor, Hezbollah a intervenit în conflictul sirian alăturându-se lui Bashar, fapt ce a creat tensiuni din punct de vedere religios. Pe de altă parte, resursele economice și infrastructura libaneze au fost afectate de valurile de refugiați sirieni. O altă țară grav afectată a fost Turcia, care s-a confruntat cu probleme mari de securitate la granițe din cauza grupărilor extremiste și ale kurzilor (care au devenit active în regiunile limitrofe), precum și cu probleme de natură economică cauzate de găzduirea celor peste 3,5 milioane de refugiați, toate acestea în urma sprijinirii opoziției siriene. Afluxul masiv de refugiați sirieni pe teritoriul Iordaniei a afectat palierul economic și stabilitatea socială și din acest stat. Forțele occidentale implicate în conflictul sirian și-au amplasat bazele pe teritoriul statului iordanian pentru ducerea luptelor armate la nivel strategic.

Pe lângă ISIS, care a ocupat teritorii însemnate în Siria și Irak, proclamându-și califatul în 2014, utilizând resursele petroliere ale statului sirian pentru finanțarea operațiunilor teroriste de la nivel global, o altă grupare asimilată de Al-Qaeda, Frontul Al-Nusra, a devenit o putere a opoziției armate, cu aspiranți militanți pe întreg mapamondul.

Rusia, în calitate de stat aliat/susținător al regimului lui Bashar, a intervenit militar în 2015 pentru a-și proteja baza navală de la Tartus din Marea Mediterană și pentru a-și menține, eventual crește, influența în Orientul Mijlociu. Violențele comise de forțele ruse asupra populației siriene, deși larg criticate, și-au atins scopul – acela de a menține la putere regimul lui Bashar al-Assad. În opoziție cu abordarea/preferințele Rusiei, SUA au sprijinit opoziția siriană și au coordonat împotriva ISIS o coaliție internațională. SUA au menținut o prezență militară limitată în nord-estul Siriei, cu misiunea de a sprijini kurzii împotriva forțelor extremiste. La rândul său, UE s-a implicat în gestionarea crizei umanitare și impunerea de sancțiuni de natură economică împotriva lui Bashar.

Retrospectiv vorbind, conflictul sirian a provocat una dintre cele mai grave crize umanitare din istoria actuală, fapt evidențiat prin migrația masivă, peste 6,6 milioane de sirieni trecând granițele în căutarea unui refugiu (cele mai afectate state de valul de migranți fiind Turcia, Liban, Iordania și, apoi, țările vest-europene). Odată cu valul de migranți, politica europeană a fost direct afectată, unele țări europene refuzând participarea la schemele de relocare.

Criza siriană a avut efecte la nivel global și pe piața energiei, unde au fost înregistrate perturbări în fluxurile de producție și în regimul transporturilor petroliere și al gazelor naturale. Pe plan financiar, costurile au fost estimate la peste 400 de miliarde de dolari, mare parte a acestei sume fiind constituită din venituri din rezervele SUA și ale Rusiei.

În ceea ce privește tendințele teroriste, Siria a devenit un stat-magnet pentru contractanți, luptători și rebeli străini, care, ulterior întoarcerii în țările de origine, au comis atacuri teroriste (cea mai afectată regiune fiind cea europeană, marcată de atentatele din Franța și Belgia). Tot în aceeași sferă, succesul misiunilor proclamate de ISIS a inspirat și alte grupuri jihadiste de pe plan global să execute atentate și masacre.

Prin prisma dreptului internațional, războiul civil din Siria a ridicat semne de întrebare despre responsabilitatea protejării civililor (atacurile cu arme chimice, ordonate de Assad, au fost generatoare de condamnări internaționale și acțiuni militare specifice din partea SUA, Marii Britanii și Franței). Totodată, conflictul sirian a scos în evidență limitele Consiliului de Securitate al ONU, unde Rusia și China au blocat rezoluțiile întocmite pentru sancționarea regimului Bashar.

RĂZBOIUL CIBERNETIC ÎN RĂZBOIUL CIVIL

Autoritățile siriene s-au folosit de tehnologie și au aplicat inclusiv tactici ce țin de războiul cibernetic pentru a-și asigura menținerea la putere și suprimarea opoziției. Acestea au abordat diverse metode pentru a monitoriza, destabiliza și intimida opoziția. Bashar al-Assad, în ciuda nerecunoașterii aderării grupării la regimul propriu, a folosit SEA (Syrian Electronic Army) drept instrument de luptă în plan cibernetic. SEA a fost responsabilă de atacuri internaționale asupra platformelor de profil. Marea majoritate a acestora au fost cele de tip phishing, SEA fiind implicată în compromiterea conturilor și rețelelor acelor militanți pentru drepturile omului care criticau regimul sirian, precum și a acelor agenții de știri care publicau materiale analitice critice la adresa conducerii siriene.

SEA s-a folosit de campaniile de dezinformare pentru discreditarea opoziției și pentru crearea de confuzie la nivel internațional. Mesajele pro-regim au fost infiltrate de SEA în conturile oficiale ale celor mai înverșunați opozanți. În general, aceste atacuri au avut la bază programe spion și malware, utilizate pentru interceptarea convorbirilor și colectarea de date cu caracter personal. Pe lângă distribuirea mesajelor pro-regim, SEA s-a folosit de DDoS (Distributed Denial of Service), atacuri pentru blocarea accesului la site-urile opoziției, mass-media independente și altor organizații critice. Cele mai importante ținte din mass-media au fost publicațiile Reuters, The Guardian și site-ul BBC, acestea fiind compromise prin distribuirea de mesaje pro-Assad.

De asemenea, folosind programe software avansate, SEA a reușit să folosească și rețelele de socializare Facebook și Skype în demersul său pentru neutralizarea opozanților. Astfel, credibilitatea informațiilor a fost pusă la îndoială pe plan internațional din cauza campaniilor de dezinformare și ale celor de hacking. UE, SUA și alte state au condamnat public SEA și regimul Assad pentru atacurile cibernetice.

În încercarea de contracarare a atacurilor cibernetice, Occidentul a încercat restricționarea exportului de tehnologie în Siria, limitând în special tehnologia pentru supravegherea populației. Acest efort a fost dublat de demersuri pentru furnizarea către opoziție de mijloace tehnologice pentru protejarea și supravegherea comunităților.

SERVICIILE SECRETE SUB CONDUCEREA LUI BASHAR

Bashar al-Assad și-a consolidat puterea prin subordonarea și conducerea serviciilor secrete. Acestea erau deja consolidate și loiale regimului Assad și erau concepute pentru prevenirea și contracararea oricărei agresiuni interne. Liderul sirian nu s-a ocupat personal de conducerea serviciilor secrete, dar le-a coordonat strategiile. Acesta primea cu regularitate rapoarte detaliate privind orice fel de amenințare (internă sau externă).

Bashar al-Assad a numit la conducerea serviciilor secrete apropiați din cercul restrâns, în special membri alawiți ai minorității din care provine, consolidând, astfel, loialitatea

mukhabaratelor față de regim. Cu toate că fiecare agenție de informații avea parte de propria autonomie, coordonarea interinstituțională a fost realizată de către conducătorul sirian și de consilierii săi, care vizau direct operațiunile și planurile de represiune a opoziției. Serviciile secrete au devenit cele mai importante instrumente pentru represiuni, monitorizări ale populației și colaborarea cu aliații externi.

CĂDEREA REGIMULUI

La 27 noiembrie 2024, coaliția de opoziție denumită COM (Comandamentul Operațiunilor Militare), aflată sub conducerea lui Hay'at Tahir al-Sham (HTS), a lansat, împreună cu alte grupări aliate din ANS (Armata Națională a Siriei) – susținute de Turcia, ofensiva împotriva regimului lui Bashar al-Assad, în guvernoratele Hama, Alep și Idlib. În decurs de câteva zile, până în data de 8 decembrie 2024, rebelii/ forțele de opoziție aflate sub conducerea HTS au ocupat marile orașe (Alep, Hama, Deir ez-Zor, Daraa și Suwayda). Astfel, în data de 7 decembrie, forțele rebele ajunseseră la 20 de kilometri de capitala Damasc, ulterior ocupării guvernoratului Daraa.

În acel moment, Iordania și Egiptul i-au cerut lui Bashar al-Assad să părăsească Siria. În urma evenimentelor produse în teren, în data de 8 decembrie 2024 liderul sirian și familia sa au fost evacuați de la baza aeriană Hmeimim (bază unde erau staționate forțe rusești) la Moscova, unde le-a fost acordat azil politic.

Ulterior, în 16 decembrie, Bashar al-Assad a precizat (pe canalul de socializare Telegram) faptul că părăsirea teritoriului sirian nu a fost planificată și că evacuarea sa de către forțele rusești a avut loc la solicitarea guvernanților de la Moscova, în contextul în care baza aeriană se afla sub atac cu UAV-uri. Potrivit analiștilor, viața lui Assad în Rusia va fi una strict controlată, iar prezența sa va fi folosită pentru interesele politice ale Kremlinului. Se cunoaște faptul că averea liderului sirian se ridică la peste 2 miliarde de dolari, dispersați în conturi offshore, companii fantomă și imobiliare pe plan global.

După înlăturarea lui Bashar al-Assad de la putere, Siria a intrat într-o perioadă de tranziție, dificilă din perspectiva reconstrucției naționale. În urma situației politice create, liderii opoziției au început negocierile pentru formarea unui guvern de tranziție.

Perioada de tranziție a venit împreună cu multiple provocări: securitatea națională (prioritatea statului este combaterea grupărilor extremiste și asigurarea securității), stabilitatea economică (redresarea economică implică reforme structurale și atragerea de investitori externi) și reconcilierea națională (stabilirea de relații de acceptare și comunicare între grupurile etnico-religioase în care este împărțit statul). Din punct de vedere politic, sprijinul internațional este crucial în realizarea tranziției către democrație.

RECONFIGURAREA INFLUENȚEI REGIONALE

Căderea regimului Assad a însemnat destabilizarea „Axei rezistenței" Iran - Siria - Hezbollah, fapt tradus printr-o pierdere, cel puțin în plan imagologic, a poziției Iranului în regiune. În prezent, Turcia și Arabia Saudită au cele mai bune perspective pentru extinderea influenței în Orientul Mijlociu, în timp ce pentru Israel schimbările din Siria ar putea însemna o destabilizare suplimentară, fapt care ar conduce la noi confruntări la graniță, având în vedere prezența grupărilor pro-iraniene pe teritoriul sirian.

Un impact semnificativ l-a avut căderea regimului sirian și asupra Rusiei, deoarece, în prezent, noua conducere siriană ar putea contesta legitimitatea prezenței militare ruse în regiune (Moscova deține în Siria două baze militare, baza navală Tartus – singura bază de la Marea Mediterană ce asigură forțelor navale ruse facilități pentru reparații și reaprovizionare, și baza aeriană Hmeimim, un punct important pentru activitățile militare ruse din Africa, în care sunt implicați mercenari din cadrul companiilor militare private, sub coordonarea Moscovei).

La rândul său, China, fiind preocupată de implementarea proiectului „Centura și Drumul",

ar putea intensifica eforturile de a grăbi medierea și de a câștiga influență economică și diplomatică în Siria.

PROIECȚII PENTRU VIITOR

Pe plan extern, noile autorități de la Damasc au vizat recunoașterea legitimității la nivel regional/ internațional și demararea procedurilor pentru delistarea HTS ca organizație teroristă, precum și ridicarea sancțiunilor impuse Siriei de SUA și UE. Liderul HTS, Ahmed Hussein al-Sharaa, mizează pe faptul că prin poziția conciliantă adoptată în raport cu guvernul de la Tel Aviv (în pofida bombardamentelor executate de aviația israeliană asupra facilităților de producție și depozitelor de arme ale fostului regim) va câștiga bunăvoința Administrației Trump, prin prisma afinităților acesteia față de Israel și a pârghiilor pe care executivul israelian le are la Washington.

Chiar dacă reprezentanții noii puteri pretind că noul guvern va fi format din tehnocrați, iar grupările insurgente vor fi dizolvate și incluse în structurile militare de stat, demersurile acestora converg spre scenariul că Ahmed Hussein al-Sharaa va capitaliza nivelul ridicat de popularitate internă pentru a deveni liderul de facto al Siriei.

În privința legitimării noii puteri de la Damasc de către comunitatea internațională, cel mai probabil „tonul" va fi dat de Administrația SUA, care nu va ezita să abordeze tranzacțional relația cu HTS, probabil prin acceptarea delistării dacă gruparea și liderii sirieni își vor asuma o guvernare bazată pe regionalizare/ federalizare (implicit pe acordarea autonomiei comunității kurde).

Căderea regimului Assad a creat pentru Turcia oportunități de a-și consolida influența la nivel regional și de a-și îndeplini unele obiective de securitate națională (lupta împotriva terorismului, problema refugiaților). Pentru moment, statele europene par dispuse să susțină inițiativa Ankarei de a-și asuma un rol principal în stabilizarea Siriei, prin relațiile stabilite cu HTS și alte grupări siriene, dacă acest lucru va permite/facilita, în final, întoarcerea refugiaților și reducerea presiunii generate de migrație asupra vestului Europei. În acest sens, cel mai probabil, statele europene vor fi dispuse să acorde sprijin financiar pentru reconstrucția Siriei.

Pentru gestionarea problemei legate de divizarea culturală și etnică a sirienilor, noul guvern sirian va putea lua în considerare trei posibile scenarii: 1) modelul federal, prin care s-ar împărți autonomia grupărilor; 2) scenariul în care forțele kurde ar putea viza o autonomie mai mare sau chiar totală (independența), tensionând implicit relațiile diplomatice cu guvernul central și aliații internaționali; 3) împărțirea sferelor de influență în Siria de către puterile regionale, care vor avea astfel misiunea prevenirii escaladărilor.

Pe plan intern, una dintre cele mai sensibile probleme ale Siriei este reprezentată de numărul mare (peste 6 milioane de refugiați în alte state) de cetățeni care ar putea reveni pe teritoriul național. Din această perspectivă, o problemă de fond ar fi reintegrarea acestora în comunitățile distruse în urma războiului. Pe plan internațional, numeroși analiști politici au concluzionat faptul că este posibilă renașterea grupărilor teroriste, precum ISIS sau Al-Qaeda, care ar putea profita de vidul de putere local.

Concluzionând, viitorul Siriei depinde de modalitatea în care tranziția politică, reconcilierea socială și reconstrucția economică vor fi gestionate. În cel mai optimist scenariu, Siria ar putea deveni un model de redresare post-conflict. Cert este faptul că totul se bazează pe capacitatea sirienilor de a trece peste diviziunile istorice, în concordanță cu voința politică internă și cu sprijinul internațional pe care conducerea de la Damasc va reuși să o atragă.

BIBLIOGRAFIE

1. ALSHAMARY Marsin, Asli Aydintaşbaş, Jeffrey Feltman și alții, ”The Assad regime falls. What happens now?”, *Commentary,* Brookings Institution, 9 Decembrie 2024, https://www.brookings.edu/articles/the-assad-regime-falls-what-happens-now/
2. AL-QAHAWI Laith Abdullah, ”Syria on the Brink of a New Era: Regime Collapse and Regional Implications”, *Jordan Pulse*, 16 Decembrie 2024, https://www.jordanpulse.com/article/6156.
3. BLINKEN J. Antony, *The Syrian People Will Decide the Future of Syria*, 11 Decembrie 2024, https://www.state.gov/the-syrian-people-will-decide-the-future-of-syria/
4. BYMAN L. Daniel, ”Comparing Al Qaeda and ISIS: Different goals, different targets”, *Commentary,* Brookings Institution, 29 Aprilie 2015, https://www.brookings.edu/articles/comparing-al-qaeda-and-isis-different-goals-different-targets/
5. CAVATORTA Francesco, ”More than Repression. The Significance of Divide et Impera in the Middle East and North Africa – The Case of Morocco”, *Journal of Contemporary African Studies*, vol. 25, nr. 2, 2007, p. 187-203, https://doras.dcu.ie/477/1/jcas_25_2_2007.pdf.
6. CHAUHAN Yamini, ”Ḥizb al-Baʿath al-ʿArabī al-Ishtirākī”, *Encyclopedia Britannica,* https://www.britannica.com/topic/Baath-Party.
7. DAGHER Sam, *Assad or We Burn the Country: How One Family's Lust for Power Destroyed Syria*, Little, Brown and Company, 2019, 592 p.
8. DANIN M. Robert, ”Remembering the Hama Massacre”, Council on Foreign Relations, 2 Februarie 2012, https://www.cfr.org/blog/remembering-hama-massacre.
9. GEBEILY Maya, Timour Azhari, ”Syrian rebels topple Assad who flees to Russia in Mideast shakeup”, *Reuters*, 9 Decembrie 2024, https://www.reuters.com/world/middle-east/syria-rebels-celebrate-captured-homs-set-sights-damascus-2024-12-07/
10. GENDLER Alex, ”Who controls Syria after Assad?”, *Voice of America*, 16 Decembrie 2024, https://www.voanews.com/a/who-controls-syria-after-assad/7903494.html.
11. GRITTEN David, ”Bashar al-Assad and family given asylum in Moscow, Russian media say”, *BBC News*, 8 decembrie 2024, https://www.bbc.com/news/articles/cqx89reeevgo.
12. LOFT Philip, Georgina Sturge, Esme Kirk-Wade, *The Syrian Civil War: Timeline and Statistics*, House of Commons Library, Research Briefing, 25 Septembrie 2023, 23 p., https://commonslibrary.parliament.uk/research-briefings/cbp-9381/
13. LOFT Philip, Claire Mills, *Syria after Assad: Consequences and next steps in 2024/25*, House of Commons Library, Research Briefing, 19 Decembrie 2024, 47 p., https://commonslibrary.parliament.uk/research-briefings/cbp-10161/
14. MARWAT Minhas Majeed Khan, ”Post-Assad Syria and the Impact on Regional Geopolitics”, 10 Decembrie 2024, https://www.linkedin.com/pulse/post-assad-syria-impact-regional-geopolitics-marwat-4jzif.
15. RATHMELL Andrew, ”Syria's Intelligence Services: Origins and Development”, *Journal of Conflict Studies*, vol. 16, nr. 2, 1996, p. 75-96, https://journals.lib.unb.ca/index.php/jcs/article/view/11815/12636.
16. SALIHA. Mohammed, ”US Policy in Northeast Syria Towards a Strategic Reconfiguration”, Analysis, Foreign Policy Research Institute, 6 Mai 2024, https://www.fpri.org/article/2024/05/us-policy-in-northeast-syria-toward-a-strategic-reconfiguration/
17. WASIELEWSKI Philip, Mohammed Soliman, Nikolas K. Gvosdev, ”What's Next for Syria, the Region, and the World?”, *Expert Commentary,* Foreign Policy Research Institute, Decembrie 2024, https://www.fpri.org/article/2024/12/whats-next-for-syria-the-region-and-the-world/
18. *** World Leaders – Presidents and Heads of States, Bashar al Assad, *Encyclopedia Britannica*, https://www.britannica.com/biography/Bashar-al-Assad/Unrest-and-civil-war.
19. *** US Department of State, *Syria Profile*, People - Ethnic and religious groups, https://2009-2017.state.gov/outofdate/bgn/syria/35817.htm.
20. *** In Meeting Following Russian Federation's Veto of Cross-Border Aid Text, General Assembly Speakers Highlight Humanitarian Consequences for Millions, https://press.un.org/en/2023/ga12517.doc.htm.
21. *** Al Jazeera, Syria's Civil War Explained http://www.aljazeera.com/news/2016/05/syria-civil-war-explained-160505084119966.html.
22. *** UNHCR, Syria Refugee Crisis Explained, https://www.unrefugees.org/news/syria-refugee-crisis-explained/

DE LA CYBERTERORISM LA CYBERSPACE – O NOUĂ DIMENSIUNE A CONFLICTELOR ACTUALE

Andreea-Elena RADU*

Abstract

The development of technology and the spectacular advancement of the virtual environment, through their use in all areas, have brought with them risks and threats both to society and the individual, and to the regional or global system. Today, the security environment is also characterized by the dynamism that virtual space has, and humanity, without awareness, watches and takes part in a war on an absolute and abstract battlefield, which is represented by cyberspace.

Over time, war took many forms, from the classical, conventional, to the hybrid, and then took shape in a non-existent physical environment, namely, the Internet, where it degenerated from a case. particularly isolated from an entire network of computers connected to the same online platform.

Keywords: *cyberspace; risk; cyber security; information.*

Secolul al XXI-lea, denumit generic *„secolul exploziei tehnologice”,* este caracterizat de patru elemente definitorii – volatilitatea, incertitudinea, complexitatea și ambiguitatea. În acest context, într-un mediu extrem de fluid, analizând mai ales din punct de vedere informațional, nu se poate afirma decât că mediul de securitate se caracterizează prin incertitudine. Cu alte cuvinte, acest mediu se poate defini ca o asociere de procese și fenomene ce aparţin domeniilor de activitate ale societății (politic, diplomatic, economic, social, cultural şi militar) și care influențează în mod decisiv atât securitatea individului, cât şi a comunității sau regiunii din care acesta face parte.

Prin sintagma *mediu de securitate* se poate înțelege „un concept relaţional, ce presupune o adaptare şi o ajustare permanentă a unui set de parametri interni (economico-sociali, politici, militari, juridici, culturali şi morali) la condiţiile mediului internaţional, un proces cu o dinamică fluidă, orientat spre prezervarea spaţiului, idealurilor şi valorilor comune şi, totodată, punerea acestor elemente într-un echilibru stabil, neafectat de factori de risc sau de ameninţări”[1].

Toate caracteristicile actualului mediu de securitate sunt derivate din procesul, tot mai galopant, de dezvoltare a tehnologiei. Cu cât tehnologia prinde proporții însemnate în ceea ce privește actualitatea, cu atât securitatea individului este tot mai mult pusă sub semnul amenințării. Astfel că una dintre cele mai recente amenințări la adresa securității indivizilor este reprezentată de apariția mediului virtual și, mai

Autoarea este expert în cadrul Ministerului Apărării Naționale.

ales, de dezvoltarea rapidă a acestuia.

În perioada recentă, mediul Internet şi mijloacele media au dat dovadă de o ascensiune fără precedent şi au devenit părți importante din vieţile cotidiene ale utilizatorilor de pretutindeni. Aceste instrumente sunt, în prezent, componente ce contribuie la o serie de schimbări majore referitoare la modul în care indivizii prelucrează date şi informații, interacţionează cu alți indivizi şi caută informaţii. Astfel că, în mediul virtual, există site-uri pe care sunt postate date și informații de către persoane care dețin o dezvoltată experiență socio-profesională, dar există și site-uri unde sunt publicate aspecte de către indivizi care nu dețin suficiente cunoștințe referitoare la problematica postată sau nu fac altceva decât să manipuleze sau să dezinformeze societatea. Mai mult decât atât, informațiile personale sau private nu sunt în siguranță atunci când utilizatorii de Internet sunt conectați la această platformă și, mai ales, când o folosesc. În acest context, toate datele și informațiile care tranzitează mediul virtual sunt stocate în baze de date complexe, de mare capacitate. Prin prisma acestui fapt, supremația mondială este influențată și de utilizarea noilor tehnologii care, în ultimul deceniu, au înregistrat o dezvoltare fără precedent.

DE LA RĂZBOIUL CONVENȚIONAL LA RĂZBOIUL HIBRID

Definim *războiul convențional* ca fiind forma de conflict purtat cu mijloace de luptă și modalități tactice convenționale/clasice între cel puțin două state care, din punct de vedere politic, sunt independente. În cadrul războiului de tip convențional sunt utilizate arme stabilite prin „convenție“ (de la arcul cu săgeți și sabie la arme de foc cu muniție letală) și în niciun caz arme biologice, chimice sau nucleare. În context, războiul convențional are drept scop general impunerea în fața adversarului și nimicirea puterii militare a acestuia, generând astfel incapacitatea oponentului de a angaja în luptă efectivele militare[2].

Odată cu trecerea timpului, tehnica a evoluat și au apărut noi modalități de ducere a unui conflict. Astfel, au fost create noi mijloace de interceptare a comunicațiilor, dar și de „vizualizare” a dezvoltării altor state, cum ar fi utilizarea sateliților (ex.: încă din timpul Războiului Rece, Statele Unite ale Americii și URSS au folosit acest tip de tehnologie pentru a spiona în timp real adversarul). Cele mai puternice arme au fost considerate cele de distrugere în masă, NBC (nuclear, biologic, chimic), însă oamenii de ştiinţă au conştientizat că efectul distrugător al acestor arme este mult prea mare, astfel încât au abordat o altă strategie care face referire la construirea de arme sofisticate, precum armele psihotronice (au efect asupra psihicului uman, contribuind la alterarea stării sale de normalitate), arme geofizice sau arme climatronice. Efectul acestora se poate limita la planul local sau poate fi dezvoltat la nivel global. Toate aceste arme dețin avantajul că, odată acționate, pierderile (de orice natură) sunt controlate. Pe de altă parte, în contextul dezvoltării alarmante a tehnologiei, Hans Moravec susținea, la începutul anilor `90, că dezvoltarea roboticii se va realiza într-un timp semnificativ mai scurt, comparativ cu evoluția omenirii, iar la jumătatea secolului XXI orice activitate umană va fi înlocuită de aparatură robotizată[3].

În prezent, amenințările clasice, convenționale, tind să fie înlocuite cu războiul hibrid, care face apel mai mult la elemente de putere de tip *soft,* utilizând metode de acțiune dintre cele mai diversificate, precum presiuni politice și economice, acțiuni specifice de sabotaj și subversiune, atât în plan socio-cultural, cât și psihologic și comportamental. Concret, războiul hibrid face referire, în mod implicit, și la tot ce se înţelege prin sintagma *diplomaţie coercitivă*[4].

Războiul desfășurat în prezent, dar şi cel care se va dezvolta în viitorul apropiat, dispune de noi caracteristici atât din punct de vedere conceptual, cât şi din cel al dinamicii metodelor de luptă aplicate, astfel încât *„acţiunea militară se integrează în noul concept şi aduce elemente noi, ea devine deosebit de flexibilă, adaptabilă la împrejurări, la acţiunea şi reacţia inamicului, dependentă de variaţia condiţiilor iniţiale, variabilă şi diferită ca amploare şi*

intensitate, în funcţie de tipul de beligeranţă, de nivelul tehnologic al războiului şi de modul de angajare"[5].

Cyberterorism

Terorismul poate fi definit printr-o violență stabilită și premeditată, având o motivație de ordin politic, împotriva unor ținte care nu iau parte la conflict, și desfășurată fie de agenți clandestini, fie de grupuri cu anumite interese, în scopul de a influența o masă de oameni. Una dintre cele mai ample lucrări cu privire la problema cyberterorismului este cea a lui Dorothy Denning. În această lucrare se face următoarea afirmație: *„Cyberterorismul este convergența terorismului și a spațiului cibernetic. În genere, cyberterorismul face referire la atacurile ilegale și amenințările inițiate împotriva computerelor, a rețelelor și a informațiilor stocate pe servere, atunci când sunt făcute pentru a intimida sau a constrânge un guvern sau oamenii săi să promoveze obiective politice sau sociale. În plus, pentru a se califica drept cyberterorism, un atac ar trebui să ducă la violență împotriva persoanelor sau a proprietății sau cel puțin să provoace suferință suficientă pentru a genera frică. Atacurile care duc la moarte sau vătămări corporale, explozii, avarii, contaminarea apei sau pierderi economice grave ar fi câteva dintre exemple. Atacurile serioase împotriva infrastructurilor critice ar putea fi acte de cyberterorism, în funcție de impactul lor"*[6].

Fiind prea preocupate pentru identificarea și contracararea unor amenințări manifestate asupra unor zone sensibile, multe dintre state nu au dat importanță asigurării protecției tuturor zonelor și domeniilor de activitate. De exemplu, o abordare orientată spre viitor a terorismului care implică computerele are o bază extrem de contextuală; ar trebui să fie implementate mijloacele antiteroriste, însă pentru aceste contramăsuri s-ar impune să fie luați în considerare foarte mulți factori virtuali. Evenimentele din 11 septembrie 2001 ne-au învățat un lucru – necesitatea de a lua întotdeauna în considerare „imaginea de ansamblu" a amenințării teroriste, în loc să privim doar un aspect izolat. Aspectele „cibernetice" ale acestui puzzle trebuie să fie țesute pe tot cuprinsul imaginii, nu pur și simplu limitate la o singură „celulă". Terorizarea cibernetică a unei țări și a cetățenilor săi poate avea mai multe niveluri de sofisticare, fiecare nivel necesitând capacități atât în ceea ce privește tehnologia, cât și investițiile făcute de atacator. Prejudiciul cauzat este direct proporțional cu nivelul investiției.

Cyberspace – o nouă etapă a conflictului virtual

Atacurile cibernetice sunt puse în aplicare în mod diferit, iar motivele sunt foarte diverse. De exemplu, teroriștii cibernetici sau anumite guverne încearcă să acceseze serverele potențialilor inamici în scopul de a obține date confidențiale sau de a contribui la sabotarea echipamentelor acestora. În anul 2010, secretarul-adjunct al Departamentului Apărării din SUA, William J. Lynn III, afirma că *„adversari străini au atacat şi au trecut cu succes, în repetate rânduri, de sistemele de securitate ale reţelelor computerizate ale Statelor Unite ale Americii. Serverele conţineau informaţii confidenţiale despre datele de identificare ale angajaţilor diverselor corporaţii şi atacatorii au reuşit să extragă o mulţime de fişiere, printre ele numărându-se proiecte de armament, planuri operaţionale şi date privind supravegherea"*[7].

Analizând aspectele menționate mai sus putem afirma că, în prezent, cyberterorismul a devenit o formă de terorism extrem, care reușește să provoace daune de ordin moral și material, să afecteze buna funcționare a instituțiilor bancare sau cu atribuții în domeniul securității, să afecteze persoane care își desfășoară activitatea în cadrul unor organizații. În acest sens, cyberterorismul nu poate face referire strictă la o latură a terorismului dezvoltată în domeniul cibernetic, ci putem vorbi despre terorismul aplicat asupra întregului spațiu virtual (cyberspace).

Spre deosebire de majoritatea termenilor din domeniile hardware și software, *spațiul cibernetic* sau *cyberspace-ul* nu are o definiție standard și obiectivă. În schimb, este folosit pentru a descrie, în întregime, lumea virtuală a computerelor. Cuvântul *cyberspace* îi este atribuit lui William Ford Gibson, care l-a folosit în cartea sa, *Neuromancer,* scrisă în anul 1984. Gibson

definea *spațiul cibernetic* ca fiind „o halucinație consensuală experimentată zilnic de miliarde de operatori legitimi, în fiecare națiune, de copii care au învățat de la vârste fragede concepte matematice... O reprezentare grafică a datelor extrase din băncile fiecărui calculator al societății omenești... O complexitate de neimaginat. Raze de lumină aliate în non-spațiul minții, roiuri și constelații de date”[8]. Gibson a criticat termenul în anii următori, numindu-l ca fiind evocativ și, în esență, lipsit de sens. Cu toate acestea, termenul este folosit pe scară largă pentru a descrie orice facilitate sau caracteristică a Internetului.

Cu alte cuvinte, termenul *cyberspace* se referă la lumea computerelor virtuale și, mai exact, este un mediu electronic folosit pentru a forma o rețea globală de calculatoare, care are scopul de a facilita comunicarea online. Practic, este o rețea mare de computere formată din numeroase rețele de calculatoare din întreaga lume, care utilizează protocolul TCP/ IP (Transmission Control Protocol/ Internet Protocol) pentru a ajuta la activitățile de comunicare și schimb de date. Caracteristica principală a cyberspace-ului este un mediu interactiv și virtual pentru o gamă largă de participanți. *Cyberspace* permite utilizatorilor să împărtășească informații, să interacționeze, să facă schimb de idei, să joace jocuri, să se angajeze în discuții sau forumuri sociale, să desfășoare afaceri și să creeze medii interactive, printre multe alte activități.

În măsura în care amenințările cibernetice sunt folosite de un actor pentru a căuta un avantaj față de altul, profitând de un spațiu virtual încă în mare parte anarhic, acestea pot fi abordate în contextul teoriei relațiilor internaționale realiste. Dar, deoarece teoria realistă a fost dezvoltată cu câteva decenii înainte ca amenințarea cibernetică să devină o posibilitate, ea trebuie extinsă și ajustată pentru a se adapta acestui nou fenomen. Amenințările de acest tip au reușit să pună arme puternice în mâinile oamenilor, astfel încât principiul găsit în teoria realistă, care face referire la faptul că statul este cel mai puternic actor, nu mai este neapărat adevărat.

Prin intermediul spațiului cibernetic o persoană poate ataca un stat și poate provoca daune semnificative, în unele cazuri chiar și mai multe daune decât poate un stat. Părțile inamice nu trebuie să fie aproape una de cealaltă pentru a avea loc un atac cibernetic. Elementele folosite ca arme cibernetice, cel mai adesea software de calculator și alte dispozitive similare, vor arăta din exterior ca orice alt sistem informatic și, prin urmare, pot fi tranzacționate peste frontierele de stat fără nici o dificultate. Un arsenal întreg poate fi păstrat pe o unitate de memorie flash care nu depășește prețul de un cent american. Asta ne conduce la descurajare. În epoca Războiului Rece, fiecare parte – Occidentul și Estul – avea arme nucleare și știa că dacă ar folosi aceste arme, cealaltă ar răspunde în natură și ambele vor fi anihilate. Această situație a creat un puternic obstacol, care a menținut relativ pașnic Războiul Rece (cu excepția unor conflicte regionale de tip „proxy”[9]).

Odată cu evoluția tehnologiei și cu dezvoltarea armelor și tehnicii militare, conflictele militare de la începutul mileniului au progresat în complexitate. În prezent, filosofia care a creat bazele construirii cadrului de securitate specific celei de-a doua jumătăți a secolului XX suferă schimbări fundamentale, în condițiile în care globalizarea a dus la multiplicarea oportunităților de dezvoltare și cooperare și la o creștere exponențială a numărului de entități care acționează pe scena globală.

Mileniul al treilea a început cu o declarație de război între terorism și societățile democratice. Acestea din urmă au propus o revoluție democratică globală, declarând pacea și securitatea drept valori supreme ale sistemului juridic mondial. În fața noilor amenințări cu care se confruntă lumea - terorismul, proliferarea nucleară, eșecul guvernării (statele eșuate), foametea, degradarea mediului etc. – Carta ONU a îmbrățișat postura de pilon principal în prezervarea păcii și progresului social.

În acest context, odată cu dezvoltarea tehnologiei informațiilor, activitatea organizațiilor depinde din ce în ce mai mult de utilizarea bazelor de date (referindu-ne aici și la instituțiile publice),

fapt care poate să genereze vulnerabilități. Așadar, fenomenul numit „globalizare" este capabil să aducă prejudicii serioase securității. În prezent, fenomenul mai sus menționat a făcut ca transmiterea de informații să nu cunoască blocaje, să fie la îndemâna tuturor, iar informația să fie transmisă în timp real. Dacă în trecut o informație era trimisă prin intermediul unui *„mesager",* în prezent aceasta se transmite foarte rapid prin intermediul mijloacelor electronice.

DE CE INTERNETUL ?

Alegerea Internetului (a mediului virtual) ca instrument important de acţiune de către organizaţiile teroriste este determinată de următoarele argumente[10]:

- anonimitatea comunicării, dar și facilitarea accesului la informaţii de interes pentru desfăşurarea diverselor activităţi;
- existenţa unor lacune legislative, fapt care permite manifestarea anumitor comportamente la limita legalităţii;
- lipsa cenzurii sau a unui control guvernamental manifestat asupra informaţiilor care circulă libere în mediul virtual;
- audienţa largă caracterizată de un indice de creștere exponențial, în toate regiunile geografice de interes;
- costurile reduse în vederea implementării și gestionării unei pagini web;
- fluxul rapid al informaţiei şi eficiența transmiterii de mesaje multimedia (text, fotografii, video etc.).

În contextul aspectelor prezentate anterior, utilizând mediul virtual (cyberspace) ca principală resursă, organizațiile teroriste sau organizațiile asociate criminalității organizate pot recurge la utilizarea unor metode prin care să aducă prejudicii grave la nivel individual sau instituțional.

Prin prisma avansului tehnologic, starea de securitate este caracterizată prin dinamism, vulnerabilități și amenințări ce depășesc limitele spațiului fizic, manifestându-se în acest fel în mediul virtual. Deoarece spațiul cibernetic nu are frontiere, contracararea amenințărilor trebuie făcută prin inovarea și adaptarea metodelor special destinate acestui scop. Una dintre soluțiile găsite de Statele Unite ale Americii în această privință este dată de decizia cooperării pe plan național, dar și internațional, în scopul găsirii celor mai bune soluții pentru aceste amenințări venite din mediul virtual. Totodată, Statele Unite ale Americii au fost un stat foarte activ în cadrul reuniunilor ONU în acest domeniu, dezvoltând planuri de cooperare bilaterală cu alte state pentru asigurarea securității în domeniul cybernetic[11]. De exemplu, în anul 2015, SUA au semnat un acord de neagresiune cibernetică cu R.P. Chineză, subiect abordat de Adam Segal[12] în *„The Top Five Cyber Policy Developments of 2015: United States-China Cyber Agreement"*[13]. Acest lucru se datorează faptului că spionajul cibernetic a fost o problemă deosebit de controversată în relația SUA-China.

TERORIȘTII DIN SPATELE ECRANULUI

Propaganda

Un exemplu îl reprezintă organizaţiile extremiste care utilizează metode moderne de relaționare și interacțiune, precum reţele de socializare virtuale, telefoane inteligente (smartphone), dar şi multe alte gadget-uri care se folosesc de conexiunea la Internet în scopul de a disemina mesajele de propagandă și de a promova anumite ideologii, atât la nivel regional, cât mai ales la nivel global. De exemplu, în contextul extinderii fenomenului terorist la începutul secolului XXI, printre cele mai eficiente metode de desfăşurare a acţiunilor de propagandă s-au regăsit înregistrările video (care făceau referire la execuţii sau mesaje ale unor lideri musulmani), care fie erau diseminate în mediul virtual, fie erau comercializate în mod ilegal în magazinele din Orientul Mijlociu. Cu atât mai mult, această metodă de desfăşurare a propagandei pe Internet a devenit din ce în ce mai populară şi în cadrul altor organizaţii teroriste, similare celor din Orientul Mijlociu, cum ar fi cele care și-au desfăşurat activitatea pe teritoriul Ceceniei şi Bosniei[14].

Războiul psihologic

Războiul psihologic este una dintre părțile componente ale războiului modern.

El caracterizează treptat o generalizare și permanentizare a violenței, „arma psihologică" fiind cel mai nou tip de armă utilizat. Influența sau influențarea este un fenomen esențial al vieții individuale și sociale și vizează transformarea atitudinilor și comportamentelor unor persoane sau unor grupuri de persoane. Organizațiile teroriste folosesc mediul virtual ca mijloc de ducere a războiului psihologic, diseminând informații cu scop de dezinformare, publicând imagini înspăimântătoare și răspândind frică (ex.: publicarea unor înregistrări video care surprind decapitarea unui jurnalist american, pe nume Daniel Pearl, în 2002).

Colectare ilegală de fonduri

Colectarea fondurilor prin folosirea tranzacţiilor online, în scopul de a sprijini grupările teroriste, a devenit o formă extrem de uzitată în ultimele două decenii. Această metodă constă într-o solicitare de fonduri adresată utilizatorilor ce accesează paginile web ale organizaţiilor teroriste; solicitările pot fi de forma unor sintagme care evidenţiază necesitatea respectivelor organizaţii de a aduna fonduri financiare, oferindu-se amănunte despre locurile unde pot fi plasate „donațiile" (de exemplu, numerele conturilor bancare) sau despre eventualitatea transmiterii respectivelor fonduri prin servicii de plată online, precum PayPal[15]. Mai mult decât atât, entităţile teroriste utilizează, de asemenea, metode simple, ce constau în crearea, cu ajutorul unor programe speciale de monitorizare, a unui profil al vizitatorilor site-urilor şi, ulterior, se realizează contactarea persoanelor clasificate ca fiind potenţiali susţinători şi finanţatori.

Networking

Structura organizatorică şi funcţională a organizațiilor teroriste a suferit transformări semnificative în ultimii 20-30 de ani, adaptându-se contextului specific. De asemenea, specialiștii ce-și desfășoară activitatea analizând organizaţiile teroriste au constatat că mediul virtual le permite acestor rețele teroriste să acționeze din aproape oricare parte a lumii, beneficiind de structuri dispersate, dar conectate continuu, fără a avea nevoie de sprijinul telefoniei sau al poștei[16]. Aşadar, organizaţiile teroriste pot desfăşura diverse acţiuni, utilizând Internetul, într-o manieră foarte descentralizată, întrucât indivizi sau grupuri aflate în părţi opuse ale globului se pot relaționa cu rapiditate sau îşi pot coordona acţiunile în mod eficient, resursele financiare folosite fiind minime. De asemenea, mediul nu facilitează doar comunicarea din interiorul grupului, ci şi socializarea între grupuri ostile.

Internetul constituie un vast spaţiu centrat pe dezbateri cu referire la diverse ideologii şi acţiuni[17] și, din această perspectivă, John Arquilla şi Michele Zanini afirmau că *„teroriştii vor continua să se dezvolte şi să facă trecerea de la reţelele de tip ierarhic la cele ale erei cunoaşterii. Vor fi depuse din ce în ce mai multe eforturi în vederea constituirii unor grupări ostile transnaţionale, interconectate prin intermediul Internetului, decât pentru formarea unor grupuri solitare"*[18].

Obținerea de informaţii

Colectarea informaţiilor prin utilizarea mediului virtual face obiectul preocupării tot mai intense a organizaţiilor teroriste de a utiliza Internetul, folosind în mod special reţelele de socializare (care constituie vaste baze de date cu conţinut referitor la viaţa personală a utilizatorilor, dar şi referitor la evoluţia unor evenimente ce prezintă interes) drept un mijloc facil şi ieftin de colectare a unor informaţii care altminteri ar fi fost mai dificil de obținut.

Antrenament

Organizaţiile teroriste folosesc mediul virtual și, în mod special, Internetul pentru a crea un cadru virtual necesar pregătirii, oferindu-se indicaţii cu privire la construirea şi utilizarea IED-urilor (dispozitive explozive improvizate), migrarea în mod ilegal în şi din ţări aflate în conflict (precum Afghanistan, Siria sau Irak) sau chiar modul de utilizare a proiectilelor de tip sol-aer[19].

Furtul prin Internet

Conform Departamentului de Justiţie al SUA, termenul de fraudă în mediul virtual reprezintă orice modalitate de fraudă prin folosirea uneia sau mai multor componente specifice Internetului, precum e-mailul, forumurile publice, canalele

de chat sau chiar site-uri web. Această activitate se desfășoară în scopul de a racola potențiale victime, de a finaliza unele tranzacții frauduloase sau pentru a transmite profituri obţinute în mod ilegal către persoane implicate în procesul de fraudă. Astfel, printre cele mai mari amenințări la adresa securității în mediul Internet se numără furtul de identitate. Atacuri de genul phishing, hacking, keylogger sau spy-phishing se propagă, de cele mai multe ori, prin e-mail. Acest tip de amenințare implică atât furtul de bani, cât și obținerea unor avantaje, utilizându-se o metodă simplă, aceea de a fi altcineva. Furtul de identitate poate constitui o problemă delicată, atât din punct de vedere financiar, cât și emoțional.

CONCLUZII

Într-o eră în care tehnologia digitală definește nu doar comunicarea, ci și securitatea globală, cyberspace-ul a devenit un câmp de luptă invizibil, dar extrem de periculos. Cyberterorismul nu mai este doar o amenințare teoretică, ci o realitate concretă, capabilă să destabilizeze guverne, să paralizeze infrastructuri critice și să influențeze cursul evenimentelor geopolitice. Atacurile cibernetice, fie că sunt lansate de grupări teroriste sau de actori statali ostili, nu mai vizează doar furtul de date, ci au devenit arme strategice în conflictele moderne.

În fața acestei escaladări, statele și organizațiile internaționale trebuie să adopte politici proactive, investind în sisteme de apărare cibernetică avansate și în mecanisme eficiente de cooperare internațională. Inteligența artificială și noile tehnologii de vârf pot oferi soluții eficiente pentru detectarea și prevenirea atacurilor, însă fără o strategie globală și o reglementare clară a spațiului digital, riscurile vor continua să crească. În același timp, educația în domeniul securității cibernetice trebuie să devină o prioritate, atât la nivel instituțional, cât și individual, pentru a reduce vulnerabilitățile exploatate de atacatori.

Pe măsură ce cyberterorismul evoluează, devine clar că viitorul conflictelor nu va fi definit doar de superioritatea militară clasică, ci și de capacitatea statelor de a proteja și controla spațiul digital. În acest nou peisaj al securității globale, cyberspace-ul nu mai este doar un mediu al schimbului de informații, ci o dimensiune esențială a puterii și influenței internaționale.

BIBLIOGRAFIE

1. CONWAY Maura, ”Terrorist `Use` of the Internet and Fighting Back”, *Information and Security: An International Journal,* vol. 19, 2006, p. 10-30.
2. DENNING Dorothy E., *Cyberterrorism,* Georgetown University, 2000.
3. GADDIS John Lewis, *Războiul Rece,* Bucureşti, Editura Rao, 2009.
4. GIBSON William, *Neuromancer,* Berkley Publishing Group, New York, 1989.
5. GRAY H. David, Albon Head, ”The Importance of the Internet to the Post-Modern Terrorist and its Role as a Form of Safe Haven”, *European Journal of Scientific Research,* vol. 25, 2009, p. 396-404.
6. KAPLAN Eben, Terrorists and the Internet, 2009, http://www.cfr.org/terrorism-and-technology/terrorists-internet/p10005, accesat la data 23.04.2021.
7. MUREŞAN Mircea, Gheorghe Văduva, *Războiul viitorului, viitorul războiului,* Bucureşti, Editura Universității Naționale de Apărare, 2004.
8. LESSER O. Ian, David F. Ronfeldt, Bruce Hoffman, John Arquilla, Michele Zanini, *Countering the New Terrorism,* RAND Corporation,1999.
9. MORAVEC Hans, *Mind Children: The Future of Robot and Human Intelligence,* Harvard University Press, 1990.
10. SUCIU Dan-Mircea, „Strategii de securitate cibernetică în era Internetului”, *Revista Română de Studii de Intelligence,* nr. 9, Serviciul Român de Informații, București, 2013, p. 99-110.
11. WRIGHT Quincy, *A Study of War* (second edition), The University of Chicago Press, Chicago and London, 1965.
12. *** Council on Foreign Relations, *Cyber Threats and International Cooperation,* Workshop Summary Report, Washington DC, 26.02.2015.

[1] Mircea Mureşan, Costică Ţenu, Lucian Stăncilă, Doru Enache, Doina Filote, *Securitatea europeană la începutul mileniului III,* Bucureşti, Editura Universităţii Naţionale de Apărare „Carol I", 2006.

[2] Quincy Wright, *A Study of War* (second edition), The University of Chicago Press, Chicago and London, 1965.

[3] Hans Moravec, *Mind Children: The Future of Robot and Human Intelligence,* Harvard University Press, 1990.

[4] Diplomația coercitivă este definită ca strategia politico-diplomatică care își propune să influențeze voința unui adversar.

[5] Mircea Mureşan, Gheorghe Văduva, *Războiul viitorului, viitorul războiului,* Bucureşti, Editura Universității Naționale de Apărare, 2004.

[6] Dorothy E. Denning, *Cyberterrorism,* Georgetown University, 2000.

[7] Secretarul-adjunct al Departamentului Apărării din SUA, https://www.cnas.org/people/william-j-lynn-iii, accesat la data de 24.05.2024.

[8] William Gibson, *Neuromancer,* Berkley Publishing Group, New York, 1989.

[9] John Lewis Gaddis, *Războiul Rece,* Bucureşti, Editura Rao, 2009.

[10] Dan-Mircea Suciu, „Strategii de securitate cibernetică în era Internetului", *Revista Română de Studii de Intelligence,* nr. 9, Serviciul Român de Informații, București, 2013, p. 99-110.

[11] Council on Foreign Relations, *Cyber Threats and International Cooperation,* Workshop Summary Report, Washington DC, 26.02.2015.

[12] Expert american în securitate cibernetică.

[13] Cooperarea internațională pentru un cyberspace sigur, https://intelligence.sri.ro/cooperarea-internationala-pentru-un-cyberspace-sigur/, accesat la data de 15.05.2021.

[14] Maura Conway, "Terrorist `Use` of the Internet and Fighting Back", *Information and Security: An International Journal,* vol. 19, 2006, p. 10-30.

[15] Ibidem.

[16] David H. Gray, Albon Head, "The Importance of the Internet to the Post-Modern Terrorist and its Role as a Form of Safe Haven", *European Journal of Scientific Research,* vol. 25, 2009, p. 396-404.

[17] Maura Conway, Op.cit

[18] Ian O. Lesser, David F. Ronfeldt, Bruce Hoffman, John Arquilla, Michele Zanini, *Countering the New Terrorism,* RAND Corporation,1999.

[19] Eben Kaplan, *Terrorists and the Internet,* 2009, http://www.cfr.org/terrorism-and- technology/terrorists-internet/p10005, accesat la data 23.04.2021.

ISR ȘI JOCUL DE RĂZBOI (I) - PROVOCĂRI ÎN DOMENIULUI ISR-

*Alin DREPTATE**

Abstract

Wargaming on ISR (intelligence, surveillance and reconnaissance) has always been a challenge, given by the multitude of the collection capabilities and their specific tradecraft. The presence of main intelligence capabilities and their specific outcomes to better understand the operational environment will always have strengths and weaknesses, and the human element will always be the one to augment one or the other. This first part of the article aims to discover some of the key aspects from the domain, which could be the basis for future scenario generation in the wargaming process. Difficulties in understanding some of the concepts, mentioned below, inherent drawbacks associated with each capability and the human factor could constitute the foundation for the main events lists and main incidents lists that could be exercised in the future.

***Keywords**: ISR; information; intelligence; collection; capabilities.*

ISR ȘI CONCEPTUL DE INFORMAȚII/ INTELLIGENCE

Termenul de ISR (*intelligence, surveillance and reconnaissance*) are calitatea de a fi atât concis, prin specificitatea celor trei direcții la care face referință, cât și ambiguu, prin utilizarea sa într-o manieră cuprinzătoare, de includere a tuturor capabilităților de culegere de informații, fără a face referire la una specifică. Această caracteristică bivalentă face ca acest concept să fie uneori neînțeles/ folosit neadecvat, fiindu-i diminuată sau exagerată importanța. ISR, prin furnizarea de informații, are rolul de sprijin al operațiilor, cu mențiunea că în centrul său este producerea de informații/ intelligence pentru informarea comandantului și că acționează ca un multiplicator de forță al acestuia[1]. Această nevoie de augmentare apare ca urmare a faptului că structurile de forțe întotdeauna vor fi limitate ca număr, cu capabilități lipsă sau insuficient dotate, într-un mediu tot mai dinamic informațional. Sincronizarea și integrarea capabilităților ISR reduc limitările unei forțe prin facilitarea eforturilor conjugate, judicioase și desfășurate în multiplan, pentru a performa într-un mediu adversarial misiunii comandantului.

Între subdomeniile ISR, cel al informațiilor de tip intelligence este ușor de remarcat, mai ales pentru că o parte dintre discipline au sufixul INT (abrevierea de la „intelligence”), termen de regulă folosit pentru indicarea activității de culegere sau pentru desemnarea produselor rezultate în urma prelucrării/ transformării datelor și informațiilor, ca urmare a parcurgerii ciclului informațional. Cele mai cunoscute capabilități sunt: HUMINT - Human Intelligence (informații din surse umane);

* ***Autorul este cercetător acreditat la Colegiul Național pentru Studierea Arhivelor Securității.***

IMINT - Imagery Intelligence (informații din imagini); MASINT - Measurement and Signature Intelligence (informații din analiza emisiilor radar sau a semnăturilor acustice sau seismice); SIGINT - Signal Intelligence (informații din semnale din spectrul electromagnetic) și OSINT - Open Source Intelligence (informații din surse deschise)[2].

Contrar acestei aparente imagini de sub-domeniu facil în înțelegerea lui, există dificultăți și în explicarea termenului de intelligence ca urmare a lipsei unei echivalențe între cuvântul informații și cel de intelligence. Astfel, termenul de „informații" este definit ca date care prezintă un element de noutate sau, într-un alt context, ca o acțiune de comunicare, respectiv o știre pentru cineva care se informează despre o situație[3]. Elementul comun al acestor două definiții este caracterul de noutate, iar prezența în limba engleză a cuvântului *information* corespunde celui de informație din limba română[4]. Ce lipsește este însă echivalentul pentru termenul de „intelligence", care în prezent este tradus prin două cuvinte, ca „informații procesate" sau prin alipirea cuvântului „intelligence" alături de cel de „informații".

Adițional, și nu în puține ocazii, termenul de „informații" se folosește eronat atât pentru termenul *information,* cât și pentru cel de *intelligence*. În această ultimă situație, apar confuzii ca urmare a multiplilor termeni specifici subdomeniului informații, printre care cei mai cunoscuți sunt „cerințele prioritare de informații de tip intelligence", „cerințele specifice de informații de tip intelligence" și „elementele esențiale de informații" (nu și intelligence)[5]. În cadrul unei structuri de informații se mai folosesc, spre exemplu, și „cerințele critice de informații ale comandantului/ CCIR (care nu sunt și intelligence) sau „cerințele de informații de tip intelligence" (intelligence requirements/ IR), atunci când anumite informații nu există în baza de date și este solicitată culegerea lor de către capabilitățile ISR[6]. Așa cum se poate observa mai sus, se utilizează mai multe sintagme, care sunt fie doar informații, fie informații de tip intelligence, iar o necunoaștere a delimitărilor dintre acestea, respectiv folosirea interșanjabilă incorectă a celor doi termeni creează confuzii, mai ales într-un mediu multinațional, unde interoperabilitatea la nivel doctrinar/ conceptual este esențială.

Pentru limitarea acestor neajunsuri, contextul folosirii termenilor informații și intelligence, precum și cunoașterea multiplelor sensuri și limitări permit folosirea judicioasă a acestora și evitarea neînțelegerilor asociate utilizării lor. Ca o posibilă soluție de reducere a ambiguității, cel mai simplu ar fi folosirea termenului de „intelligence" în limba română și care, chiar dacă ar atrage critici pentru folosirea sa în calitate de cuvânt străin într-un text românesc, mesajul ar rămâne clar, concis și corect, fiind bine delimitat de cel de informație.

INFORMAȚII DE TIP INTELLIGENCE ÎN CONCEPȚIA NATO

NATO definește informațiile de tip intelligence drept un rezultat al fazei de culegere și procesare a informației[7]. Această informație obținută prin disciplinele de culegere este specifică și poate descrie mediul operațional, capabilitățile și intențiile unor actori, cu scopul de informare a comandantului, respectiv pentru luarea unor decizii care să anticipeze amenințările viitoare. După nivelurile la care se utilizează, informațiile de tip intelligence pot fi strategice, operaționale sau tactice[8]. Aceste niveluri sunt mai mult doctrinare, deoarece delimitarea lor este una estompată, ca urmare a faptului că un eveniment de ordin tactic poate schimba politica unei țări vizavi de o alta sau inițiа o nouă strategie de dezvoltare a unei organizații internaționale, cum este NATO, cu efecte pentru următorii zeci de ani. Cu această mențiune, intelligence-ul de nivel strategic poate fi folosit pentru elaborarea de planuri și politici militare, respectiv direcții de dezvoltare pentru state/ organizații și pentru previzionarea unor evenimente, de tip indici/ indicatori și avertizări, cu aplicabilitate și efecte pe termen lung.

Spre deosebire de intelligence-ul tactic, cel operațional permite înțelegerea mediului pe un spațiu geografic mai mare, care poate cuprinde mai multe misiuni, fiind concentrat, totodată, către identificarea și contracararea acelor actori care pot destabiliza un areal. Aceasta se realizează similar principiului vaselor comunicante, când se destabilizează o zonă care apoi impactează negativ alte zone limitrofe sau prin tranzitarea zonelor, prin trecerea dintr-o arie de operații în alta[9]. La nivel tactic, termenul de intelligence este specific, limitat în timp și spațiu și orientat către acei actori care pot destabiliza operația militară la un anumit moment sau într-un interval de timp definit[10].

Dacă împărțirea pe niveluri pare ambiguă, o provocare mai mare o constituie identificarea și evaluarea corectă a intelligence-ului pentru adoptarea unor decizii în concordanță cu impactul/efectele sale; astfel, există situații când deși vorbim de un intelligence de ordin tactic, impactul său este însă unul strategic, și, viceversa, respectiv situația în care intelligence-ul deși pare de nivel strategic, efectul produs este unul redus. Indiferent de situație, trebuie accentuat faptul că intelligence-ul are scopul de a crește gradul de cunoaștere al unei structuri prin oferirea acelor informații care să faciliteze luarea unor decizii mai informate. De asemenea, în cazul produselor de intelligence, acestea trebuie să conțină analize predictive în care se estimează evoluția mediului de securitate, astfel încât misiunea să dispună de timpul necesar pentru a-și pregăti numărul adecvat de forțe, să-și actualizeze misiunile și să-și modifice planificarea privitoare la liniile de efort pentru atingerea obiectivelor sale finale[11].

Important de menționat este că produsele de intelligence sunt un proces condus (nu controlat) de către comandantul forței. Chiar dacă CCIR, sub forma PIR (priority intelligence requirements), reprezintă baza conducerii culegerii de informații, dinamica mediului operațional dictează deciziile de contracarare, ameliorare sau prevenire a unor evoluții, necesar a fi luate de către un comandant, care, pentru a fi cât mai eficiente, necesită dinamism, flexibilitate și adaptare a capabilităților de culegere de informații.

PROVOCĂRILE LA NIVELUL UNEI STRUCTURI DE INFORMAȚII

Elementul de culegere de informații la nivel tactic, operațional și strategic este o parte esențială a comenzii, cu sarcina de a primi, procesa și disemina informații, respectiv de a acționa în coordonare cu celelalte structuri pentru a evita duplicarea de efort și acțiunile singulare[12]. Pentru acest lucru este nevoie de personal pregătit pentru pozițiile din structura de conducere a culegerii de informații și care, totodată, să se poate adapta ușor la dinamica mediului operațional. „Personal pregătit" semnifică, de regulă, specializare în cel puțin una dintre disciplinele de culegere și cunoștințe minime despre celelalte structuri de comandament (operații, planificare), cu care nivelul de conducere ar trebui să aibă o cooperare și o coordonare strânse. Cum aceste cunoștințe nu sunt deținute a priori rezultă o neînțelegere a obiectivelor structurilor de informații sau chiar conflicte cauzate de specificitatea domeniului; din acest punct de vedere, personalul ce urmează să încadreze activitatea de informații are nevoie de pregătire/ antrenament pentru a înțelege mai bine specificul organizației în care urmează să lucreze[13].

De asemenea, simpla prezentare a funcționării și a obiectivelor informațiilor celorlaltor structuri nu este suficientă, deoarece nu se particularizează aportul structurii de informații la misiunea celorlalte componente ale forței și necesarul de date de la acestea, de care structura are nevoie pentru estimarea evoluției amenințării. Astfel, scopul acestui ultim demers este nu de a arăta ce sunt informațiile, ci mai mult ceea ce pot face informațiile pentru alte structuri și cum acestea pot susține misiunea sa. În acest fel se evită misiunile izolate, necoordonate, care în unele operații kinetice pot cauza acțiuni fratricide.

O prezentare succintă a sarcinilor esențiale ale structurilor de informații includ cunoașterea comprehensivă a doctrinelor ce reglementează domeniul, respectiv a caracteristicilor capabilităților de culegere organice și de sprijin, respectiv a limitărilor acestora. Adițional, structura de informații este responsabilă de realizarea unui

plan de culegere de informații pe baza unei estimări realiste de informații; integrarea în produsele analitice proprii a informațiilor provenite din alte surse (structuri aliate sau partenere); respectiv, sincronizarea planului de culegere de informații cu cel de executare a operațiilor[14]. Alte două elemente critice pentru succesul misiunii unui comandament este ca șeful structurii de informații să se asigure că tot personalul din subordine cunoaște intenția comandantului, detaliată de acesta prin briefing-urile desfășurate regulat sau prin sarcinile/ solicitările curente formulate și termenele de răspuns la acestea[15]. Un simplu email sau încărcarea produselor pe un portal nu sunt suficiente, motiv pentru care comunicarea (directă între șefii de structuri sau indirectă, prin intermediul persoanelor de legătură desemnate pentru relaționare) este mai eficientă și, în consecință, recomandată.

ARHITECTURA STRUCTURII DE INFORMAȚII

Componența de principiu a unei structuri de informații include o secție de analiză a tuturor informațiilor primite, elemente de sprijin din SIGINT/ IMINT/ OSINT sau GEOINT, aflate în organică sau în suport și elementul cel mai productiv informativ, dar nu neapărat și cel mai de încredere, elementul de 2X (counterintelligence)[16]. Toate capabilitățile de culegere trebuie conduse centralizat și acest lucru se face prin elementul ISR din organica structurii de informații. La acestea se mai pot adăuga în sprijin structuri de cercetare sau de forțe speciale, care, spre exemplu, pot executa misiuni de culegere de informații prin contact cu adversarul, și structuri de tip reach-back pentru analiză integrată (cu previziuni pe termen mediu și lung), respectiv elemente specializate în protecția forței, de tip asigurarea securității sau de contrainformații[17].

Dintre toate structurile componente, cea de analiză integrată are ca sarcină principală procesarea tuturor informațiilor primite la nivelul forței, indiferent de emitentul lor. Pentru a fi relevantă, acest tip de analiză necesită o strânsă colaborare cu structura de planificare, pentru a înțelege intențiile și planurile comandantului, precum și o monitorizare continuă a evenimentelor curente din mediul operațional[18]. Erori frecvente care se fac în ceea ce privește analiza sunt lipsa de direcționare cu nevoile beneficiarului și lipsa de sincronizare între alegerea informațiilor care să fie prezentate comandantului și evenimentele din mediul public care îi pot influența misiunea[19]. Toate acestea sunt însă relativ ușor de remediat, mai ales dacă personalul responsabil este antrenat în analiză; în acest fel se confirmă și importanța prezenței unei structuri de informații în toate activitățile curente ale unui comandament.

Elementul de GEOINT/ IMINT, care poate fi atât în organică, cât și în sprijin, poate facilita procesul de elaborare a produselor de analiză prin oferirea unei imagini de ansamblu asupra terenului[20]. Aceste structuri au un rol central în vizualizarea mediului operațional, fără de care informația ar rămâne doar la nivel de concept și, foarte probabil, neînțeleasă de o parte din personal. Elementul vizual este cel care face informația accesibilă, ușor de folosit și, cel mai important, înțeleasă într-un timp mai scurt decât în absența reprezentării vizuale a acesteia. Fiind o structură cu personal ce necesită pregătire calificată și dotare cu tehnică costisitoare, care în permanență evoluează, elementul de GEOINT/ IMINT va avea întotdeauna provocări la încadrare/ dotare, aspecte care, cel mai probabil, vor afecta negativ îndeplinirea obiectivelor misiunii forței.

În ceea ce privește OSINT, în ultimii ani s-a observat cât de importantă poate fi contribuția sa în informările către beneficiari[21]. Drept urmare, orice structură de informații care nu are o astfel de capabilitate va întâmpina dificultăți în informarea riguroasă a comandatului cu cele mai relevante evoluții din mediul operațional. Nu de puține ori, în cunoașterea evoluției situației de securitate un rol de bază l-au avut informațiile prezente în surse deschise. Ca și în cazul structurii de analiză integrată, personalul care operează în OSINT trebuie să dețină cunoștințe exhaustive în tehnicile de analiză și ar fi de dorit să provină din rândurile unor analiști cu experiență în domeniul intelligence. Motivația acestei recomandări este

gradul mare de dezinformare prezent în acest tip de informații și pe care un analist începător ar putea avea dificultăți în a-l identifica.

INTELLIGENCE ȘI INFORMAȚIILE DIN SURSE DESCHISE

Activitatea de tip OSINT nu este ceva nou, dar relevanța sa a fost poate demonstrată cel mai bine începând cu cel de-al Doilea Război Mondial, când în unele state aliate erau analizate propaganda nazistă și evoluția politico-militară sau economică a Germaniei în urma lecturii a diverse publicații. OSINT a continuat, apoi, în timpul Războiului Rece, când a existat o supraîncărcare informațională a statelor din Occident cu activitățile și evoluțiile din URSS și din țările membre ale Tratatului de la Varșovia. Odată cu evoluțiile tehnologice și apariția Internetului, respectiv a comunicațiilor prin satelit, accesul populației la informație s-a extins și a depășit limitarea inițială, prin care doar anumite structuri statale o puteau accesa. Simultan, s-a dezvoltat și interpretarea informației de către diverse grupuri sau persoane, fapt care a redus controlul statului asupra acesteia și a eliminat monopolul unei singure interpretări. Astfel, au apărut multiple surse de informații, unde informația primară era mascată de surse secundare sau interpretări eronate, respectiv intenționat false, pentru a manipula statul sau a galvaniza masele de oameni. În această complexitate, contextul informației și realitatea curentă au devenit doi factori care permit interpretarea coerentă și realizarea diferenței dintre o informație/ analiză de valoare și una lipsită de relevanță sau toxică.

Din perspectivă tradițională, informațiile provenite din surse deschise sunt privite cu neîncredere de specialiștii în informații, dar accesul factorilor de decizie la acestea, în forma lor brută, neverificată, obligă o structură de informații să nu le ignore. De multe ori, decidenții politico-militari, expuși la surse deschise, solicită informații care să detalieze/ să nuanțeze ceea ce s-a prezentat în spațiul public. Din acest motiv și fără a mai lua în calcul beneficiile acestui mediu în înțelegerea mediului operațional, este imperativ ca structura de informații să includă în munca sa și monitorizarea/exploatarea informațiilor din OSINT. Reticența unor specialiști din domeniul intelligence față de acest tip de informații nu se justifică în contextul realității curente, iar ignorarea acestora pe baza argumentului că informațiile trebuie să parvină doar din surse secrete reprezintă un mod de gândire depășit.

Mulți practicieni din domeniul intelligence, ce au publicat studii pe acest subiect, au susținut că, în experiența lor, informările către factorii de decizie s-au bazat în proporție de peste 80% pe informații obținute din surse deschise, unii afirmând că cifra ar putea fi și mai mare[22]. Un exemplu concludent este oferit chiar de către un fost șef de informații externe britanic, care a recunoscut că obișnuia să monitorizeze în mod constant politica Franței și să includă informațiile din surse deschise în documentele redactate către guvernul britanic, justificarea sa fiind că politicienii francezi nu își disimulau interesele, obiectivele și, uneori, nici chiar capabilitățile de care dispuneau[23]. Prin acest tip de abordare deschisă, oficialii francezi considerau că informau electoratul asupra viziunilor lor și, totodată, creșteau avantajul propriei țări/ structuri în momentul în care se punea problema luării unei decizii, reușind astfel să elimine efectul surpriză care ar fi putut provoca eventuale frământări/ tensiuni sociale.

OSINT ȘI ISR

Intelligence-ul din OSINT prezintă similitudini cu intelligence-ul clasic, cu diferența notabilă că dacă acesta din urmă utilizează metode specifice pentru identificarea informațiilor relevante, OSINT-ul își caută informațiile în spațiul public. Conform lui Miller (2018), capabilitățile de culegere clasificate sunt direcționate „împotriva unei game de ținte și tipuri, fie ele țări, lideri, grupuri teroriste, carteluri de droguri, traficanți de oameni, sisteme de arme, decizie, procese sau planuri ascunse”[24] și implică eforturi financiare mari. În eventualitatea scurgerii unor informații culese din surse clasificate în spațiul public, aceste informații își pierd din valoare,

iar sursele sunt compromise. Prin comparație, în OSINT obținerea de informații în mod deschis implică mai puține costuri și mai puține riscuri, fiind folosite ca surse mass-media, Internetul, revistele/publicațiile de specialitate, diverse studii, conferințe etc.[25]. Procesul, deși simplu la prima vedere, este în esență complex, informațiile publice sunt identificate, colectate, exploatate și apoi diseminate în timp util și în formatul adecvat necesităților beneficiarilor, pentru a răspunde la o cerință specifică de informații. Pe scurt, a răspunde la o cerință specifică de informații presupune ca informațiile din spațiul public să fie transformate într-un produs de intelligence de tip acționabil.

Adițional, OSINT prezintă similitudini și cu alte domenii de intelligence, precum GEOINT – ce utilizează platforme publice de analiză a terenului, SIGINT – ce monitorizează anumite semnale ale unor emisii electronice publice, sau MASINT – unde senzorii identifică cutremure, radiații sau teste nucleare[26]. În ceea ce privește relația HUMINT – OSINT, aceasta este una de tip bidirecțional, în sensul că surse umane (HUMINT) pot (și uneori o fac) furniza informații către mass-media, iar jurnaliștii (categorie de lucrători în OSINT) folosesc proceduri similare domeniului HUMINT pentru managementul informațiilor (de la culegere până la analiză). Cu toate acestea, diferența majoră a HUMINT-ului față de OSINT constă în faptul că, în cazul capabilităților de culegere, aici avem de-a face cu o culegere specializată protejată/ ascunsă și cu modalități specifice (ce țin de munca de culegere de informații clasificate) de abordare a țintei[27]. Dacă la celelalte discipline identificarea și accesarea țintei este dificilă, la OSINT provocarea este mai mult analitică, prin identificarea din multitudinea de informații a acelora care sunt relevante și, apoi, validarea și exploatarea lor.

Deși comportă unele dezavantaje, OSINT-ul susține totuși domeniul ISR prin aportul de informații pe care îl aduce (poate de multe ori acestea sunt de context, acesta fiind și unul dintre principalele dezavantaje ale domeniului, dar există și destule cazuri în care acestea sunt de substanță) și rapiditatea cu care identifică schimbări în mediul operațional, îndeosebi pe cele care au un impact asupra comunității. O contribuție semnificativă a OSINT-ului este abilitatea de a acționa ca un factor de direcționare a culegerii de informații clasificate, spre exemplu prin identificarea apariției în spațiul public a unei imagini de interes sau a unor documente sensibile[28]. Mai mult, informații (prezente pe rețelele de socializare) despre un protest în desfășurare, un incident terorist sau dezastru natural pot determina activarea HUMINT, IMINT sau GEOINT pentru confirmarea evenimentului și/sau pentru determinarea impactului acestora asupra mediului operațional.

Marele dezavantaj al OSINT-ului este potențialul de dezinformare, mai ales atunci când informațiile prezente în spațiul public par a fi de nivel strategic, adică având un impact major asupra mediului operațional, iar acestea sunt folosite de decidenți fără ca anterior să fi fost verificate/ trecute prin etapa de procesare a ciclului informațional[29]. În context, deciziile adoptate pot conduce la schimbări la nivelul mediului operațional sau pot fi consumatoare de resurse în detrimentul unor operațiuni de anvergură care se află în derulare. În astfel de situații, structura de informații trebuie să intervină rapid pentru clarificarea evenimentului și identificarea unor potențiale acțiuni de provocare sau dezinformare. Rapiditatea intervenției este esențială pentru limitarea impactului negativ. Orice întârziere sau ambiguitate neadresată prin procesul de analiză, amplifică influența primei informații, cu efecte adverse pe termen scurt și mediu.

În concluzie, OSINT, ca parte a domeniului ISR, contribuie semnificativ la înțelegerea mediului operațional prin multitudinea și varietatea de informații pe care le pune la dispoziția unei structuri de informații. Aceasta, la rândul său, creează o bază de date care-i este utilă în monitorizarea evoluției mediului operațional și în decelarea acelor evenimente repetitive care au potențialul de a declanșa decizii nefundamentate.

Pentru o structură de informații, principalele provocări din mediul OSINT sunt identificarea informațiilor relevante din multitudinea celor disponibile, limitarea efectelor dezinformării (atunci când este cazul) și integrarea informațiilor identificate și verificate (prin fuziunea lor cu alte informații din surse clasificate), pentru a realiza un produs relevant și cu valoare predictivă.

În ceea ce privește structura de 2X (și conform doctrinei NATO), aceasta este, de regulă, însărcinată cu contracararea activităților adversarului prin, spre exemplu, aflarea intențiilor acestuia de destabilizare a mediului operațional[30]. Având o relație bine fundamentată cu alte structuri însărcinate cu contracararea amenințărilor asimetrice, 2X reprezintă, în majoritatea situațiilor, un centru de greutate al capabilităților de culegere. Informațiile obținute de 2X pot fi preluate de celelalte capabilități, urmând ca după culegerea specifică acestea să fie integrate în ciclul de analiză de intelligence și prezentate în briefing-uri de informare pentru beneficiari[31].

CONCLUZII

În cadrul organicii unei structuri de informații, elementul de comandă ISR (exercitat asupra tuturor capabilităților de culegere) are un rol central în direcționarea procesului de obținere de informații și întâmpinarea nevoilor informaționale ale comandantului, prin adaptarea structurii la schimbările mediului operațional. Un personal antrenat, o direcționare continuă, realizată de șeful structurii de informații, cooperarea cu operațiile și planificarea asigură componentele necesare îndeplinirii cu succes a misiunii.

În contextul unei realități în care delimitarea dintre informații clasificate, obținute în mod tradițional prin capabilități secrete, și cele prezente în spațiul public este diminuată, gândirea analitică structurată și integrarea informațiilor provenite din diferite surse, respectiv fuziunea tuturor capabilităților, trăsătură dominantă a domeniului ISR, devin mijloacele prin care se menține supremația informațională într-un mediul operațional volatil/ în continuă schimbare.

BIBLIOGRAFIE

1. ACKERMAN Gary, Peterson Hayley, ”Terrorism and COVID-19: Actual and Potential Impacts”, *Perspectives on Terrorism,* vol. 14, nr. 3, 2020, p. 59-73.
2. BARNETT G. Gary, ”MI tactical HUMINT team operations in Kosovo”, *Military Intelligence Professional Bulletin*, vol. 27, nr. 1, 2001, p. 20-22.
3. BERNARD Rose, Sullivan Richard, ”The use of HUMINT in epidemics: a practical assessment”, *Intelligence and National Security*, vol. 35, nr. 4, 2020, p. 493-501.
4. BOWMAN H. Miller, ”Open Source Intelligence (OSINT): An Oxymoron?”, *International Journal of Intelligence and CounterIntelligence*, vol. 31, nr. 4, 2018, p. 702-719.
5. BRUNEAU C. Thomas, Steven C. Boraz (eds.), *Reforming Intelligence. Obstacles to Democratic Control and Effectiveness*, University of Texas Press, 2007.
6. CRIEZIS Meili, ”Online Deceptions: Renegotiating Gender Boundaries on ISIS Telegram”, *Perspectives on Terrorism*, vol. 14, nr. 1, 2020, p. 67-73.
7. HARE Nick, Coghill Peter, ”The future of the intelligence analysis task”, *Intelligence and National Security*, vol. 31, nr. 6, 2016, p.1-13.
8. HOLBROOK Donald, ”Internal Debates, Doubts and Discussions on the Scope of Jihadi Violence: The Case of the Turnup Terror Squad”, *Perspectives on Terrorism. Special Issue - Restraint in Terrorist Groups and Radical Milieus*, vol. 14, nr. 6, 2020, p. 77-90.
9. JOHNSON K. Loch, ”Analysis for a new age”, *Intelligence and National Security*, vol. 11, nr. 4, 1996, p. 657-671.
10. JONES W. Jerry, ”CI and HUMINT or HUMINT and CI or CI/HUMINT or TAC HUMINT (confusing, isn’t it?)”, *Military Intelligence Professional Bulletin*, vol. 28, nr. 2, 2002, p. 28-33.
11. KORKISCH W. Friedrich, *NATO gets better intelligence. New challenges require new answers to satisfy intelligence needs for headquarters and deployed/employed forces*, Center for Foreign and Defense Policy, Institut fur Aussen- und Sicherheitspolitik (IAS), IAS Reader, Strategy Paper, nr. 1, Viena, 2010, 75 p., disponibil la www.natowatch.org.
12. REEVE Zoey, ”Repeated and Extensive Exposure to Online Terrorist Content: Counter-Terrorism Internet Referral Unit Perceived Stresses and Strategies”, *Studies in Conflict & Terrorism*, vol. 46, nr. 6, 2023, p. 888-912,.
13. ROPEK Lucas, Disinformation Online Could Be Making the COVID-19 Crisis Worse, *Government Technology*, 26 martie 2020, govtech.com/security/disinformation-online-could-be-making-the-covid-19-crisis-worse.html.
14. SCRIVENS Ryan, ”Exploring Radical Right-Wing Posting Behaviors Online”, *Deviant Behavior*, vol. 42, nr. 11, 2021, p. 1470-1484.
15. SHELTON Christina, ”An Attempt to Sort Out the IC’s Overload”, Book Reviews, *International Journal of Intelligence and CounterIntelligence*, vol. 25, nr. 3, 2012, p. 619-630.
16. STOTTLEMYRE A. Steven, ”HUMINT, OSINT, or Something New? Defining Crowdsourced Intelligence”, *International Journal of Intelligence and Counter Intelligence*, vol. 28, nr. 3, 2015, p. 578-589.
17. *** Joint Doctrine Publication 2-00: understanding and intelligence support to joint operations, 2011, disponibilă la adresa www.assets.publishing.service.gov.uk.
18. *** AAP-6, NATO Glossary of terms and definitions, 2013, disponibil la www.jcs.mil (accesat prin motorul de căutare pe www.google.com).
19. *** AJP-2 Allied Joint Doctrine for Intelligence, Counterintelligence and Security, 2003, disponibilă la adresa www.jadl.act.nato.int (accesat prin motorul de căutare pe www.google.com).
20. *** AJP-3 Allied Joint Doctrine for the Conduct of Operations, 2019, disponibilă la www.coemed.org (accesat prin motorul de căutare pe www.google.com).
21. *** *Wargaming Handbook*, Development, Concepts and Doctrine Centre, UK Ministry of Defence, 2017, 97 p.

[1] *** AJP-3 Allied Joint Doctrine for the Conduct of Operations, 2019, p. 1-24.
[2] *** AJP-2 Allied Joint Doctrine for Intelligence, Counterintelligence and Security, 2003, p. 1-2-6.
[3] https://dexonline.ro/definitie/informatii.
[4] *** AJP-2 Allied Joint Doctrine for Intelligence, Counterintelligence and Security, p. 1-2-1.
[5] Ibidem.
[6] Ibidem, p.1-4-8.
[7] *** AJP-3 Allied Joint Doctrine for the Conduct of Operations, p. 1-23.
[8] *** AJP-2 Allied Joint Doctrine for Intelligence, Counterintelligence and Security, p.1-4.
[9] Ibidem.
[10] Ibidem.
[11] *** AJP-3 Allied Joint Doctrine for the Conduct of Operations, 2019, p. A-3.
[12] Ibidem.
[13] Friedrich W. Korkisch, *NATO gets better intelligence. New challenges require new answers to satisfy intelligence needs for headquarters and deployed/employed forces*, Center for Foreign and Defense Policy, Institut fur Aussen- und Sicherheitspolitik (IAS), IAS Reader, Strategy Paper, nr. 1, Viena, 2010, p. 35, disponibil la www.natowatch.org.
[14] *** AJP-3 Allied Joint Doctrine for the Conduct of Operations, p. A-2; AJP-2 Allied Joint Doctrine for Intelligence, Counterintelligence and Security, p. 1-4-4.
[15] *** AJP-3 Allied Joint Doctrine for the Conduct of Operations, 2019, p. 3-8.
[16] AJP-2 Allied Joint Doctrine for Intelligence, Counterintelligence and Security, p. 1-2-5–1-2-6; Steven A. Stottlemyre,"HUMINT, OSINT, or Something New? Defining Crowdsourced Intelligence", *International Journal of Intelligence and CounterIntelligence*, vol. 28, nr. 3, 2015, p. 578-589; Col. Thomas Spahr, Cpt. Michel Weiss, "4th Infantry Division Military Intelligence Training Strategy", *Military Intelligence Professional Bulletin*, vol. 45, nr. 2, 2019, p. 78-82; Gary G. Barnett, "MI tactical HUMINT team operations in Kosovo", *Military Intelligence Professional Bulletin*, vol. 27, nr. 1, 2001, p. 20-22; Rose Bernard, Richard Sullivan, "The use of HUMINT in epidemics: a practical assessment", *Intelligence and National Security*, vol. 35, nr. 4, 2020, p. 1-9.
[17] Jerry W Jones, "CI and HUMINT or HUMINT and CI or CI/HUMINT or TAC HUMINT (confusing, isn't it?)", *Military Intelligence Professional Bulletin*, vol. 28, nr. 2, 2002, p. 28-33.
[18] Nick Hare, Peter Coghill, "The future of the intelligence analysis task", *Intelligence and National Security*, vol. 31, nr. 6, 2016, p. 860-865.
[19] Loch K. Johnson, "Analysis for a new age", *Intelligence and National Security*, vol. 11, nr. 4, 1996, p. 657-671.
[20] Christina Shelton, "An Attempt to Sort Out the IC's Overload", *International Journal of Intelligence and CounterIntelligence*, vol. 25, nr. 3, 2012, p. 619-630.
[21] Ibidem.
[22] Ibidem.
[23] Sir Richard Dearlove, Prezentare publică a rolului informațiilor în conducerea unui stat, Universitatea Cambridge, 2019.
[24] Miller H. Bowman, "Open Source Intelligence (OSINT): An Oxymoron?", *International Journal of Intelligence and CounterIntelligence*, vol. 31, nr. 4, 2018, p. 704.
[25] Thomas C. Bruneau, Steven C. Boraz, *Reforming Intelligence. Obstacles to Democratic Control and Effectiveness*, University of Texas Press, 2007, p. 8.
[26] Ibidem., p. 78-80.
[27] Ibidem.
[28] Ibidem., p.8.
[29] Ibidem, p. 98-101.
[30] AJP-2 Allied Joint Doctrine for Intelligence, Counterintelligence and Security, p. 8-2.
[31] Ibidem., p. 3-5.

UTILIZAREA ȘI LIMITĂRILE INTELIGENȚEI ARTIFICIALE ÎN DOMENIUL SECURITĂȚII NAȚIONALE

Alin VICLIUC*

Abstract

The article discusses the potential of AI and machine learning in various fields, including national security, decision-making or OSINT. It highlights the rapid progress of AI and the ability of machine learning models to perform tasks that were previously thought impossible or time consuming. The article also touches on the trust and assurance aspects of AI and the barriers to AI adoption, such as the lack of data literacy.

However, it is important to ensure that AI systems are developed and deployed ethically, with appropriate safeguards and human oversight to prevent unintended consequences and ensure accountability. Delegating authority to AI systems presents several risks and challenges. One of the main risks is the potential for errors or biases in the decision-making process. AI systems are trained on data, and if that data is biased or incomplete, it can lead to biased or incorrect decisions. This is particularly concerning in sensitive areas such as national security, where the consequences of errors can be significant.

In terms of accountability, when decisions are made by AI systems, it can be difficult to determine who is responsible for any negative outcomes. In traditional decision-making processes, humans can be held accountable for their actions. However, with AI systems, the responsibility becomes more diffuse, making it challenging to assign blame or address issues of accountability. There are also concerns about the potential for AI systems to be manipulated or hacked. If an AI system is compromised, it could lead to incorrect or malicious decisions being made. This highlights the importance of robust cybersecurity measures to protect AI systems from external threats.

Overall, while there are significant benefits to delegating authority to AI systems, it is crucial to carefully consider and address these risks and challenges to ensure the responsible and ethical use of AI in decision-making processes. In summary, trust and assurance in AI decision-making can be established through transparency, accountability, data quality, human involvement, and ongoing monitoring and evaluation. These measures help ensure that AI decisions are reliable, explainable, and aligned with ethical standards. The article concludes by discussing how AI can be effectively utilized in national security and defense in several ways.

Keywords: *AI; machine learning; AI-powered systems; defense; national security; decision-making process; Intelligence; OSINT; cybersecurity; responsible AI; intelligence cycle; ethical standards.*

Autorul este expert în cadrul Ministerului Apărării Naționale.

INTRODUCERE

Transformarea digitală implică adoptarea tehnologiilor digitale de către organizații și serviciile publice, precum și evalurea impactului acestor tehnologii asupra societății. Având în vedere numeroasele avantaje pe care promovarea digitalizării le oferă și pentru a se adapta la era digitală, Uniunea Europeană (UE) și-a asumat obiectivele asigurării suveranității digitale și definirea propriilor standarde, cu un accent clar pe date, tehnologie și infrastructură[1]. Aceste ținte și obiective ale UE sunt concretizate în programul denumit sugestiv „Secolul digital al Europei". Mai mult decât atât, în marja strategiei sale digitale, UE și-a creat cadrul legislativ privind folosirea inteligenței artificiale (IA), pentru a asigura condiții optime de dezvoltare și folosire a acestei tehnologii inovatoare. Prin reglementarea IA, Parlamentul UE își propune să se asigure că „sistemele IA folosite în UE sunt sigure, transparente, trasabile, nediscriminatorii și ecologice" și că vor fi „supravegheate de oameni și nu prin procese automatizate, pentru a evita rezultatele dăunătoare"[2], mai ales că IA este deja în curs de transformare a fiecărui aspect al vieții noastre.

Prosperitatea și dezvoltarea Europei sunt strâns legate de utilizarea datelor și a tehnologiilor interconectate. În condițiile în care IA are potențialul de a ne transforma existența, fie în mod pozitiv, fie negativ, discuțiile despre această tehnologie sunt la ordinea zilei. Majoritatea dintre noi folosim deja IA și beneficiem de avantajele pe care le aduce, de la asistenți digitali personali pentru telefoane, sisteme de climatizare inteligente și vehicule autonome până la motoare de căutare pe Internet, traducere automată, securitate cibernetică, optimizarea produselor și a strategiilor de vânzare sau agricultura inteligentă (irigare, alimentarea animalelor sau roboți care se ocupă de cultivare). Se estimează că volumul de date produse în întreaga lume a crescut de la 33 de zetabiți[3] în 2018 la 175 de zetabiți în 2025[4].

IA este un domeniu vast care permite oamenilor să reconsidere modul în care integrează informațiile, analizează datele și folosesc produsele generate pentru a îmbunătăți procesul de luare a deciziilor. Având în vedere că transformarea digitală este una dintre prioritățile UE, acest proces ar trebui să reprezinte, implicit, și una dintre prioritățile autorităților din România, inclusiv utilizarea IA în varii domenii de activitate, precum sistemul de apărare, ordine publică și siguranță națională.

Deoarece „IA este o familie de tehnologii cu evoluție rapidă, care poate genera o gamă largă de beneficii economice și societale în întregul spectru de industrii și activități sociale", Comisia Europeană a decis, în 24 ianuarie 2024, instituirea Oficiului European pentru inteligența artificială. Această nouă structură își propune, pe de o parte, dezvoltarea de instrumente, metodologii și criterii de referință pentru evaluarea capacităților modelelor de IA de uz general, în special a acelor modele de mari dimensiuni care prezintă riscuri sistemice, iar, pe de altă parte, sprijinirea punerii în aplicare a normelor privind practicile interzise în domeniul IA și facilitarea schimbului de informații, colaborarea între autoritățile naționale, colectarea notificărilor și instituirea unor platforme de informații și baze de date, în special atunci când un model sau un sistem de IA de uz general este integrat într-un sistem de IA cu grad ridicat de risc[5].

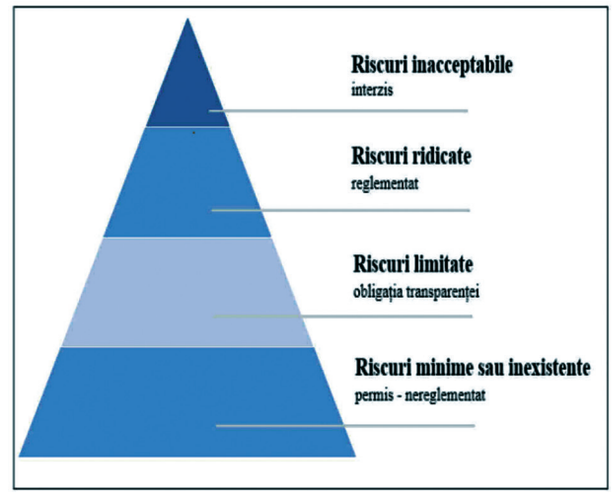


Figura 1: *Nivelurile de risc*

Punctual, sistemele considerate o amenințare la siguranța, mijloacele de trai și drepturile individuale ale oamenilor vor fi interzise (sistemele și aplicațiile IA utilizate pentru evaluarea socială sau aplicațiile care manipulează comportamentul uman pentru a interveni în voința liberă a utilizatorilor sunt exemple de tipuri

de sisteme IA care vor fi interzise), sistemele de mare risc (adică cele folosite în instruirea educațională sau profesională, angajare, resurse umane, aplicarea legii, managementul migrației, azilului și controlului la frontiere) vor trebui să îndeplinească criterii stricte înainte de a putea fi puse pe piața UE. În ceea ce privește sistemele cu risc limitat (adică chatboturile), acestea vor fi permise, dar utilizatorii vor trebui să fie conștienți că interacționează cu IA, iar soluțiile cu risc minim (cea mai mare parte a sistemelor IA) vor fi disponibile ca și înainte[6].

Articolul de față analizează utilizarea și limitările IA în sprijinul securității naționale și apărării țării. IA poate contribui la eficientizarea proceselor din domeniul securității naționale (prin intermediul diverselor aplicații și tehnologii inovatoare) și, din această perspectivă, este de o importanță crucială să înțelegem definiția și conceptele cheie asociate IA, precum și impactul acesteia asupra securității naționale înainte de abordarea subiectului utilizării specifice și potențialului extraordinar al acestei tehnologii emergente și disruptive.

DEFINIRE ȘI CONCEPTE CHEIE

Deși subiectul folosirii IA este unul de actualitate, suntem nevoiți să admitem că încă nu avem o definiție general acceptată a ceea ce este IA, aceasta fiind o chestiune care suscită vii dezbateri. De exemplu, Parlamentul European își propune stabilirea unei definiții uniforme și neutre din punct de vedere tehnologic pentru IA, care să poată fi aplicată și sistemelor IA viitoare, iar Departamentul Apărării (DoD) al SUA definește IA ca fiind un sistem informatic conceput pentru a reproduce o gamă largă de funcții umane și care se îmbunătățește continuu pentru efectuarea sarcinilor atribuite.

Înainte de a explora utilizarea IA în sprijinul securității naționale, este necesar să înțelegem conceptele cheie asociate acestei tehnologii, pornind de la faptul că IA se referă la capacitatea sistemelor de a descifra și de a imita comportamentul uman, utilizând algoritmi și modele matematice complexe. Astfel, printre conceptele cheie se numără învățarea automată, rețelele neuronale artificiale și procesarea limbajului natural. Aceste concepte sunt fundamentale în dezvoltarea și implementarea de proiecte bazate pe IA pentru apărarea țării și securitatea națională.

Învățarea automată (Figura 2) este un subset al IA care se concentrează pe predarea sistemelor pentru a învăța din date și pentru a îmbunătăți experiența, în loc să fie programat în mod explicit pentru a face acest lucru. IA procesează datele pentru a lua decizii și formula previziuni, iar algoritmii de învățare automată permit IA nu numai să proceseze acele date, ci și să le utilizeze pentru a învăța și pentru a se îmbunătăți, fără a avea nevoie de programare inteligentă.

Într-o foarte mare măsură, istoria IA seamănă cu istoria ciberneticii de la sfârșitul celui de-al Doilea Război Mondial. Norbert Wiener, considerat părintele ciberneticii, a cercetat un sistem de artilerie antiaeriană care să poată fi înclinat automat, nemaifiind necesar ca unui militar să-i fie atribuită această funcțiune, crescând astfel eficiența procesului de ochire. Acest episod a reprezentat ceea ce specialiștii

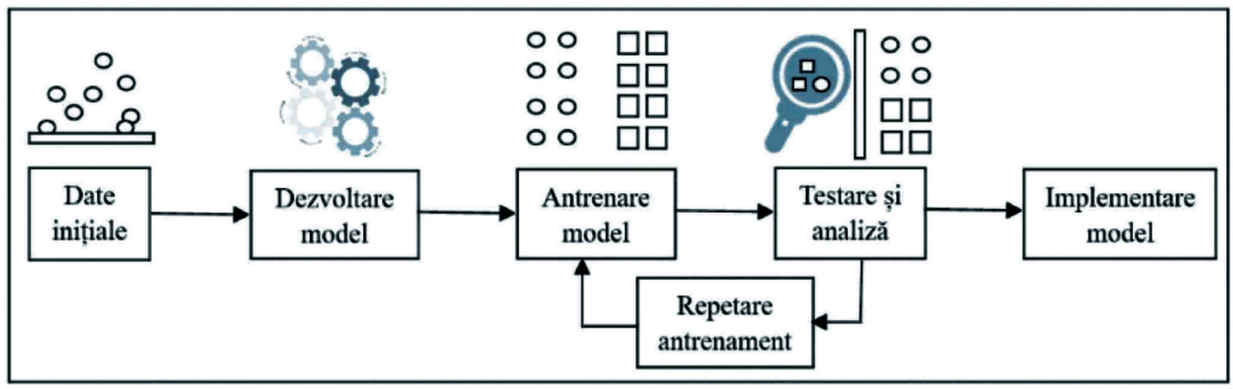


Figura 2: *Învățarea automată*

numesc *feedback loop*. Wiener, aflat în plin proces de proiectare a sistemului, a realizat că inovația are sens și aplicabilitate în lumea reală. În general, acest tip de feedback este comun modului de a gândi al oamenilor.

Ulterior, în 1956, John McCarthy, considerat unul dintre fondatorii IA, a folosit pentru prima dată termenul din dorința de a redenumi cibernetica deoarece avea nevoie de finanțare pentru cercetările sale, iar IA era un termen mai academic și mai convingător decât cibernetica. În urma acestui demers a apărut domeniul emergent al IA, care este într-adevăr doar o continuare a mișcării ciberneticii care reprezenta începutul pentru ceea ce numim astăzi *machine learning* (învățare automată). Așadar, în acest sens IA poate fi împărțită clar în două domenii: IA simbolică tradițională și domeniul învățării automate/ inteligența computațională. În ceea ce privește IA simbolică, vom da exemplul lui Garry Kasparov, din 1997, când a fost învins la șah de Deep Blue de la IBM (Deep Blue poate fi considerat IA simbolică deoarece a reprezentat o formulă sau o codificare a tuturor cunoștințelor umane despre șah/ trebuie precizat faptul că, în cele din urmă, Deep Blue devenise limitat la ceea ce cunoșteau oamenii despre șah). Ulterior, a fost realizat saltul tehnologic și de prin anul 2010 apare la știri, aproape în fiecare zi, câte o informație privind domeniul învățării automate: în acest sens este elocvent exemplul programului de calculator AlphaGo, care învață din datele procesate și a ajuns să exceleze la jocul de societate Go, reușind să învingă chiar și jucători umani profesioniști. Concret, programul învață din datele procesate, identifică tipare pe care oamenii nu le-ar observa în mod normal și atinge performanțe remarcabile, dar îi lipsește explicabilitatea și are probleme în privința variațiilor algoritmilor de bază, fiind vorba de un fel de rețele neuronale.

Cum am putea totuși să definim IA? Unul dintre motivele pentru care acest domeniu este atât de contestat este și acela că îl redefinim continuu. Considerăm că cea mai simplă definiție pe care cei mai mulți dintre noi ajungem să o acceptăm este aceea că IA reprezintă sistemul care are capacitatea de a imita funcții umane, cum ar fi raționamentul, învățarea, planificarea și creativitatea. Cu toate acestea, rămân încă o serie de activități pe care pe care IA încă nu le poate face, prin comparație cu oamenii, însă această listă devine din ce în ce mai restrânsă odată cu trecerea timpului.

În același timp, continuăm să redefinim ceea ce înțelegem prin inteligență, raportându-ne la modul în care definim IA. Deci, este un alt mod de a spune că acesta este, în esență, un concept contestat, singurul lucru cert cu privire la definirea IA fiind acela că nu există o definiție general acceptată. Putem considera, astfel, că IA se referă la sistemele informatice capabile de a efectua sarcini complexe, pe care, tradițional, numai un om le-ar putea face, cum ar fi raționamentul, luarea deciziilor sau rezolvarea problemelor. În prezent, termenul „IA" descrie o gamă largă de tehnologii care facilitează multe dintre serviciile și bunurile pe care le folosim în fiecare zi; de aceea, este important să înțelegem că utilizând algoritmi special creați pentru antrenarea IA, componenta IA a unei aplicații este „învățată" să identifice modelele din seturile mari de date și, prin urmare, este dependentă de cantitatea și calitatea acestora[7].

IMPERATIVUL UTILIZĂRII IA ÎN DOMENIUL MILITAR

Utilizarea IA în domeniul apărării naționale poate contribui la sporirea eficienței și rapidității acțiunilor de securitate, precum și la identificarea și prevenirea mai eficientă a amenințărilor. Pe de altă parte, dezbaterea științifică despre utilizarea IA în scopuri militare, deși de o importanță strategică ridicată, pare să fie limitată în ceea ce privește domeniul său de aplicare și perspectiva. În plus, utilizarea științei datelor la nivel operațional și strategic pare să fie, în mare măsură, mai puțin examinată în literatura actuală[8].

Trebuie evidențiat că, în domeniul militar, IA poate fi utilizată în diverse moduri, de la întrebuințarea sa pentru strategii de apărare și atac în hacking și phishing până la vizarea sistemelor vitale în războiul cibernetic. În plus, sistemele bazate pe IA sunt sisteme de arme autonome, iar principalul avantaj îl reprezintă potențialul de a

se implica într-un conflict armat cu un risc redus de vătămare fizică a trupelor proprii[9].

Dr. Kaja Kowalczewska[10] este de părere că, la nivelul forțelor armate, IA poate fi folosită în două moduri: pentru a susține deciziile luate de comandanți sau ca entitate care ia decizii în mod autonom. Aceasta consideră primul mod ca fiind mai puțin controversat, deoarece IA este folosită astfel de ani de zile - există soft-uri care procesează datele oferite de sateliți, informațiile secrete, imaginile captate de sistemele de supraveghere etc., o problemă putând să apară în eventualitatea în care forțele armate vor decide să acorde libertate decizională acestor programe. Totodată, dr. Kowalczewska prezintă exemplul dronelor autonome care urmăresc și elimină ținta, omorând astfel o persoană. „Este știut faptul că atunci când un militar ia o decizie greșită, el poate fi tras la răspundere în fața tribunalului militar și/sau superiorul lui poate fi considerat responsabil. În cazul în care o mașinărie face o eroare, situația devine mai complexă, țara care a folosit dispozitivul ar trebui să răspundă. Dar cine, mai exact? Cumpărătorul, producătorul sau poate programatorul care a creat algoritmul defectuos?”[11].

În conformitate cu abordarea „pe cale de consecință” [12] în ceea ce privește etica folosirii IA în domeniul militar, în discuția despre tehnicile de suport decizional bazate pe IA ar trebui să fie luate în considerare eficacitatea militară și întregul lanț decizional în operațiile militare. De exemplu, anumite tipuri de roboți militari bazați pe IA, supuși controlului și judecății umane, ar putea fi acceptați în domeniul militar în scopuri de autoapărare, deoarece colaborarea între operatorul uman și IA ar putea duce la luarea deciziilor adecvate mai rapid, într-un context caracterizat de presiune și incertitudine, iar sistemele bazate pe IA ar putea fi utilizate pe scară largă pentru pregătirea adaptativă a personalului militar, contribuind astfel la reducerea erorilor de judecată sau ideilor preconcepute din procesul de luare a deciziilor militare (MDMP).

Procesul de luare a deciziilor militare constă în aplicarea unei metode logice iterative de planificare pentru a selecta cel mai bun curs de acțiune într-o anumită situație de pe câmpul de luptă și poate fi aplicat la toate nivelurile - strategic, operativ şi tactic. Fiecare pas în acest proces se pretează automatizării. Acest lucru nu se aplică doar la MDMP, ci și la procese conexe precum ciclul informațional și procesul de identificare a țintelor.

Armata SUA definește șapte pași în procesul de luare a deciziilor militare: (1) primirea misiunii, (2) analiza misiunii, (3) dezvoltarea cursului de acțiune (CoA), (4) analiza CoA, (5) compararea CoA, (6) aprobarea CoA și (7) producția comenzii, diseminarea și tranziția. Nivelul de detaliu al MDMP depinde de timpul și resursele disponibile, precum și de alți factori. Fiecare etapă în MDMP are numeroase sub-etape care generează produse intermediare. Exemple pot fi produsele de informații dezvoltate în timpul derulării procesului de pregătire informativă a câmpului de luptă (IPB), care sunt utilizate în dezvoltarea cursurilor de acțiune și indicarea punctelor de decizie, sau produselor geospațiale rezultate din analizele terenului, care pot include recomandări privind pozițiile de luptă și căile optime de abordare.

În Figura 3 putem vedea în ce constă dezbaterea actuală privind utilizarea IA în mod responsabil în context militar și punctele sale focale, iar în partea de jos a imaginii punctele slabe ale IA și punctul final al procesului militar de luare a deciziilor. Chenarul roșu reprezintă zona asupra căreia își concentrează efortul literatura de specialitate la momentul actual, în timp ce modul ideal de a realiza dezbaterea privind acest subiect este reprezentat în chenarul albastru.

Un alt exemplu privind întrebuințarea IA de armată este reprezentat de modul de utilizare al Clearview AI în conflictul din Ucraina, unde această tehnologie sprijină procesele de identificare a soldaților ruși, de noi ținte și interceptarea comunicațiilor inamice. Militari ruși care pretindeau că fac parte din armata ucraineană au fost deconspirați în doar câteva minute prin utilizarea Clearview AI și, mai mult decât atât, programul are capacitatea de a realiza

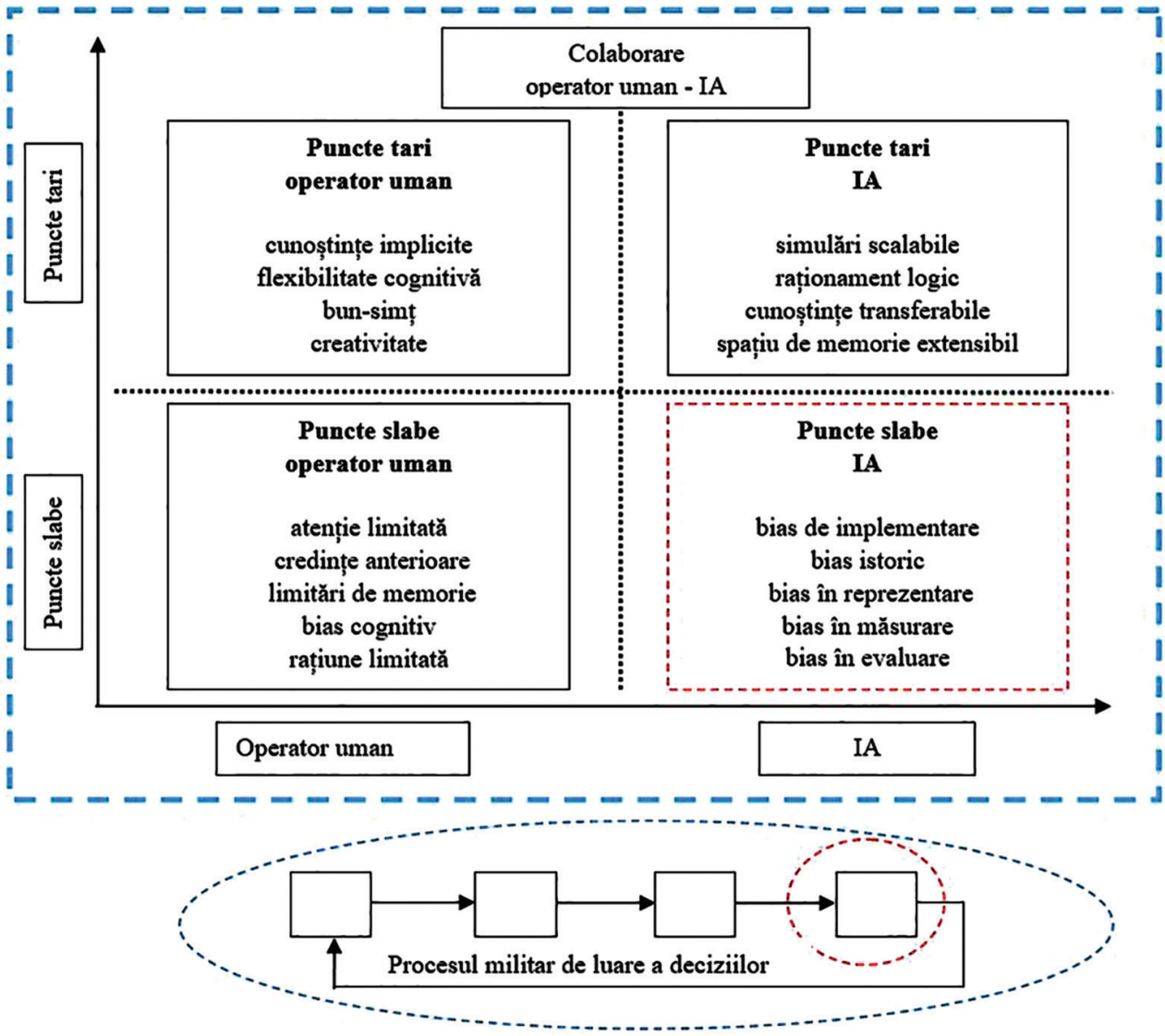


Figura 3: *Binomul operator uman-IA*

recunoașterea facială a cadavrelor afectate de leziuni grave, fiind de real ajutor în procesul de identificare a victimelor războiului. Tot în conflictul din Ucraina, CEO-ul Palantir, Alex Karp[13], a declarat că partea ucraineană utilizează MetaConstellation pentru monitorizarea țintelor și folosește datele colectate de sateliți comerciali, senzori de căldură și drone de recunoaștere, dar și din surse tradiționale (adică surse umane). Totodată, ultimul război Israel-Hamas reprezintă o oportunitate pentru armata israeliană de a întrebuința un sistem bazat pe IA, numit Habsora (Evanghelia), care a accelerat semnificativ procesul de identificare a țintelor. Practic, armata israeliană folosește produsele generate de IA pentru atacarea unor ținte, cum ar fi locuințele sau casele conspirative ale unor indivizi suspectați că ar fi membri ai grupărilor Hamas sau Jihadul Islamic.

Prin urmare, în ultimul deceniu, conflictul armat modern a cunoscut o mutație evidentă – de la războaiele din Afganistan și Irak, care pot fi apreciate ca fiind primele confruntări majore din era informaticii – la cele din Ucraina sau Fâșia Gaza. Ceea ce, nu demult, analiștii militari numeau conflictele inteligente ale viitorului reprezintă acum o realitate; din acest motiv, se poate aprecia că suntem în plină revoluție în domeniul militar, provocată de aplicarea unor noi tehnologii bazate și pe IA, iar acesta reprezintă doar începutul deoarece avansul tehnologic va influența decisiv mediul de securitate.

UTILIZAREA IA PENTRU REALIZAREA SECURITĂȚII NAȚIONALE

Securitatea națională reprezintă un concept extins care cuprinde toate aspectele legate de protejarea și promovarea intereselor și valorilor naționale. Importanța securității naționale constă în asigurarea stabilității, suveranității și prosperității statului, iar principalele obiective ale securității naționale includ protejarea teritoriului și a populației împotriva amenințărilor interne și externe, protejarea infrastructurii critice și promovarea stabilității sociale și economice.

Dar cum este întrebuințată efectiv IA pentru realizarea securității naționale, implicit în comunitatea de informații? Credem că este necesar ca, mai întâi, să luăm în considerare tehnologiile cognitive și, bineînțeles, conceptul de *Homo prospectus*[14]. Tehnologia cognitivă este un domeniu al informaticii care imită funcțiile creierului uman prin diferite mijloace, inclusiv prelucrarea limbajului natural, extragerea datelor și recunoașterea tiparelor. De altfel, unii specialiști apreciază că specia noastră este denumită greșit drept *Homo sapiens*. Deși *sapiens* definește ființele umane ca fiind „înțelepte”, de fapt ceea ce oamenii fac deosebit de bine este să anticipeze viitorul și să îl planifice; suntem, așadar, mai degrabă *Homo prospectus*. Asta seamănă foarte mult cu ceea ce se întâmplă în general, dar și în particular, în comunitatea de informații. Deci, orice activitate care extrage perspectivă sau previziune din date, trebuie să ne trimită imediat cu gândul la tehnologiile cognitive, care includ și sunt, în esență, IA, iar aceasta acoperă toate etapele ciclului informațional, care nu este altceva decât un set de procese utilizate pentru a furniza informații utile în procesul de luare a deciziilor.

Concret, un element esențial în activitatea specifică este acela al întrebuințării asset-ului potrivit la momentul oportun. Aceasta reprezintă o chestiune fundamentală: dacă un operator uman poate căuta sau analiza seturi de date semnificative, ceea ce poate face deja IA este să acționeze într-o măsură considerabil mai mare din punct de vedere matematic – poate consulta surse de informații mai ample, seturi de date vaste, dincolo de orice poate executa un operator uman și, în egală măsură, poate gândi într-o manieră recurentă dincolo de limitele umane. De aceea, putem spune despre tehnologiile cognitive că revoluționează procesul de luare a deciziilor.

Firesc, se pune întrebarea unde ar putea avea IA cea mai mare contribuție? Considerăm că aceste tehnologii pot contribui decisiv la analiza bazelor de date care conțin cantități mari de imagini și/sau capturi video colectate de diverse asset-uri, și chiar și la analiza de sunet/imagine, unde volumul datelor înregistrate însumează ani. Este evident că operatorii umani au fost complet depășiți de cantitatea de date care trebuie analizată, iar procesul pe care analiștii de imagini îl desfășoară este, în general, liniar; din această perspectivă, implementarea de sisteme bazate pe IA s-ar putea dovedi foarte utilă. Dat fiind faptul că am fost depășiți de mărimea seturilor de date pe care le căutăm și analizăm, inclusiv în intelligence, IA poate fi întrebuințată pentru procesarea datelor.

IA este capabilă să proceseze cantități uriașe de date pe care operatorii umani pur și simplu nu pot să le gestioneze într-un mod la fel de eficient și de rapid. Astfel, în anul 2010, IA aproape că nu exista nicăieri, în afara laboratoarelor, o diferență foarte mare față de starea actuală a lucrurilor. Apoi, fiecare descoperire majoră dintre anii 2012 și 2018 a venit cu creșterea puterii de calcul și implementarea învățării automate. De aceea, opinăm că este ușor să pierzi evidența a cât de repede a evoluat domeniul, deoarece numai între 2012 și 2018 a existat o creștere de 300.000 de ori a puterii de calcul. Pentru a sublinia mai clar despre cât de departe s-a ajuns, vom da un exemplu banal despre ce ar însemna o astfel de evoluție în privința tehnologiei acumulatorilor pentru telefoanele mobile: un telefon mobil ar putea funcționa opt ani cu o singură încărcare.

Întrebuințarea IA presupune folosirea unor sisteme dotate cu puteri de calcul uriașe la procesarea unor seturi de date vaste și, respectiv, adăugarea graduală a mai multor parametri pentru a obține performanțe supraomenești într-un anumit domeniu. IA poate automatiza colectarea și analiza unor volume mari de date, permițând

analiștilor de informații să proceseze informații mai eficient și să identifice modele sau anomalii care pot fi omise de operatorii umani. Algoritmii IA pot ajuta, de asemenea, la identificarea și prioritizarea surselor de informații relevante, ajutând analiștii să-și concentreze eforturile asupra informațiilor critice.

Ceea ce vedem acum sunt schimbări specifice fazei în care ne aflăm, astfel încât să obținem îmbunătățiri liniare ale performanței modelelor cu creșteri foarte mari ale puterii de calcul. Contextul tehnologic le dă de gândit specialiștilor, iar o parte dintre ei nu se grăbesc să numească aceste tehnologii ca „emergente", deoarece inteligența specifică creierului uman este emergentă. Așadar, speța este controversată, dar un lucru este cert: există lucruri pe care nu le-ai fi putut prezice că le va face modelul, dar ulterior a fost adăugată putere de calcul și, dintr-o dată, au apărut sisteme precum ChatGPT. Continuând cu acest exemplu, inițial ChatGPT prezenta foarte multe limitări, dar treptat a putut genera cu acuratețe întrebări și răspunsuri (deși anterior nu ne-am gândit că ar fi capabil să facă asta). Nu putea să facă aritmetică și apoi, dintr-o dată, a avut capacitatea de a face aritmetică. Nu putea traduce automatizarea procesării informațiilor și, deodată, a putut să o facă. Astfel, aceste schimbări de fază sunt motivele pentru care nu ar trebui să intrăm în dezbaterea amenințărilor existențiale, dar motivul pentru care cei mai mulți oameni sunt îngrijorați este generat de aceste capacități emergente ale sistemelor de IA. De exemplu, în decembrie 2022, Anthropic, companie de IA generativă, a publicat un document în care a dat opt exemple de schimbări de fază și lucruri pe care modelele puteau să le facă. Astfel, creșterile succesive ale puterii de calcul vor face ca viteza și costul antrenării modelelor să scadă. Se poate aprecia că ne putem aștepta să vedem, în continuare, o creștere a acestor tipuri de schimbări de fază, dar trebuie precizat că ne aflăm într-o eră a incertitudinii și este dificil de apreciat cu exactitate care vor fi evoluțiile viitoare cu privire la IA.

Dacă aducem în discuție acțiunea cinetică, lucrurile devin și mai complicate deoarece IA va rezolva algoritmii, va arunca bomba asupra unei ținte, dar nu e necesar oare să existe factorul uman care să ia în considerare și alte lucruri, precum dreptul internațional umanitar sau proporționalitatea răspunsului? Dezbaterea este dezirabilă și în termeni de bine sau rău, în termeni de obținere a unui avantaj militar concret prin folosirea IA: aceasta este partea poate cea mai complexă, cea în care comunitatea de intelligence discută dacă IA va fi lăsată singură să ia decizia sau doar va sprijini procesul de luare a deciziilor militare.

Există foarte multe limite ale prognozei umane și ale modului în care oamenii iau decizii. Un exemplu este acela al confabulației. În termeni medicali, confabulația este definită drept producerea spontană de amintiri false: mai exact, cel în cauză fie are amintiri despre evenimente sau situații care de fapt nu s-au petrecut niciodată în realitate, fie se luptă cu amintiri despre unele situații reale, dar nu mai știe când au avut loc evenimentele (timpul se estompează în memorie/ evenimente actuale se amestecă în creier cu evenimente care nu s-au întâmplat). Acest lucru poate face ca persoana să devină confuză sau chiar să pară că încearcă să influențeze realitatea. Ei bine, situații asemănătoare pot fi întâlnite și în cazul anumitor sisteme bazate pe IA, care atunci când nu știu ceva generează date false sau, cum mai spun unii specialiști, halucinează.

În prezent, IA poate fi utilizată în procesul de identificare a țintelor pentru a îmbunătăți acuratețea și eficacitatea analizei. Astfel, algoritmii de IA pot ajuta la identificarea potențialelor ținte analizând mai multe surse de date, cum ar fi imagini din satelit, fluxuri de rețele sociale și interceptări de comunicații, pentru a detecta modele sau activități suspecte. Acest lucru poate ajuta agențiile de informații să identifice și să urmărească potențialele amenințări mai eficient. Un alt exemplu privind procesul de identificare a țintelor: dacă am instala un sistem computerizat în interiorul unui vehicul blindat, care să găsească automat țintele în baza unor parametri pe care i-am stabilit în prealabil (de exemplu, un individ echipat într-o anumită uniformă, cu anumite caracteristici sau chiar

programarea IA ca să țină cont de anumite reguli de angajare și delegare a altor sarcini), modelul ne va spune întotdeauna cu precizie de ce a decis că acea entitate este o țintă; în schimb un militar aflat pe câmpul de luptă sub o presiune uriașă nu va putea întotdeauna să explice toate deciziile luate. Prin urmare, tot ce contează cu adevărat în aceste circumstanțe este că modelul are o rată de fals pozitiv și fals negativ mai mică decât cea a unui operator uman.

VALOAREA ADĂUGATĂ DE UTILIZAREA IA ÎN INTELLIGENCE

IA are potențialul de a influența semnificativ fiecare etapă a ciclului informațional, astfel:

- poate ajuta la identificarea automată a zonelor de interes și la stabilirea priorităților, prin analiza datelor istorice și a tendințelor actuale/ de asemenea, poate contribui la optimizarea alocării resurselor;
- tehnologiile IA pot fi utilizate pentru a colecta și a prelucra date dintr-o varietate de surse, inclusiv texte, imagini, audio și video (de exemplu, IA poate fi folosită pentru a transcrie convorbiri sau pentru a identifica obiecte în imagini);
- poate ajuta la filtrarea și la clasificarea datelor colectate, reducând astfel volumul de informații care trebuie analizate manual/ de asemenea, poate contribui la identificarea informațiilor relevante și la eliminarea zgomotului de fond;
- algoritmii de învățare automată pot fi utilizați pentru a identifica modele și tendințe în date, pentru a face predicții și pentru a genera rapoarte de intelligence și pot fi folosiți pentru a identifica legături între diferite seturi de date;
- poate ajuta la personalizarea și la livrarea produselor de intelligence către utilizatorii finali, în funcție de nevoile și de preferințele acestora/ poate contribui la securitatea transmisiunii datelor.

Constatăm că IA are potențialul de a revoluționa ciclul informațional, îmbunătățind eficiența și acuratețea proceselor de intelligence. Cu toate acestea, este important să se țină cont de provocările etice și de securitate asociate cu utilizarea IA în acest context.

În activitatea de Intelligence, un concept tot mai frecvent întrebuințat este cel de *Intelligence augmentat*, care, bineînțeles, include beneficiile IA. Să luăm în considerare analiza unui specialist IBM[15], care apreciază că din punct de vedere al informaţiilor de securitate s-a ajuns la nivelul la care finalitatea acestor tehnologii este aceea de a prelungi posibilităţile intelectului uman, de a le îmbunătăți și nicidecum de a le înlocui. Iată de ce noile sisteme cognitive vor asigura integrarea şi vor crea premisele pentru un parteneriat solid între oameni şi maşini, parteneriat care va facilita și o mai bună înţelegere a mediului securitar. Componentele IA precum machine learning-ul, vederea computerizată, procesarea limbajului natural sau automatizarea pot reprezenta instrumente importante pentru materializarea intențiilor statelor în domeniul informaţiilor de securitate[16].

Figura 4: *Imagine generata de IA*

Din moment ce ne aflăm în plin proces de schimbare a paradigmei, din perspectiva Intelligence-ului trebuie să ne punem întrebarea: am putea avea încredere în operatorul uman mai mult decât în IA sau invers? Există momente în care oamenii nu sunt la fel de atenți, la fel de logici, ca sistemele bazate pe IA. Apare implicit problema persoanelor care trebuie să lucreze cu sisteme bazate pe IA și nu au pregătirea și înțelegerea noțiunilor de bază. După ce informatizarea a fost considerată a fi o a doua alfabetizare, în mod asemănător lucrul cu IA poate fi considerat o a treia astfel de etapă de formare. Firește, este esențială specializarea forței de muncă pentru a utiliza în mod eficient

sistemele bazate pe IA și produsele generate de aceasta, pentru a perfecționa raționamentul uman. Fără această pregătire, de exemplu, analiștii ar putea avea dificultăți să interpreteze și să utilizeze rezultatele modelelor de IA, ceea ce poate duce la inferențe distorsionate care ar putea lipsi decidentul de perspective critice.

Să admitem, totuși, că integrarea IA în domeniul securității naționale necesită o schimbare de paradigmă în domeniul informațiilor și al profesiei militare, în care analiștii lucrează alături de modele de IA pentru a monitoriza și analiza date complexe. Din această perspectivă, având educația și formarea necesare, analiștii vor putea valorifica puterea IA pentru a-și îmbunătăți capacitățile analitice și a formula aprecieri mai consistente.

Există date puține pentru a fi în măsură să evaluăm situația, dar dacă aducem în discuție lecțiile învățate în teatrele de operații, unde factorii de decizie au fost uneori părtinitori în ceea ce privește luarea deciziilor pe baza produselor analitice realizate de operatorii umani, ne întrebăm dacă aceștia ar fi avut aceeași atitudine în situația în care produsele ar fi fost generate de IA. Apreciem că implementarea IA în domeniul apărării ar conduce la creșterea rigorii în procesul de luare a deciziilor militare, forțându-ne să fim expliciți în manifestarea intențiilor noastre, în logica, dovezile și datele în baza cărora luăm deciziile. Provocarea cea mai mare în calea schimbării de paradigmă și adoptării anumitor modele va fi aceea a acceptării faptului că activitatea umană este supusă erorilor, în schimb IA artificială poate oferi o acuratețe mai mare în executarea anumitor procese.

În plus, pe lângă lecțiile învățate în teatrele de operații, mai putem privi și către actori statali care sunt mai avansați în procesul de implementare a IA. De pildă, la nivelul Comunității de informații[17] a SUA a fost formulată, încă din anul 2019, o strategie[18] cu privire la întrebuințarea IA, în care directorul din acel an al Comunității (Dan Coats)[19] stabilea ca obiectiv prioritar pentru instituție reducerea decalajului dintre decizii și culegerea datelor și informațiilor. Dan Coats aprecia că ritmul în care datele sunt generate și colectate crește exponențial, iar personalul disponibil pentru a analiza și interpreta aceste date este limitat și, din acest motiv, implementarea IA poate contribui decisiv la îmbunătățirea capacității personalului de a-și îndeplini misiunile specifice. În plus, strategia propunea patru obiective principale: în primul rând, Comunitatea de informații trebuia să-și îmbunătățească înțelegerea privind tehnologiile AAA[20], inclusiv oferta civilă, programele guvernamentale în curs de execuție, dar și programele bazate pe IA desfășurate de adversari; în al doilea rând, pe termen scurt, Comunitatea de informații trebuia să identifice și folosească eficient resursele generate de sectoarele public și privat prin tranziția rapidă de la o capabilitate IA la alta; în al treilea rând, pe termen mediu, Comunitatea de informații își propunea realizarea și menținerea avantajului strategic prin dezvoltarea capabilităților IA, simultan cu dezvoltarea capacității de a întrebuința datele și informațiile obținute prin toate disciplinele de culegere; în final, pe termen lung, nu va fi suficientă integrarea datelor și informațiilor obținute prin mai multe discipline.

După cercetări realizate în domeniu, s-a constatat că vor trebui construite modele de lucru integrate de tipul binomului operator uman-IA. În acest context, opinăm că IA are un potențial ridicat de implementare în disciplinele tehnice de culegere de date și informaţii, inclusiv în OSINT, pentru a îmbunătăți culegerea, analiza și interpretarea informațiilor disponibile publicului. Algoritmii IA pot automatiza procesul de culegere a datelor din diverse surse online, cum ar fi platformele de social media, articolele de știri și site-urile web, permițând analiștilor să acceseze un volum mai mare de informații într-un timp mai scurt. Mai mult, IA poate ajuta la analiza datelor OSINT prin identificarea tiparelor, tendințelor și anomaliilor care pot fi relevante pentru analiza informațiilor.

Totodată, tehnicile de procesare a limbajului natural pot fi aplicate pentru a extrage informații cheie din sursele de text, în timp ce algoritmii de învățare automată pot fi utilizați pentru a clasifica și sorta datele. IA poate fi utilizată în OSINT pentru determinarea tiparelor de trafic, dincolo de

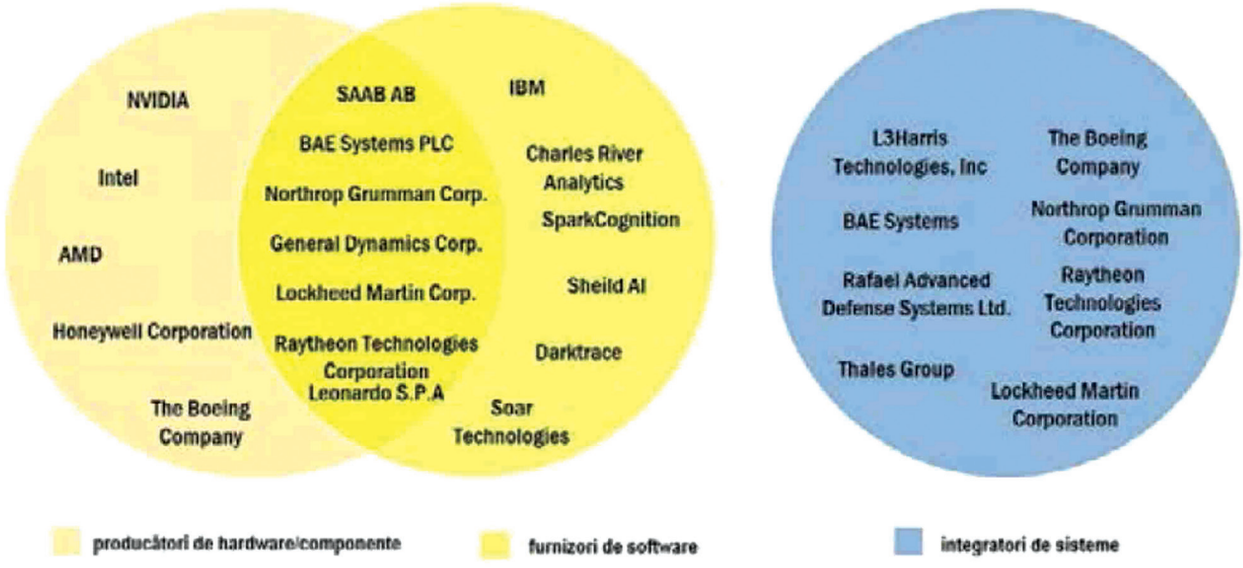


Figura 5: *Producători/furnizori/integratori*

posibilităţile reţelelor neurale, inclusiv în Deep Web. În acest sens, IA poate folosi „algoritmii genetici", care evoluează secvenţial, aşa cum evoluează organismele vii. De asemenea, nivelul Deep Learning, cunoscut şi sub numele de „învăţare ierarhică" sau „tehnică de învăţare profundă", poate fi utilizat pentru dezvoltarea de aplicaţii care, la rândul lor, au capacitatea de a executa sarcini complexe, precum recunoaşterea vorbirii sau filtrarea reţelelor de socializare, cu rezultate superioare celor obţinute de operatorii umani şi într-un timp mai scurt.

De asemenea, un studiu al *National Instruments*[21] aduce informaţii de interes în domeniul conceptelor de sisteme radio definite prin software[22] şi aplicarea acestor concepte în acţiunile SIGINT şi în activitatea mai largă de management al spectrului electromagnetic în câmpul tactic. Studiul arată că utilizarea IA și Deep Learning-ului pot reprezenta și un răspuns la creşterea exponenţială a complexităţii managementului spectrului electromagnetic în condiţiile acţiunii unor actori ostili asupra spaţiului de luptă definit de spectrul electromagnetic. Astfel, IA poate fi utilizată în SIGINT pentru supravegherea spațiului electromagnetic şi identificarea anomaliilor comportamentale, pentru a învăța caracteristicile comportamentale din spectrul electromagnetic.

În procesarea și analiza informațiilor, IA ar putea fi utilizată pentru recunoașterea vocii, aspect care le-ar permite analiștilor să formuleze produse analitice mai complete, deoarece această capabilitate le-ar clarifica aspecte precum tipul dialectului folosit sau ar permite chiar identificarea unor persoane și/sau particularități regionale, coroborarea de informații și chiar identificarea unor tipare anormale. Tot programe specializate, bazate pe IA, ar putea sprijini analiștii să interogheze baze de date care au un volum mare de informații. Cu toate acestea, foarte puține structuri de intelligence folosesc IA la potențialul actual al tehnologiei.

Potrivit analizei realizate de compania *Research and markets*, piața de soluții bazate pe IA pentru apărare a fost evaluată la 6,9 miliarde dolari în 2022 și este de așteptat să ajungă la 13,2 miliarde dolari până în 2028. Astfel, se așteaptă să înregistreze o rată de creștere anuală compusă de 11,7% din 2023 până în 2028. Pe de altă parte, *Markets and markets* a evaluat aceeași piață la 4,6 miliarde dolari în 2022, la 9,2 miliarde dolari în 2023 și se așteaptă să înregistreze o rată de creștere anuală compusă de 33,3% până în 2028, astfel încât să ajungă la 38,8 miliarde dolari.

Apreciem că, deși există foarte multe modele spre care beneficiarii se pot îndrepta, sunt mai multe bariere în calea adoptării IA la scară largă. Aproape instinctiv presupunem, de cele mai multe ori, că procesul luării deciziilor umane este superior, dar în același timp realizăm că, de fapt, acest proces este unul viciat de diverși factori.

Există în natura umană o tendință de a se opune la tot ceea ce este nou, de a privi cu neîncredere ceea ce nu se cunoaște îndeajuns, este vorba despre rezistența la schimbare. În aceste condiții ar trebui să ne preocupe, în special, care ar fi principalele avantaje care decurg din implementarea IA, precum identificarea rapidă a amenințărilor și/sau riscurilor și, implicit, identificarea celor mai bune soluții pentru eliminarea vulnerabilităților.

Competitorii strategici, cum ar fi China și Rusia, fac investiții semnificative în IA destinată apărării. De asemenea, Departamentul Apărării al SUA alocă miliarde de dolari pentru a dezvolta și a integra IA în sistemele de apărare. Încă din 2011, China a vorbit despre *„războiul inteligent”,* deci despre tranziția de la ideea de război informațional la cea de război inteligent. Deși preocuparea multor grupuri a fost dezbaterea privind delegarea anumitor sarcini IA sau etica întrebuințării IA, în alte state, unde sistemul poate fi caracterizat ca fiind centralizat (precum China), procesul de centralizare a datelor și informațiilor necesare antrenării IA este mai facil.

Necunoașterea modului de întrebuințare și de interpretare a datelor în sensul doctrinar reprezintă una dintre cele mai mari limitări în adoptarea IA pentru exploatarea surselor deschise și a altor surse de informații. Poate că ar trebui să învățăm încă din școală, odată cu alfabetizarea, o serie de elemente legate de modul în care privim informațiile care vin spre noi, iar proiectul ar putea fi unul generațional. Uneori, decidenții nu au cultura de intelligence adecvată, iar în ceea ce privește comunitatea de informații, așteptările sunt foarte mari, de exemplu în calitate de analist trebuie să explici cum ai ajuns la o serie de concluzii care, cel mai probabil, vor fi privite cu reticență. Și, din aceste motive, trebuie să conștientizăm faptul că IA poate aduce îmbunătățiri semnificative în ciclul informațional prin:

- realizarea unor analize îmbunătățite: algoritmii de învățare automată pot identifica modele și tendințe în date care ar putea fi trecute cu vederea de analiștii umani/ aceasta poate duce la o mai bună înțelegere a situației și la formularea de previziuni sau prognoze mai precise;
- particularizarea produselor: IA poate ajuta la personalizarea produselor de intelligence pentru diferiți utilizatori, în funcție de nevoile și preferințele lor specifice;
- asigurarea unei securități îmbunătățite: tehnologiile IA pot fi utilizate pentru a detecta și a preveni amenințările la adresa securității, cum ar fi atacurile cibernetice;
- asigurarea învățării continue: sistemele bazate pe IA pot învăța și se pot adapta în mod continuu, ceea ce le permite să se îmbunătățească în timp și să răspundă mai bine la noi provocări și situații.

Cu toate acestea, este imperativ să se țină cont de provocările etice și de securitate asociate cu utilizarea IA în acest context. De asemenea, este esențial să se asigure că IA este utilizată într-un mod care respectă drepturile și libertățile individuale. De aceea, opinăm că, pentru moment, utilizarea binomului operator uman - IA reprezintă varianta optimă de întrebuințare a acestor tehnologii în intelligence. Procesul de înțelegere a informațiilor prin întrebuințarea binomului operator uman-IA se conturează, de asemenea, și pentru viitorul disciplinelor precum analiza de informații și planificarea misiunilor, în care fuziunea de date facilitată de IA, detectarea de modele și anomalii și suportul pentru cercetare și analiză ajută analiștii să gestioneze și să exploateze volumul uriaș de surse și seturi de date disponibile. Activități care ar dura zile, dacă ar fi executate de către operatori umani, pot fi acum realizate în ore, permițând acestora să se concentreze pe cele mai relevante informații obținute din seturile de date mari.

De exemplu, în războiul din Ucraina, forțele armate ucrainene folosesc deja instrumente de procesare a limbajului natural care utilizează IA pentru a traduce și analiza comunicațiile interceptate din limba rusă, economisind timpul analiștilor umani și permițându-le să se concentreze pe mesajele cheie și informațiile deținute[23]. Utilizarea IA nu numai că accelerează analiza, dar demonstrează și valoare adăugată aducând la cunoștința analistului conexiuni observate, dar ignorate sau uitate, insight-uri

și informații, articulând valoarea sau calitatea informațiilor pentru luarea deciziilor umane[24].

În ianuarie 2023, Agenția pentru Cercetări Avansate în Intelligence (IARPA), aflată în subordinea Biroului Directorului Informațiilor Naționale din SUA, a anunțat un program cunoscut sub numele de REASON[25]. Programul presupune implementarea unor soluții software care întrebuințează IA pentru a îmbunătăți produsele analitice realizate de operatori umani. Software-ul revizuiește rapoartele întocmite de oameni și generează automat recomandări pentru surse suplimentare pe care expertul s-ar putea să nu le cunoască (sau să nu le fi folosit) și oferă, de asemenea, sugestii despre cum să îmbunătățească calitatea produsului analitic, îndeplinind rolul unui recenzor autonom al adversarului (Red Team). Acest program reprezintă un pas în direcția corectă, demonstrând una dintre multele modalități în care IA poate ajuta oamenii să facă conexiuni între date și surse și să îmbunătățească analiza și procesul de luare a deciziilor.

Având în vedere limitările umane în ceea ce privește luarea deciziilor, avantajul automatizării (parțiale) cu IA poate fi găsit atât în dimensiunea temporală, cât și în calitatea deciziei. De exemplu, un grup de lucru de cercetare al NATO[27] a documentat nevoia de automatizare în fiecare etapă al ciclului informațional și a constatat că IA ajută la automatizarea sarcinilor manuale, identificarea modelelor în seturile de date complexe și accelerarea procesului de luare a deciziilor. Deoarece colectarea mai multor informații și perspective duce la produse de informații mai puțin părtinitoare, amplificarea puterii de calcul duce la creșterea cantității de date care pot fi procesate și analizate, iar aceasta poate reduce într-o foarte mare măsură biasul cognitiv.

Totodată, NATO Communications and Information Agency (NCIA) a reușit acreditarea de securitate a unui mediu de calcul de înaltă performanță destinat științei datelor și IA. Astfel, The Data Science and AI Sandbox/ SANDI oferă un spațiu sigur pentru dezvoltarea și testarea instrumentelor IA, permite specialiștilor să lucreze cu seturile uriașe de date necesare pentru a dezvolta modele IA și oferă puterea de calcul pentru a antrena, cu viteză, aceste modele.

Din perspectiva implementării pe termen scurt a IA în structurile de intelligence naționale, o provocare o reprezintă tocmai nevoia unui mediu clasificat în care big data pot fi procesate și modelele IA pot fi antrenate, optimizate și validate, iar până la dezvoltarea unor soluții autohtone adaptate, rezolvarea acestei situații poate fi aceea a achiziționării unor sisteme de intelligence, bazate pe IA, specializate în exploatarea volumelor mari de date (procese automatizate pentru realizarea culegerii datelor, manipulării acestora, procesării, exploatării, analizei, producției și alertării) care să poată integra informații din domenii multiple.

PROVOCĂRI ETICE ASOCIATE CU UTILIZAREA IA ÎN INTELLIGENCE

Utilizarea IA în Intelligence ridică mai multe provocări etice importante, printre care transparența și responsabilitatea algoritmilor IA, fiind esențial să înțelegem cum iau deciziile acești algoritmi, și să ne asigurăm că acestea sunt nediscriminatorii și etice. Dintr-o perspectivă mai generală, o altă provocare o reprezintă asimetria de putere dintre cei care utilizează tehnologiile bazate pe IA și cei vizați de ele; de aceea, este imperativ ca utilizarea de instrumente bazate pe IA de către organele de specialitate ale administrației publice centrale sau locale care sunt parte din sistemul de apărare, ordine publică și siguranță națională sau desfășoară activități conexe și autoritățile care au competențe judiciare să nu devină un factor de inegalitate, fragmentare socială sau excluziune. Totodată, există riscul ca utilizarea instrumentelor bazate pe IA să aibă un impact asupra drepturilor la apărare ale persoanelor fizice și juridice, din cauza dificultății de a obține informații pertinente cu privire la funcționarea acestora și, în consecință, dificultatea de a contesta rezultatele lor în instanță.

În acest sens, încă din 2020, Departamentul Apărării al SUA a adoptat, în mod oficial, cinci principii pentru dezvoltarea etică a capabilităților de IA, după ce în prealabil membrii Comitetului

pentru inovare în domeniul apărării, timp de aproximativ 15 luni, au consultat experți în IA, ingineri, actuali și foști lideri ai DoD și simpli cetățeni, iar în urma acestui proces au dezvoltat principii care au aplicabilitate în întrebuințarea capabilităților bazate pe IA atât la pace, cât și în situații de luptă. În context, Centrul Întrunit pentru IA al DoD este instituția care a primit misiunea de a exercita funcția de coordonare a implementării principiilor etice în IA. Cele cinci principii etice ale IA, adoptate în domeniul apărării de către aliatul strategic al României, sunt:

- responsabilitatea - personalul DoD va aborda cu precauție dezvoltarea, implementarea și utilizarea capabilităților bazate pe IA, menținând în același timp o atitudine responsabilă;
- echitabilitatea - DoD va adopta o serie de măsuri menite să reducă/elimine eventualele idei preconcepute legate de capabilitățile IA;
- trasabilitatea - înțelegerea adecvată a tehnologiei, proceselor de dezvoltare și metodelor operaționale aplicabile capabilităților bazate pe IA, inclusiv prin întrebuințarea unor metodologii transparente și auditabile, a surselor de date și procedurilor de proiectare și documentației specifice;
- grad de încredere - capabilitățile bazate pe IA ale DoD vor face obiectul testării pe parcursul întregului ciclu de viață pentru asigurarea utilizărilor predefinite;
- guvernabilitatea - DoD va proiecta capabilitățile bazate pe IA pentru a-și îndeplini funcțiile predefinite, având în același timp capacitatea de a identifica și evita consecințele neintenționate, respectiv capacitatea de a dezangaja sau dezactiva sistemele care manifestă un comportament neintenționat.

Ulterior, în anul 2021, în baza angajamentelor etice, juridice și politice existente și în temeiul cărora NATO a funcționat și va continua să opereze în mod istoric, Alianța a formulat *Principiile NATO de utilizare responsabilă a IA* în domeniul apărării[28]. Aliații și-au luat angajamentul că se vor asigura că aplicațiile bazate pe IA pe care le dezvoltă și pe care le vor întrebuința vor respecta, în toate etapele ciclului lor de viață, următoarele șase principii:

1) legalitate: aplicațiile bazate pe IA vor fi dezvoltate și utilizate în conformitate cu legislația națională și internațională, inclusiv dreptul internațional umanitar și drepturile omului, după caz;
2) responsabilitate și răspundere: aplicațiile IA vor fi dezvoltate și utilizate cu precauție și responsabilitate umană;
3) explicabilitate și trasabilitate: aplicațiile IA vor fi dezvoltate transparent astfel încât să fie înțelese în mod corespunzător de personalul implicat, inclusiv prin utilizarea metodologiilor, surselor și procedurilor de revizuire/ aceasta include mecanisme de verificare, evaluare și validare fie la nivel NATO, fie la nivel național;
4) grad de încredere: aplicațiile IA vor avea utilizări explicite și bine definite – în vederea menținerii siguranței, securității și robusteții, aceste capabilități vor face obiectul testării periodice, prin procedurile NATO și/sau naționale de certificare prestabilite;
5) guvernabilitate: aplicațiile IA vor fi dezvoltate și utilizate în conformitate cu funcțiile predefinite și vor permite interacțiunea adecvată om-mașină, capacitatea de a detecta și de a evita consecințele nedorite și capacitatea de a lua măsuri, cum ar fi dezangajarea sau dezactivarea sistemelor bazate pe IA, atunci când astfel de sisteme demonstrează un comportament neintenționat;
6) combaterea eventualelor idei preconcepute: se vor lua măsuri proactive pentru a reduce acest tip de idei în dezvoltarea și utilizarea aplicațiilor bazate pe IA și în seturile de date folosite.

CONCLUZII

Provocările amintite anterior subliniază importanța realizării unor dezbateri privind etica în domeniul IA și necesitatea efectuării unor analize riguroase și echilibrate care să încurajeze reflecția și dezbaterea în acest domeniu în continuă expansiune.

Așadar, IA este deja în curs de schimbare a societății într-un ritm rapid și are potențialul de a aduce numeroase schimbări pozitive în societate, inclusiv îmbunătățirea productivității, îmbunătățirea serviciilor medicale și creșterea accesului la educație. IA schimbă inclusiv mediul global de securitate și domeniul apărării, oferind NATO o oportunitate fără precedent de a-și consolida avansul tehnologic, dar creează premisele creșterii vitezei de propagare a amenințărilor cu care ne confruntăm. Această tehnologie de bază va afecta probabil întregul spectru de activități întreprinse de Alianță în sprijinul celor trei sarcini fundamentale ale organizației, definite în Conceptul Strategic al NATO: apărarea colectivă, gestionarea crizelor și securitatea prin cooperare. În acest context, utilizarea IA în sprijinul securității naționale ar putea aduce beneficii semnificative, cum ar fi creșterea capacității de analiză și prevenire a amenințărilor, îmbunătățirea securității cibernetice și sprijinirea luării deciziilor strategice.

Sistemele bazate pe IA pot analiza volume mari de date rapid și precis, sprijinind serviciile de informații să adune și să proceseze informații mai eficient, algoritmii IA pot identifica modele și tendințe în datele analizate, permițând analiștilor să detecteze potențiale amenințări sau conexiuni ascunse. În plus, IA poate fi folosită pentru a transcrie și analiza înregistrări audio sau pentru a identifica obiecte și persoane în imagini, sprijinind eforturile de supraveghere, investigare sau documentare.

Totodată, sistemele bazate pe IA pot înțelege și extrage informații din texte nestructurate, cum ar fi postările de pe rețelele sociale, ajutând la identificarea și analizarea aspectelor relevante. De asemenea, pot fi analizate și datele mai vechi, iar pe baza lor se pot face predicții despre evenimente viitoare, permițând serviciilor de informații să anticipeze și să prevină potențialele amenințări. De asemenea, algoritmii IA pot ajuta la detectarea amenințărilor cibernetice, analizând traficul de rețea și identificând comportamentul anormal care ar putea indica un atac cibernetic, iar în final sistemele IA pot oferi operatorilor recomandări și perspective, ajutându-i să ia decizii mai informate. Utilizarea IA poate aduce beneficii semnificative în ceea ce privește prevenirea și contracararea activităților ilegale. Prin implementarea sistemelor inteligente de supraveghere și analiză a datelor, se pot identifica acele modele suspecte și comportamente anormale, în timp real, permițând totodată intervenția promptă și eficientă.

Mai mult decât atât, IA poate spori capacitatea structurilor de analiză de a gestiona cantități mari de informații. Cu ajutorul algoritmilor avansați, se pot analiza și interpreta datele culese din surse multiple, facilitând o înțelegere mai profundă și oferind, totodată, o paletă exhaustivă de soluții asupra potențialelor amenințări cibernetice. Astfel, pot fi luate decizii mai informate, chiar de nivel strategic, pentru a contracara diverse atacuri și a asigura securitatea țării. Totuși, este necesar să ținem cont de limitările IA. Deși tehnologia avansează rapid, există încă provocări în ceea ce privește înțelegerea contextului și interpretarea semnificației profunde a datelor. Acest aspect poate duce la erori sau la interpretări greșite ale informațiilor, ceea ce poate afecta negativ deciziile luate în domeniul securității naționale.

În opinia noastră, IA reprezintă o tehnologie emergentă și disruptivă, care cunoaște o dezvoltare rapidă, cu potențial de adoptare pe scară largă, care datorită creșterilor exponențiale va ajunge la maturitate până în 2030 și care va avea un impact semnificativ asupra securității globale. De aceea, pentru a profita la maximum de potențialul IA în domeniul securității naționale, este esențial să fie angajați experți în domeniu și să fie dezvoltată o abordare multidisciplinară. Cooperarea între specialiștii în securitate cibernetică, analiștii de date și profesioniștii din domeniul IA este vitală pentru a găsi cele mai bune soluții inovatoare. Doar prin colaborare și eforturi comune se poate utiliza IA în mod eficient astfel încât să fie asigurată securitatea națională în fața amenințărilor în continuă evoluție.

Iată de ce este important de reținut că utilizarea IA în intelligence ar trebui gestionată

cu atenție, elemente precum acuratețea, transparența, părtinirea și confidențialitatea fiind esențiale. În acest sens, considerațiile etice și supravegherea umană sunt cruciale pentru a asigura utilizarea responsabilă și eficientă a IA în activitățile specifice de intelligence, iar binomul operator uman-IA oferă multiple avantaje pentru armatele secolului XXI. Ca atare, instituțiile care sunt parte din sistemul de apărare, ordine publică și siguranță națională trebuie să investească suficient timp și resurse pentru a aborda provocările adoptării tehnologiilor discutate mai sus.

În concluzie, utilizarea IA în sprijinul securității naționale aduce o serie de oportunități și provocări, iar prin înțelegerea clară a tehnologiei și a implicațiilor utilizării ei, se poate valorifica din plin potențialul acesteia și, implicit, contracara amenințările într-un mod mai eficient și mai eficace.

BIBLIOGRAFIE

1. KNIGHT Will, ”As Russia Plots Its Next Move, an AI Listens to the Chatter”, *Wired.com*, 4 aprilie 2022; https://www.wired.com/story/russia-ukraine-war-ai-surveillance.
2. KOWALCZEWSKA Kaja, *Inteligența artificială în război. Perspectiva dreptului internațional umanitar cu privire la conflictele armate* (în limba poloneză), Editura științifică Scholar, Varșovia, 2021.
3. MEERVELD Herwin, LINDELAUF Roy, *Data Science in Military Decision-Making: A Literature Review*, în Social Science Research Network, Ianuarie 2022.
4. MEERVELD Herwin, LINDELAUF Roy, ”Data Science in Military Decision-Making: Foci and Gaps”, în *Global Society*, iunie 2024, la adresa tandfonline.com/doi/epdf/10.1080/13600826.2024.2353657.
5. NORA Dominique, „Alex Karp, PDG de Palantir: <Les Ukrainiens utilisent notre logiciel contre l`armée russe>”, *NouvelObs.com.,* 13.03.2023; https://www.nouvelobs.com/economie/20230313.OBS70724/alex-karp-pdg-de-palantir-les-ukrainiens-utilisent-notre-logiciel-contre-l-armee-russe.html.
6. RICHEY K. Melonie, ”From Crowds to Crystal Balls: Hybrid Analytic Methods for Anticipatory Intelligence”, în *American Intelligence Journal*, vol. 32, nr. 1, 2015, p. 146-151.
7. VINCENT Brandi, ”IARPA to develop novel AI that automatically generates tips to improve intel reports”, în *FedScoop*, ianuarie 2023, la adresa fedscoop.com/iarpa-to-develop-novel-ai-that- automatically-generates-tips-to-improve- intel- reports/
8. van WEELDEN Evy, ALIMARDANI Maryam, WILTSHIRE J. Travis, LOUWERSE M. Max, ”Aviation and neurophysiology: a systematic review”, în *Applied Ergonomics. Human Factors in Technology and Society*, vol. 105, noiembrie 2022, la adresa sciencedirect.com/science/article/pii/S0003687022001612.

[1] https://www.europarl.europa.eu/news/ro/headlines/society/20210414STO02010/transformarea-digitala-importanta-avantaje-si-politici-ue, accesat la 13.01.2025.

[2] https://www.europarl.europa.eu/news/ro/headlines/society/20230601STO93804/legea-ue-privind-ia-prima-reglementare-a-inteligentei-artificiale, accesat la 13.01.2025.

[3] Un zetabit reprezintă o mie de miliarde de gigabiți.

[4] https://www.europarl.europa.eu/news/ro/headlines/society/20200918STO87404/inteligenta-artificiala-oportunitati-si-pericole, accesat la 13.01.2025.

[5] https://eurlex.europa.eu/legalcontent/RO/TXT/?pk_keyword=DigitalEU&pk_content=Decision&pk_campaign=todays_OJ&pk_cid=EURLEX_todaysOJ&uri=OJ%3AC_202401459&pk_source=EURLEX&pk_medium=TW, accesat la 08.02.2024.

[6] https://www.consilium.europa.eu/en/your-online-life-and-the-eu/#group-section-trustworthy-AI-tBusxga6wd, accesat la 14.01.2025.

[7] Eric Nyberg, Foundations of Computational Data Science, prelegere la Universitatea Carnegie Mellon, Pittsburgh, PA, 2020< https://mcds.cs.cmu.edu/11-637-foundations-computational-data-science, accesat la 14.01.2025.

[8] Herwin Meerveld, Roy Lindelauf, Știința datelor în procesul de luare a deciziilor militare: o revizuire a literaturii. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id= 4217447, accesat la 14.01.2025.

[9] David Sculley, Gary Holt, Daniel Golovin, Eugene Davidov, Todd Phillips, Dietmar Ebner, Vinay Chaudhary, Michael Young, Jean-Francois Crespo, Dan Dennison, "Hidden Technical Debt in Machine Learning Systems", în deschiderea celei de-a 28-a conferințe internaționale privind evoluțiile în domeniul sistemelor neuronale de procesare a informațiilor, 2015; http://papers.nips.cc/paper/5656-hid¬den-technical-debt-in-machine-learning-systems.pdf., accesat la 14.01.2025.

[10] Avocat la Universitatea din Wrocław, doctor în drept internațional și tehnologii disruptive și autoare a volumului *Inteligența artificială în război. Perspectiva dreptului internațional umanitar cu privire la conflictele armate (2021).*

[11] *** „Inteligența artificială în războiul din Ucraina – IA salvează sau scurtează vieți și stârnește controverse", 07.07.2023; https://www.veridica.ro/analize/inteligenta-artificiala-in-razboiul-din-ucraina-ia-salveaza-sau-scurteaza-vieti-si-starneste-controverse, accesat la 15.01.2025.

[12] Evy van Weelden, Maryam Alimardani, Travis J.Wiltshire, Max M. Louwerse, "Aviation and neurophysiology: A systematic review", în *Applied Ergonomics. Human Factors in Technology and Society,* vol. 105, noiembrie 2022, p. 105; https://doi.org/10.1016/j.apergo.2022.103838, accesat la 15.01.2025.

[13] Dominique Nora, „Alex Karp, PDG de Palantir: <Les Ukrainiens utilisent notre logiciel contre l`armée russe>", *NouvelObs.com.,* 13.03.2023; https://www.nouvelobs.com/economie/20230313.OBS70724/alex-karp-pdg-de-palantir-les-ukrainiens-utilisent-notre-logiciel-contre-l-armee-russe.html, accesat la 15.01.2025.

[14] Carte scrisă de Martin E. P. Seligman, Peter Railton, Roy F. Baumeister și Chandra Sripada, care susțin că anticiparea și evaluarea posibilităților viitoare pentru îndrumarea gândirii și acțiunii reprezintă piatra de temelie a succesului uman.

[15] IBM - acronim din engleză de la International Business Machines, este o corporație americană producătoare de tehnologie avansată.

[16] https://www.ibm.com/industries/government/defense-intelligence, accesat la 15.01.2025.

[17] Comunitatea de informații a SUA este alcătuită din 16 agenții guvernamentale federale, servicii, departamente sau organizații din cadrul executivului american, care desfășoară activități informative în vederea asigurării securității naționale a SUA.

[18] https://www.dni.gov/files/ODNI/documents/AIM-Strategy.pdf, accesat la 16.01.2025.

[19] Directorul Comunității de Informații a SUA.

[20] Artificial intelligence, process automation, and IC officer augmentation.

[21] https://www.b2b-knowhow.com/assets/4215-artificial-intelligence-in-software-defined-sigint-systems, accesat la 16.01.2025.

[22] SDR - Software Defined Radios

[23] Will Knight, "As Russia Plots Its Next Move, an AI Listens to the Chatter", *Wired.com,* 4 aprilie 2022; https://www.wired.com/story/russia-ukraine-war-ai-surveillance/, accesat la 16.01.2025.

[24] Interviu telefonic cu Harry Kemsley, vicepreședinte Janes, 2023; https://www.janes.com/intelligence-resources/open-source-intelligence-podcasts/podcast-details/review-of-2023, accesat la 16.01.2025.

[25] Explicare Rapidă, Analiză și Sursă Online.

[26] Brandi Vincent, "IARPA to develop novel AI that automatically generates tips to improve intel reports", în *FedScoop,* ianuarie 2023, la adresa fedscoop.com/iarpa-to-develop-novel-ai-that- automatically-generates-tips-to-improve- intel-reports/; a se vedea și date despre programul IARPA, https://www.iarpa.gov/research-programs/reason, accesate la 16.01.2025.

[27] Organizația pentru știință și tehnologie a NATO, Automatizarea în ciclul informațional, 2020. URL: https://www.sto.nato.int/Lists/STONewsArchive/displaynewsitem.aspx?ID=552, accesat la 16.01.2025.

[28] https://www.nato.int/cps/en/natohq/official_texts_187617.htm, accesat la 16.01.2025.

ANALIZA STRATEGICĂ - O ABORDARE SINTETICĂ

Octavian VOICU*

Abstract

This article provides an approach to the term "strategic analysis" in the field of intelligence analysis, trying to capture some defining details of the term as understood by various authors in the field, as well as certain specific aspects of this type of analysis. The aim of strategic analysis is to provide beneficiaries with an overview that highlights relevant aspects impacting their decisions and, additionally, to create a representation of significant events that may affect the organization, aiming to prevent strategic surprises. The following section present aspects related to the preparation, content and language of strategic intelligence products. Finally, some benefits of strategic analysis are highlighted, and the conclusions review the specific details that enable strategic analysis to stand out through the potential advantages it can offer to the recipients of such analytical products.

Keywords: *strategic analysis; tactical analysis; operational analysis; data; information; intelligence; decisions; intelligence products.*

ASPECTE DE NATURĂ CONCEPTUALĂ

Analiza strategică reprezintă procesul prin care se dezvoltă cunoștințe cu ajutorul datelor/ informațiilor avute la dispoziție, pentru a facilita înțelegerea unor activități, comportamente și medii de interes[1]. Dintr-o altă perspectivă, analiza strategică este considerată o abordare multisectorială și multisursă a fenomenelor cu impact major în sfera securității naționale (în plan politico-militar, economic, social), cu o consistentă dimensiune predictiv-anticipativă[2]. O altă abordare surprinde faptul că acest tip de analiză (destinată securității naționale) vizează fenomene, manifestări sau acțiuni cu potențial impact major în domeniul securității, iar concluziile sale fundamentează decizia de nivel strategic și sprijină managementul integrat în situații complexe[3]. De asemenea, analiza strategică reprezintă sinteza informaţiilor obţinute din surse secrete umane/ tehnice şi/sau surse deschise cu relevanţă pentru persoanele cu drept de decizie în stat, cu atribuţii în stabilirea şi implementarea obiectivelor naţionale majore[4].

Conform accepţiunilor curente, analiza strategică este utilizată în domenii diverse, inclusiv în strategia militară, securitatea națională și *intelligence*-ul afacerilor. La nivelul strategiei militare, aceasta are rolul de a sprijini din punct de vedere informativ procesul de luare a deciziilor și ajută liderii militari să înțeleagă atât mediul operațional, cât și amenințările viitoare. În ceea ce privește zona de afaceri, analiza strategică sprijină conducerea/ liderii organizațiilor să înțeleagă mediul competitiv în care își desfășoară activitatea și să adopte decizii strategice fundamentate.

Autorul este expert în cadrul Ministerului Apărării Naționale.

LOCUL ȘI ROLUL ANALIZEI STRATEGICE

Pentru a evidenţia locul pe care îl ocupă analiza strategică este important de evidențiat locul acesteia faţă de alte tipuri de analiză de *intelligence*. Abordările din domeniu menţionează, în cadrul analizei de *intelligence*, trei niveluri la care se derulează procesul analitic:

- *analiza operativă* – se referă în principal la analiza operațiilor curente, având o abordare a problematicii pe termen scurt;
- *analiza tactică* – preocupată de studiul de fenomen, direcție de acțiune, latură specifică etc., având o abordare pe termen scurt și mediu, în funcție de cerințele desemnate ca responsabilități;
- *analiza strategică* – abordează direcțiile principale de acțiune, prezentate în termeni larg definiți, pe termen lung, care nu intenționează să releve date sau obiective exacte.

Nivelurile tipurilor de analiză

În mod concret, analiza strategică are nevoie să fie conectată cu cea operativă și tactică prin prisma includerii informațiilor semnificative din cadrul acestora în tabloul strategic care face obiectul informării factorilor de decizie.

Analiza strategică vizează două dimensiuni și anume cea temporală și cea spațială. Din punct de vedere temporal, aceasta se axează pe aspectele cu impact pe termen mediu sau lung, iar din punct de vedere spațial are în vedere evenimentele care au efect asupra unui spațiu întins de tipul național, regional, internațional. Totodată, din punct de vedere al finalității, analiza de nivel strategic furnizează produse destinate nivelului superior de management al organizației și conține informații și evaluări care pot avea impact asupra organizației. Un obiectiv principal al analizei strategice este *evitarea surprinderii strategice:* mai specific, prin informările către management se fac evaluări/ prognoze asupra evenimentelor cu posibil impact major asupra organizaţiei/ societăţii. În acest mod, organizaţia poate planifica şi adopta măsuri preventive în scopul adaptării la condiţiile preconizate într-un orizont de timp specificat.

În vederea realizării de materiale de analiză strategică analiștii au în vedere permanent monitorizarea aspectelor de noutate din zona de responsabilitate, iar această activitate se realizează, în principal, prin:

- ***culegerea de informaţii din surse multiple*** (secrete şi/sau deschise) în scopul identificării tendinţelor, schimbărilor, factorilor de risc şi ameninţare;
- ***evaluarea ameninţărilor*** *(threat assessment)* ***potenţiale*** la adresa securităţii naţionale, ţinând cont de factori diverşi, inclusiv context geopolitic, economic, militar și social/ aceste estimări sunt utile în înţelegerea unor eventuale capabilităţi şi intenţii ostile;
- ***analiza de risc*** (cuantificarea riscurilor și a impactului acestora): identificarea şi estimarea riscurilor care ar putea impacta obiectivele strategice/ aceasta implică analizarea vulnerabilităţilor şi a probabilităţii de materializare a ameninţărilor;
- ***identificarea oportunităţilor*** care ar putea fi utilizate în scopul întăririi securităţii naţionale şi pentru atingerea obiectivelor strategice/ aceasta poate necesita identificarea potenţialilor aliaţi, a progreselor tehnologice sau a parteneriatelor economice.

PRODUSE DE INFORMARE STRATEGICĂ

Pe scurt, analiza strategică vizează informarea decidenților pe anumite problematici de interes, în scopul sprijinirii acestora pentru fundamentarea deciziilor ulterioare. Acest tip de analiză nu poate oferi răspunsuri exacte la cerințe (întrebări) care se referă la orizonturi de timp mai apropiate sau mai îndepărtate, dar poate oferi o proiecție a unor estimări realizate prin aplicarea unor metode specifice de analiză (fiind dependentă de experiența analiștilor implicați în acest proces, dar și de disponibilitatea datelor și informațiilor relevante pentru cerință și care au potențialul de a impacta domeniul de interes). Produsul de analiză strategică reprezintă un punct de vedere profesional asupra unei situații/ eveniment/ acțiune, precum și o prognoză referitoare la premisele afectării organizației.

Produsele de informare conțin prezentarea succintă a datelor și informațiilor cu relevanță pe o problematică, pe baza cărora se realizează estimări, previziuni, prognoze etc. Aspectele prezentate în aceste produse se bazează pe informațiile deținute la momentul desfășurării procesului de analiză. Lipsa unor informații este compensată cu aprecieri care au la bază experiența analistului, scopul final fiind fie prezentarea unui răspuns la o cerință de informare, fie informarea operativă asupra unei problematici relevante din cadrul domeniului curent de activitate. De multe ori produsul de analiză strategică nu poate prezenta cu fidelitate complexitatea realității și nici nu poate avea o valoare definitivă. De aceea, în măsura în care noi aspecte/ informații devin disponibile, acestea pot contribui la redefinirea produsului de analiză, fiind necesară, periodic, o reevaluare a situației de interes. Produsul de analiză strategică (explicarea și evaluarea unui eveniment de interes pentru organizație) ar trebui să fie prezentat într-o formă clară, concisă și folosind un limbaj ușor de urmărit. Este de dorit să se evite orice formă de exprimare care ar putea induce în eroare. De asemenea, o importanță aparte o reprezintă utilizarea limbajului probabilității. În acest context, este importantă utilizarea potrivită a nuanțelor care prezintă posibilitatea vs. probabilitatea, în sensul în care sunt de interes aspectele legate de probabilitate, în special în cadrul evaluărilor.

Din punct de vedere al utilității, analiza strategică[5] urmărește: (a) înțelegerea/ stăpânirea zonelor/ domeniilor de interes; (b) evaluarea organizației proprii; (c) sprijinul/ fundamentarea luării unor decizii; (d) anticiparea unor evenimente posibile; (e) estimarea probabilității de apariție a unor evenimente importante.

CONCLUZII

Abordările aferente domeniului *intelligence* converg spre accepțiuni conform cărora analiza strategică se află în strânsă legătură cu analiza operativă şi cea tactică, scopul său fiind însă informarea factorilor de decizie cu acele aspecte relevante care pot avea posibile efecte la nivel organizaţional/ naţional, astfel încât să furnizeze beneficiarilor săi instrumentele necesare pentru evitarea surprinderii strategice. În general, analiza strategică este orientată pe abordarea, în principal, a subiectelor/ problematicilor cu efecte pe termen mediu şi lung și/sau care afectează zone întinse de teritoriu.

În ceea ce privește limitările acestui tip de analiză se poate menţiona faptul că există o serie de condiționări directe între calitatea/utilitatea/ acuratețea produsului final și disponibilitatea şi calitatea datelor şi informaţiilor deţinute la momentul redactării analizei, pe de o parte, iar pe de altă parte, lipsa unor informații este suplinită de filtrul experienței/ expertizei analiştilor implicaţi (evaluări/prognoze obținute prin aplicarea de tehnici și metode de analiză).

Aspectele prezentate susțin ideea centrală că utilizarea analizei strategice de către organizaţiile din domeniul securităţii naţionale este indispensabilă pentru a înțelege și a putea acționa preventiv într-un mediu de securitate multidisciplinar și dinamic.

BIBLIOGRAFIE

1. FLEISHER S. Craig, Bensoussan B. E., *Strategic and Competitive Analysis. Methods and Techniques for Analyzing Business Competition,* Prentice Hall, 2003, 457 p.
2. HARVEY S. Andrew, ”The Levels of War as Levels of Analysis”, *Military Review*, vol. 101, nr. 6, 2021, p. 75-81.
3. HEUER J. Richard, Pherson R.H., *Structured Analytic Techniques for Intelligence Analysis,* CQ Press, Washington DC, 2011, 343 p.
4. NEAG M. Mihai, Simion E., Kis A., *Intelligence și globalizare*, Editura Techno Media, ISBN 978-606-616-189-3, Sibiu, 2015, 175 p.
5. NIȚU Ionel, *Ghidul analistului de intelligence: compendiu pentru analiștii debutanți*, București, Editura Academiei Naționale de Informații ”Mihai Viteazul”, 2011.
6. PAIUC D., Săniuță A., Parincu A., ”Strategic Intelligence: A Semantic Leadership Perspective”, *Encyclopedia,* vol. 4, nr. 2, 2024, p. 785-798, https://doi.ergj10.3390/encyclopedia4020050, accesat în 03.01.2025.
7. RUSSELL L. Richard*, Sharpening Strategic Intelligence. Why the CIA Gets it Wrong, and What Needs to be Done to Get it Right,* Cambridge University Press, 2007, 228 p.
8. SĂVULESCU Ștefan, *Manual de Analiză Strategică*, Editura Ministerului de Interne, ISBN 978-973-745-201-6, București 2022, 311 p.
9. VLĂDUȚESCU Ș., Bizadea C., *Metode şi tehnici în analiza informaţiilor. Procese, produse analitice şi tehnici de auditare a acestora*, Universitatea din Bucureşti, Facultatea de Sociologie şi Asistenţă Socială, Master Analiza informaţiilor, București, 2009.
10. WHEATON J. Kristan, Mosco E. E., Chido D. E. (eds.), *The Analyst`s Cookbook*, volumul 1, Mercyhurst College Institute of Intelligence Studies, 2006, 165 p.
11. *** Organization of American States, The Egmont Group of Financial Intelligence Units, *Strategic Intelligence Course* (traducere din limba engleză), https://www.oas.org/cicaddocs/Document.aspx?Id=2554, accesat în 24.11.2024.
12. *** https://www.totalmilitaryinsight.com, accesat în 24.11.2024, traducere din limba engleză.

[1] The Egmont Group of Financial Intelligence Units, Strategic Intelligence Course (traducere din limba engleză), https://www.oas.org/cicaddocs/Document.aspx?Id=2554.

[2] Ionel Nițu, *Ghidul Analistului de Intelligence: compendiu pentru analiștii debutanți,* Editura Academiei Naționale de Informații „Mihai Viteazul”, București, 2011, p.21.

[3] Ștefan Săvulescu, *Manual de Analiză Strategică,* Editura Ministerului de Interne, ISBN: 978-973-745-201-6, București 2022, p.17.

[4] Richard L. Russell, *Sharpening Strategic Intelligence – Why the CIA Gets it Wrong and What Needs to be Done to Get it Right,* Cambridge University Press.

[5] *** Organization of American States, The Egmont Group, *Participant manual - Understanding strategic analysis,* Egmont Strategic Analysis Course, Session 3, p. 7., https://www.oas.org/cicaddocs/Document.aspx?Id=2554.

INTELIGENȚA ARTIFICIALĂ: SCHIMBĂRI ȘI PROVOCĂRI ÎN ANALIZA DE INTELLIGENCE

*Alexandru-Florian BĂRĂSCU**

Abstract

This paper explores the profound changes that artificial intelligence brings to intelligence analysis, highlighting both transformative opportunities and complex challenges. We will examine how artificial intelligence is redefining the process of data collection and analysis, its impact on security and privacy, as well as the ethical and legal aspects that accompany this technological evolution.

This article provides a detailed analysis of how advanced artificial intelligence tools, such as machine learning and predictive analytics, contribute to enhancing the capabilities of intelligence services. Finally, we will discuss the future of artificial intelligence in the field of intelligence and how professionals can successfully navigate these changes to maximize benefits and minimize risks.

Keywords: *artificial intelligence; predictive analysis; legality; advanced systems; strategic advantage.*

INTRODUCERE

În era digitală contemporană, inteligența artificială (IA) joacă un rol din ce în ce mai important în transformarea multor domenii, printre care și analiza de intelligence. IA se remarcă prin capacitatea sa de a procesa și analiza rapid și eficient volume mari de date, descoperind tipare și relații complexe care ar putea scăpa observației umane.

În contextul analizei de intelligence, aceste abilități sunt esențiale pentru a anticipa amenințări, a înțelege rețelele de conexiuni și a prezice comportamente viitoare. Cu toate acestea, integrarea IA în analiza de intelligence nu este lipsită de dificultăți. Provocările legate de confidențialitate, securitate, etică și legalitate nu sunt încă pe deplin reglementate, date fiind, în primul rând, dificultățile survenite ca urmare a multitudinii de informații sensibile ce necesită gestionare. În plus, adoptarea tehnologiei bazate pe inteligență artificială presupune adaptări semnificative în infrastructură și în formarea personalului, ceea ce poate genera rezistență și dificultăți operaționale. Cu toate acestea, fiabilitatea și acuratețea algoritmilor de IA sunt cruciale, întrucât erorile pot avea consecințe grave.

AUTOMATIZAREA PROCESELOR DE COLECTARE ȘI ANALIZĂ A DATELOR

Inteligența artificială are potențialul de a transforma radical procesele de colectare și analiză a datelor prin automatizarea sarcinilor complexe și reducerea semnificativă a erorilor umane. Prin aplicarea algoritmilor avansați și a tehnologiilor

Autorul este expert în cadrul Ministerului Apărării Naționale.

de învățare automată (machine learning), IA poate optimiza procesele de prelucrare a informațiilor, permițând o analiză mai rapidă și mai precisă a datelor. Această capacitate de a prelucra și interpreta rapid volume mari de date facilitează reacția promptă la amenințări imprevizibile și anticiparea potențialelor riscuri.

Algoritmii de IA pot să identifice pattern-uri subtile și aspecte ieșite din comun în seturile de date, oferind astfel o perspectivă detaliată și acționabilă asupra activităților ostile și a comportamentelor atipice. În domeniile securității și apărării, IA devine un instrument esențial pentru menținerea unui avantaj strategic față de adversari – prin integrarea tehnologiilor de inteligență artificială se pot dezvolta sisteme avansate de supraveghere și detecție a amenințărilor, asigurând protecția infrastructurilor critice și a resurselor naționale. De asemenea, IA contribuie la îmbunătățirea capacităților de predicție și prevenire, aspect ce permite anticiparea și neutralizarea proactivă a amenințărilor înainte ca acestea să se materializeze. În acest fel, inteligența artificială nu doar că sprijină apărarea împotriva atacurilor actuale, dar joacă și un rol crucial în dezvoltarea de strategii pe termen lung pentru securitatea națională.

În domeniul colectării de informații, explozia de date (generată de dispozitivele inteligente) și activitatea umană online generează un potențial imens de informații. Volumul vast de date oferit de spațiul online ar fi imposibil de procesat manual de către analiștii de informații, însă instrumentele bazate pe inteligență artificială pot analiza eficient conexiunile dintre date; aceste instrumente pot detecta activități suspecte, identifica tendințe, integra date disparate, cartografia rețele și anticipa comportamente viitoare.

INTEGRAREA IA ÎN PROCESELE TRADIȚIONALE DE INTELLIGENCE

Automatizarea cognitivă presupune transferul unor sarcini complexe, anterior realizate de analiști, către sisteme automatizate. De exemplu, aceste sarcini includ procesarea avansată a limbajului natural, identificarea și recunoașterea tiparelor de vorbire, clasificarea și potrivirea, precum și transcrierea exactă a textului din surse audio[1]. Această automatizare permite analiștilor să efectueze căutări eficiente utilizând cuvinte cheie sau categorii predefinite. O tendință marcantă în dezvoltarea inteligenței artificiale, în ultimii ani, este reprezentată de crearea unor

modele de limbaj extrem de avansate, cum ar fi GPT-4. Aceste modele de ultimă generație, bazate pe rețele neuronale avansate, au capacitatea de a simula procesele de înțelegere a textului și de rezumare[2]. Modelele lingvistice avansate contribuie substanțial la eficientizarea proceselor de prelucrare și exploatare a datelor, prin abilități de traducere automată a materialelor în multiple limbi străine și generare de rezumate comprimate și pertinente ale textelor. Această capacitate reduce considerabil timpul și efortul necesar analiștilor pentru a parcurge și evalua materialele, optimizând astfel fluxul de lucru și permițând focalizarea pe aspectele critice/ strategice ale informațiilor[3].

Prin urmare, automatizarea cognitivă are un potențial semnificativ în susținerea etapelor de procesare și exploatare a datelor în cadrul ciclului de intelligence, permițând astfel analiza rapidă și eficientă a volumelor mari de date. În plus, avansurile în tehnologiile de automatizare cognitivă pot oferi un suport esențial analiștilor, îmbunătățind considerabil organizarea, clasificarea și gestionarea informațiilor, facilitând astfel interpretarea și utilizarea lor strategică.

În context, integrarea instrumentelor de IA în procesele tradiționale ale analizei de intelligence ar putea aduce următoarele modificări:

- capacitatea de a integra și armoniza volume mari de date provenite din surse diverse într-un sistem unificat, ceea ce permite realizarea unei analize mult mai coerente și eficiente; această capacitate nu doar elimină discontinuitățile și lacunele de informații, dar furnizează și o imagine comprehensivă asupra situației de securitate/ în acest fel, IA facilitează luarea unor decizii informate și proactive, asigurând o gestionare optimă a resurselor și a riscurilor;
- clasificarea și organizarea datelor în categorii relevante, facilitând analiza ulterioară/ acest proces este esențial pentru identificarea și prioritizarea amenințărilor, bazându-se pe nivelurile de risc asociate fiecărei categorii; prin organizarea sistematică a informațiilor, se creează un cadru analitic robust, care sprijină evaluarea precisă a pericolelor și alocarea eficientă a resurselor pentru gestionarea acestora;
- folosirea de modele predictive pentru a anticipa evoluția amenințărilor și a identifica potențialele riscuri înainte ca acestea să se materializeze/ această metodă proactivă asigură o abordare anticipativă, prin care se pot gestiona eficient vulnerabilitățile și se poate menține o stare optimă de securitate;
- generarea de simulări și scenarii care evaluează impactul diferitelor acțiuni asupra securității/ acest proces analitic permite anticiparea consecințelor și optimizarea strategiilor, asigurând astfel o abordare anticipativă și bine fundamentată în gestionarea securității;
- automatizarea proceselor de colectare și analiză a datelor elimină erorile asociate transcrierii și interpretării manuale, garantând astfel o acuratețe superioară și o consistență ridicată în evaluarea informațiilor/ acest mecanism avansat asigură o fiabilitate sporită a datelor și permite realizarea unor analize coerente și precise, optimizând eficiența proceselor decizionale.

RISCURI ASOCIATE CU AUTOMATIZAREA ANALIZEI DE INTELLIGENCE

Automatizarea analizei de intelligence, prin utilizarea inteligenței artificiale și a tehnologiilor de *machine learning*, aduce numeroase beneficii, dar și o serie de riscuri și provocări semnificative. În timp ce aceste tehnologii pot îmbunătăți considerabil eficiența și acuratețea proceselor de analiză, ele pot, de asemenea, introduce vulnerabilități și limitări care trebuie abordate cu atenție[4]. Printre principalele riscuri asociate cu automatizarea analizei de intelligence se numără următoarele:

- *Erori în date și algoritmi.* Algoritmii de IA se bazează pe datele de intrare pentru a genera rezultate precise – dacă datele

sunt incomplete, inexacte sau părtinitoare, acestea pot conduce la concluzii eronate. De exemplu, lipsa unor informații critice poate duce la omisiuni în identificarea amenințărilor. Este esențial să se mențină un proces de curățare și validare a datelor pentru a asigura calitatea acestora (chiar și mici erori în datele de intrare pot genera probleme mari în cadrul procesului de analiză).

- *Vulnerabilități la atacuri cibernetice.* Sistemele automatizate de analiză a informațiilor sunt expuse la atacuri cibernetice, iar breșele de securitate pot compromite datele sensibile și pot afecta integritatea acestora. Hackerii pot manipula algoritmii pentru a-și ascunde activitățile sau pentru a induce informații false. Datele sensibile pot fi accesate de persoane neautorizate, ceea ce poate conduce la scurgeri de informații și la utilizarea abuzivă a datelor colectate.
- *Dependența de tehnologie și automatizare.* În timp ce automatizarea poate îmbunătăți eficiența, dependența excesivă de tehnologie poate duce la pierderea expertizei umane și la lipsa de flexibilitate în abordarea problemelor neprevăzute. Sistemele automate pot să nu fie în măsură să interpreteze corect situațiile complexe sau ambigue care necesită judecata umană. Automatizarea completă a deciziilor critice poate conduce la decizii automate fără supraveghere umană, ceea ce poate avea consecințe neprevăzute.
- *Vulnerabilități la defecțiuni tehnice.* Sistemele automatizate pot fi vulnerabile la defecțiuni tehnice, erori software sau hardware, care pot afecta capacitatea de a răspunde rapid și eficient la amenințări; astfel, securizarea infrastructurii tehnologice devine esențială pentru a proteja procesele analitice de interferențe malițioase și pentru a menține un nivel înalt de acuratețe și consistență în evaluarea informațiilor.
- *Complexitatea integrării și implementării IA.* Integrarea tehnologiilor de IA în procesele existente poate fi complexă și costisitoare – într-o primă fază este necesară asigurarea compatibilității între sistemele vechi și noile tehnologii pentru a evita perturbările. Serviciile de informații trebuie să fie pregătite să gestioneze provocările asociate cu schimbarea tehnologică, inclusiv formarea personalului și adaptarea la noile procese.

GESTIONAREA ALGORITMILOR ÎN ANALIZA DE INTELLIGENCE

Utilizarea algoritmilor în munca de intelligence contribuie la îmbunătățirea muncii analiștilor, atât în etapa de culegere a datelor, cât și în cea de analiză propriu-zisă. Pe măsură ce tehnologiile de inteligență artificială și *machine learning* devin tot mai avansate, rolul analiștilor de informații evoluează, expertiza acestora, cunoștințele proprii despre contexte culturale, sociale și politice devin esențiale pentru interpretarea corectă a datelor și validarea estimărilor puse la dispoziție de IA. Această înțelegere ajută la identificarea implicațiilor mai profunde ale informațiilor colectate și corelate.

Având în vedere expertiza analiștilor de informații (specializați în analize critice și contextualizare date), aceștia pot interpreta nuanțe și conexiuni subtile care pot fi ignorate de algoritmi, aplicând judecata umană și experiența profesională. De cealaltă parte, algoritmii pot corela/ analiza rapid și eficient volume mari de date, detectând pattern-uri pe care analiștii umani ar putea să le rateze; acești algoritmi pot filtra *„zgomotul”* din date și pot oferi analiștilor informațiile relevante și acționabile; pot, de asemenea, estima (pe baza datelor colectate) pentru a face predicții, oferind o perspectivă anticipativă asupra potențialelor amenințări și tendințe[5].

Astfel, în vederea sprijinirii procesului decizional, este necesară și oportună integrarea

tehnologiei în munca analistului, scopul fiind eficientizarea muncii de intelligence:

- algoritmii asigură analiștilor suport decizional prin furnizarea de informații și perspective analitice, situație care facilitează luarea unor decizii mai informate și dezvoltarea unor strategii pertinente ancorate în realitate;
- IA automatizează sarcinile repetitive și consumatoare de timp, cum ar fi colectarea și interpretarea datelor, permițând analiștilor să se concentreze pe aspectele mai complexe și critice ale analizei;
- introducerea algoritmilor în procesul de analiză îmbunătățește calitatea și acuratețea analizei, deoarece combinația dintre judecata umană și capacitatea de procesare automată oferă o viziune mai completă asupra datelor;
- analiștii pot oricând să intervină și să ofere feedback IA, contribuind astfel la îmbunătățirea procesului de culegere și analiză prin ajustarea parametrilor și rafinarea modelului pentru a obține rezultate mai precise și mai relevante; feedback-ul uman este crucial pentru a corecta erorile algoritmice și pentru a adapta algoritmii la situația din teren/ problematica avută în vedere.

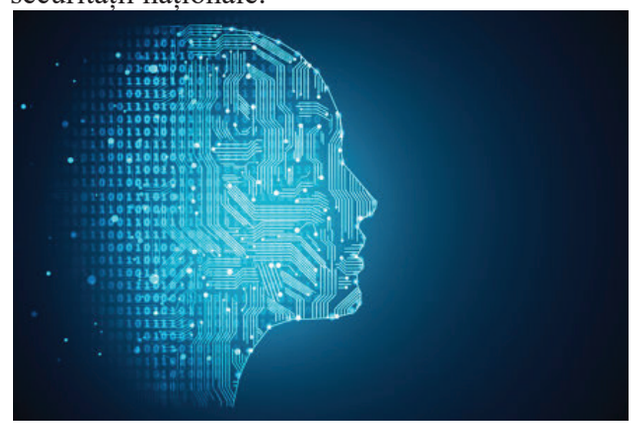
INOVAȚII TEHNOLOGICE ȘI VIITORUL ANALIZEI DE INTELLIGENCE

Inteligența artificială este pe cale să transforme fundamental domeniul analizei de intelligence prin automatizarea proceselor de sortare și interpretare a datelor. Această evoluție promite să îmbunătățească semnificativ eficiența și rapiditatea cu care serviciile de informații pot răspunde la amenințări emergente, aducând o serie de beneficii notabile pentru securitatea națională și globală.

Din această perspectivă, în viitorul apropiat IA va automatiza și mai multe aspecte ale analizei de intelligence, facilitând procesarea și interpretarea rapidă a volumelor mari de date provenite din surse diverse, cum ar fi rețelele sociale, comunicațiile digitale și datele senzoriale. Algoritmii de învățare automată vor deveni din ce în ce mai sofisticați, capabili să extragă informații critice și să identifice pattern-uri complexe, totul cu o intervenție minimă din partea analiștilor de informații. Acest lucru va elibera analiștii de sarcinile repetitive și consumatoare de timp, permițându-le să se concentreze pe interpretarea și utilizarea strategică a datelor[6]. De asemenea, odată cu dezvoltarea tehnologiilor IA, ciclul de răspuns al serviciilor de informații va fi scurtat semnificativ; capacitatea de a analiza datele aproape în timp real va permite serviciilor să anticipeze și să răspundă rapid la amenințări emergente, reducând riscul apariției de incidente.

Cu toate avantajele pe care le aduce, automatizarea proceselor de analiză în domeniul intelligence-ului nu este lipsită de provocări. Unul dintre principalele obstacole este asigurarea calității și integrității datelor, deoarece deciziile critice se bazează pe informațiile stocate și analizate de IA. De asemenea, trebuie gestionate preocupările legate de confidențialitate și securitate.

Automatizarea proceselor de analiză cu ajutorul inteligenței artificiale reprezintă un pas esențial în evoluția domeniului de intelligence. Pe măsură ce tehnologia continuă să avanseze, serviciile de informații vor trebui să se adapteze la noile realități și să dezvolte strategii care să valorifice pe deplin potențialul tehnologic, asigurându-se totodată că utilizarea sa este etică și responsabilă. Prin integrarea acesteia în procesele lor operaționale, serviciile de informații vor putea să își îmbunătățească capacitățile de prevenire și răspuns, contribuind astfel la menținerea securității naționale.



CONCLUZII

Tehnologia IA are un potențial considerabil de a sprijini activitatea serviciilor de informații și de a îmbunătăți semnificativ eficiența analizei de date. Cu toate acestea, IA nu este un instrument universal aplicabil pentru toate sarcinile. Astfel, utilizarea sa pentru a augmenta inteligența umană trebuie să fie parte a unei strategii bine gândite, modelată de principii solide de guvernanță. Această strategie ar trebui să includă, de exemplu, o analiză atentă a riscurilor și beneficiilor, evaluând riscurile etice și implementând mecanisme de guvernare inspirate de experiențele acumulate în alte domenii care folosesc IA.

În contextul analizei de intelligence, volumul și diversitatea datelor care trebuie gestionate sunt într-o continuă expansiune, ceea ce creează o provocare semnificativă în maximizarea eficienței procesării acestor informații, având în vedere resursele umane limitate disponibile. Obiectivul principal devine, din această perspectivă, recalibrarea rolurilor analiștilor pentru a se concentra pe activități cu valoare adăugată semnificativă; acest obiectiv poate fi realizat prin valorificarea capacităților avansate ale IA de a automatiza procesele de prelucrare a datelor și de a optimiza referințele încrucișate între domenii și surse multiple.

Prin urmare, IA poate facilita integrarea și analiza complexă a datelor provenite din diverse surse, eliberând analiștii umani de sarcinile repetitive și permițându-le să se concentreze pe evaluări strategice și interpretări aprofundate, care pot avea un rol substanțial în procesul decizional.

BIBLIOGRAFIE

1. BABUTA Alexander, Oswald M., Janjeva A., *Artificial Intelligence and UK National Security: Policy Considerations*, Occasional Paper, Royal United Services Institute for Defence Studies, London, 2020, 46 p.
2. BOSTROM Nick, Yudkowsky Eliezer, ”The Ethics of Artificial Intelligence”, *The Cambridge Handbook of Artificial Intelligence*, 2014, p. 316-334.
3. BRUNDAGE Miles, Garfinkel B., Avin S., Clark J., Toner H. et. all, *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*, Future of Humanity Institute/ University of Oxford, Centre for the Study of Existential Risk/ University of Cambridge, 2018, 100 p.
4. CATH Corinne, Wachter S., Mittelstadt B., Taddeo M. & Floridi L., ”Artificial Intelligence and the “Good Society”: the US, EU, and UK approach”, *Science and Engineering Ethics,* Springer, vol. 24, nr. 2, 2018, p. 505-528.
5. FLORIDI Luciano, Cowls J., King T. C. & Taddeo M., ”How to Design AI for Social Good: Seven Essential Factors”, *Science and Engineering Ethics,* Springer, vol. 26, nr. 1, 2020, p. 1771-1796.
6. FREEMAN Lindsay, ”Weapons of War, Tools of Justice: Using Artificial Intelligence to Investigate International Crimes”, *Journal of International Criminal Justice*, vol.19, nr. 1, 2021, p. 35-53.
7. HAQUE A., Ahmad A., *Predictive Analytics for Security and Intelligence: Advances and Trends*, Springer, 2021.
8. HOLLAND Michel A., *The Black Box, Unlocked: Predictability and Understandability in Military AI*, The United Nations Institute for Disarmament Research (UNIDIR), 2020, 36 p.
9. MARR Bernard, *Artificial Intelligence in Practice: How 50 Successful Companies Used AI and Machine Learning to Solve Problems*, Wiley, 2019, 352 p.
10. VINCENT Brandi, ”How the CIA is working to ethically deploy Artificial Intelligence”, NextGov.Fcw, 2019, https://www.nextgov.com/emerging-tech/2019/05/how-cia-working-ethically-deploy-artificial-intelligence/157395/
11. WEST M. Darrell, ”Using AI and machine learning to reduce government fraud”, The Brookings Institution (blog), 2021, https://www.brookings.edu/research/using-ai-and-machine-learning-to-reduce-government-fraud/

[1] Floridi L., Cowls J., King T. C., Taddeo, M., ”How to Design AI for Social Good: Seven Essential factors, *Science and Engineering Ethics,* 2020.

[2] Bender E. M., On NYT Magazine on AI: Resist the urge to be impressed, 2022.

[3] Alexander Babuta, Oswald M., Janjeva A., *Artificial Intelligence and UK national security: policy considerations*, Occasional Paper, Royal United Services Institute for Defence Studies, London, 2020.

[4] Haque A., Ahmad A., *Predictive Analytics for Security and Intelligence: Advances and Trends*, Springer, 2021.

[5] Darrell M. West, ”Using AI and machine learning to reduce government fraud”, *The Brookings Institution* (blog), 2021, https://www.brookings.edu/research/using-ai-and-machine-learning-to-reduce-government-fraud; accesat la data de 27.07.2024;

[6] Brandi Vincent, ”How the CIA is working to ethically deploy artificial intelligence”, 2019, NextGov., https://www.nextgov.com/emerging-tech/2019/05/how-cia-working-ethically-deploy-artificial-intelligence/157395/; accesat la data de 21.07.2024.

PROVOCĂRI LA ADRESA ACTIVITĂȚII DE CONTRAINFORMAȚII ȘI SECURITATE

Ioana COVRIG*
Răducu-Vasile RUSU*

Abstract

Counter-intelligence and security represents a cornerstone of national security and defence, aiming to prevent hostile infiltrations, protect operational secrets, and ensure the integrity of military missions. Its role has become increasingly critical in the current context of global security degradation.

Regional conflicts, the expansion of hybrid tactics, and the growing influence of non-state actors have created an unstable and unpredictable environment. Added to this is the accelerated pace of technological advancements, which further broadens the range of vulnerabilities and threats.

This article explores the main current and future challenges in the field of counter-intelligence and security, aiming to highlight the importance of this area of activity and to identify the issues that must be addressed for effective operations.

Keywords: *counter-intelligence; security; threats; challenges; quantum computers; Schengen Area; hybrid threats.*

INTRODUCERE

Activitatea de contrainformații reprezintă o componentă esențială a securității naționale, având ca obiectiv principal protejarea statului în fața riscurilor, amenințărilor și vulnerabilităților pe linie de terorism, spionaj, subversiune, sabotaj, crimă organizată și cibernetică (TESSOCC), generate de actori ostili, atât din mediul extern, cât și din interior.[1] Aceasta cuprinde activități menite să identifice, să prevină și să contracareze materializarea acestor amenințări.

Într-o lume în continuă schimbare, care generează un context internațional tot mai complex, în care evenimentele geopolitice și intensificarea competiției între marile puteri favorizează răspândirea conflictelor hibride, reînarmarea, avansurile tehnologice rapide, amenințările hibride și competiția strategică, contrainformațiile se confruntă cu provocări fără precedent, ce pun o presiune sporită asupra structurilor contrainformative autohtone și aliate.[2] Totodată, provocările globale, cum ar fi schimbările climatice, crizele economice

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

și migrația în masă, generează noi tipuri de vulnerabilități care pot fi exploatate în scopuri ostile. În plus, entități statale și non-statale, cum ar fi organizațiile teroriste, grupările paramilitare și rețelele criminale internaționale au devenit mai sofisticate, utilizând tehnologii moderne și structuri descentralizate pentru a evita detectarea, crescând implicit instabilitatea și imprevizibilitatea mediului ce se vrea asigurat.[3]

Conștientizând că epoca activității de contrainformații focusată pe identificarea și neutralizarea riscurilor, amenințărilor și vulnerabilităților generate de un singur vector al amenințării, în special de natură umană (Human Threat Counter-Intelligence), a ajuns la final odată cu escaladarea noilor crize și conflicte armate în desfășurare, la nivel aliat se consideră că activitatea de contrainformații ar trebui abordată într-o manieră cuprinzătoare, care să ia în calcul noii vectori ai amenințării, ce pot acționa în diferite domenii și discipline (Multidisciplinary Counter-Intelligence)[4].

Pornind de la constatarea autorilor privind imposibilitatea documentării unitare, dintr-o singură sursă bibliografică, cu privire la provocările pe linie de contrainformații și securitate, prezentul articol se dorește a fi o listă sintetizată a acestor provocări, respectiv a implicațiilor concrete ale acestora asupra securității și apărării naționale, menită să conștientizeze cititorul cu privire la complexitatea activității de contrainformații și securitate și să-i faciliteze acestuia eventuala documentare ulterioară asupra direcțiilor sau conceptelor semnalate.

Astfel, din dorința de a fi accesibili oricui, indiferent de experiența și cunoștințele din domeniul informațiilor pentru apărare, vom împărți provocările identificate în patru categorii generale, oferind pentru fiecare concept o definiție general recunoscută și exemple simple privind modul în care aceste provocări se pot materializa, impactând activitatea structurilor responsabile cu asigurarea securității naționale.

ASCENSIUNEA AMENINȚĂRILOR HIBRIDE

Amenințările hibride sunt definite de NATO ca fiind combinații deliberate de activități coercitive și subversive, mijloace convenționale și neconvenționale, metode militare și non-militare, care sunt utilizate în mod sincronizat pentru a viza vulnerabilitățile unui stat sau ale unei organizații. Acestea sunt concepute pentru a destabiliza și submina ordinea, fără a declanșa un conflict militar deschis.[5] Printre principalele amenințări hibride care influențează activitatea de contrainformații, la momentul actual, se numără ***campaniile de dezinformare, influența economică*** și ***implicarea actorilor non-statali.***

Referitor la ***campaniile de dezinformare***, acestea implică diseminarea deliberată de informații false pentru a influența opinia publică, adesea prin intermediul rețelelor sociale. Conform NATO, actorii rău intenționați desfășoară în mod obișnuit operațiuni informaționale ostile împotriva aliaților și a partenerilor acestora. Aceste amenințări informaționale includ activități intenționate, dăunătoare, manipulative și coordonate – precum manipularea și interferența informațiilor de către actori străini și dezinformarea răspândită prin mass-media tradiționale și rețele sociale – concepute pentru a crea confuzie, a adânci diviziunile, a destabiliza societățile și, în cele din urmă, a slăbi Alianța.[6]

Un exemplu concret de materializare a campaniilor de dezinformare sunt cazurile confirmate de interferențe rusești în diverse procese electorale, inclusiv campania prezidențială din Statele Unite din 2016 și alegerile pentru Parlamentul European din 2019[7].

Tot în acest context, amenințările interne devin din ce în ce mai relevante, pe măsură ce statele se confruntă cu extremismul intern, subminarea democrației și influențele externe, intensificate prin acțiuni de dezinformare. Astfel de acțiuni hibride reprezintă o provocare de

proporții pentru activitatea de contrainformații, dat fiind faptul că identificarea entității ostile care a generat dezinformarea necesită un consum substanțial de resurse și timp.

Influența economică se referă la utilizarea instrumentelor economice, precum *sancțiunile*, *embargourile și investițiile strategice*, pentru a constrânge deciziile politice ale unui stat, respectiv a-l forța să acționeze contrar intereselor proprii[8]. Un exemplu în acest sens poate fi identificat încă din anul 2014, în contextul conflictului din Ucraina. Astfel, odată cu sancțiunile internaționale aplicate F.Ruse, aceasta a răspuns prin impunerea de sancțiuni proprii statelor occidentale, în speță a introdus un embargo asupra importurilor de produse alimentare. Acest embargo a vizat în special produsele din Uniunea Europeană, afectând exportatorii europeni și demonstrând capacitatea Rusiei de a utiliza embargourile ca instrument de influență economică și politică. Totodată, proiecte de investiții strategice, cum ar fi Nord Stream 2, au fost concepute pentru a crește dependența energetică a Europei de resursele rusești.[9]

Implicarea actorilor non-statali, precum o*rganizațiile teroriste, grupările paramilitare internaționale* și *rețelele criminale transfrontaliere*, în colaborare cu state ostile, contribuie semnificativ la instabilitatea securității naționale, respectiv la suprasolicitarea structurilor contrainformative responsabile de menținerea securității. Aceste grupări sunt folosite pentru a submina stabilitatea și coeziunea internă a democrațiilor, exploatând vulnerabilitățile acestora prin metode neconvenționale și asimetrice. Un exemplu notabil în acest sens este utilizarea grupărilor paramilitare pentru desfășurarea de operațiuni clandestine, cum ar fi cele efectuate de gruparea Wagner în Siria, Ucraina și alte zone intens disputate de pe glob[10].

DIGITALIZAREA ACCELERATĂ ȘI EXPANSIUNEA SPAȚIULUI CIBERNETIC

Unul dintre cele mai semnificative fenomene din ultimii ani este digitalizarea rapidă a societății. Deși avansurile tehnologice și digitalizarea facilitează activitatea de contrainformații și securitate, acestea au extins spațiul cibernetic și au deschis noi fronturi pentru acțiunile ostile la adresa securității statelor și aliaților. Printre principalele provocări vizând activitatea de contrainformații din această categorie se numără ***atacurile cibernetice, tehnologia deepfake*** și ***anonimitatea online***.

Atacurile cibernetice reprezintă încercări de a obține acces neautorizat la sisteme informatice, cu scopul de a fura, modifica sau distruge date, respectiv de a perturba infrastructura critică sau activitatea socială, per ansamblu. Aceste atacuri sunt adesea orchestrate de actori statali sau grupări criminale, care utilizează diverse metode, precum malware, phishing sau ransomware, pentru a-și atinge obiectivele.

Subiectul este amplu dezbătut în literatura de specialitate, iar eforturi constante sunt făcute de autoritățile de pretutindeni pentru a minimiza impactul milioanelor de atacuri cibernetice executate zilnic de entități ostile[11]. Din punct de vedere al activității de contrainformații, aceste atacuri sunt relevante din perspectiva posibilității pierderii, deteriorării sau alterării datelor și informațiilor cu caracter secret, manipulate la nivelul instituțiilor din cadrul sistemului de apărare, ordine publică și securitate națională, în ceea ce se numește, în termeni generali, *spionaj cibernetic*. Totodată, aducem în atenție impactul extrem de grav asupra securității naționale pe care îl pot avea astfel de atacuri asupra unei centrale nucleare sau altor astfel de infrastructuri critice.

Tehnologia deepfake presupune realizarea de conținut audio sau video generat cu ajutorul inteligenței artificiale (IA), care manipulează realitatea pentru a induce în eroare. Această

tehnologie poate fi utilizată pentru dezinformare, înșelăciune sau compromiterea unor persoane, organizații sau instituții de interes pentru actorii ostili inițiatori ai acțiunii. De exemplu, un videoclip falsificat poate fi folosit pentru a destabiliza sau diviza exponenții unei societăți, prin influențarea percepțiilor acestora cu privire la autoritatea și buna-credință a conducerii statului.

Anonimitatea online se referă la procesul de eliminare sau modificare a datelor de identificare a unei entități din datele colectate pe Internet, astfel încât entitățile să nu poată fi identificate direct sau indirect. Acest proces contribuie la protejarea confidențialității utilizatorilor și la respectarea reglementărilor privind protecția datelor. Însă, tot acest proces facilitează și desfășurarea activităților ilegale, deoarece *rețelele criptate,* care facilitează accesarea dark web-ului[12], și utilizarea *criptomonedelor* permit actorilor rău intenționați să comunice și să efectueze tranzacții financiare fără a-și dezvălui identitatea.

Din punctul de vedere al activității de contrainformații, amplificarea utilizării criptomonedelor la nivel mondial crește riscul de materializare a unor amenințări la adresa securității naționale, fapt pentru care reglementarea acestui domeniu a devenit o prioritate pentru state și organizații internaționale încă din anul 2020, existând desigur și excepții care interzic acest tip de tranzacții din motive de securitate pragmatice.[13]

EVOLUȚIA TEHNOLOGIILOR EMERGENTE

Tehnologiile emergente sunt acele tehnologii caracterizate prin noutate radicală, creștere rapidă, coerență, impact proeminent și un grad ridicat de incertitudine și ambiguitate[14]. După cum am menționat și anterior, progresul tehnologic accelerează ritmul în care amenințările se materializează, iar tehnologii precum ***inteligența artificială (IA)***, ***calculatoarele cuantice*** și ***Internetul lucrurilor (IoT)*** pot aduce, pe lângă oportunități pentru colectarea, analiza și criptarea datelor, riscuri și vulnerabilități noi, generate de următorii factori: creșterea volumului de date captate - gestionarea și protejarea unui flux uriaș de informații devin din ce în ce mai dificile; posibilitatea executării unor atacuri cibernetice avansate de către entități ostile - în scopul de a compromite sisteme critice; facilitarea creării de conținut deepfake convingător - ce poate fi folosit ca mijloc de dezinformare în efortul adversarilor de a obține superioritatea informațională.[15]

Inteligența artificială (IA) joacă un rol dual în domeniul analizei datelor și al securității cibernetice. Pe de o parte, IA este esențială pentru detectarea tiparelor în seturi mari de date, facilitând procesarea informațiilor în cadrul ciclului informațional și oferind predicții și clasificări precise (atât de necesare beneficiarilor produselor de intelligence); pe de altă parte, poate oferi avantaje adversarilor pentru a-și perfecționa atacurile cibernetice sau pentru a aplica o dezinformare credibilă. De exemplu, infractorii cibernetici utilizează IA pentru a rafina și automatiza atacurile de tip phishing, făcându-le mai eficiente sau chiar imposibil de detectat.[16]

Internetul lucrurilor (IoT) se referă la rețeaua de dispozitive fizice conectate la Internet, care colectează și schimbă date. Deși aceste dispozitive aduc numeroase beneficii, ele prezintă și vulnerabilități semnificative în ceea ce privește securitatea cibernetică, în special în contextul infrastructurilor critice. Concret, studiile arată că există o tendință accentuată de proliferare rapidă a dispozitivelor IoT în infrastructurile critice. Acest trend a dus la creșterea suprafeței de atac pentru infractorii cibernetici, vulnerabilizând sistemele sensibile ale infrastructurilor critice.[17] Aceste constatări subliniază necesitatea implementării unor măsuri de securitate robuste și a unei monitorizări continue pentru a proteja infrastructurile critice de potențiale atacuri cibernetice facilitate de vulnerabilitățile dispozitivelor IoT.

Calculatoarele cuantice sunt dispozitive de calcul care utilizează principiile mecanicii cuantice pentru a procesa informații. Spre deosebire de computerele clasice, care folosesc biți ce reprezintă fie 0, fie 1, calculatoarele cuantice folosesc biți cuantici sau qubiți. Acești qubiți pot exista în multiple stări simultan datorită fenomenului de suprapunere cuantică, permițând astfel procesarea unui număr vast de rezultate în paralel. De asemenea, qubiții pot fi interconectați prin inseparabilitate cuantică, ceea ce înseamnă că starea unui qubit poate depinde direct de starea altuia, chiar și la distanțe mari. Aceste proprietăți oferă calculatoarelor cuantice potențialul de a rezolva probleme complexe mult mai eficient decât computerele tradiționale.[18]

Menținerea securității naționale depinde în foarte mare măsură de canale de comunicații securizate și de criptarea datelor, pentru a proteja informațiile sensibile împotriva spionajului cibernetic. Astfel, informațiile confidențiale deținute de instituțiile guvernamentale, serviciile militare și agențiile de informații, fie că este vorba despre planuri de securitate de nivel strategic, informații despre tehnologia avansată deținută sau corespondență diplomatică, sunt toate vizate de către entitățile ostile. Prin urmare, criptografia este piatra de temelie a securității informațiilor, iar dezvoltarea mijloacelor de decriptare a fost și va fi mereu în topul priorităților unui adversar.[19]

Revenind la calculatoarele cuantice, specialiștii consideră că această tehnologie inovatoare are potențialul de a sparge metodele de criptare existente, amenințând securitatea comunicațiilor. În paralel, această tehnologie poate asigura celui care o posedă soluții de securitate cibernetică aproape impenetrabile. Totodată, se consideră că această tehnologie ar putea permite dezvoltarea de mijloace pentru soluționarea problemei actuale a SIGINT privind procesarea semnalelor în medii cu niveluri ridicate de zgomot, prin optimizarea circuitelor cuantice în vederea extragerii semnalului de interes din zgomot, respectiv pentru eficientizarea procesului de analiză a acestuia[20]. Pe măsură ce tehnologiile cuantice încep să fie integrate tot mai mult în cadrul infrastructurilor critice globale, importanța obținerii supremației în acest domeniu devine tot mai evidentă.

Capacitatea de a controla rețelele de comunicații securizate, de a compromite sistemele criptografice tradiționale și de a dezvolta aplicații militare avansate bazate pe tehnologia cuantică aduce cu sine implicații geopolitice și strategice profunde. Astfel, progresele rapide ale Chinei în acest domeniu, care își propune ca până în anul 2030 să obțină întâietatea în domeniul comunicațiilor și calculului cuantic (vizând extinderea infrastructurii naționale cuantice, dezvoltarea unui prototip de calculator cuantic și construirea unui simulator cuantic), amenință să destabilizeze balanța puterii la nivel global, fapt ce va amplifica rivalitățile geopolitice existente, în special cu Statele Unite ale Americii. Deși această competiție poate stimula inovația tehnologică, ea generează noi vulnerabilități care vor determina celelalte națiuni să își reconsidere strategiile de securitate.

GLOBALIZAREA ȘI DEPENDENȚA TRANSNAȚIONALĂ

Globalizarea a creat o rețea complexă de interdependențe economice, sociale și tehnologice între state, facilitând însă și activitățile rețelelor criminale și ale actorilor statali ostili. În această categorie de provocări la adresa activității de contrainformații se regăsesc: lacunele existente cu privire la capacitatea de ***identificare a actorilor ostili*** care pot acționa itinerant pe teritoriul unui stat, ***mobilitatea crescută*** a persoanelor și a bunurilor, precum și ***reglementările variate*** ale statelor în ceea ce privește coridoarele transfrontaliere.

Identificarea actorilor ostili în contextul securității naționale și internaționale este o provocare majoră, având în vedere complexitatea

relațiilor transfrontaliere și capacitatea acestor actori ostili de a se ascunde în rețele economice globale sau în fluxurile de migranți generate de diferitele conflicte regionale sau crize umanitare în desfășurare. Totodată, actualul context de securitate a influențat creșterea semnificativă a cazurilor în care actori statali ostili finanțează acțiuni subsumate spionajului sau încearcă evitarea embargourilor și a sancțiunilor (prin intermediul unor companii de fațadă[21] sau al tranzacțiilor comerciale aparent legale).

Mobilitatea crescută a persoanelor și a bunurilor, asigurată prin transporturi rapide și rețele logistice globale, permite infiltrarea actorilor ostili sau transportul materialelor ilicite. Actorii non-statali și organizațiile criminale utilizează coridoarele transfrontaliere insuficient reglementate și puncte de tranzit pentru a evita detectarea, astfel fiind favorizat traficul de arme, droguri, migranți sau materiale nucleare, prin rețelele comerciale internaționale.

Reglementările variate ale statelor ce împart aceeași graniță, în ceea ce privește tranzitul frontierelor, pot crea lacune pe care entități ostile le pot fructifica în detrimentul siguranței naționale. Pentru a corobora cele menționate anterior, este necesară aducerea în discuție a implicațiilor asupra activității de contrainformații rezultate din accederea României în spațiul Schengen.

La 01.01.2025 România și Bulgaria au devenit membre cu drepturi depline ale spațiului Schengen, ridicând astfel numărul statelor membre la 29[22]. Odată cu această accedere au fost create premisele unor avantaje privind: eliminarea controalelor la frontierele interne, ce va facilita schimburile economice și mobilitatea persoanelor; accesul la sistemele informatice și resursele de securitate din spațiul Schengen, cum ar fi Sistemul de Informații Schengen (SIS), va permite schimburi rapide de informații cu partenerii europeni și va contribui la prevenirea riscurilor[23]; atragerea de investiții și resurse europene suplimentare pentru consolidarea securității granițelor exterioare ale spațiului comunitar; creșterea influenței României în politica de securitate europeană și consolidarea cooperării cu alte structuri contrainformative ale statelor membre.

Pe de altă parte, este important de menționat că accederea în spațiul Schengen aduce noi provocări pentru activitatea de contrainformații. Astfel, accesul la bazele de date comunitare ce conțin informații clasificate poate genera noi riscuri, amenințări și vulnerabilități, iar serviciile de contrainformații autohtone vor trebui să gestioneze eficient noile capabilități informaționale pentru a preveni scurgerile de informații. Nu în subsidiar, responsabilitatea protecției frontierelor externe ale spațiului Schengen va presupune intensificarea eforturilor de contrainformații în zone sensibile, cum ar fi granița cu Ucraina și Republica Moldova.

Însă, cea mai importantă provocare generată de accederea la spațiul Schengen constă în faptul că, odată cu creșterea fluxurilor de persoane și bunuri, se amplifică riscul infiltrării unor elemente care pot genera amenințări la adresa securității naționale, precum spioni, organizații criminale transfrontaliere sau teroriști. Sensibilitatea acestei provocări poate veni din însuși avantajul de a nu avea un acces strict monitorizat prin puncte de trecere ale frontierei cu celelalte state membre. Astfel, entități ostile care au accesat spațiul Schengen în diferite alte state membre ar putea intra în țara noastră nesesizate, având posibilitatea de a întreprinde acțiuni subsumate amenințărilor la adresa securității naționale în mod itinerant, fără a fi niciodată identificate.

Această ipoteză este coroborată și cu recentele decizii ale Ungariei de a include cetățenii Federației Ruse și ai Belarusului în cadrul Programului Cardul Naţional al Ungariei, program ce conferă participanților agreați drepturi de muncă și de ședere pe teritoriul statului vecin pentru o perioadă de doi ani, cu posibilitatea prelungirii perioadei cu trei ani,

fără o limită de consecutivitate a posibilității prelungirii[24]. Această decizie diplomatică a Ungariei ar putea avea consecințe semnificative asupra securității naționale a țării noastre, fiind de natură să crească riscurile de materializare a amenințărilor.

CONCLUZII

După cum se poate înțelege din ideile formulate anterior, activitatea de contrainformații se află într-un punct critic, confruntându-se cu provocări fără precedent. Abordarea provocărilor semnalate necesită o combinație de inovație, adaptabilitate și angajament ferm față de valorile democratice. Doar printr-un efort concertat și coordonat, societățile pot rămâne reziliente în fața amenințărilor actuale și viitoare.

Este evident că identificarea problemei nu este decât jumătate din drumul necesar a fi parcurs pentru soluționarea acesteia. Astfel, pentru a răspunde provocărilor enunțate anterior, responsabilii pe linie de contrainformații și securitate trebuie să adopte o postură flexiblă și inovatoare, care să susțină evoluția capabilităților necesare identificării, prevenirii și contracarării riscurilor, amenințărilor și vulnerabilităților reieșite din dinamica mediului de securitate actual și viitor.

Printre principalele direcții de acțiune necesare pentru adaptarea structurilor contrainformative autohtone la rigorile impuse de noile realități se numără necesitatea investițiilor constante în tehnologie și educație, extinderea colaborării internaționale și participarea activă la dezvoltarea unei culturi de securitate sănătoase, atât de necesară pentru atingerea nivelului scontat de reziliență socială. În încheiere, reiterăm că articolul de față este o sinteză a principalelor provocări pe linie de contrainformații și securitate, neavând pretenții de exhaustivitate, fiind mai degrabă un îndemn la studiu suplimentar asupra conceptelor și ideilor semnalate.

BIBLIOGRAFIE

1. CONSTĂNȚEANU Radu, „Evoluția inteligenței artificiale în atacurile de tip phishing: de ce chiar și cei mai experimentați pot deveni victime”, 13.01.2025, https://itchannel.ro/evolutia-inteligentei-artificiale-in-atacurile-de-tip-phishing-de-ce-chiar-si-cei-mai-experimentati-pot-deveni-victime/?utm.
2. DAVIES P. H. J., Steward T. J., „The trouble with TESSOC: the coming crisis in British and allied military counterintelligence doctrine”, *Defence Studies*, vol. 24, nr. 2, 2024, https://www.tandfonline.com/doi/epdf/10.1080/14702436.2024.2303084?needAccess=true
3. IANCU Sânziana, „Războiul hibrid al Rusiei împotriva Occidentului (I). Doctrina Gherasimov, forte paramilitare (iPb) și grupurile de voluntari”, *Defense Romania*, 23.09.2024, https://www.defenseromania.ro/razboiul-hibrid-al-rusiei-impotriva-occidentului-i-doctrina-gherasimov-forte-paramilitare-ipb-si-grupurile-de-voluntari-iv_630347.html?utm.
4. OPREA Bogdan. „Dezinformarea în era digitală. Concepte și abordări”, *Sociologie Românească*, vol. 19, nr. 1, 2021, https://revistasociologieromaneasca.ro/sr/article/view/1715/1637.
5. PARKER Edward, “When a Quantum Computer Is Able to Break Our Encryption, It Won’t Be a Secret”, *Commentary*, RAND Corporation, 13.09.2023, https://www.rand.org/pubs/commentary/2023/09/when-

a-quantum-computer-is-ableto-break-our-encryption.html.
6. ROTOLO Daniele, Hicks Diana, Martin Ben R., „What Is an Emerging Technology?”, *Research Policy*, vol. 44, nr. 10, 2015, p. 1827–1843, https://www.sciencedirect.com/science/article/abs/pii/S0048733315001031.
7. SCRIPCARIU V. George, „Adaptarea strategiei de contrainformații a României: Lecții din strategia națională de contrainformații a SUA”, *Intelligence Info*, vol. 3, nr. 4, 2024, https://www.intelligenceinfo.org/wp-content/uploads/woocommerce_uploads/2024/05/Revista_Intelligence_Info-Volumul_3-Numarul_2-Iunie_2024-Rezumate-wgnvch.pdf.
8. STAN Andrei, ”Primele explicații oficiale ale Ungariei după ce a decis să faciliteze accesul rușilor în UE”, *HotNews*, 21 August 2024, https://hotnews.ro/primele-explicatii-oficiale-ale-ungariei-dupa-ce-a-decis-sa-faciliteze-accesul-rusilor-in-ue-1775844.
9. USTIAN Anatol, „Relațiile Uniunii Europene cu Federația Rusă: evoluție și cooperare sau stagnare?”, Masa rotundă *„Acțiunea de politică externă a Uniunii Europene: direcții, realizări și perspective*”, 15 aprilie 2022, https://ibn.idsi.md/sites/default/files/imag_file/88-93_50.pdf?utm.
10. *** AJP-2 Allied Joint Doctrine for Intelligence, Counterintelligence and Security, Februarie 2016, https://jadl.act.nato.int/ILIAS/data/testclient/lm_data/lm_152845/Linear/JISR04222102/sharedFiles/AJP2.pdf
11. *** Parlamentul European, *Ingerințe străine: cum combate Parlamentul amenințările la adresa democrației UE*, Direcția Generală de Comunicare, 10.04.2024, https://www.europarl.europa.eu/topics/ro/article/20240404STO20215/ingerinte-cum-combate-parlamentul-amenintarile-la-adresa-democratiei-ue.
12. *** NATO, *Countering hybrid threats*, 07.05.2024, https://www.nato.int/cps/en/natohq/topics_156338.htm.
13. *** NATO, *NATO's approach to counter information threats*, 03.02.2025, https://www.nato.int/cps/en/natohq/topics_219728.htm?utm.
14. *** „Costurile cauzate de atacurile cibernetice globale vor ajunge la aproximativ 24 trilioane de dolari până în 2027 (estimări)”, *Agenția națională de presă AGERPRES*, 29.11.2024, https://agerpres.ro/economic-intern/2024/11/29/costurile-cauzate-de-atacurile-cibernetice-globale-vor-ajunge-la-aproximativ-24-trilioane-de-dolari-pana-in-2027-estimari--1395235?utm.
15. *** https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-quantum-computing.
16. *** https://cercetare.ase.ro/wp-content/uploads/2024/12/STUDIU-CU-PRIVIRE-LA-CONTEXTUL-SI-EFECTELE-ADERARII-ROMANIEI-LA-SPATIUL-SCHENGEN.pdf.
17. *** https://ieeexplore.ieee.org/document/8796409?utm.
18. *** https://initiativaprivata.ro/termen/sanctiuni-economice/?utm.
19. *** https://www.consilium.europa.eu/ro/policies/schengen-area/?utm.
20. *** „Agenți sub acoperire și o călătorie în Fiji: cum a căzut în capcana FBI șeful unei rețele de contrabandă vitale pentru armata lui Putin”, *DIGI24.ro*, 03.01.2025, https://www.digi24.ro/stiri/externe/rusia/agenti-sub-acoperire-si-o-calatorie-in-fiji-cum-a-cazut-in-capcana-fbi-seful-unei-retele-de-contrabanda-vitale-pentru-armata-lui-putin-3066709. _
21. *** „Ce țări reglementează criptomonedele”, *Forbes România*, 04.04.2022, https://www.forbes.ro/ce-tari-reglementeaza-criptomonedele-255536.
22. *** https://www.tudelft.nl/over-tu-delft/strategie/vision-teams/quantum-internet/impact-governance/the-possible-dark-side-of-quantum-communication-technologies.

[1] *** AJP-2 Allied Joint Doctrine for Intelligence, Counterintelligence and Security, February 2016, p. 71, https://jadl.act.nato.int/ILIAS/data/testclient/lm_data/lm_152845/Linear/JISR04222102/sharedFiles/AJP2.pdf., accesat în data de 12.12.2024.

[2] George V. Scripcariu, „Adaptarea strategiei de contrainformații a României: Lecții din Strategia Națională de Contrainformații a SUA", *Intelligence Info,* vol. 3, nr. 4, 2024, p. 25-28; https://www.intelligenceinfo.org/wp-content/uploads/woocommerce_uploads/2024/05/Revista_Intelligence_Info-Volumul_3-Numarul_2-Iunie_2024-Rezumate-wgnvch.pdf, accesat în data de 12.12.2024.

[3] Bogdan Oprea,. „Dezinformarea în era digitală. Concepte și abordări.", *Sociologie Românească,* vol. 19, nr. 1, 2021, https://revistasociologieromaneasca.ro/sr/article/view/1715/1637, accesat în data de 12.12.2024.

[4] Philip H. J. Davies, Steward T. J., "The trouble with TESSOC: the coming crisis in British and allied military counter-intelligence doctrine", *Defence Studies,* vol. 24, nr. 2, 2024, p. 234–256 https://www.tandfonline.com/doi/epdf/10.1080/14702436.2024.2303084?needAccess=true, accesat în data de 12.12.2024.

[5] *** NATO Publications, *Countering hybrid threats,* May 2024, https://www.nato.int/cps/en/natohq/topics_156338.htm, accesat în data de 09.01.2025.

[6] *** NATO Publications, *NATO's approach to counter information threats,* December 2024, https://www.nato.int/cps/en/natohq/topics_219728.htm?utm, accesat în data de 05.01.2025.

[7] *** European Parliament Publications, *Ingerințe străine: cum combate Parlamentul amenințările la adresa democrației UE,* 2024, https://www.europarl.europa.eu/topics/ro/article/20240404STO20215/ingerinte-cum-combate-parlamentul-amenintarile-la-adresa-democratiei-ue, accesat în data de 13.01.2025.

[8] https://initiativaprivata.ro/termen/sanctiuni-economice/?utm, accesat în data de 03.01.2025.

[9] Anatol Ustian, „Relațiile Uniunii Europene cu Federația Rusă: evoluție și cooperare sau stagnare?", Masa rotundă „Acțiunea de politică externă a Uniunii Europene: direcții, realizări și perspective", 15 aprilie 2022, https://ibn.idsi.md/sites/default/files/imag_file/88-93_50.pdf?utm, accesat în data de 03.01.2025.

[10] https://www.defenseromania.ro/razboiul-hibrid-al-rusiei-impotriva-occidentului-i-doctrina-gherasimov-forte-paramilitare-ipb-si-grupurile-de-voluntari-iv_630347.html?utm, accesat în data de 10.01.2025.

[11] https://agerpres.ro/economic-intern/2024/11/29/costurile-cauzate-de-atacurile-cibernetice-globale-vor-ajunge-la-aproximativ- 24-trilioane-de-dolari-pana-in-2027-estimari--1395235?utm, accesat în data de 10.01.2025.

[12] Dark web este o parte a Internetului care nu este indexată de motoarele de căutare tradiționale și care necesită software specializat, cum ar fi Tor (The Onion Router) sau I2P (Invisible Internet Project), pentru a putea fi accesată. Această rețea oferă anonimitate atât utilizatorilor, cât și site-urilor, ascunzând locația și identitatea lor.

[13] https://www.forbes.ro/ce-tari-reglementeaza-criptomonedele-255536, accesat în data de 10.01.2025.

[14] Daniele Rotolo, Diana Hicks și Ben R. Martin, "What Is an Emerging Technology?", *Research Policy,* vol. 44, nr. 10, 2015, p. 1827–1843, https://www.sciencedirect.com/science/article/abs/pii/S0048733315001031, accesat în data de 19.01.2025.

[15] George V. Scripcariu, Op.cit.

[16] Radu Constănțeanu, „Evoluția inteligenței artificiale în atacurile de tip phishing: de ce chiar și cei mai experimentați pot deveni victime", 13.01.2025, https://itchannel.ro/evolutia-inteligentei-artificiale-in-atacurile-de-tip-phishing-de-ce-chiar-si-cei-mai-experimentati-pot-deveni-victime/?utm, accesat în data de 19.01.2025.

[17] https://ieeexplore.ieee.org/document/8796409?utm, accesat în data de 19.01.2025.

[18] https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-quantum-computing, accesat în data de 19.01.2025.

[19] https://www.tudelft.nl/over-tu-delft/strategie/vision-teams/quantum-internet/impact-governance/the-possible-dark-side-of-quantum-communication-technologies, accesat în data de 19.01.2025.

[20] Edward Parker, "When a Quantum Computer Is Able to Break Our Encryption, It Won't Be a Secret", *Commentary,* RAND Corporation, 13.09.2023, https://www.rand.org/pubs/commentary/2023/09/when-a-quantum-computer-is-able-to-break-our-encryption.html, accesat în data de 19.01.2025.

[21] https://www.digi24.ro/stiri/externe/rusia/agenti-sub-acoperire-si-o-calatorie-in-fiji-cum-a-cazut-in-capcana-fbi-seful-unei-retele-de-contrabanda-vitale-pentru-armata-lui-putin-3066709?fbclid=IwZXh0bgNhZW0CMTEAAR07JOX-HWqWr4sya4MRs6UjB1C7hhWGg14EERjDyc05SfwiIOXCiOxtT1tE_aem_f1PcWPNqs_iM28TC3t3L9g&__grsc=cookieIsUndef0&__grts=57910400&__grua=6d90e1b9ecb7e97b8d69942f0da22557&__grrn=1, accesat în data de 19.01.2025.

[22] https://www.consilium.europa.eu/ro/policies/schengen-area/?utm_, accesat în data de 19.01.2025.

[23] https://cercetare.ase.ro/wp-content/uploads/2024/12/STUDIU-CU-PRIVIRE-LA-CONTEXTUL-SI-EFECTELE-ADERARII-ROMANIEI-LA-SPATIUL-SCHENGEN.pdf, accesat în data de 19.01.2025.

[24] https://hotnews.ro/primele-explicatii-oficiale-ale-ungariei-dupa-ce-a-decis-sa-faciliteze-accesul-rusilor-in-ue-1775844, accesat în data de 19.01.2025.

O PERSPECTIVĂ PSIHOLOGICĂ PRIVIND EFECTUL PANDEMIILOR ASUPRA SERVICIILOR DE INFORMAȚII

Flavia-Emilia STAN*

***Motto**:* „Momentele de ruptură pot fi ocazii de diagnosticare societală și de reparație.”

Adrian Deoancă

Abstract

The article aims to highlight the contribution of psychology in understanding the human psyche, restoring the emotional balance and helping individuals adapt to the demands of the external environment. These contributions have beneficial effects on work quality and provide guidance towards viable solutions for the multiple challenges arising in the context of the pandemic.

Why are we talking about pandemics? Because they pose an additional threat to any state. Moreover, when they emerge in a context already marked by societal vulnerabilities such as poverty, migration, terrorism etc., they create a state of imminent danger to national security, especially when they exacerbate existing issues or trigger new ones.

Why did we choose to examine the role of intelligence services in crisis situations? Because, in any state, these services play a crucial role in providing relevant information to decision-makers, who, based on this intelligence, adopt the most effective measures to ensure national security. This process reduces uncertainty, allows for more accurate understanding of the crisis and, last but not least, enables the development of better-grounded and more effective action plans and capabilities.

***Keywords**: pandemics; reducing stress; intelligence structures; psychology resilience.*

O situație pandemică este, în sine, o stare de criză medicală la nivel mondial, care afectează normalitatea desfășurării vieții. O pandemie nu apare brusc, fiind precedată de un stadiu epidemic; însă, chiar și în această etapă este pus sub semnul întrebării cursul firesc al vieții, fiind destabilizate sentimentele de încredere și de siguranță ale persoanelor, primând aspecte de genul incertitudinea zilei de mâine, procurarea hranei și a celor necesare, cel mai grav fiind inocularea fricii față de o eventuală îmbolnăvire sau chiar de moarte. Un astfel de fenomen medical transcende cu mult granițele personale și își răsfrânge efectele la toate nivelurile societății. Nevoia de securitate este cel mai grav afectată pe timpul unei pandemii întrucât afectează încrederea în

Autoarea este expert în cadrul Ministerului Apărării Naționale.

structuri ale statului, cum ar fi sistemul sanitar, aparatul politic, economic, de apărare, presa etc.

Așa cum spune Paulo Coelho în cartea sa, „Alchimistul", *„Tot ceea ce se întâmplă o dată poate să nu se mai întâmple niciodată, dar tot ceea ce se întâmplă de două ori se va întâmpla, cu siguranță, și a treia oară"*. Această aserţiune ne duce cu gândul la vremuri nu foarte îndepărtate, când omenirea s-a confruntat cu situații pandemice grave[1] (cu pierderi importante de vieți omenești), cu impact major asupra întregii societăți și cu repercusiuni asupra celor mai importante instituții statale. Pandemiile rămân în istorie ca având puternice efecte devastatoare și reprezentând un real pericol pentru omenire.

În unele state, pe un fundal al neîncrederii anterioare în structurile politico-administrative, o situație pandemică va accentua starea negativă emoțională a populației. De aceea, astfel de momente de răscruce pot impune o reconsiderare a statului, în general, și a instituțiilor statale, care erau, poate, privite până atunci cu neîncredere sau păreau lipsite de importanță. Așa cum subliniază Adrian Deoancă, antropolog la Universitatea din Michigan, *„momentele de ruptură pot fi ocazii de diagnosticare societală și de reparație."*[2]

Prin urmare, orice criză are și o parte pozitivă, materializată prin identificarea oportunităților și prin luarea măsurilor necesare asigurării evoluției, adaptării și gestionării corecte a resurselor. Toate acestea se pot realiza în urma unor informări corecte și oportune din partea serviciilor de informații; iată de ce serviciile de intelligence joacă un rol esențial în avertizarea apariției unor astfel de situații și devin un element important pentru stoparea crizei la nivel statal.

STRUCTURILE DE INTELLIGENCE PE TIMPUL PANDEMIILOR

Anterior unei situații de criză, serviciile de intelligence culeg informații relevante şi detaliate, pe baza cărora factorul politic poate acţiona discret, eficient şi în timp util în direcția prevenirii și evitării surprinderii strategice. Astfel, serviciile de informații contribuie decisiv, inclusiv prin avertizări privind iminența unei viitoare pandemii, fapt ce permite decidenților să adopte din timp măsuri de prevenție și gestionare. Pe timpul unor crize de tipul pandemiilor, deficiențele apărute în mod inevitabil în pregătirea și colectarea, procesarea și exploatarea, analiza și diseminarea informațiilor vor diminua capacitatea structurilor de intelligence de avertizare timpurie a decidenților, fapt care ar putea genera tragerea la răspundere a acestora pentru gestionarea defectuoasă a impactului crizei sanitate (amploarea pierderilor de vieți omenești sau insuficienta alocare de fonduri financiare/ reversul medaliei - risipa materială, cu eventuale acuzații îndreptate către favorizarea anumitor contractori de medicamente sau echipamente medicale).

Avertizarea timpurie constituie primul pas în demersul reducerii impactului negativ major al unor stări de criză inevitabile. În acest sens, menționăm că, în cotidianul german *Die Welt*, s-a dezvăluit faptul că, încă din anul 2002, serviciul german de informaţii externe a reuşit să transmită în avans decidenţilor şi experţilor medicali date confidenţiale privind manifestările medicale dezvoltate de pacienţii infectaţi cu virusul SARS-CoV-2, aspecte referitoare la epidemia de SARS din China şi strategia iniţială a guvernului chinez de a ascunde realitatea. *„Această dezvăluire nesolicitată, în contextul unei rate foarte scăzute a mortalităţii la pacienţii germani infectaţi cu virusul SARS-CoV-2, atribuită în special organizării excepţionale a tuturor instituţiilor implicate în acest efort, a confirmat voalat faptul că au fost realizate şi de această dată informări precoce şi detaliate pe baza cărora factorul politic a acţionat discret şi eficient."*[3]

Activitățile structurilor de intelligence în timpul unei pandemii sunt deosebit de valoroase întrucât oferă date și informații despre impactul crizei asupra securității naționale, economiei, bugetului, calității vieții cetățenilor, gradului de succes sau de eșec în lupta pentru eradicarea bolii sau în repoziționarea statului în relațiile cu ceilalți actori. Informația înseamnă șansa de a acționa eficient, raportat la resurse și timp, iar efectele se cuantifică în numărul cât mai redus de pierderi umane sau de natură materială.

Este recunoscut faptul că o criză globală impune adoptarea unor hotărâri rapide și tranșante, însă nu trebuie neglijat și efectul pe termen lung al schimbării. Strategiile viitoare vor reconfigura lumea, așa cum spunea Yuval Noah Harari într-un articol pentru cotidianul *Financial Times*: „Natura urgențelor este de a accelera procesele istorice, iar decizii care ar necesita în mod normal ani de deliberări vor fi adoptate în câteva ore. Toate acestea pentru că riscul de a nu face nimic este mult mai mare”[4]. Din această perspectivă, considerăm că structurile de intelligence au rolul major în informarea oportună a decidenților, informațiile furnizate stând la baza procesului elaborării strategiilor de acțiune precriză, criză și postcriză.

PROTEJAREA PERSONALULUI DE INTELLIGENCE ÎN SITUAȚII DE VULNERABILITATE MEDICALĂ

Resursa umană, indiferent dacă ne referim la domeniul militar sau civil, reprezintă o verigă cheie, vitală, creatoare de valoare, menită să asigure supraviețuirea, dezvoltarea și succesul organizațional. Din păcate, în situații de criză, cum este cea generată de izbucnirea unui pandemii, este resursa cea mai vulnerabilă. Dacă privim structurile de intelligence din perspectiva resurselor umane, putem afirma că acestea reprezintă bunul cel mai de preţ al organizaţiei: este singura resursă inepuizabilă de creativitate și de generare de soluții/ idei noi, originale şi valoroase. Și, în același timp, constituie un important factor care trebuie înțeles, motivat şi antrenat în vederea implicării cât mai depline şi profunde în realizarea obiectivelor organizaţionale. Din această perspectivă, este necesar ca personalului să îi fie asigurate cele mai bune condiții de desfășurare a activității, în limitele posibile, și să fie protejat în fața vulnerabilităților provocate de situația de criză.

Menţinerea ridicată a moralului şi combaterea stresului psihologic rămân obiective importante în timpul pandemiilor, aspect subliniat şi de către unul dintre foștii directori ai Defense Intelligence Agency (DIA)/SUA, Robert Ashley, într-o notă internă destinată angajaţilor[5]. Nu mai puțin importantă este sănătatea fizică a angajaților. De asemenea, formarea personalului implică o pregătire specifică, de durată, care necesită aprofundare teoretică, dar mai ales practică. Experiența în domeniu constituie un atu important și, din această perspectivă, a avea în parametri funcționali întregul personal reprezintă o prioritate. În cazul unor pandemii, funcționalitatea reiese atât din nivelul sănătății fizice, cât și din cel al funcționării psihice.

În sprijinul celor afirmate, menționăm opinia unor specialiști din domeniu privitor la structura de informații militare: „...valoarea profesională și umană a personalului de informații militare constituie elementul principal care asigură succesul. Personalul se formează cu eforturi mari și de lungă durată, pentru că informațiile militare constituie un domeniu complex, multidisciplinar și dinamic, care presupune o bună pregătire generală și de specialitate, dublată de calități umane absolut obligatorii: cinste, corectitudine, putere de muncă, iubire de țară și profesie, spirit de sacrificiu, rezistență la efort și stres, discreție, memorie și imaginație dezvoltate, spirit critic și analitic etc.”[6] Provocările profesionale multiple, dar și calitățile psihomorale ale personalului menționate mai sus sunt descrieri potrivite tuturor structurilor de intelligence. De aceea, orice *„pierdere”* umană este dificil de suplinit într-un timp scurt și, mai ales, într-o situație critică.

În general, chiar și în condiții normale, activitatea în domeniul intelligence-ului este puternic generatoare de stres, din cauza responsabilității crescute, a volumului mare de muncă, dar și a mediului de acțiune mereu în schimbare, care necesită adaptare rapidă. Suprapunând un astfel de stres peste cel generat de o situație pandemică putem aprecia, intuitiv, că nivelul stresului va crește. Prin restricțiile implementate pe timpul pandemiei, persoanele nu mai pot desfășura o serie de activități cu rol de a restabili echilibrul emoțional, ceea ce îngreunează ieșirea din starea psihică negativă.

Specialiștii din domeniul psihologiei admit că un anumit nivel de stres este necesar pentru funcționarea optimă a psihicului, dar, dacă se trece

peste o anumită limită, acesta va avea consecințe negative (erori în muncă, scăderea atenției, luarea unor decizii greșite, îngustarea câmpului conștiinței, scăderea vitezei de reacție, instalându-se pe acest fundal surmenajul și oboseala). Toate acestea conduc, în final, la slăbirea sistemului imunitar al persoanei și la creșterea probabilității unor îmbolnăviri la nivel fizic. Psihicul uman este susceptibil de a fi influenţat în diferite moduri (în funcţie de particularităţile psihice ale fiecărei persoane), care, de fapt, dau în final nota distinctivă a reacției. Psihologii susțin că în situații moderate de stres nu contează foarte mult ceea ce se întâmplă concret, ci modul cum se raportează fiecare la eveniment în sine. În schimb, o situație de criză, cum este cea determinată de o pandemie, nu mai reprezintă un stres moderat, astfel încât se preconizează că majoritatea populației va reacționa asemănător, ajungând în final să afișeze un întreg tablou de disfuncții specifice[7].

Pregătirea psihologică a personalului din structurile de intelligence privind creșterea rezilienței la factorii de stres își găsește utilitatea pornind de la următoarea constatare: cunoașterea și formarea în plan teoretic a unor mecanisme de „coping" adaptative reprezintă un real suport în gestionarea optimă a stresului individual. Totodată, selecția riguroasă a personalului care accede în astfel de structuri are și ea un rol însemnat, mai ales din perspectiva reducerii la minimum a posibilității apariției unor comportamente dezadaptative și a eșecului profesional.

De asemenea, o serie de valori implementate la nivelul structurilor și, implicit, de comportamente ce decurg din acestea, au în cadrul pandemiilor un rol benefic în adaptarea rapidă a personalului. Un exemplu în acest sens constă în respectarea cu strictețe a regulilor. Astfel, în context pandemic respectarea regulilor aduce siguranță, stabilitate și, în final, reprezintă o soluție pentru a gestiona cât mai corect noile provocări. Și, deosebit de importantă, cu rol adaptativ, este obișnuința de a obține informații relevante din surse de încredere, astfel încât dezinformarea să rămână la cote cât mai mici. Capacitatea de a te informa corect și conștientizarea faptului că anumite știri sunt false pot face o mare diferență în modul în care un individ ajunge să ia decizii personale și să se adapteze la noile realități.

În opinia noastră, vulnerabilitatea la nivel individual pe parcursul unei stări de criză este dată de legi universale, după care funcționează psihicul uman. În sprijinul acestei afirmații amintim *„Piramida nevoilor umane"*, elaborată de Abraham Maslow[8], și observăm că în orice situație neprevăzută, de răscruce, ce apare brusc în viață, omul se va reîntoarce la nevoile sale primordiale, lăsând pe plan secund nevoile care duc la atingerea potențialului maxim. Deoarece are loc o repoziționare a întregului sistem valoric personal, efectele sunt vizibile și la nivel ocupațional, pentru că orice angajat, privit ca individ, se raportează la această piramidă de nevoi, fiind supus acelorași legi. Astfel, nevoile fizice, de siguranță, acaparează centrul atenției persoanei și, până în momentul în care nu sunt satisfăcute, întreg spectrul motivațional este amprentat, activitatea profesională fiind afectată în mod direct. Pentru ca angajații să revină la potențialul maxim este necesar ca aceștia să își rezolve cu celeritate nevoile de la baza piramidei. Reechilibrarea nevoii de securitate într-un timp relativ scurt va avea efecte pozitive asupra calității muncii, rezultatele fiind mai rapid și mai ușor observabile.

În funcție de tipul provocărilor, demersul psihologic se axează pe diferite zone de acțiune:

a) în plan individual:

- restabilirea echilibrului emoțional al persoanei;
- utilizarea unor metode cu rol în gestionarea eficientă a stresorilor;
- creșterea adaptabilității persoanei la schimbare;
- înlăturarea barierelor cognitive în interpretarea corectă a situației;
- accesarea resurselor persoanei de a face față unor situații limită etc.

b) în plan organizațional:

- optimizarea stării de confort la locul de muncă prin consilierea comenzii;
- pregătirea sistematică a personalului pentru creșterea rezilienței la factorii de stres

cu ajutorul unor materiale informative sau sesiuni de antrenament;
- evaluarea riguroasă a personalului pentru identificarea celor mai vunerabili față de stresori, precum și a celor care nu au mecanisme de coping adaptative suficient dezvoltate;
- elaborarea unor materiale cu sfaturi psihologice utile în situații de criză;
- monitorizarea stării moralului angajaților prin mijloacele avute la dispoziție etc.

În esență, elementele de natură psihologică sprijină actul decizional privind asigurarea bunăstării fizice și psihice la nivel organizațional. Pe lângă demersurile inițiate de psihologi pentru a garanta buna funcționare psihică a resursei umane, un rol esențial îl are chiar organizația în sine, care menține un climat organizațional benefic diminuării efectelor negative ale pandemiei. Preocuparea față de nevoile angajaților, accesul la informații utile privind siguranța fizică impusă de noile condiții, asigurarea unui mediu de muncă igienizat corespunzător, reorganizarea activității fără a diminua calitatea actului profesional, reprezintă metode cu impact dublu pozitiv, atât în direcţia prevenirii infectării personalului propriu, cât și a creșterii moralului organizației.

PROVOCĂRI PSIHOLOGICE INDUSE DE PANDEMII

Pandemiile provoacă foarte multe schimbări pe toate palierele vieții, iar când vorbim despre aria profesională observăm modificări importante, de la simpla deplasare spre locul de muncă până la condițiile în care se poate desfășura activitatea profesională. Una dintre recomandările cel mai des folosite în reducerea numărului de îmbolnăviri este izolarea, reducerea contactelor sociale sau munca la domiciliu. Când vorbim despre serviciile de intelligence, varianta muncii din confortul căminului propriu este exclusă din mai multe rațiuni: obţinerea, prelucrarea și transmiterea informațiilor cu un anumit grad de secretizare nu se poate realiza prin mijloace informatice nesecurizate, lucru care ar crea, în scurt timp, o mare vulnerabilitate întregului sistem.

În același timp, nu pot fi excluse total contactele umane de la locul de muncă. Astfel, respectarea cu strictețe a regulilor de prevenție a îmbolnăvirilor devine deosebit de importantă, mai ales când se lucrează în echipe sau în anumite locații restrânse ca suprafață. În principiu, structurile de intelligence au grade diferite de vulnerabilitate față de restricțiile impuse în urma declanșării unei pandemii și sunt afectate într-o proporție mai mică sau mai mare în modul normal de acțiune[9]. Pornind de la aceste considerente, vom trece în revistă câteva dintre aspectele semnificative constatate.

- ***Structuri OSINT***

Privind global situația pe timpul unei pandemii, remarcăm că una dintre cele mai mari provocări la nivelul populației este nevoia de a cunoaște, de a ști. Chiar dacă informațiile abundă pe toate canalele mass-media, există nenumărate motive pentru care sunt generate și fake-news-uri[10]. Inițial, acestea apar din cauză că cercetătorii înșiși, din diverse arii profesionale, nu au un răspuns concret, bine documentat, legat de situația respectivă, ci mai degrabă aduc soluții care au fost viabile cu alte ocazii, în alte contexte asemănătoare. Dezinformarea, în acest caz, nu are la bază o intenție negativă, ci una pozitivă, iar rezultatul nesatisfăcător este dat de necunoașterea suficientă a situației actuale și de timpul scurt avut la dispoziție pentru a genera evaluări consolidate.

În schimb, există o paletă largă de informații generate cu intenția clară de a dezinforma populația, cum ar fi cele referitoare la găsirea vinovaților privind izbucnirea pandemiei, despre natura virusului, anumite predicții apocaliptice legate de viitorul omenirii, tratamente miraculoase nefundamentate științific, propunerea unor soluții radicale care subminează economia sau duc la o falsă ieșire din situație, alterarea imaginii unui stat, a unei structuri a statului, de acoperire a propriei incompetențe în gestionarea crizei etc. Infodemia devine în acest context la fel de periculoasă ca și virusul în sine, însă efectele acesteia nu sunt atât de ușor cuantificabile.

La nivel psihologic, orice informație primită este considerată în primă fază ca fiind adevărată și abia ulterior ea va fi verificată și i se va stabili

valoarea de adevăr sau minciună[11]. Însă, în situația în care persoana este permanent contaminată psihologic, nu mai are timpul necesar de a filtra datele primite și ajunge să fie intoxicată cu astfel de mesaje, pe care le ia ca atare. Așa cum susține și prof. univ. dr. psiholog Daniel David, ceea ce este cel mai grav reiese din faptul că undeva, la nivelul minții, procesul normal de gândire este alterat iremediabil de către informația falsă primită și vorbim în acest caz, în termeni psihologici, de contaminare intelectuală (efectul său se exprimă în comportamentele și emoțiile persoanei).

Din această perspectivă, la nivelul contextului în care acționează una dintre structurile serviciilor de intelligence, mai exact cea care culege date și informații din surse deschise/ OSINT, putem descoperi adevăratele provocări profesionale legate de pregătirea psihologică, dar și de specialitate a celor care desfășoară astfel de acțiuni. Amintim aici doar câteva dintre calitățile psihologice necesare acestui domeniu de activitate: spirit și gândire critică, conștientizarea bias-urilor de gândire (erori de judecată, prejudecăți), răbdare, intuiție, perseverență, capacitatea de a face legături între informații culese din surse diferite și de tipuri diferite, capacitatea de a valida informația etc. Trierea unui volum mare de date, urmărirea cu stoicism a direcției de acțiune corecte ce reiese din mesajele validate, capacitatea crescută de a lupta contra contaminării psihologice, dar și a responsabilității de a garanta valoarea de adevăr a mesajelor reprezintă o muncă solicitantă, ce implică multă experiență. Tocmai de aceea, produsele de intelligence sunt vitale pe timpul pandemiilor și al altor situații de criză.

- ***Structuri HUMINT***

În timp ce analiza mesajelor culese din mass-media scoate în evidență neconcordanțe și anomalii ale datelor și departajează datele în adevărate și false, este imperios necesară întărirea valorii de cunoaștere a informațiilor culese și prin intermediul exploatării surselor umane. Structura care folosește în mod special exploatarea informativă din surse umane, HUMINT, aduce date importante despre intențiile adversarilor, moralul și relațiile dintr-un colectiv, furnizează elemente despre percepțiile adversarului, mentalitățile acestuia, conturând întregul tablou cu detalii mult mai fine, exacte și personalizate. Este o activitate cu un puternic caracter social.

Din punct de vedere al desfășurării activității, personalul care lucrează în astfel de structuri este cel mai afectat pe timpul pandemiei deoarece nevoile misiunii intră în conflict cu cele mai bune practici de sănătate publică, cum ar fi interzicerea contactelor sociale, limitarea deplasărilor, închiderea spațiilor publice, anularea zborurilor, carantina la ieșirea și intrarea din țară etc. În aceste condiții de austeritate, în care nu mai poți practic să te strecori „în mulțime", nu poți avea un dialog decât de la cel puțin doi metri, personalul specializat în activități HUMINT își desfășoară activitatea cu dificultate, mai ales dacă anumite țări practică supravegherea video a populației sau a contactelor, pentru controlul răspândirii maladiei infecțioase.

În acest context, sursa umană nu mai are acces direct la informații. Problemele apar atât din partea celor care culeg informațiile, dar și din partea celor care le furnizează, deoarece vulnerabilitatea în fața unor boli pentru care nu există tratament sau vaccin este resimțită de ambele părți. Aceleași tipuri de provocări le întâmpină și adversarii. Astfel, în perioada unei pandemii este recomandat ca misiunile să fie realizate cu personal care deține o bogată experiență în domeniu și abilități deja formate, deoarece stresul crește direct proporțional cu gravitatea situației. Este de preferat să se apeleze la sursele umane validate anterior, căci este dificil să dezvolți relații de încredere doar prin Zoom/ Skype sau alte mijloace impersonale, în condiții improprii și cu o multitidine de vulnerabilități.

Pe lângă comunicarea verbală în sine, este afectată și comunicarea nonverbală. Anumiți indicatori paraverbali pot susține operatorul HUMINT în munca sa, cu intenția de a spori nivelul de încredere al sursei, de a induce starea de calm și siguranță, în timp ce alte elemente de limbaj nonverbal trec pe locul secund, cum ar fi expresiile faciale, care, de cele mai multe ori, vor fi acoperite de o mască. Zâmbetul - semnul

cel mai elocvent de acceptare a celuilalt și de bună dispoziție - devine ineficient. Postura este alterată și ea, iar semnele care denotă simularea sau minciuna nu mai pot fi observate.

Pe fundalul unei stări generale marcate de reticență, teamă și panică, se construiesc mai dificil relații noi interumane și cresc șansele unui refuz de colaborare, însă se pot consolida parteneriate mai vechi. Criza poate fi folosită de operatorul HUMINT pentru a aprofunda legăturile, prin oferirea sprijinului și trăirea „împreună" a experienței comune. Niciodată o mașinărie sau un aparat nu va putea înlocui valoarea unei persoane în a furniza date relevante legate de o speță, de un caz etc. Omul rămâne indispensabil în procesul de culegere a informațiilor și, de aceea, toate structurile de intelligence care implică munca cu sursele umane pot fi afectate pe timpul restricțiilor impuse de pandemie.

- ***Structuri IMINT***

Când vorbim despre IMINT ne referim la culegerea informațiilor din analiza unor imagini obținute prin senzori, dar și la o categorie profesională specială, care posedă calități deosebite ale atenției și ale memoriei vizuale, cu o bună capacitate de abstractizare și de a face conexiuni între informații, activitate ce se finalizează cu emiterea unor ipoteze cât mai plauzibile. Activitatea personalului care deservește astfel de structuri este afectată pe timpul pandemiei într-o proporție mai redusă, structura putând desfășura, în principal, la cerere, activități de sprijin, cum ar fi cea de supraveghere a populației, fără a se expune îmbolnăvirii. Monitorizarea respectării izolării la domiciliu sau a carantinării unor persoane în anumite locații, supravegherea activității de deplasare pietonală sau cu autoturismele în zonele de focar – sunt doar câteva noi sarcini care ar putea fi desfășurate cu risc minim de expunere la factorii patogeni.

- ***Structuri SIGINT***

Specialiștii care activează în domeniul SIGINT nu resimt atât de acut efectele pandemiei asupra activității profesionale și chiar recunosc că volumul de muncă este oarecum diminuat. La acest nivel, cea mai mare vulnerabilitate o constituie starea de sănătate a personalului, pentru că activitatea se desfășoară împreună cu alți colegi, în spații restrânse și special destinate acestui tip de activitate. Așadar, trierea riguroasă a personalului la începerea programului de muncă, aerisirea și igienizarea frecventă a spațiilor de muncă și a echipamentelor din dotare, precum și purtarea unor dispozitive medicale (măști) reprezintă comportamente sanogene, de prevenție a răspândirii infecției cu factorii patogeni specifici pandemiei.

- ***Alte elemente cu impact asupra structurilor de intelligence***

Activitatea profesională poate fi afectată în multe moduri, de la simpla comunicare a mesajelor la desfășurarea activităților de pregătire a personalului. În principal, pe timpul pandemiilor, transmiterea verbală a informațiilor la nivel organizațional este preponderent înlocuită cu cea scrisă, iar folosirea acestei căi de comunicare are atât avantaje, dar și dezavantaje[12]. Avantajele comunicării scrise constau în faptul că oferă posibilitatea organizării mai clare a conţinutului informaţional, prin revenirea şi îmbunătăţirea succesivă a textului, care poate fi oricând consultat şi confruntat cu ceea ce s-a precizat a se executa. De asemenea, asigură condiţii pentru o argumentare largă a celor înscrise.

Comunicarea scrisă prezintă unele dezavantaje: nu realizează legătura directă între interlocutori (parteneri); îi lipseşte puterea de influenţare a cuvântului vorbit; nu permite conexiunea inversă imediată, ci numai cu un anumit decalaj în timp; îi lipseşte pe interlocutori de informaţia emoţională pe care o asigură schimbul mesajelor orale; dispare posibilitatea ca emiţătorul să intervină, pe loc, asupra mesajului/ informaţiei transmise (pentru completări sau explicații), de a sublinia anumite idei, în raport cu reacţia cititorului; realizarea feedback-ului este reluată şi completată prin alte mesaje. Transmiterea informațiilor în scris îngreunează comunicarea și necesită un efort în plus din partea emițătorului, mai ales când avem ca punct de reper, de exemplu, un briefing de informare sau o prezentare. Se prelungește, astfel, fluxul de la decident la executant.

Prin limitarea formării unor grupuri mai mari, instruirea personalului se va orienta spre mijloace alternative, care vor consta preponderent în accesarea platformelor de e-learning, în detrimentul învățământului clasic. Și la acest nivel trebuie avute în vedere avantajele și dezavantajele comunicării scrise, pentru a nu se pierde din valoarea informațională a materialelor didactice. De asemenea, informațiile cu un grad ridicat de clasificare vor necesita rețele securizate corespunzător.

Totodată, continuarea procesului de instrucţie, simultan cu adoptarea de măsuri adecvate de protecţie a constituit o nouă provocare față de nevoia de pregătire a personalului. Folosirea viitoare a unor platforme tehnologice, software și hardware, pentru derularea unor scenarii în care participanții sunt introduși și evaluați într-un mediu virtual, care redă fidel contextul de manifestare a unei probleme de securitate, va reprezenta un mijloc modern de instruire, fără de care pregătirea ar rămâne doar la nivelul acumulării de cunoștințe[13].

Așa cum am mai precizat în acest articol, pandemiile afectează și capacitatea de dislocare a personalului în teatrele de operații, prin impunerea carantinei înainte și după îndeplinirea unei misiuni. Astfel, capacitatea de reacție rapidă este diminuată, iar numărul misiunilor este redus semnificativ în aceste condiții. De asemenea, dialogul cu partenerii se face preponderent online, deci vor exista precauții și în transmiterea informațiilor pe canale nesecurizate. Găsirea unor soluții în acest sens reprezintă un alt obiectiv de realizat.

Chiar dacă vor fi necesare schimbări majore, ele nu trebuie considerate neapărat ca fiind negative, ci printr-o perspectivă diferită, să fie privite ca modalități prin care organizația învață în permanență să se adapteze și să integreze ceea ce este nou. Atitudinea flexibilă oferă întotdeauna o deschidere către adaptare, cercetare și inovare.

Deşi determină mari dificultăţi de management, creează panică şi stări de stres sau de disconfort psihologic, în unele împrejurări criza este o fereastră deschisă către noi oportunităţi. Între specialiștii care au studiat aceste procese se numără şi Gerald Meyers[14], care depistează şapte tipuri de oportunităţi, astfel:

- gestionată corespunzător, criza poate naşte eroi;
- sub presiunea ei, cele mai multe organizaţii ies din inerţie şi conservatorism şi recurg la adoptarea unui ritm accelerat al schimbărilor;
- dificultăţi ignorate, din conservatorism şi comoditate, sunt rezolvate uneori sub incidenţa manifestărilor de criză;
- contribuie implicit la schimbări la nivelul personalului organizaţiilor;
- poate duce la depistarea unor noi strategii şi tehnici de lucru, mult mai simple şi mai eficiente;
- prin valorificarea experienţei dobândite orice organizaţie devine mai prudentă, constituindu-şi mecanisme proprii de prevenţie;
- după anularea efectelor crizei, orice organizaţie devine mai puternică, sporindu-şi vizibil coeziunea, competitivitatea şi eficienţa.

O stare pandemică generează numeroase provocări asupra serviciilor de intelligence, însă acolo unde există probleme, există și soluții. Focusarea pe găsirea celor mai bune strategii, care să răspundă noilor amenințări, și implementarea acestora vor crește performanța sistemului în viitor.

CONCLUZII

Structurile de intelligence au grade diferite de vulnerabilitate în modul lor curent de acțiune, după cum am argumentat în acest articol, cauza principală fiind dată de restricțiile impuse în urma declanșării unei pandemii. Pentru elaborarea unor strategii privind adaptabilitatea sistemului la viitoarele amenințări de tip pandemic este necesară colaborarea mai multor specialiști din diverse structuri, implicând chiar experți ai unor servicii partenere, deoarece lupta împotriva unei

amenințări globale nu se poate realiza doar prin mijloace proprii.

Din punct de vedere psihologic, protejarea personalului propriu față de vulnerabilitățile generate de starea de criză devine obiectivul principal al specialiștilor din domeniu. Există intervenție în criză, dar și în post-criză, activitățile fiind destinate optimizării gradului de confort emoțional și de creștere a adaptării la noile provocări, în plan personal, dar și la nivel organizațional.

Natura și amploarea schimbărilor ulterioare unei pandemii asupra serviciilor de intelligence trebuie gândite cu mare responsabilitate, având în vedere atât soluții pe termen scurt, dar mai ales soluții pe termen lung. De funcționalitatea întregului sistem de informații depind o serie de factori decizionali, cu repercusiuni asupra nivelului de securitate al țării, dar și al bunăstării și stării de securitate ale populației.

BIBLIOGAFIE

1. DRĂGHICI Mihai, „Yuval Noah Harari: Lumea după coronavirus. Furtuna va trece, omenirea va supraviețui, dar vom locui într-o lume diferită", în *Mediafax.ro*, 23.03.2020, https://www.mediafax.ro/externe/cum-va-arata-lumea-dupa-coronavirus-furtuna-va-trece-omenirea-va-supravietui-dar-vom-locui-intr-o-lume-diferita-19005264.
2. DUGAN Cosmin, „COVID-19 și serviciile secrete" (II), Laborator de Analiză a Războiului Informațional și Comunicare Strategică, în *Adevărul.ro,* 21.04.2020, https://adevarul.ro/international/in-lume/covid-19-serviciile-secrete-ii-15e9e79565163ec4271f6497c/index.html.
3. FLYNN Carol Rollie, "What Role Does the Intelligence Community Play in a Pandemic?", *Analysis*, Foreign Policy Research Institute, 28.04.2020, https://www.fpri.org/article/2020/04/what-role-does-the-intelligence-community-play-in-a-pandemic/
4. HARARI Yuval Noah, *21 de lecții pentru secolul XXI,* Editura Polirom, 2018, p. 257-268.
5. HARARI Yuval Noah, *Scurtă istorie a viitorului*, Editura Polirom, 2018. p.13-20.
6. MEYERS Gerald, John Holusha, *Managing Crisis. A Positive Approach*, Routledge/ Taylor & Francis Group, 2018, 290 p.
7. SAVU Gheorghe, *Spionajul militar modern*, Editura RAO, 2017, p. 210.
8. *** https://www.historia.ro/sectiune/general/articol/cele-mai-grave-epidemii-din-istorie.
9. *** https://www.scena9.ro/article/coronavirus-efecte.
10. *** https://www.intelligenceonline.com.
11. ***http://www.umfcv.ro/files/c/u/Curs%206%20PSY%20MED%20-%20Cauze%20psihosociale%20si%20modificari%20patologice%20induse%20de%20stres.pdf.
12. *** https://ro.wikipedia.org/wiki/Abraham_Maslow.
13. *** https://www.dw.com/en/coronavirus-and-the-fake-news-outbreak/av-52999958/
14. *** https://www.youtube.com/watch?v=vwjwQvXohdI.
15. *** http://www.univath.ro/pdf/tematica_licenta/Curs_Comunicare_in_AP.pdf.
16. *** https://animv.ro/centrul-national-de-simulare-in-intelligence/
17. *** http://www.diacronia.ro/ro/indexing/details/A6506/pdf.

[1] https://www.historia.ro/sectiune/general/top-10-cele-mai-grave-epidemii-din-istorie-574962.html, accesat în 01.05.2024.
[2] https://www.scena9.ro/article/coronavirus-efecte, accesat în 04.05.2024.
[3] Cosmin Dugan, „COVID-19 și serviciile secrete" (II), Laborator de Analiză a Războiului Informațional și Comunicare Strategică, în Adevărul.ro, 21.04.2020, https://adevarul.ro/international/in-lume/covid-19-serviciile-secrete-ii-1_5e9e79565163ec4271f6497c/index.html, accesat în 01.05.2024.
[4] Mihai Drăghici, „Yuval Noah Harari: Lumea după coronavirus. Furtuna va trece, omenirea va supraviețui, dar vom locui într-o lume diferită", în Mediafax.ro, 23.03.2020, https://www.mediafax.ro/externe/cum-va-arata-lumea-dupa-coronavirus-furtuna-va-trece-omenirea-va-supravietui-dar-vom-locui-intr-o-lume-diferita-19005264, accesat la 04.05.2024.
[5] https://www.intelligenceonline.com, accesată în 02.05.2024;
[6] Gheorghe Savu, *Spionajul militar modern,* Editura RAO, 2017, p. 210.
[7] http://www.umfcv.ro/files/c/u/Curs%206%20PSY%20MED%20-%20Cauze%20psihosociale%20si%20modificari%20patologice%20induse%20de%20stres.pdf, accesată în 02.05.2024.
[8] https://ro.wikipedia.org/wiki/Abraham_Maslow, accesat în 03.05.2024.
[9] Carol Rollie Flynn, "What Role Does the Intelligence Community Play in a Pandemic?", *Analysis,* Foreign Policy Research Institute, 28.04.2020, https://www.fpri.org/article/2020/04/what-role-does-the-intelligence-community-play-in-a-pandemic/, accesat în 07.05.2024
[10] https://www.dw.com/en/coronavirus-and-the-fake-news-outbreak/av-52999958, accesat în 06.05.2024.
[11] https://www.youtube.com/watch?v=vwjwQvXohdI
[12] http://www.univath.ro/pdf/tematica_licenta/Curs_Comunicare_in_AP.pdf, accesat în 10.05.2024.
[13] https://animv.ro/centrul-national-de-simulare-in-intelligence/, accesat în 10.05.2024.
[14] Gerald Meyers, John Holusha, *Managing Crisis. A Positive Approach,* Routledge/ Taylor & Francis Group, 2018; a se vedea și http://www.diacronia.ro/ro/indexing/details/A6506/pdf, accesat în 10.05.2024.

EVOLUȚIA RELAȚIEI DINTRE POPULAȚIE ȘI STAT ÎN EPOCA MODERNĂ. IMPACTUL INFORMAȚIILOR DIN SURSE DESCHISE

Alin BARAITARU*

Abstract

The OSINT domain has been regarded by the intelligence community as both important and insignificant, yet it has found its place in the intelligence cycle, constituting one of the current nine collection disciplines. Even those who find it useful have a hard time explaining why open-source data can have an impact, at times as significant as intelligence derived from expensive and carefully planned from classified intelligence operations.

This paper aims to explore the historical evolution of the described system, forming the basis for the argument that in contemporary times, state activity (in terms of government and administration), which is the object of strategic intelligence gathering operations, is variably dependent on the population. The population, in turn, relies solely on publicly available data, diverging from the historical state monopoly on the term, classified when referring to data circulating within governments.

Keywords: *OSINT; public data; intelligence; collection disciplines; the state; governance; the population.*

STATELE

În mod generic, statul reprezintă o populație de pe un teritoriu care respectă de bună voie un set de reguli la care a contribuit (direct sau indirect) și care reguli (sau legi) au fost decise de un grup de persoane (reprezentanți) căruia respectiva populație i-a acordat voluntar puterea de a decide în locul ei și în favoarea ei. Concomitent, termenului de „stat”, în anumite situații, îi este atribuită și valoarea de „guvernare”, „conducere” sau administrație. Suprafața globului este împărțită, cu câteva excepții (terra nullius[1], Antarctica, apele internaționale, etc), în zone aparținând statelor și nu există spații care să nu intre în aceste categorii și, prin urmare, statele se află în contact fizic direct sau indirect unele cu altele și se influențează reciproc.

Influența poate fi considerată și presiune, putând fi exprimată prin starea de expansiune sau starea de conservare în care statul se regăsește. Un stat nu va urmări niciodată să regreseze sau

Autorul este expert în cadrul Ministerului Apărării Naționale.

să scadă în dimensiune, nici măcar în cazurile de izolaționism (situație în care va încerca să diminueze contactele cu alte state și influența proprie exercitată, dar și influența unor state terțe).

Presiunea generată de contactele dintre state variază în funcție de numărul de interacțiuni și de calitatea acestora, dar și de obiectivele stabilite de aceste state, aflate în contact, în ceea ce privește extinderea sau conservarea. Starea de expansiune a unui stat se manifestă în momentul în care nevoile într-un domeniu de activitate nu mai sunt satisfăcute doar la nivel local/ în interiorul statului. Pe de altă parte, starea de conservare intervine în situația în care membrii societății își desfășoară toate activitățile în mod satisfăcător pentru aceștia, având la dispoziție resursele furnizate local de ceilalți membri. În această stare contactele interstatale sunt limitate, rareori anulate.

Ambele stări, de expansiune sau de conservare, vor aduce statele în situații de competiție sau de coordonare în diferitele domenii în care se află în contact, în funcție de obiectivele acestora. Situațiile de coordonare produc, în mod inevitabil, cele mai multe interacțiuni datorită caracterului inerent al deschiderii. Situațiile de competiție produc, în schimb, reducerea numărului de interacțiuni la nivel de stat, iar scăderea este cu atât mai intensă cu cât competiția devine mai violentă.

Totalitatea situațiilor în care se poate afla un stat în cazul relației de competiție cu un oponent variază în funcție de stadiul în care se află acțiunile adversarului și care pot fi subsumate ca acțiuni potențiale, acțiuni planificate, acțiuni în desfășurare și acțiuni anterioare. Luând în considerare pericolul cel mai iminent din toate situațiile rezultă că acțiunile în desfășurare ale oponentului sunt cele mai importante. Această observație este ușor de identificat în activitatea organizațiilor de intelligence care dedică resurse captării de informații curente. Pentru ca activitatea să fie eficientă, instituțiile alocă resurse culegerii de date cu privire la acțiunile planificate de oponent, din care să fie extrași (conform unei metodologii) indicatorii relevanți de a fi monitorizați – acești indicatori sunt folosiți pentru a observa dacă acțiunile curente ale adversarului decurg conform planificării acestuia. Împreună, din acțiunile planificate și din cele curente, se pot extrage concluzii referitoare la regulamentele și doctrinele oponentului și la cât de mult le respectă în funcție de circumstanțe. Cuantificarea aplicării doctrinelor adversarului este utilă în momentul conceperii de planuri potențiale, moment care este influențat de totalitatea resurselor pe care adversarul le are la dispoziție.

Privind în interiorul statului, dacă luăm în considerare că indivizii se asociază aproape instinctiv în grupuri (cea mai mică unitate socială), atunci statul se află în vârful „lanțului trofic", reprezentând cel mai înalt construct societal. Grupul social, în concepția lui M. Sherif, este compus din minim două persoane care sunt de acord să urmeze un set de reguli, sunt de acord cu valorile grupului și cu relația dintre statut și rol care parvin între ele[2]. Astfel, statul este rezultanta directă a comportamentelor asumate ale indivizilor din societate și a setului de reguli pe care aceștia au stabilit în comun să le urmeze (sau în comun să le schimbe). Prin urmare, este necesar a fi lămurită utilizarea cuvântului „stat", care ar trebui să definească două lucruri: unul ar fi totalitatea cetățenilor și a grupurilor formate în interiorul unei suprafețe terestre, iar al doilea ar fi guvernarea (acel grup extins care este delegat cu autoritate de către totalitatea cetățenilor și de către toate grupurile, le reprezintă interesele și ia decizii care îi afectează pozitiv pe aceștia).

Privind în exteriorul statului, membrii acestuia sunt influențați de contactele pe care le au cu reprezentanții altor state. Nivelul de formalitate și de conformare față de normele de comportare crește cu cât grupul este mai aproape de guvernare. Astfel, la nivel individual s-ar putea regăsi un număr foarte scăzut de reguli stabilite în comun de către state care să reglementeze interacțiunea. Desigur, există exemplul statelor „închise", în special cele dictatoriale, care interzic cetățenilor lor orice interacțiune neformalizată cu orice membru al vreunei societăți exterioare statului din care fac parte.

Interacțiunile, fie că sunt între membri ai aceluiași stat, fie că sunt între reprezentanți din state diferite, produc asupra altor membri sau grupuri presiuni diferite la diverse niveluri, cu diferite intensități, iar mediul rezultat este cu atât mai complex cu cât societatea este mai evoluată. Acel mediu rezultat este obiectul disciplinei de culegere a informațiilor din surse deschise – OSINT.

OSINT - DISCIPLINĂ DE CULEGERE A CICLULUI INFORMAȚIONAL

OSINT este una dintre disciplinele integrate în etapa de culegere din cadrul ciclului informațional. Termenul de „OSINT" provine din prescurtarea termenilor din limba engleză „Open Source INTelligence", adică Intelligence provenit din surse deschise (în genere, orice informație care este disponibilă sau accesibilă publicului). Pentru a înțelege mai bine valoarea intrinsecă a OSINT mai trebuie insistat asupra noțiunii de „deschis" din termenul „surse deschise", care presupune și existența de „surse închise", noțiune care nu există în limbajul de specialitate. Însă, putem presupune că antonimul noțiunii poate fi considerat cel de „surse clasificate".

Prin urmare, OSINT nu ar trebui să fie orientat către sursele sau informațiile clasificate deoarece acestea vizează, în mod special, partea de intenție și de planificare a adversarului, parte care, în mod tradițional, nu este făcută publică. Însă, OSINT trebuie să aibă în vedere partea de rezultat a acțiunii adversarului, acele efecte publice ale punerii în practică a intenției și planificării oponentului asupra mediului operațional. În acest mod, sursele deschise oferă indirect informații cu privire la intenții și planuri, anterioare și viitoare. O consecință a acestei medieri o reprezintă capacitatea de prognoză rezultată din analiza unor tipare care apar și sunt bazate pe informații publice.

În același timp, antonimia dintre „surse deschise" și „surse clasificate" determină existența unui sistem format din producătorii și utilizatorii informațiilor provenite din sursele descrise de cei doi termeni. Astfel, pot fi identificate două categorii de generatori care produc informații necesare funcționării sistemului: statali (guvernamentali, oficiali, etc) și privați (ex.: societatea civilă, mediul privat). Este, astfel, evidentă relația dintre stat și „sursele clasificate", la fel cum este evidentă relația dintre civili și „sursele deschise", mai ales că utilizarea de către mediul guvernamental a sintagmei „informații clasificate" este rezultatul unui proces istoric îndelungat de folosire a informațiilor pentru funcționarea administrațiilor. Putem concluziona că guvernarea funcționează cu informații „clasificate", iar populația cu informații din surse „deschise".

Ținând cont că administrația este rezultanta directă a comportamentelor asumate ale indivizilor din societate și a setului de reguli pe care aceștia au stabilit în comun să le urmeze, mai putem adăuga și faptul că sursele deschise influențează indirect statul, iar sursele clasificate influențează indirect populația. Din explicația dihotomiei „surse deschise" vs. „surse clasificate" mai poate reieși și ideea că simplul fapt al producerii sau utilizării aleatoare de informații de către stat conduce la descrierea acelor informații ca fiind „clasificate", în special datorită faptului că „a clasifica" presupune aranjare sistematică (adică un proces utilizabil în orice domeniu). Astfel, utilizarea expresiilor de genul „informație clasificată" sau „sursă clasificată" devine terminologie specifică informațiilor relevante pentru stat.

Concomitent cu indicarea informațiilor ca făcând parte din instrumentarul aparatului de stat, procesul de „clasificare" a informațiilor proprii este executat în scopul protejării acestora față de un oponent, intern sau extern, prin aplicarea de reguli restrictive de diseminare în funcție de importanța pentru sistemul statal.

ISTORIA DINAMICII POPULAȚIE-STAT

În condițiile în care statul deține monopolul asupra informațiilor clasificate, iar într-o competiție cu un stat terț obiectivele activității de culegere sunt informațiile clasificate ale oponentului, nu este evidentă imediat importanța informațiilor provenite din surse deschise. Evidența reiese din studierea relației dintre stat

și populație, iar punerea în perspectivă a relației oferă o imagine mai concludentă.

În epoca modernă, populația este beneficiarul final al deciziilor statului. Dar nu a fost întotdeauna așa – populația, de-a lungul istoriei, cu câteva excepții, nu a avut o influență decisivă în deciziile liderilor politici din diferite perioade. Grupurile care guvernau în diferite maniere, în frunte cu prinți, lorzi, regi, voievozi, etc, și-au creat un sistem în care dominația fizică asupra populației crea avantaje materiale și sociale, iar cel mai elocvent sistem a fost cel feudal. În linii mari, populația era incultă, deținea puține informații cu privire la ce se întâmpla în alte zone și era dependentă (până la robie, inclusiv) de capriciile liderilor. Înainte de Pacea din Westphalia[3], relația dintre populație și grupul conducător era bazată, în special, pe interesele categoriei din urmă din diverse motive; pe de altă parte, acordurile de pace din 1648 nu au însemnat o trecere bruscă la formele de statalitate existente în contemporaneitate, însă au deschis calea spre acestea, fiind o bornă identificabilă în procesul evolutiv al societăților moderne (proces catalizat de apariția și utilizarea tiparului cu caractere mobile).

Înainte de invenția lui Johannes Gutenberg, din 1450, producția de materiale scrise era limitată (Fig. 1), iar categoriile sociale și profesionale implicate în proces erau puține la număr și foarte specializate. Cei mai reprezentativi pentru aceste grupuri erau monahii și scriptorii profesioniști, care erau angajați de nobilime, și copiștii care copiau manual texte (uneori fără a înțelege ce copiază). Populația, în acele vremuri, în general, era analfabetă, în special pentru că nu avea niciun interes în a deprinde aptitudini al căror proces de învățare era costisitor în materie de finanțe (Fig. 3) și de timp alocat, în detrimentul altor activități importante.

Producția limitată de materiale scrise avea un impact, de asemenea, asupra circulației informațiilor dintr-o zonă în alta. Evenimentele dintr-o altă zonă nu puteau fi aflate decât prin scrisori sau prin viu grai. Dar cum populația era în majoritate analfabetă, scrisorile deveneau atributul clasei conducătoare (de exemplu, la început de secol al XVI-lea, în Anglia doar 10% dintre bărbați și 2% dintre femei erau capabili să citească). Difuzarea știrilor prin viu-grai fiind dependentă de prezența fizică a difuzorului, răspândirea pe cale orală devenea caracteristica negustorilor și a persoanelor care călătoreau. Prin urmare, persoanele înstărite, în special cele din categoria descrisă generos „clasa conducătoare", aveau un monopol aproape total asupra circulației știrilor, iar populația era limitată în a cunoaște doar evenimentele ce se petreceau local, rareori luând la cunoștință de evenimente ce se petreceau departe de localitatea de baștină. Din această situație rezulta un bun control al locuitorilor de către „guvernanți" și limitarea accesului populației la guvernare (al cărei efect indirect a fost și ereditatea statutului de conducător).

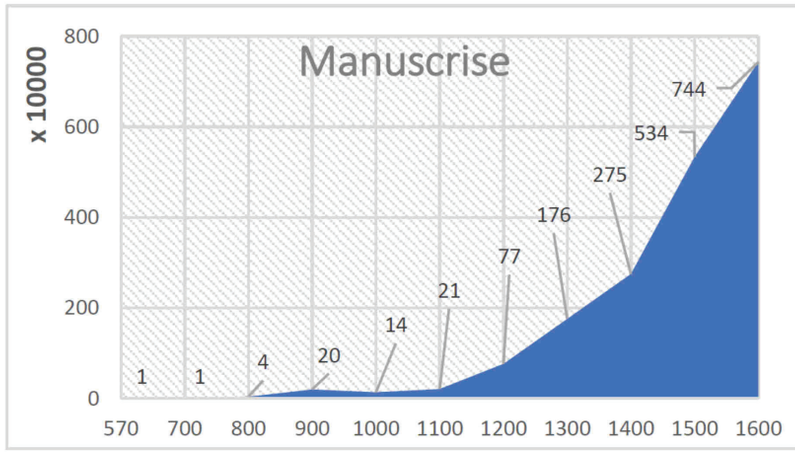


***Figura 1**: Manuscrise produse în perioada 570-1600 în Europa de Vest (înmulțit cu 10.000).*

Controlul locuitorilor era manifestat, în special, în situații de comportamente care contraveneau interesului „guvernării", când aceasta putea preveni coordonarea acțiunilor locuitorilor prin simpla blocare a fluxului de informații; sarcină relativ facilă considerând că pentru populație era necesară prezența fizică a unui mesager pentru a putea fi informată.

Limitarea accesului populației la guvernare era cauzată tot de numărul redus de informații care parveneau locuitorilor prin faptul

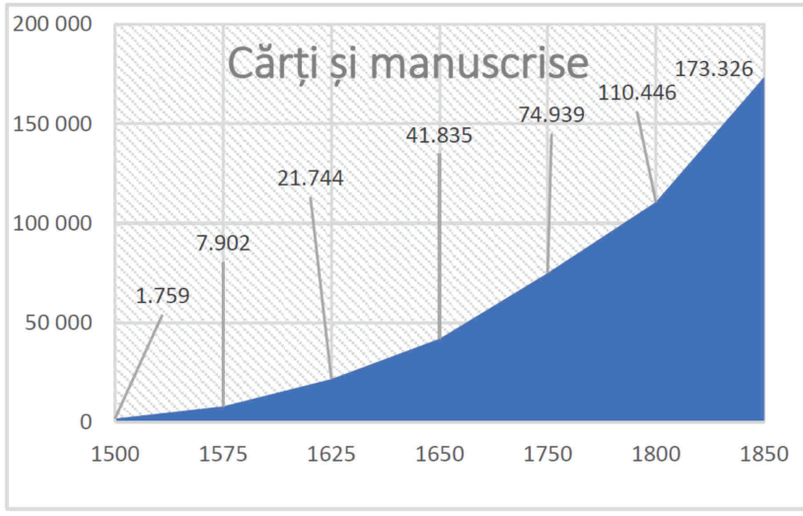


***Figura 2**: Cărți și manuscrise produse în perioada 1500-1850 în Europa de Vest (înmulțit cu 10.000).*

că având date, în mare parte, doar din zona unde locuiau și rareori din alte zone, oamenii nu puteau emite pretenții să aibă acces pentru a lua decizii despre evenimente sau situații față de care nu dețineau informații. Astfel, persoanele aflate în poziții de putere nu erau în pericol să-și piardă privilegiile în fața cuiva din afara „curții". În consecință, pozițiile de putere deveneau ereditare și puteau fi pierdute doar prin lupte interne, de „curte", sau prin lupte externe cu adversari de același calibru.

Toate acestea s-au schimbat, gradual, după inventarea și utilizarea tiparului cu caractere mobile, al cărui efect principal a fost generarea de mai multă informație la un cost de producție mult mai mic și într-un timp mult redus. Iar consecințele s-au manifestat vizibil și în rândul populației, cu urmări în sfera politică. Astfel, datorită cantității în creștere de informație disponibilă, analfabetismul în rândul populației a început să scadă, proces ce a generat un lanț de evenimente ce au culminat cu creșterea implicării populației în procesele de luare a deciziei de către guvernanți.

În primul rând, populația a început să fie mai informată asupra fenomenelor ce aveau loc în alte zone. Astfel, în plan social, comunitățile începeau să identifice elemente similare în alte comunități, lucru ce a contribuit la creșterea coeziunii între respectivele grupuri, în special în fața amenințărilor. În domeniul economic s-au produs, probabil, cele mai vizibile schimbări. Beneficiind de noile condiții de răspândire a informațiilor, idei noi despre moduri de a confecționa produse sau de a face afaceri s-au răspândit în zone în care acestea nu existau, iar invențiile au găsit teren fertil. Acest proces de diseminare a cunoașterii a dus la îmbunătățirea și diversificarea capacității de producție; în același timp, creșterea productivității muncii a însemnat, în ultimă instanță, diminuarea diferențelor financiare față de grupurile guvernante (diferențe care, anterior, constituiseră un obstacol în plus în calea spre accederea la guvernare). Transformarea populației într-un grup mai informat și mai potent financiar a permis unor persoane care nu proveneau din cercurile guvernamentale să solicite acces în structurile de guvernare și să emită pretenții asupra modului în care erau guvernate teritoriile. Unul dintre rezultatele importante ale acestor presiuni a fost schimbarea modalității de acces la guvernare.

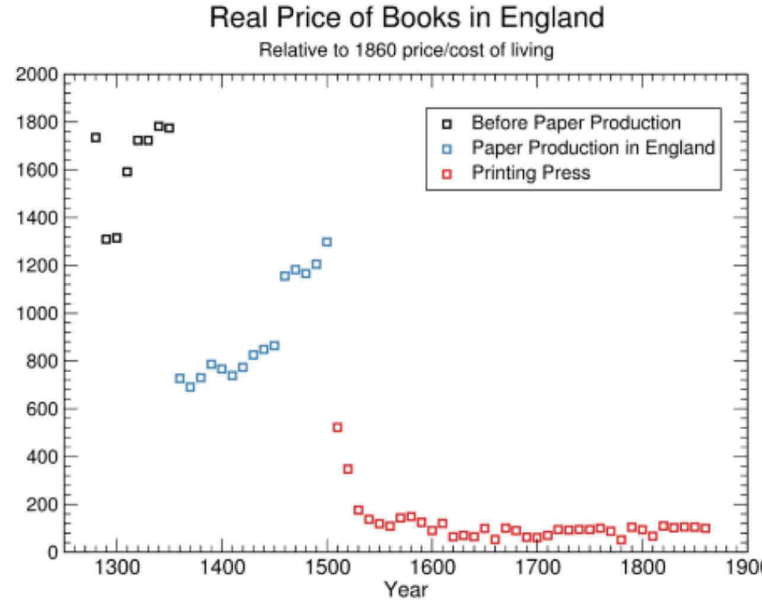


***Figura 3**: Costul relativ al producerii unei cărți în Anglia între anii 1250 și 1850.*

***Figura 4**: „Cititul știrilor (1871), Pictură de Richard Staunton Cahill*

Din punct de vedere politic este etapa apariției partidelor politice și a sistemului de alegere a guvernanților prin vot, moment în care populația a deveni un actor în jocul politic. Joc ce a devenit mai complex atât pe verticală, cât și pe orizontală, cu actori tot mai educați și mai potenți financiar. Luptele pentru putere au coborât de la nivelul curților regale sau princiare către niveluri apropiate de cetățenii de rând, generând diversificarea și fragmentarea intereselor în diferite „triburi". Ceea ce a însemnat diluarea puterii regelui până la nivelul la care populația să nu mai poată fi constrânsă de interesul regal.

Punctul de cotitură în confirmarea populației ca actor politic a fost Războiul de 30 de ani, încheiat în anul 1648, când au fost semnate tratatele cunoscute colectiv drept „Pacea din Westphalia", prin care s-au pus bazele creării statelor europene moderne. Perioada ulterioară semnării tratatelor de pace a însemnat dezvoltarea conceptului de „stat", o perioadă de cristalizare care poate explica motivul pentru care în contemporaneitate termenii „stat" și „guvernare" sunt folosiți ca termeni echivalenți. Echivalarea era un gest reflex al populației post-1648 care nu era încă obișnuită în rolul de actor politic independent și suveran și asocia vechea administrație cu nou-venitul termen de „stat". Însă nu doar populația nu era obișnuită cu noul rol, regele francez Ludovic al XIV-lea declarând în fața parlamentului în 1655: „Statul sunt eu.", declarație care confirma continuitatea unor privilegii nobiliare, precum „drepturile rezervate".

CONCLUZIE

Populația a evoluat de la un grup lipsit de informații și putere de decizie la actor politic de prim-rang, în timp ce statul a evoluat de la un grup de persoane, care acționau neuniform pe teritoriile pe care le guvernau în interes propriu, la o instituție al cărei scop este satisfacerea interesului populației. În contemporaneitate, modalitatea prin care țelul este atins variază de la un stat la altul și chiar și statele evident dictatoriale încearcă să păstreze o fărâmă de legitimitate că servesc interesul națiunii (de exemplu, statul nord-coreean și-a luat denumirea de Republica Populară Democrată Coreeană).

În prezent, informațiile disponibile în spațiul public informează și educă populația și, pe baza lor, populația influențează actul decizional al guvernării. Cu cât statul este mai democratic, cu atât populația este mai implicată în procesul de luare a deciziilor administrației. În același timp, însă, cu cât un oponent cunoaște mai bine populația și îi „servește" informații care să descrie o altă realitate, cu atât adversarul este mai eficient în competiția interstatală. Astfel, un stat cu o democrație puternică, dar a cărui populație este permeabilă la acțiunile de influențare inițiate de un adversar, se află în situația în care este probabilă deturnarea procesului de luare a deciziilor în beneficiul acelui adversar.

Pe de altă parte, capacitatea populației de a produce schimbări în cadrul guvernărilor este catalizată de lipsa ereditații în procesul de atribuire a pozițiilor în organizațiile administrative (manifestat prin vot și concursuri de selecție), fapt ce permite periodic informațiilor clasificate să fie transferate limitat și indirect în spațiul public, iar informațiilor din surse deschise să influențeze actul guvernamental.

În consecință, în lumea contemporană devine vizibil impactul pe care îl au informațiile publice asupra comportamentului populației (în dezvoltarea de afaceri, în transmiterea valorilor culturale sau, în special, în domeniul politic), din

ale cărei rânduri s-a dezvoltat, cu un grad variabil de dependență, guvernarea care funcționează emițând reguli atât obligatorii pentru toți cetățenii, cât și în beneficiul acestora. În acest context, informațiile din surse deschise oferă valoare deoarece au potențialul să explice comportamente ale populației atât pe termen scurt, cât și pe termen lung, și, pe cale de consecință, să explice comportamente ale societăților. În majoritatea cazurilor, explicațiile comportamentelor nu vor fi simple deoarece, în condițiile în care volumul de informații este mare, acestea vor fi nestructurate și fragmentare, necesitând resurse mari pentru culegere și procesare pentru a fi transformate în informații de valoare pentru decidenți.

BIBLIOGRAFIE

1. CROXTON Derek, Anuschka Tischer, *The Peace of Westphalia: A Historical Dictionary*, Greenwood Press, 2001, 400 p.
2. FUKUYAMA Francis, *State-building: Governance and World Order in the 21st Century*, Cornell University Press, 2004.
3. HOUSTON Robert Allan, *Literacy in Early Modern Europe: Culture and Education, 1500-1800*, Routledge, 2002, 295 p.
4. RADY Martyn, *Nobility, Land and Service in Medieval Hungary* (Studies in Russia and East Europe), Palgrave Macmillan, 2000, 231 p.
5. SCHOFIELD R. S., 1973. „Dimensions of illiteracy, 1750-1850", *Explorations in Economic History*, vol. 10, nr. 4, 1973, p. 437-454.
6. SHERIF Muzafer, Sherif W. Carolyn, *Social Psychology*, Harper & Row Publishers, 1969, 616 p.
7. *** „Calcule pentru stabilirea prețului cărților în Marea Britanie", https://wiki.aiimpacts.org/takeoff_speed/continuity_of_progress/historic_trends_in_book_

[1] „Terra nullius" este un termen ce se referă la un „teritoriu fără stăpân". În dreptul internațional descrie un spațiu care poate fi locuit, dar care nu aparține niciunui stat; https://www.law.cornell.edu/wex/terra_nullius (accesat la 20.12.2024).

[2] Grupul este unitate socială care constă dintr-un număr de indivizi care, la un moment dat, se află în relații de statut și rol mai mult sau mai puțin definite și interdependente unul cu celălalt și care posedă, explicit sau implicit, un set de valori sau norme care reglementează comportamentul membrilor, cel puțin în chestiuni importante pentru grup; a se vedea Muzafer Sherif și Carolyn W. Sherif, *"The Psychology of Social Norms"* (Psihologia normelor sociale), 1956.

[3] Pacea westfalică reprezintă totalitatea tratatelor de pace care au fost negociate și încheiate în orașele Münster și Osnabrück în 1648 și prin care s-a finalizat Războiul de Treizeci de Ani (1618-1648), în care au fost implicate toate marile puteri europene și care a reprezentat un conflict între state, dar și între religii; https://culture.ec.europa.eu/ro/cultural-heritage/initiatives-and-success-stori es/european-heritage-label/european-heritage-label-sites/munster-and-osnabruck-sites-of-the-peace-of-westphalia-germany